1. Computer Forensics in Today's World

1. Computer Forensics in Today's World Part 1
    a. Computer forensics
        i. **A set of methodological procedures and techniques that help identify, gather, preserve, extract, interpret, document, and preserve evidence from computers in a way that is legally admissible**
    b. Objectives of Computer forensics include
        i. **Identify, gather, and preserve the evidence of a cybercrime**
        ii. **Track and prosecute the perpetrators in a court of law**
            1. Criminal case would involve jail time if found guilty
            2. Civil case would involve a monetary penalty if found guilty
            3. Administrative cases are non-criminal in nature
                a. Internal focus of businesses used to understand issues that occurred in a business
        iii. **Interpret, document and present evidence to be admissible during prosecution**
            1. There are rules that allows evidence to be admissible
        iv. Estimate the potential impact of malicious activity on the victim and assess the intent of the perpetrator
        v. Find vulnerabilities and security loopholes that may help attackers
        vi. Understand the techniques and methods used by attackers to avoid prosecution, and overcome them
        vii. Recover deleted filed, hidden files, and temporary data that could be used as evidence
            1. DD Tool in linux can be used locate residual data
            2. Creating a bit by bit copy using a drive imaging tool would allow us to examine the sectors of the drive looking and finding remnant data
            3. Netstat tool
                a. Networking/protocol stack tool and function
            4. Nbtstat in Windows
                a. Allow view of information in the name resolution cache in a Windows machine
            5. Route print
                a. Allows view of routing table
        viii. Perform incident response to prevent further loss of intellectual property, finances and reputation during an attack
        ix. Have knowledge about the laws of various regions and areas, as digital crimes are omnipresent and remote in nature.
        x. Know the process of handling multiple platforms, data types and operating systems.
        xi. Understand the usage of proper tools for forensic investigations.
        xii. **To minimize the tangible and intangible losses to the organization**

TOOLS Methodologies, Frameworks and Processes Term

xiii. To protect the organization from similar incidents in future

c. An assumption we always have to work under
   i. Everything we do with be under scrutiny
   ii. We must always follow the rules of evidence
   iii. We must always follow the code of ethics
   iv. We must always follow the standards of our occupation and industry
   v. Always operate in way that creates auditability, verifiability, and validity so that any action we take, can be cross-referenced, questioned, and validated, and proven to be legitimate

d. ASR or ASLR
   i. Attack surface reduction or attack surface level reduction
   ii. Trying to reduce the footprints of the vulnerabilities and therefore reduce the number of attack vectors

e. Write blocker
   i. A tool that blocks modification of the source drive

2. Computer Forensics in Today's World Part 2

a. Cyber Crime
   i. Any illegal act that involves a computer, its systems, or its applications

b. Cyber Crime Investigation
   i. process of studying a digital crime, its impact and other details to identify the source and perpetrators of the attack and prove their guilt.
   ii. Involves
      1. **Collection of clues and evidence**
      2. **Analysis of evidence**
      3. Reconstruction of the incident
      4. **Presentation of admissible evidence**

c. Types of Cyber Crime investigation cases
   i. Civil investigation
      1. **involve disputes between two parties**
      2. brought for violation of contracts and lawsuits where a guilty outcome generally results in monetary damages to the plaintiff
      3. Investigators try to show some information to the opposite party to support the claims and induce them for settlement
      4. Searching of the devices is generally based on mutual understanding and provides a wider time window to the opposite party to hide the evidence.
      5. **The initial reporting of the evidence is generally informal**
      6. The claimant is responsible for the collection and analysis of the evidence.
      7. Punishments include monetary compensation.
      8. Poorly documented or unknown chain-of-custody for evidence.
      9. Sometimes, evidence can be within the third party control.

TOOLS Methodologies, Frameworks and Processes Term

ii. Criminal

1. brought by law enforcement agencies in response to a suspected violation of law where a guilty outcome may result in monetary damages, imprisonment, or both
2. Investigators must follow a set of standard forensic processes accepted by law in the respective jurisdiction.
3. **Investigators, under court's warrant, have the authority to force seize the computing devices.**
4. A formal investigation report is required.
5. The law enforcement agencies are responsible for collecting and analyzing evidence.
6. Punishments are harsh and include fine, jail sentence or both.
7. Standard of proof needs to be very high.
8. Difficult to capture certain evidence, e.g., GPS device evidences.

iii. Administrative

1. non-criminal in nature and are related to misconduct or activities of an employee
2. Involves an agency or government performing inquiries to identify facts with reference to its own management and performance
3. Non-criminal in nature and related to misconduct or activities of an employee that includes but are not limed to:
    a. Violation of organization's policies, rules, or protocols
    b. Resources misuse or damage or theft
    c. Threatening or violent behavior
    d. Improper promotion or pay rises
    e. Corruption and bribery
    f. Sexual Exploitation, harassment and abuse
4. Any violation may result in disciplinary action such as demotion, suspension, revocation, penalties, and dismissal
5. For situations like promotions, increments, transfers, etc. administrative investigations can result in positive outcomes, like modifications to existing policies, rules, or protocols

d. Network
    i. Connecting multiple computers allowing them to exchange information with each other

e. Internal cyber crimes
    i. Insider attacks
    ii. Primary threat
    iii. espionage, theft of intellectual property, manipulation of records, and Trojan horse attack

f. External cyber crimes
    i. Originate from outside the org

TOOLS Methodologies, Frameworks and Processes Term

ii. Can be remote in nature
iii. **occur when there are inadequate information security policies and procedures**
iv. Attackers use the systemas a tool

g. Challenges Cyber Crimes Present to Investigators
i. **Speed** - Advancing technology and the increasing speed of accessing data
ii. **Anonymity** - attackers hide their identity **by masquerading**
iii. **Volatility** – volatile data can be easily lost and requires special tools
iv. **Evidence Size and Complexity** – results from diversity and distributed nature of digital devices
v. Anti-Digital Forensics (ADF) - increased use of encryption and hiding techniques
vi. Global origin and difference in laws – attackers can initiate a crime from any part of the world
vii. Limited legal understanding – ignorance of the law violated during the incident

h. Rules of forensic investigation
i. Limited access to and examination of the original evidence
ii. Record all changes made to any evidence files
iii. Create an evidence chain of custody document for tracking all access to the evidence
iv. Set standards for investigating all evidence and follow/comply with them
v. Hire professionals for analysis of evidence if special skill sets are required
vi. Evidence should be strictly related to the incident
vii. The evidence should comply with all jurisdiction standards
viii. Document the procedures applied to all evidence
ix. Security store all evidence
x. Use recognized and appropriate tools for analysis

i. Cyber Crime Investigation Methodology/Steps:
i. Identify the computer crime
ii. Collect preliminary evidence
iii. Obtain court warrant for discovery/seizure of evidence (if required)
iv. Perform first responder procedures
v. Seize evidence at the crime scene
vi. Transport evidence to the lab
vii. Create two bit stream copies of the evidence
viii. Generate MD5 checksum of the images
ix. Maintain chain of custody
x. Store original evidence in secure location
xi. Analyze the image copy for evidence
xii. Prepare a forensic report
xiii. Submit report to client
xiv. Testify in court as an expert witness (if required)

j. Corporate Investigations / Enterprise Theory of Investigation (ETI)

TOOLS Methodologies, Frameworks and Processes Term

i. **Methodology for investigating criminal activity to identify criminals who have escaped prosecution**
ii. Adopts a holistic approach toward any criminal activity as a criminal operation rather than as a single criminal act
iii. **Standard investigative model used by the FBI when conducting investigations against major criminal organizations**

3. Computer Forensics in Today's World Part 3
    a. Locard's exchange principle
        i. Concept used to understand the mindset and methodology of the criminal actor
        ii. In a crime, the criminal will take something, but will also leave something as clues or evidence
        iii. Focus on what is missing and what is added
        iv. Focusing on the changes will help us to identify the criminal
        v. Approach used to help understand what has transpired
    b. Types of digital evidence
        i. Volatile
        ii. Non-volatile
    c. Charactaristics of digital evidence (Page 14)
        i. **authentic**
        ii. **complete**
        iii. **admissible**
        iv. **Reliable**
        v. **Believable**
        vi. Digital evidence has to be all of these things
    d. The rules that govern digital evidence
    e. Digital evidence definition
        i. Any information of probative value that is either stored or transmitted in digital form.
    f. Challenges of digital evidence
        i. Ensuring integrity
        ii. Maintaining the viability of evidence throughout the lifecycle
        iii. Care and feeding of the evidence lifecycle
        iv. The fragility of data
        v. Anti-digital forensics
            1. Seeks to take advantage of the fragility of data
            2. Goal is to modify and obfuscate date to invalidate evidence
            3. Steps taken to render evidence unusable
    g. Best evidence rule
        i. The court will only allow the original evidence rather than a copy
        ii. If we can't present the original, a forensic duplicate will be allowed, but only under certain conditions

TOOLS Methodologies, Frameworks and Processes Term

iii. The original will not be questioned, but the copy will be questioned and must always prove that it is forensically sound
iv. The duplicate will suffice as evidence under the following conditions
    1. If the original was destroyed in fire, flood, or in the normal course of business because of a retention policy
    2. In possession of a third party

4. Computer Forensics in Today's World Part 4
    a. U.S. Federal rules of evidence (The most pertinent)
        i. http://rulesofevidence.org
        ii. Rule 101
            1. Lays out how we have the right to interact with certain kinds of cases
            2. Can present a case in U.S. courts
            3. **Govern proceedings in the courts** of the U.S. and before U.S. bankruptcy judges and the U.S. magistrate judges, to the extent and with the exceptions stated in rule 1101.
        iii. Rule 102 - Purpose and construction
            1. Focuses on purpose and construction
            2. Rules are being created to promote a fairness and a speedy trial and ascertain the truth
            3. Rule shall be construed to secure fairness is administration, elimination of unjustifiable expense and delay, and promotion of growth and development of the law of evidence to the end that **the truth may be ascertained and proceedings justly determined**
        iv. Rule 103 - **Rulings on evidence**
            1. Effect of erroneous ruling
                a. If evidence is provided erroneously, how do we deal with that
                b. If there was an error, how do we deal with that
                c. If there is an objection, how do we deal with that
                d. If we have to have a hearing, how do we do that
            2. Record of offer and ruling
                a. Lays out the structure of how a tradition trial is carried out
                b. The court may add any other or further statement which shows the character of the evidence, the form in which it was offered, the objection made, and the ruling there on. It may direct the making of an offer in question and answer form
            3. Hearing of jury
                a. Doesn't all inferences to evidence that is inadmissible
                b. Prevent inadmissible evidence from being suggested to the jury by any means, such as making statements of offers of proof or asking questions in the hearing of the jury
            4. Plain error
                a. If there is an obvious error, you are allowed to point that out

b. Nothing in the rule precludes taking notice of plain errors affecting substantial righst although they were not brought to the attention of the court

v. Rule 105 - Limited Admissibility
    1. **When evidence is admissible or not** and under what conditions
    2. When evidence is admissible for one purpose but not another, the court will **restrict the evidence to its scope**

vi. Rule 801
    1. **Hearsay** is a statement other than the one made by the declarant while testifying at an ongoing trial or hearing
        a. Relaying something as a third party of what another party stated
        b. It is not allowed except by the Supreme Court or by Act of Congress
    2. The following is not hearsay
        a. A prior statement by a declarant witness
            i. The declarant testifies at the trial or hearing and is subjected to cross-examination concerning the statement, and the statement is:
                1. Inconsistent with the declarant's testimony, and was given under oath subject to the penalty of perjury at a trial, hearing, or other proceeding, or in a deposition, or
                2. Consistent with the declarant's testimony and is offered to rebut an express or implied charge against the declarant of recent fabrication or improper influence or motive, or
                3. One of identification of a person made after perceiving the person
        b. An opposing party's statement
            i. The statement is offered against an opposing party and is:
                1. The party's own statement, either in an individual or a representative capacity
                2. A statement of which the party has manifested an adoption or belief in its truth, or
                3. A statement by a person authorized by the party to make a statement concerning the subject, or
                4. A statement by the party's agent or servant concerning a matter within the scope of the

agency or employment, made during the existence of the relationship, or

5. A statement by a coconspirator of a party during the course and in furtherance of the conspiracy

vii. Rule 803 – **Hearsay Exceptions Declarant available**

1. Even if the declarant is available as a witness, the following are not excluded by the Hearsay rule:
    a. Records of vital statistics
    b. Public records and reports
    c. Present sense impression
    d. Excited utterance
    e. Statements for purposes of medical diagnosis or treatment
    f. Recorded recollection
    g. Records of regularly conducted activity
    h. Absence of entry in records kept in accordance with the provisions

viii. Rule 804 – **Hearsay Exceptions Declarant unavailable**

1. If the declarant is unavailable as a witness, the following are not excluded by the Hearsay Rule:
    a. Former testimony
    b. Dying utterance – Statement under belief of impending death
    c. Statement or personal or family history
    d. Content of Writings, Recordings, and Photographs

ix. Rule 1001 – **Definitions**

1. Writings and recordings
    a. Consist of letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electric recording, or other forms of data
2. Photographs
    a. Still photographs, x-ray films, video tapes, and motion pictures
3. Original
    a. The writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it
4. Duplicate
    a. A counterpart produced by the same impression as the original, or from the same matrix, or by means of photography, including enlargements and miniatures, or by mechanical or electronic re-recording, or by chemical reproductions, or by other equivalent techniques that accurately reproduce the original.
    b. Gray area here

c. May be open to the interpretation of a judge
d. Can be open to challenges from new technologies or new techniques

x. Rule 1002 – Requirement of original

1. **To prove the content of evidence, the original is require, except as otherwise provided in these rules or act of Congress**

xi. Rule 1003 – Admissibly of duplicates

1. A duplicate is admissible to the same extent as the original unless the authenticity is in question or it is unfair to admit the duplicate in lieu of the original

xii. Rule 1004 – Admissibility of other evidence of content

1. Original is not required and duplicate is admissible if the orginal is lost, destroyed, not obtainable (examples: Mona Lisa or Declaration of Independence), someone else who is counter to our interest has ownership, or the original may not be pertinent and the original is not required.

5. Computer Forensics in Today's World Part 5
   a. Digital Forensics Magazine
      i. www.Digitalforensicsmagazine.com
   b. SWGDE
      i. Scientific Working Group on Digital Evidence
      ii. Brings together organizations to foster communication and cooperation as well as to ensure quality and consistency within the forensic community
   c. FBI
      i. https://archives.fbi.gov
      ii. Created the International Organization on Digital Evidence (IOCE)
         1. https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm
         2. Based on the SWGDE work to create the set of standards for gathering of digital evidence.
         3. Criteria 1.1 - All agencies that seize and/or examine digital evidence must maintain an appropriate SOP document
         4. Criteria 1.2 - Agency management must review the SOPs
         5. **Criteria 1.3 - Procedures used must be generally accepted in the field**
         6. Criteria 1.4 - The agency must maintain written copies of appropriate technical procedures
         7. Criteria 1.5 - The agency must use hardware and software that is appropriate and effective
         8. Criteria 1.6 – All activities must be recorded in writing and be available for review and testimony

9. Criteria 1.7 - Any action that has the potential to alter, damage, or destroy any aspect of original evidence must be performed by qualified persons in a forensically sound manner

iii. IOCE International Principles for Digital Evidence

1. When dealing with digital evidence, all of the general forensic and procedural principles must be applied
2. Upon seizing digital evidence, actions taken should not changes that evidence
3. When it is necessary for a person to access the original digital evidence, that person should be trained for the purpose
4. All activities relating to the seizure, access, storage, or transfer of the digital evidence must be fully documented, preserved, and available for review
5. An individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession
6. Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles

d. Forensic readiness planning refers to an **organization's ability to make optimal use of digital evidence in a limited period and with minimal investigation costs utilizing including technical and non-technical actions that maximize an organization's competence to use digital evidence**.

i. Identify potential evidence required for an incident
ii. Determine the source of the evidence
iii. Define a policy that determined the pathway to legally extract electronic evidence with minimal disruption
iv. Establish a policy for securely handling and storing the collected evidence
v. Identify if the incident requires full or formal investigation
vi. Train the staff to handle the incident and preserve the evidence
vii. Create a special process for documenting the procedure
viii. Establish a legal advisory board to guide the investigation process

e. Digital evidence examination process

i. 5 steps
ii. Evidence assessment – scoping and tailoring
iii. Evidence acquisition – what is/was the role of the system

1. Imaging/bit-stream copy
2. Write protection
3. Complete documentation of all evidence
4. Storage device examination to ensure all space is account for
5. Logs, logs, logs
6. Memory, processes, caches

iv. Evidence preservation – do no harm, full body armor and details

TOOLS Methodologies, Frameworks and Processes Term

v. Evidence examination & analysis – nothing original
    1. 2 types of data extraction
        a. Physical – no file system, just data
            i. Keyword searches
            ii. File carving
            iii. Examination of the partition structure
        b. Logical – OS dependent
            i. Extraction of the file system information to reveal characteristics such as
                1. Directory structure, file attributes, file names, date and time stamps, file size, and file location
            ii. Data reduction to identify and eliminate known files through the comparison of the calculated hash values to the authenticated hash values
            iii. Extraction of files pertinent to the examination
                1. Methods to accomplish this may be based on the file's name and extension, file header, file content, and location on the drive
            iv. Recovery of the deleted files
            v. Extraction of the password-protected, encrypted, and compressed data
            vi. Extraction of fileslack
            vii. Extraction of the unallocated space
vi. Evidence documentation and reporting
    1. Understand audience and make it relevant for them

2. The Investigation Process

6. The Investigation Process Part 1
    a. 3 Phases of the investigation process
        i. Pre-investigation phase
            1. The prep work
            2. Build the team
            3. Build the forensics lab
                a. Think about a lab that can be certified as meeting certain standards.
                b. Think about location
                c. Think about security
                    i. **Lab exteriors should have no windows**
            4. Build the analysis capability
            5. Set up our workspace
                a. Consider backup power or reliable power
                b. Consider environmental controls

TOOLS Methodologies, Frameworks and Processes Term

c. Consider power converters AC/DC DC/DC, EU to US adapter
6. Gather imaging platforms
7. Planning and budgeting
    a. **Break down of costs into daily and annual expenditure**
8. Consider the software you need and how you need to staff for that
9. What documentation and materials do you need access to?
    a. Manuals
    b. Specs
10. What kind and how many workstations
    a. **Examiner station requires an area of about 50–63 square feet**
11. Forensics workstations need to be hardened
    a. Create minimum requirements
12. Consider lockers-pace and the security for it
    a. Must be authorized to access lockers
    b. Use proper password hygiene for lock combos and keys
13. Security considerations
    a. Audit
14. Consider network connectivity
15. Gather adapters or connectors, switches, hubs, and other physical layer items
16. Consider communication needs
    a. Dedicated network connection
17. Consider certifying or licensing
    a. ASCLD – American Society of Crime Laboratory Directors
    b. ISO17025 – Requirements for the competence of testing and calibration laboratories
    c. Tempest
        i. National Industrial Security Program Operating Manual (NISPOM)
        ii. Refers to investigations and studies of compromising emanations
        iii. Prevent eavesdropping by preventing radiation and adding filters to phones
        iv. Expensive
18. Consider fire suppression
19. Need the ability to scale to 64TB Plus partitions
20. Need to be able to access many different media and platforms i.e. SATA, PATA, USB, Tape, SD Cards, etc.

ii. Investigation
    1. What did happen and documenting that

iii. Post-investigation
    1. How do we do our reporting

TOOLS Methodologies, Frameworks and Processes Term

2. Testify

7. The investigation Process Part 2
    a. Need an imaging system to capture a bitstream copy
        i. Need automatic write protection
        ii. Use Linux tool dd to create a drive image
    b. Data types
        i. Static – Non-volatile
        ii. Dynamic – volatile
        iii. Remnant Data
    c. Standards for data wiping
        i. DOD 5220.22m Standard
        ii. Gost standard Russian GOST P50739-95
        iii. VSITR Standard (German)
    d. Write blockers
        i. http://DigitalIntelligence.com
        ii. http://logicube.com
    e. US. Federal Rules of Evidence
        i. http://rulesofevidence.org
    f. Forensics Laws
        i. https://www.gpo.gov/fdsys/search/home.action
        ii. 18 USC 1029 – Fraud and related activity in connection with access devices
        iii. 18 USC 1030 – Fraud and related activity in connection with computers
        iv. 18 USC 1361-2 – Prohibits malicious mischief
        v. Rule 402 – Relevant evidence generally admissible; Irrelevant evidence inadmissible
        vi. Rule 901 – **Requirement of authentication or identification**
        vii. Rule 608 – Evidence of character and conduct of witness
        viii. Rule 609 – Impeachment by evidence of conviction of crime
        ix. Rule 502 – Attorney-Client privilege and work product; Limitations on waiver
        x. Rule 614 – Calling and interrogation of witnesses by court
        xi. Rule 701 – Opinion testimony by lay witnesses
        xii. Rule 705 – Disclosure of facts or data underlying expert opinion
        xiii. Rule 1002 – Requirement of original
        xiv. Rule 1003 – Admissibility of duplicates
    g. CFTT
        i. Computer Forensic Tool Testing Project
        ii. Launched by NIST
        iii. Establishes a “methodology for testing computer forensic software tools by development of general tool specifications, test procedures, test criteria, test sets, and test hardware.”
8. The investigation process part 3
    a. Consequence or impact

TOOLS Methodologies, Frameworks and Processes Term

i. Slightly harmful
ii. Harmful
iii. Extremely harmful

b. Likelihood
   i. Highly unlikely
   ii. Unlikely
   iii. Likely
c. NIST SP 800-30 Risk Management Guide
d. NIST SP 800-53 V4 Security Assessment Template
e. Use of standard frameworks allows
   i. The ability to present the information in a standardized way to allow more people to interact and gain value
   ii. Sharing of information so that the results may be easily interpreted
   iii. The results to be more readily and easily validated
f. Other Certs
   i. ISACA
      1. CISA – Certified Information System Auditor
      2. CISM - Certified Information System Manager
      3. CRISK – Certified Risk Management
      4. CGIT – Certified Governance
g. Phase 2 – Investigation phase
   i. 5 steps
   ii. Determine if there has been an incident
   iii. Find clues left behind
      1. Locard's principle of exchange
   iv. Preliminary search for evidence
   v. Bag and tag all evidence
   vi. Transport securely
h. Checklist to Prepare for a Computer Forensics Investigation (Page 85)
   i. Do not turn the computer off or on, run any programs, or attempt to access data on the computer.
      1. An expert should have the appropriate tools and experience to prevent data overwriting, damage from static electricity, or other concerns
   ii. Secure any relevant media including hard drives, cell phones, DVDs, USB drives, etc. the subject may have used
   iii. Suspend automated document destruction and recycling policies that may pertain to any relevant media or users at the time of the issue
   iv. Perform a preliminary assessment of the crime scene and identify the type of data you are seeking, the information you are looking for, and the urgency level of the examination
   v. Once the machine is secured, obtain information about the machine, the peripherals, and the network to which it is connected

vi. If possible, obtain passwords to access encrypted or password-protected files
vii. Compile a list of names, e-mail addresses, and other identifying information of those with whom the subject might have communicated
viii. If the computer is accessed before the forensic expert is able to secure a mirror image, note the user(s) who accessed it, what files they accessed, and when the access occurred. If possible, find out why the computer was accessed
ix. Maintain a chain of custody for each piece of original media, indicating where the media has been, whose possession it has been in, and the reason for that possession.
x. Create a list of key words or phrases to use when searching for relevant data

i. Computer Forensics Investigation Methodology (Page 86)
    i. First Response
    ii. Search and Seizure
    iii. Collect the Evidence
    iv. Secure the Evidence
    v. Data Acquisition
    vi. Data Analysis
    vii. Evidence Assessment
    viii. Documentation and Reporting
    ix. Testify as an Expert Witness

9. The investigation process part 4
    a. 14pt Methodology – Complete
        i. Identify the computer crime
        ii. Collect preliminary evidence
        iii. Obtain court warrant for discovery/seizure of evidence (if required)
        iv. Perform first responder procedures
        v. Seize evidence at the crime scene
        vi. Transport evidence to the lab
        vii. Create two bit stream copies of the evidence
        viii. Generate MD5 checksum of the images
        ix. Maintain chain of custody
        x. Store original evidence in secure location
        xi. Analyze the image copy for evidence
        xii. Prepare a forensic report
        xiii. Submit report to client
        xiv. Testify in court as an expert witness (if required)
    b. Methodology – Condensed
        i. Obtain court warrant for discovery/seizure of evidence (if required)
        ii. Evaluate and secure the scene
        iii. Collect evidence
        iv. Secure evidence
        v. Acquire data

TOOLS Methodologies, Frameworks and Processes Term

vi. Analyze data
vii. Assess evidence
viii. Prepare report
ix. Testify in court as an expert witness (If required)

c. Must train first responders to the extent you ensure they do no compromise evidence
   i. Collecting evidence is a expert level competency so first responders do not need to be training to the extent they should be expected to collect evidence forensically.
   ii. Train see something say something
d. First responders
   i. First ones on the scene
   ii. If they are not trained
      1. Rule number 1 – Do no harm
      2. Should protect the crime scene
      3. Get a forensic expert
   iii. If they are trained
      1. Protect and preserve volatile evidence
      2. Make sure there is an accurate representation of the crime scene
      3. Take photographic and documentary evidence
      4. Gather witnesses and information and detailed statements from them
   iv. The amount of training depends on the role of the first responders
e. Forensic Investigator toolkit
   i. Paraben's First Responder Bundle
      1. DeepSpar Disk Imager
         a. DeepSpar Recovery Environment is a free Windows-based application
         b. DeepSpar Operations Server
         c. Forensics Add-on
      2. Fred system
         a. acquire data directly from IDE/EIDE/ATA/SATA/ATAPI/SAS/Firewire/USB hard drives and storage devices and save forensic images to Blu-Ray, DVD, CD, or hard drives
      3. UltraBay 3d
      4. Paraben's StronHold Faraday Bags
      5. Paraben's Chat Stick
         a. Searches for chat logs
      6. PC-300 Data Extractor
         a. hardware and software suite for recovering flash- based storage
      7. Rapid Image 7020 X2 IT Hard drive duplicator
         a. designed to copy one "Master" hard drive to up to 19 "Target" hard drives

TOOLS Methodologies, Frameworks and Processes Term

8. IMAGE MASSTER WIPEPRO Hard drive sanitization station
    a. hard Drive Sanitization Station
9. WriteProtect-DESKTOP Portable wire blocker
10. Data Recovery Stick (Page 65)
    a. Recovers deleted files
    b. No software. Just plug in and recover
11. Tableau T8-R2 Forensic USB Bridge (Page 65)
    a. hardware-based write blocking of USB mass storage devices
12. Tableau TP3 Power Supply (Page 65)
    a. powers the Tableau TD1 duplicator and two hard disks.
13. VOOM Hardcopy 3P (Page 65)
    a. SATA/IDE Hard Drive Imager, Cloner, and Wiper with NIST approved SHA256 built into the hardware
14. µFRED (MicroFRED) (Page 65)
    a. micro Forensic Recovery of Evidence Device
    b. much of the processing power of a full size FRED system but in a package only a fraction of the size (9" x 8" x 13").
15. Phone Recovery Stick recovers data from Android phones

ii. Forensic software tools
1. Cain & Abel (Page 66)
    a. pw recovery for MS OS.
    b. Uses sniffing, dictionary, brute-force, and cryptanalysis attacks.
    c. Also record VoIP, decode scrambled passwords, recover wireless keys, reveal password boxes, uncover cached passwords and analyze routing protocols.
2. Recuva (Page 66)
    a. recover lost pictures, music, docs, video, email, or other file type from all types of media
    b. Can recover data from any rewriteable media like memory cards, external hard drives, USB sticks, etc.
3. Colasoft Capsa (Page 67)
    a. sniffer with support for over 300 network protocols
4. File Viewer (Page 68)
    a. Disk/File Utility
    b. Helps to locate, view, print, organize, and exchange files over the internet using e-mail components
    c. It can search for many common file types, or groups of file types, display, print, organize or send files over the internet, find and display pictures, videos, sounds, music, text files, documents, spread sheets, database, and system files, locally over the LAN or on the internet.
5. R-Drive (Page 69)

    a. Image utility that provides creation of disk image files for backup or duplication purposes.
    b. restores the images on the original disks, on any other partitions, or even on a hard drive's free space.
    c. can restore the system after heavy data loss caused by an operating system crash, virus attack, or hardware failure
6. FileMerlin (Page 70)
    a. converts word processing, xls, ppt and database files between a wide range of file formats.
7. AccessData FTK (Page 71)
    a. court-cited digital investigations platform that provides processing and indexing up front
    b. can be setup for distributed processing and incorporate web-based case management and collaborative analysis
8. Guidance Software's EnCase (Page 71)
    a. Acquires data from variety of devices to unearth potential evidence with disk-level forensic analysis.
    b. Produces comprehensive reports on your findings and maintains the integrity of your evidence
9. Nuix Corporate Investigation Suite (Page 71)
    a. used to collect, process, analyze, review, and report evidence
10. PALADIN Forensic Suite (Page 72)
    a. Modified "live" Linux distribution
    b. Fulfills various forensics tasks via the PALADIN Toolbox.
11. mailXaminer (Page 72)
    a. Conducts, coordinates, and monitors a case with an investigative team to get thorough and unambiguous evidence
12. OSForensics (Page 72)
    a. Extracts forensic data from computers, and uncover the data hidden inside a PC
13. Hex Editor Neo (Page 72)
    a. Freeware Hex Editor
    b. Allows viewing, modifying, analyzing hexadecimal data and binary files, editing, exchanging data with other applications through the clipboard, inserting new data and deleting existing data, as well as performing other editing actions.
14. Bulk extractor (Page 72)
    a. Computer forensics tool that scans a disk image, a file or a directory of files and extracts useful information without parsing the file system or file system structures.
15. Xplico (Page 72)
    a. Extracts the application data from an internet traffic capture.

TOOLS Methodologies, Frameworks and Processes Term

    b. Xplico is an open source Network Forensic Analysis Tool (NFAT).
16. The Sleuth Kit (Page 72)
    a. Collection of cmd line tools and a C library to analyze disk images and recover files from them
17. Autopsy (Page 72)
    a. digital forensics platform and GUI to The Sleuth Kit and other digital forensics tools.
18. Oxygen Forensic Kit (Page 72)
    a. Ready-to-use and customizable mobile forensic solution
    b. Allows extraction of data from the device but also creates reports and analyzes data in the field.
19. Paraben's DP2C (Page 73)
    a. data targeted collection tool for triage forensics
    b. DP2C from a USB drive and allows the collection of specific type of data from Windows-based systems to the evidence drive
20. MiniTool Power Data Recovery Enterprise (Page 73)
    a. can recover data including images, texts, videos, music, and emails
    b. It supports different data loss situations like important data lost because of deletion by mistake, formatting, logical damage, etc.
21. L0phtCrack (Page 73)
    a. a password auditing and recovery software.
    b. Performs scheduling, hash extraction from 64 bit Windows versions, multiprocessor algorithms, and network monitoring and decoding
22. Ophcrack (Page 73)
    a. free GUI driven Windows password cracker based on rainbow tables
23. Paraben's P2C (P2 Commander) (Page 73)
    a. It has an integrated database with multi-threading
    b. built on Paraben's email examination tools for network email and personal email archive analysis.
24. IrfanView (Page 73)
    a. IrfanView is a small FREEWARE (for non-commercial use) graphic viewer for Windows
25. SnowBatch (Page 73)
    a. Windows –based
    b. converts large batches of image or document files from one format to another
26. Zamzar (Page 73)

TOOLS Methodologies, Frameworks and Processes Term

            a. Supports over 1200 different conversions such as Video Converter, Audio Converter, Music Converter, eBook Converter, Image Converter, and CAD Converter
        iii. Mobile toolkit
        iv. Workstations with appropriate software
        v. Documentary templates
            1. Custody forms
            2. Evidence tracking forms
            3. Evidence gathering forms
        vi. Gloves to ensure evidence is not contaminated
        vii. Camera for pictures
    f. Trained forensic responder
        i. 6 steps
            1. Secure and evaluate crime scene
            2. Conduct interviews
            3. Document crime scene
                a. Photographing or video the scene
                b. Take detailed notes
                c.
            4. Collect and preservice evidence
            5. Package evidence
            6. Transport evidence
            7. SIDPPT
        ii. Document the 5 Questions
            1. Who
            2. What
            3. Where
            4. When
            5. And How
        iii. Must gain consent to collect evidence
            1. Consent must come from an reprehensive with the authority
10. The investigation process part 5
    a. Tools to find information
        i. Netstat – Highly volatile
        ii. Nbtstat
        iii. Ipconfig
        iv. Routeprint
    b. Evidence sources in order of volatility – Most to least
        i. Registers/Cache
        ii. Routing tables, process tables, memory
        iii. Temp file system

TOOLS Methodologies, Frameworks and Processes Term

1. Went we mount a usb drive, a temp file system pointer that tells the OS how to access the device, which only lasts as long as the drive is connected to the system

iv. Disk of storage media
v. Remote logging and monitoring data
vi. Configuration and topologies
vii. Archival media

c. Tagging and bagging
   i. Items to note on the bag
      1. Who seized
      2. Date and time bagged
      3. A tracking number or unique identifier
      4. Location information
      5. Details of contents
   ii. Exhibit numbering
      1. aaa/ddmmyy/nnnn/zz. Where:
      2. aaa are the initials of the forensic analyst or law enforcement officer seizing the equipment.
      3. dd/mm/yy is the date of seizure.
      4. **nnnn is the sequential number of the exhibits seized by aaa**
         a. **starting with 001 and going to nnnn.**
      5. **zz is the sequence number for parts of the same exhibit (e.g., 'A' could be the CPU, 'B' the monitor, 'C' the keyboard, etc.)**

d. Common mistakes
   i. Shutting down or rebooting
   ii. Assuming components will be reliable
   iii. Not having any baseline documentation
   iv. Not documenting the data collection process
   v. Not documenting obvious things

e. When searching can be done without a warrant
   i. Imminent destruction of evidence
      1. US V. David
   ii. Consent of person with authority
      1. Schneckloth v. Bustamonte

f. What do I see/what do I need to know
   i. Date and time
   ii. Place and location of the incident
   iii. Evidence from a volatile system and non-volatile system
   iv. Details of the persons present at the crime scene
   v. Name and id of the people or person who can serve as a potential witness

g. What do I collect
   i. http://crime-scene-investigator.net

h. Evidence collection forms
    i. Unique identifier
    ii. Type of case it is
    iii. Date and time
    iv. Name of person filling out report
    v. Property status
    vi. Name of victim and identifying info such as DOB or race
        1. Contact info
    vii. Accounting of evidence
    viii. Notes field
    ix. Types of systems
    x. Type of volatility of each system
    xi. Clock drift of every system
        1. Issue time command to check system time
        2. Different in system time from NTP may be a clue
    xii. Unique system identifiers
        1. Serial numbers
        2. License codes
        3. Baseline

i. Chain of custody
    i. Ability to tell the story of where the evidence has been, under whose control, for how long, and under what circumstances.
    ii. Every moment between the time it is taken and the time it is either returned or destroyed must be recorded
    iii. Written record consisting of
        1. Seizure
        2. Custody
        3. Control
        4. Transfer
        5. Analysis
        6. Disposition of evidence
    iv. Provides legal validation of appropriate evidence handling
    v. Form – This would be a legal document
        1. Unique identifier
        2. Date/time
        3. Item#
        4. Released by (ID number, title and name)
        5. Received by ID number, title and name)
        6. Signature
        7. Any comments/location
        8. Final disposition authority
            a. What is being done with the evidence

i. Returned to owner
ii. Destroyed
iii. Name and ID of dispositioning person
iv. Date/time of disposition

b. Witness information to destruction of release

j. NEVER use original evidence to do anything with, always use a forensically sound copy
   i. Validate/hash
   ii. Verify integrity of copy

k. Tools to obtain information from different common social media websites (Page 136)
   i. Netvizz, twecoll, divud, Digitalfootprints, Netlytic, X1 Social Discovery, Facebook Forensic Software, H&A forensics, Geo360, Navigator by LifeRaft Social, Emotive

11. The investigation process part 6
    a. Privacy related search and seizure
       i. If government's conduct does not violate a person's reasonable expectation of privacy then the search can be conducted without a warrant
          1. Capps vs. U.S.
       ii. What is that reasonable expectation of privacy with a computer
          1. Office worker may not have an expectation of privacy
             a. If overhearing then it is not violated
             b. If line is tapped, then it may be violated
          2. Courts have interpreted the 4th amendment for computers as a "closed container"
             a. Access to the information is seen as opening the container
          3. For companies, the container is owned by the company and can be searched with proper consent by the company
          4. 4th amendment does not apply to private/3rd parties
    b. Entrapment is illegal
       i. Forcing someone to do something and then holding them accountable to that thing
       ii. By engaging in these dubious practices, it may taint other evidence or call other evidence into question
    c. Use of remote monitoring to obtain information may require a warrant
       i. Wireless monitoring
       ii. Wireless monitoring
       iii. Wiretapping
    d. When warrants are not needed
       i. Consent
       ii. Immediate threat of harm of death
       iii. Search as a result of a lawful arrest
       iv. Inventory searches
       v. Border searches

TOOLS Methodologies, Frameworks and Processes Term

vi. International issues – transiting to the country subject to the requirement of entry
vii. What is the scope of consent to a search
    1. U.S. vs Pena 1998
    2. Expressed object and is limited by the breadth of the consent given
    3. Scope is extent of objective reasonableness
        a. What would the typical reasonable person have understood between the conversation of the agent and the person granting consent
viii. Exigent circumstance
    1. An emergency situation requiring swift action to prevent imminent danger to life or serious damage to property, or to forestall the imminent escape of a suspect, or destruction of evidence.
ix. Plain view – evidence in plain view may be seized without a warrant, but files may not be opened or viewed
    1. Computers may be seized, but it cannot be accessed without consent or warrant

e. Types of third party consent
    i. General
        1. Any authorized user of a computer, under their authority, may permit a search, even if the authorized user is not the owner of the computer
        2. Parental consent – under 18 in the U.S.
        3. Spouse or domestic partner may give consent
        4. System administrators
            a. They serve as agents of the providers of electronic communication services under Electronic Communications Privacy Act (ECPA) because they are duly appointed representatives of leadership
        5. Implied
            a. Entering into an agreement which implies consent
            b. Storage locations have the right to allow law enforcement to search even though someone is renting the locker

f. Council of Europe Treaty No. 185
    i. Obliges all signatories to act on behalf of another signatories to obtain and preserve data with respect to cyber crime
    ii. Have the ability to affect cross-border preservation
    iii. common criminal policy aimed at the protection of society against cybercrime
    iv. Forensic investigation and data preservation is done internationally under this treaty

12. The investigation process part 7
    a. PPA – Privacy Protection Act
        i. Lawful for a government officer to search for or seize when

ii. If materials are a product of work, a warrant is needed
    1. Mental impressions, conclusions, or theories and/or materials possessed for the purpose of communicating the material to the public by the person in some form of communication
    2. Cannot suppress the freedom of speech
iii. Privacy rights afforded to individuals
iv. Each building with a different address is considered an individual entity
    1. Multiple locations, multiple warrants

b. No knock warrants
    i. Warrants issued by a court that don't require authorities to announce themselves

c. Delayed notice warrants
    i. Sneaking and peaking
    ii. Surveillance where we have the right due to the consent of the course to observe activities where we would normally not have that rights such as wire tapping or video surveillance

d. Privilege
    i. Dr-patient privilege
    ii. Clergy
    iii. There is an expectation where conversations are private
    iv. Lawyer-client privilege
    v. Privileged conversations

e. Electronic Communications Privacy Act (ECPA)
    i. Store communication and the portion of those communications protected under ECPA ensures privacy rights for customers and subscribers of computer network service providers
    ii. Your content in the could with you ISP is covered under ECPA to a certain degree
    iii. 2 types or service providers
        1. ECS – Electronic communication service providers
        2. RCS – Remote computing service providers
    iv. Information is considered to be 1 of 3 types
        1. Basic subscriber information
        2. Records or other information pertaining to subscribers
            a. Metadata of subscribers
        3. Contents of the data itself
    v. 5 mechanisms that are often used with ECPA
        1. Subpoena
            a. Compels someone to do something
        2. Subpoena with prior notice to subscriber or customer
        3. Court order
            a. Must comply by such or such date

4. Court order with prior notice
5. Search warrant
    a. Allows for search under certain circumstances

vi. Voluntary disclosure
1. Providers of services not available to the public may freely disclose both content and other records relating to those communications
2. NSA and CIA work with service providers under voluntary disclosure to see data

f. European Council Directive 9546
i. Provides for rights and individuals in many circumstances in different areas and extends to electronic information

g. 2 federal statutes govern real-time electronic surveillance in federal criminal investigation
i. Wire-tap statute – Title 3
1. Regulates the real-time gathering of evidence on the wire
2. Must have interception pursuant to a court order
    a. Or consent exception
    b. Or provider exception
        i. payphone
    c. Or computer trespasser exception
    d. Or the extension telephone exception
    e. Or inadvertently obtained criminal evidence exception
    f. And the accessible to the public exception

ii. Pen registers and trap and trap devices statue – Title 18
1. Regulates the supporting metadata
2. Have to put in an application for a warrant to do this
3. Maybe be done in the FISA court

h. 3 categories of computer records
i. Computer generated
ii. Computer stored
iii. Computer generated and stored

i. Hearsay rules
i. Hearsay evidence may or may not be admissible
ii. Computer stored records contain human generated statements
1. human generated statements may satisfy an exception to the hearsay rule if they are offered for the truth of the matter asserted

j. When evidence is submitted, we have to go through the assessment of evidence to ensure it can be presented
i. Review file names for relevancy and patterns
ii. Review file headers and extensions
1. Do they match or mismatch

iii. Review date and timestamps

iv. Review metadata
v. Are we able to correlate the activity on a machine against logs, routers firewalls, traffic flow, etc

13. The Investigation Process Demo
    a. Tools
        i. HashCalc
            1. Calculates hashes using an input
        ii. EaseUS Data Recovery Tool
            1. Tool used to recover files
            2. Never install on the drive you want to recovery files from
            3. Can recovery the pagefile.sys and swapfile.sys
                a. These are the volatile memory files
                b. Can use a hex editor or a tool to analyze these files
        iii. Paraben's P2C
            1. Can be used to create a case

3. Hard Disks and File Systems

14. Hard Disks and File Systems Part 1
    a. Disk Drive
        i. Storage device to store digital files
    b. Disk drive types:
        i. Magnetic Storage - Floppy Drives, Tape Drives
        ii. Optical Storage - CD | DVD | Blue Ray
        iii. Flash Memory Storage - USB | BIOS | SD cards
        iv. HDD
        v. SSD
            1. **NAND based**
            2. Volatile RAM based
    c. Components of a hard drive 4:30 – 10:33
        i. Cylinders are on or within the platters
            1. The set of tracks of equal diameter
            2. Singular circle that cuts through all of the platers
            3. These are used to form a barrel like structure that groups the tracks together
        ii. Platters
            1. Coated with a magnetic substrate
        iii. Tracks are on the platter at equal distances from the center
        iv. Arms – 1 per platter that write onto the platter
        v. Head is on the tip of the arm
        vi. Spindle is the shaft that binds the platters together
        vii. The actuator is what controls the read/write am
        viii. The **track density** is the number of tracks in the hard disk over all

TOOLS Methodologies, Frameworks and Processes Term

ix. **Areal density** is the number of bits per sqin on the platter
x. **Bit density** is the number of bits per unit length of the track
xi. The zoned bit recording methodology is grouping tracks into zones

d. File systems 11:20 – 14:00
    i. FAT32
        1. File allocation table
    ii. FAT16
    iii. FAT12
        1. Used on floppy disks
    iv. NTFS
    v. EXT
    vi. EXT2
        1. In Linux OS
    vii. EXT3
    viii. EXT4
    ix. EFS
        1. Encrypting file system
        2. A subset of NTFS
        3. Used for cryptographic protection of data
    x. HFS
        1. Apple
        2. From a Linux/Unix background

e. Hard Drive Interfaces 14:00 - 18:11 (Page 158)
    i. 6 of the most common
    ii. SCSI
        1. Small computer system interface
        2. Enables up to 16 peripheral devices over 1 PCI board through daisychaining
            a. iSCSI
                i. Internet based SCSI
    iii. ATA
        1. SATA and PATA
        2. Advance Technology Attachment
        3. Serial
            a. Half duplex
            b. 1.5Gbps – 6Gbps
        4. Parallel
            a. Cable length can be up to 18in
    iv. USB
        1. Universal Serial Bus
    v. Fiber Channel
        1. Point-to-point

2. bi-directional
3. High speed interface supports up to 40Gbps

vi. IDE/EIDE
1. Integrated drive electronics
2. Enhanced integrated drive electronics
3. Older
4. Master and slave designation
5. Ribbon cable attachment

vii. SAS
1. Serial attached SCSI
2. Point to point serial
3. Could support up to 65535 device per chain

f. Tracks (Page 164)
i. Each of the two surfaces of a platter divided into concentric circles
ii. They store all the information on a hard disk
iii. Each track contains a number of smaller units called sectors.

g. Track numbering schemes 18:15
i. Tracks start numbering with 0 from the outer edge of the platter and move in
ii. 0-1023 circles from outside in on each side of the platter
iii. Heads are moved in and out jointly so that both heads are always located together at the same track number
iv. A cylinder is a group of all tracks that start at the same head position on the disk

h. Sectors 19:50 (Page 165)
i. Smallest physical storage unit on the platter
1. Hold 512 bytes of data in a sector
a. Some additional bytes for drive control and error correction
2. Advanced formatting will use 8 – 512 byte sectors bound together into a 4k sector (4096 bytes)
a. This is how we chunk out data and lay it out onto the drive
3. If the file is larger than 512 bytes, then sectors are stored side by side (contiguous)
a. However if data isn't a factor of 512 bytes, then the last sector is not used entirely.

ii. Bad sectors
1. Areas of the drive we cannot read or write on the drive
a. May be due to a flaw or mechanical failure
b. Can be marked as a bad sector
i. A bad actor can use a drive editor to make sectors as bad and hide data within them
ii. Use tools to search bad sectors for hidden data

i. Clusters 22:40 – 25:15 (Page 166)
i. Clusters form by combining sectors

ii. **Smallest allocation unit (unit of storage) of a hard drive overall**
iii. Set of tracks and sectors from 2 to 32 grouped together
iv. Minimum of two tracks
v. Typically 4k in size, but depends on the size of the disk partition
vi. With a large cluster size, the fragmentation problem diminishes, but it will greatly increase the chances of unused space

j. Lost clusters are a FAT error that results from the OS marking clusters as being used, but not allocating them out
   i. Logical errors, not physical
   ii. If you don't close files properly or shutdown improperly, you tend to get lost clusters
   iii. Use chkdsk
      1. used to find and recover lost clusters or mark bad sectors
      2. built-in Windows utility

k. Slack space 26:00 (Page 167)
   i. Free space on the cluster left over after writing data into the cluster
   ii. Unused area in the cluster reserved for the file even if not used
   iii. Space that is allocated, but not used
   iv. There are tools that allow writing into that space even though the system does not allow for that
   v. NTFS allows much smaller clusters on large partitions reducing slack space

l. Bit, Byte and Nibble 27:25
   i. Bit – Binary digit (Page 170)
      1. Smallest unit of data
      2. 0 or 1
   ii. Bytes are made up of bits
      1. A collection of 8 bits
      2. 1 character
      3. Smallest addressable unit of memory
      4. A memory unit
      5. Octet
      6. 2 nibbles
   iii. Nibble is a half byte or tetrad
      1. A collection of 4 bits
   iv. Octet
      1. 2 hexadecimal digits

m. Hard disk data addressing 29:40 – 31:00
   i. CHS (Page 171)
      1. **Cylinder head sector**
      2. Addresses data by specifying the cylinder, head, platter side, and sector
      3. Most IDE drives uses this type of addressing
      4. **Determines the address of the individual sector on the Disk**

ii. LBA
    1. Logical block addressing
    2. Addresses data by allotting and specifying and allocating a sequential number for each sector of the hard disk
    3. SCSI and EIDE drives use LBA

n. Track Density - refers to the space a particular number of tracks require on a disk.
o. Areal Density - refers to the number of bits per square inch on a platter, and it represents the amount of data a hard disk can hold.
p. Bit Density - the number of bits a unit length of track can accommodate.
q. Data density on a hard disk
    i. Hard disks store data using the zoned bit recording method
        1. also known as multiple-zone recording.
    ii. Tracks form a collection of zones depending on their distance from the center of the disk
    iii. The outer tracks have more sectors on them than the inner tracks.
    iv. Drives store more bits in each outer track compared to the innermost zone and helps to achieve a higher total data capacity.
    v. Bit density, track density, and area density are all used to calculate HDD density
r. Calculating Disk capacity 32:50 – 36:15
    i. 18,121 cylinders, 70 heads, and 43 sectors per track, assume a sector has 512 bytes
    ii. Total bytes = 1 disk * 18,121 cylinders/disk * 70 heads/cylinder * 1 track/head * 43 sectors/track * 512 bytes/sector = 27,926,635,520 bytes

15. Hard Disks and File Systems Part 2
    a. Partition 1:05 – 3:00
        i. The act of carving up the drive into allocatable space
        ii. Logical drive for storing the data
        iii. Logical divisions on the hard drive using the file system of your choosing
        iv. Primary (Page 174)
            1. Primary is the bootable partition with the operating system
            2. Max is 4 primary partitions
        v. Extended
            1. The logical drive that holds the information regarding the data and files stored on the disk
            2. 22 extended partitions possible
        vi. Inter-partition gap
            1. Space between the primary partition and the secondary partition
            2. contains the hidden data
            3. Disk Editor can be used to change the information in the partition table
        vii. Tools
            1. Disk Edit

TOOLS Methodologies, Frameworks and Processes Term

2. WinHex
3. HexWorkshop
4. available for examining the disk partitions
5. help users to view the file headers and important information about the file

b. **BPB – Bios parameter block** 3:00 – 3:56
   i. Sector 1 in the volume boot record of the hard drive
   ii. Explains the physical layout of the disc volume
   iii. Tells how the disk is laid out, where to find things, and how to access them
   iv. This describes the volume partition on partition device
   v. In a partitioned disk, the BPB describes the allocated amount, and how to read that volume
   vi. In an unpartitioned disk, it describes the entire drive, the physicality of the entire space available

c. **MBR** – Master Boot Record 3:59 – 8:10 (Page 176)
   i. Sector 0 in the volume boot record of the hard drive
   ii. Specifies the location of an operating system for the system to load into the main storage
   iii. Information regarding the files on the disk, location, size, information of how we access data on the drive
   iv. 512-byte boot sector
   v. Holds the partition table
      1. 64 bytes in size
      2. Stores information about the partitions on the hard drive
   vi. Holds the master boot code
      1. identifies which partition is active
      2. Implements the ability to examine the partition table
      3. Locates the first sector of the active partition
         a. The boot sector copy is then loaded from the active partition into memory
         b. The boot sector copy is parsed in order to load the kernel and whatever else needs to be loaded for the OS
         c. Then transfer control to the executable code in the boot sector which essentially transfers control to the OS and the OS boots up
   vii. MBR signature or end of sector is always 0x55AA
   viii. Boot sector
      1. Consists of data used by the file system to get to the volume and utilizes the framework parcel to stack the working partition documents
   ix. Recognizes hard drive media with a 32bit individual disk signature so HDD can be uniquely identified (Drive signature)

d. How to backup the MBR 9:00 – 11:25

i. In Unix/Linux, use DD
    1. Used to create a block by block copy of an input file
    2. Backup
        a. dd if=/dev/xxx of=mbr.backup bs=512 count=1
        b. bs is block size
            i. buffer size
        c. if is input file
        d. of is output file
    3. Restore
        a. dd if=mbr.backup of=/dev/xxx bs=512 count=1
ii. In Windows

e. GPT Format 11:30 – 21:30
    i. GUID Partition Table (Page 179)
        1. Overcomes the issues with the MBR
            a. Could go over a certain disk size – larger than 2TB
            b. Overcame issues with partition sizes – 128 partitions in Windows
            c. More secure storage mechanism
            d. Scatters the data on the drive, not sequentially on the sectors
            e. Uses checksums to detect errors and ensure data integrity
        2. Each logical block is 512 bytes and each partition entry is 128 bytes,
    ii. Used within UEFI
        1. Unified Extensible Firmware Interface
        2. Replaces legacy BIOS systems
    iii. Uses LBA Instead of CHS
        1. Logical Block Addressing
        2. MBR partition scheme uses 32 bits for storing LBA and the size information on 512-byte sector
        3. LBA0 stores a protective MBR
            a. Stores allocation information for backwards compatibility in order to run an older OS and software
            b. Allows to use older boot discs
        4. LBA1 contains the GPT header where the BIOS boot sector would sit
            a. GPT header comprise a pointer to the PEA
        5. LBA2 contains the PEA
            a. PEA – Partition Entry Array
            b. UEFI assigns 16,384 bytes for the PEA
        6. LBA3-33 are used for used for various admin, set up, and control sectors on the drive
        7. LBA34 is the first usable sector
    iv. GUID (Page 178)
        1. Used within UEFI instead of the MBR

2. Global unique identifier
3. The Windows user and a Windows account has a GUID associated with it
4. **128-bit unique number generated by Windows**
5. Created for identifying a specific device, document, a database entry, and/or the user
6. Displayed as 32 hexadecimal digits with groups separated by hyphens

v. Uses CRC 32-bit checksums for error checking
1. Cyclic redundancy check
2. Used for error control and correction
3. A hashing that will be used for integrity
4. Used to check for errors in the partition table, flag them, and protect them

vi. Unified Extensible Firmware Interface Specification defined the GUID

f. Windows File System – Essential files 21:30
i. Ntoskrnl.exe
ii. Ntkrnlpa.exe
iii. Hal.dll
iv. Win32k.sys
v. Ntdll.dll
vi. Kernel32.dll
vii. Advapi32.dll
viii. User32.dll
ix. Gdi32.dll

g. The Windows Boot Process 22:45 – 28:15
i. Windows 8 and later versions use either the BIOS-MBR or the UEFI-GPT method
ii. Step1. System is powered on and the CPU sends a Power Good signal to the motherboard and checks for the PC's BIOS firmware
iii. BIOS starts **Power-On Self-Test (POST)** and checks if all the required hardware for system boot is available
1. This loads all the firmware settings from the non-volatile memory (CMOS) on the mobo

iv. Step 3. If POST successful, add-on adapters perform a self-test for integration with the system
v. Step4. Pre-boot process completes POST, detecting a valid system boot disk
vi. Step 5. After POST, the PC's firmware scans the boot disk and loads the MBR, which searches for basic boot info on the Boot Configuration Data (BCD)
vii. Step 6. The MBR triggers the Bootmgr.exe, which locates the Windows loader (Winload.exe)
viii. Step 7. The Windows loader loads the OS kernel ntoskrnl.exe

ix. When Kernel starts running, the Windows loader loads HAL.DLL, boot-class device drivers marked BOOT_START and the SYSTEM registry hive into memory
x. Step 9. The Kernel passes control of the boot process to the Session Manger Process (SMSS.exe)
    1. SMSS loads all other registry hives and drivers required to configure the Win32 subsystem run environment.
xi. Step 10. The Sesssion Manager Process triggers Winlogon.exe
    1. This presents the user login screen for user auth
xii. Step 11. The Session Manager Process initiates Service control manager
    1. This starts all the services, the rest of the non-essential device drivers, the security subsystem LSASS.EXE and executes Group policy scripts.
xiii. Step 12. When user logs in, Windows creates a session for the user
xiv. Step 13. Ther Service control manager starts Explorer.exe
    1. This initiates the Desktop Window Manger (DMW) process, which provides the desktop for the user.

h. Cold boot (Page 184)
    i. **Aka hard boot**
    ii. **Happens by cutting power to the system**

i. Warm boot
    i. **Happens when user restarts via the OS**

j. UEFI boot Process 29:10 – 31:40
    i. SEC Phase
        1. Security
            a. Initialization after powering up
            b. Finds, validates, installs, and runs the PEI
    ii. PEI Phase
        1. Pre-EFI Initialization
            a. **Initializes the CPU, temp memory, boot firmware volume (BFV)**.
            b. Locates and executes the pre initializations modules (PEIMs) associated with functionality present in the BFV
            c. Initializes all the found hardware in the system.
            d. It **creates a Hand-Off block list (HOBL) with all found resources interface descriptors** and passes it to the next phase
    iii. DXE Phase
        1. Driver Execution Environment
            a. Most of the initialization happens in this phase
            b. Using HOBL, it initializes the entire system physical memory, I/O and MIMO (memory mapped input output) resources
            c. Begins dispatching DXE drivers present in the system firmware volumes in the HOBL

d. DXE core produces a set of EFI Boot Services and EFI Runtime Services
    i. EFI Boot Services are allocating memory and loading executable images.
    ii. EFI Runtime Services are converting memory addresses from physical to virtual while handing over to the kernel, and resetting the CPU, to code running within the EFI environment or within the OS kernel once the CPU takes control of the system

iv. BDS Phase
    1. Boot Device Section Phase
        a. Interprest the boot config data and selects the Boot Policy for later implementation
        b. This phase works with the DXE to check if the deive drivers require sig verification
        c. The system loads MBR boot code into memory for legacy BIOS Boot or loads the Bootloader program from the EFI partition for UEFI Boot.
        d. Also provides an option for the user to choose EFI Shell or EUFI application as the Boot device for the setup

v. RT Phase
    1. Run Time Phase

k. Identifying GPT 31:45 – 34:25
    i. Use the Get-GPT command
        1. Part of a powershell commandset that must be installed
        2. Analyzes the GUID Partition Table data structure of the hard disk
        3. If Get-GPT is run against a disk formatted with a MBR, it will throw an error prompting to use Get-MBR instead
        4. http://www.invoke-ir.com
            a. Location for commandset
        5. Get-BootSector
            a. a command used parse GPTs of disks with either UEFI or MBR
        6. Get-PartitionTable
            a. Analyzes the GUID partition table to find the exact type of boot sector and displays the partition object
        7. DiskPart
            a. Windows tool used to display the partition details

16. Hard Disks and File Systems Part 3
    a. MAC Boot Process 1:30 – 5:05 (Page 192)
        i. Starts with the activation of BootROM
            1. Initializes system hw and selects an OS to run

TOOLS Methodologies, Frameworks and Processes Term

ii. Once you power on the Mac, BootROM performs POST to test hw interfaces required for startup
iii. On PowerPC-based MAC computers, Open Firmware initialized the rest of the hardware interfaces
iv. On Intel-based MAC computers, EFI initializes the rest of the hw interfaces
v. After initialization the hw interfaces, the system selects the OS
vi. If the system contains multiple OS, then is allows the user to choose the OS by holding down the Option key
vii. Once the BootROM operation is finished, the control passes the BootX (PowerPC) or boot.efi (Intel) boot loader, which is located in the /System/Library/CoresServices directory
viii. The boot loader loads a pre-linked version of the kernel, which is located at /System/Library/Caches/com.apple.kernelcaches
ix. If the pre-linked kernel is missing, the boot loader attempts to load the mkext cache file, which contains a set of device drivers.
x. If the mkext cache file is also missing, the boot loader searches for drivers in the /System/Library/Extensions directory
xi. Once the essential drivers are loaded, the boot loader starts initialization of the kernel, Mach and BSD data structers, as well as the I/O kit
xii. The I/O kit uses the device tree to link the loaded drivers to the kernel
xiii. The launchd (launch daemon), which has replaced the mach_init process in newer versions, runs startup items and prepares the system for the user.

b. Linux Boot Process 5:05 – 6:30 (Page 193)
   i. **The BIOS stage**
      1. **Initializes system hw during the booting process**
   ii. The Bootloader Stage
      1. **Loads the Linux kernel and RAM disk (if used)**
   iii. The Kernel Stage
      1. The virtual root file system created by the initrd image executes the Linuxrc program.
      2. The program generates the real file system for the kernel and later removes the initrd image.
      3. The kernel then searches for new hw and loads any suitable device drivers found
      4. It then mounts the actual root file system and then performs the init process.
      5. The init process reads the file “etc/inittab” and uses this file to load the rest of the system daemons

c. Types of files systems 8:00 – 14:42
   i. Disk file systems (Page 196)
      1. designed for storing and recovering the file on a storage device, usually a hard disk, directly or indirectly connected to the computer

2. A few examples of the disk file system are FAT, NTFS, ext2, ISO 9660, ODS-5, and UDF.

ii. Network file systems
    1. helps the users to access the files on other computers connected through a network.
    2. The file systems are transparent to the user
    3. A few examples of network file systems are NFS, CIFS, and GFS.

iii. Database file systems
    1. It is a new method of storing data on the computer and effectively managing the file system
    2. identifies the files by their characteristics, such as the name of the file, type of the file, topic, author, or similar metadata.
    3. User can search for a file by formulating the SQL query or in natural speech.

iv. Flash file systems
    1. stores the files or data in flash memory devices

v. Tape file systems
    1. It stores files on tape in a self-describing form.

vi. **Shared disk file system** (Page 197)
    1. works on the principle of accessing an external disk subsystem (SAN) through a number of servers

vii. Special-purpose file systems
    1. the software organizes files during the run time and uses them for tasks such as communication between computer processes or temporary file space
    2. File-centric operating systems such as UNIX use this file system.
    3. Any file system that is not a disk file system or network file system is a special-purpose file system.

viii. A file system is a set of data types employed for:
    1. Storage
    2. Hierarchical categorization
    3. Management
    4. Navigation
    5. Access
    6. Recovering the data

ix. Windows file systems
    1. FAT
        a. Older file system designed in 1976
        b. The file allocation table stores all the files and resides at the beginning of the volume
        c. Almost all the operating systems installed on the personal computers implement FAT file system

    d. **0x0FFFFFFF is used to make the end of a file**
    e. **Originally designed for floppy disks**
2. FAT12
3. FAT16
4. FAT32
    a. Reserved Area
        i. First reserved sector is the Volume Boot Record or VBR, which comprises the BIOS Parameter Block (BPB) containing basic file system information
    b. FAT Area
        i. holds two duplicates of the File Allocation Table to help the system check for the empty or idle spaces
    c. Data Area
        i. largest part of a partition
        ii. stores the actual file and directory data
    d. FAT Partition Boot Sector
        i. **consists of data the document framework uses to get to the volume**
        ii.
    e. Directory Entries and Cluster Chains
        i. 32 byte data structure allotted for each file and directory.
        ii. Used to store additional metadata
    f. Uses smaller clusters with more address bits to support larger disks as well as offer better storage
    g. Utilizes space 10-15% more effectively due to use of smaller clusters
5. NTFS (Page 204)
    a. New Technology File System
    b. More traditional in Windows
    c. Sparse file support
    d. Disk usage quotas
    e. Reparse points
    f. EFS
        i. A sub file system
        ii. Encryption file systm
    g. System files
        i. $attrdef
            1. Contains definitions of all system and user-defined attributes of the volume
        ii. $badclus
            1. All bad clusters

iii. $bitmap
    1. Bitmap for the entire volume
iv. $boot
    1. Volume bootstrap
v. $logfile
    1. Used for recovery
vi. $mft
    1. A record for every file
vii. $mftmirr
    1. Mirror of $mft used for recovery
viii. $quota
    1. Disk quota list of all users
ix. $upcase
    1. Converts characters into uppercase UNICODE
x. $volume
    1. volume name and version number
xi. Ntfs.sys
    1. Computer system file driver for NTFS
xii. NTFS boot sector
    1. First 16 sectors are assigned to the boot sector
        a. This is called the boot strap code
    2. Partition identifier: 0x07 (MBR) EBD0A0A2-B9E5-4433-87C0-68B6B72699C7 (GPT)
xiii. Cluster sizer for NTFS volumes
    1. NTFS uses variable cluster sizes depending on the volume size
xiv. 512MB or less = 512 bytes cluster
xv. 513MG – 1GB = 1KB cluster
xvi. 1GB-2GB = 2KB cluster
xvii. Larger than 2GB = 4KB cluster
xviii. Supports files up to 16GB
xix. NTFS Master File Table (MFT)
    1. Relational database which consists of info related to files and the files attributes
    2. The rows consist of file records and the columns consist of file attributes
    3. It has info of every file on the NTFS volume including info about itself
    4. It has 16 records reserved for system files

6. REFS
    a. New in Server16
    b. Resilient File System

d. ADS 15:25 – 22:58
    i. Alternate data streams
    ii. Notepad sample.txt:secret.txt
    iii. A lot of data can be hidden with ADS
    iv. Creates two files
        1. Secret.txt has the data and is a hidden file
        2. Sample.txt has no data but is the container
        3. Sample.txt is what can be called
        4. Secret.txt cannot readily be seen
    v. Can read about this on forensicsfocus.com
    vi. Tools to find ADS
        1. LADS.exe
        2. Streamarmor – securityexploded.com
            a. tool used to discover Hidden Alternate Data Streams (ADS) and clean them completely from system (Page 495)
        3. Sysinternals tools
            a. Microsoft.com/technet
    vii. Unaccounted data or missing data can indicate ADS
e. EFS 23:00 - 24:10
    i. Used to encrypt data in the Windows environment
    ii. In order to recover, the data has be encrypted
        1. Only way to de-encrypt is to either have the keys and certificates or break the encryption
        2. Admins have the keys and certificates assigned to them
f. Linux file systems 24:10 - 25:20 (Page 221)
    i. Architecture
        1. User Space
            a. The protected memory area where the user processes run and this area contains the available memory
        2. Kernel Space
            a. The memory space where the system supplies all kernel services through kernel processes
            b. The users can access this space through the system call only
            c. A user process turns into kernel process only when it executes a system call
        3. GNUC Library (glibc)
            a. Sits between the User Space and Kernel Space
            b. Provides the system call interface that connects the kernel to the user-space applications
        4. VFS – Virtual File System
            a. An abstract layer, residing on top of a complete file system
            b. Allows client applications to access various file systems

TOOLS Methodologies, Frameworks and Processes Term

ii. Minix
    1. First Linux file system
iii. FHS
    1. File Hierarchy Standard
iv. Xia
v. Msdos
vi. Umsdos
vii. Vfat
viii. /proc
ix. Nfs
x. Iso 9660
xi. Hpfs
xii. Sysv
xiii. Smb
xiv. ncpfs
xv. EXT2 (Page 223)
    1. Remy Card developed the second extended file system (ext2) as an extensible and powerful file system for Linux
    2. Ext2 is the basis for all of the currently shipping Linux distributions
    3. Older file system
    4. Each file and directory is described by a single node
    5. Inode is a basic building block of the EXT2 file system
    6. Only one inode describes every file and directory in the file system
    7. Inodes for each file system block are placed together in an inode table
    8. Superblock
        a. Stores information about the size and shape of the Ext2 file system
        b. Enables the file system manager to use and manage the file system
        c. Magic Number allows the mounting software to verify the Superblock for the EXT2 file system. For the present EXT2 version, it is 0xEF53.
        d. Revision Level - **The major and minor revision levels allow the mounting code to determine whether or not this file system supports features that are only available in particular revisions of the file system**.
        e. Feature compatibility fields help the mounting code to determine which new features can safely be used on this file system
        f. Mount Count and Maximum Mount Count allow the system to determine if it needs to fully check the file system. The mount count increments each time the system mounts the file system

and displays the warning message of “maximal mount count reached, running e2fsck is recommended'' when it equals the maximum mount count

xvi. EXT3 (Page 227)
    1. **Developed by Stephen Tweedie in the year 2001**
    2. Command to convert EXT2 to EXT3 file system
        a. # /sbin/tune2fs –j <partition-name>

xvii. EXT4 (Page 229)
    1. Designed as a replacement for EXT3
    2. Supported in Linux v2.6.19 onward
    3. Max file size of 16TB and volume size of 1 Exibyte

g. MAC OS X file systems 25:20 – 26:57

i. HFS (Page 230)
    1. Hierarchical File System (HFS)
    2. Designed in 1985 for MAC
    3. Divides the volume into logical blocks of 512 bytes each
    4. **Uses a 16-bit value to address allocation blocks**
    5. Restricts the number of allocation blocks to 65,535
    6. Groups files into directories and each directory also groups with other directories
    7. Logical volume blocks 0 and 1 are the boot blocks
    8. The Logical block 2 has the Master Directory Block (MDB) which defines data about the volume s

ii. HFS+ (Page 231)
    1. For MAC OS Extended
    2. volumes are divided into logical blocks (sectors) of size 512 bytes
    3. sectors are clustered into allocation blocks
    4. Total number of allocation blocks depends on the volume size
    5. The bulk of an HFS+ volume consists of seven types of sectors
        a. User file fork
        b. Allocation file
        c. Catalog File
        d. Extent overflow files
        e. Attribute file
        f. Startup file
        g. Unused space

iii. UFS (Page 231)
    1. Unix file system
    2. Architecture
        a. A few blocks at the beginning of the partition are reserved for boot blocks

b. A super block, including a magic number identifying this as a UFS file system, and some other vital numbers describing this file system's geometry and statistics and behavioral tuning parameters
c. A collection of cylinder groups

h. ZFS (Page 237)
   i. Oracle Solaris 11 (SUN)
   ii. file system can compress, encrypt, checksum, and de-duplicate a block during writes

i. CD-ROM/DVDFileSystem (Page 239)
   i. ISO 9660
      1. Reserves 32,768 bytes at the beginning of the CD-ROM for booting a computer
      2. defines uses for file systems of CD-ROM and DVD media
      3. The first field in a volume descriptor is the type (Page 240)
         a. Number 0 - refers that the volume descriptor is a boot record
         b. Number 1 - refers that the volume descriptor is a primary volume descriptor
            i. Describes the location of the contiguous root directory similar to the super block of the UNIX file system
         c. Number 2 - refers that the volume descriptor is a supplementary volume descriptor
         d. **Number 3 - refers that the volume descriptor is a volume partition descriptor**
         e. Number 255 - refers that the volume descriptor is a volume descriptor set terminator
      4. Second field is the standard identifier
         a. set to CD001
   ii. ISO 13490
      1. Improvement over ISO 9660
      2. Permits the ISO 9660 format and the ISO/IEC 13490 format to exist on the same media
      3. Specifies using multicasting properly
   iii. CDFS – Compact Disc File System
      1. File system for the Linux operating system
      2. Transfers all tracks and boot images on a CD, as normal files
      3. Files can then be mounted (for example, for ISO and boot images), copied, and played
      4. Goal was to unlock information in old ISO images

j. VirtualFileSystem(VFS)
   i. Linux

ii. A programming that acts as an interface between the OS's kernel and the different file systems
iii. Caches information in memory from each file system when mounted and used

k. UniversalDiskFormatFileSystem (UDF)
i. Defined by Optical Storage Technology Association (OSTA) to replace the ISO9660 file system on optical media and also FAT on removable media
ii. Open source file system based on ISO/IEC 13346 and ECMA- 167 standards that defines how a variety of optical media store and interchange the data

l. RAID storage systems 26:57 - 29:37
i. Main advantage is that if any disk in the RAID array fails or is susceptible to damage; the system still continues to function without any loss of data
ii. RAID 0 (Page 243)
1. Striping with no parity
2. Simplest RAID level
3. If we lose one of the drives in the striped set, we lose all data across striped set
4. No capability to recover from drive failure
5. Fast
6. Stripes in 64kb chunks
7. At least 2 drives
iii. RAID 1
1. Drive mirror
2. Drive duplexing means mirror controllers as well
3. 2 drives of equal approx. size, set up and formatted the same way
4. Data is written to both simultaneously through a common control or interface
5. If one drive fails, the other drive can be used
iv. RAID 5
1. Striping with parity
2. Writes data across all drives in a stripe with parity block information
3. At least 3 drive at min and as much as 32 drives
4. Parity block information will give the ability to recover the set to access the data to continue to operate in a reduced capacity while drive is replaced and data is regenerated
v. RAID 10 (Page 246)
1. Striping with drive mirroring
2. RAID 1+0
3. Combines RAID 0 and RAID 1 to combine the speed, functionality, and recoverability of both

17. Hard Disks and File Systems Part 4
a. HPA (Page 247)
i. Host protected areas of the HDD

ii. Reserved area of the HDD
iii. Data is stored in the read only area here that users do not have access directly to in any way

b. DCO
   i. Device Configuration Overlay
   ii. Another area of protected space of the HDD
   iii. The vendor may put tools for data recovery or to restore image or information about the drive
   iv. May be used by the vendor before the HDD leaves the factory

c. Encase 8:10
   i. Tool that can go in and image these areas

d. TAFT 8:19
   i. ATA/IDE forensics tool designed for older drives and can image these areas

e. Sluth kit
   i. May be able to image these areas

f. Character sets 10:23 – 15:15
   i. ASCII (Page 248)
      1. Character encoding standard used in most computers
      2. **machine readable language, used in major digital operations such as sending and receiving emails**
      3. 128 specified characters
      4. Coded in 7bit integers
      5. Source code or macros
      6. A-Z, a-z, 0-9, basic punctuation symbols, control codes, and space
      7. Came from teletype machines where they were for
      8. Original character sets used
      9. 3 specific divisions
         a. Non-printable
         b. Lower asci chacters
         c. Higher asci characters
   ii. Unicode
      1. Computing standard developed shortly after ACSII
      2. Contains 128,000 characters
      3. UTF-8
      4. UTF-16
      5. UTF-32

g. Hex editors 15:15 – 27:10
   i. WinHex
      1. Can search for file types
      2. Can restore files
      3. Converts binary to hex and back
      4. Can search for deleted data in hidden partitions

5. Can do
    a. volume snapshotting
    b. Directory browsing

ii. Offset (Page 249)
1. Help to understand what line of data we're looking at and where it is
2. Can be used to track data in the HDD
3. Left margin is the beginning point
4. The top shows the column number
5. Help to grab raw data and interpret it
6. Header information will describe the type of file
7. Hexadecimal codes that an operating system identifies and uses to maintain the file system

h. File carving – looking for files and pulling them out based on parsing 25:57
i. Recovering files from fragments and pieces in typically damaged areas or unallocated areas of space on the HDD

i. Hex values are used to identify files types
i. Doesn't change even if someone changes it in the OS
ii. 25 50 44 46 – PDF
iii. 89 50 4e 47 – PNG
iv. 42 4D – BMP
v. FF D8 FF – JPEG
vi. FF Ex or FF Fx – MPEG or MP3
vii. 49 44 33 03 – MP3
viii. 57 41 56 45 – WAV
ix. 50 4B 03 04 14 00 06 00 – DOCX
x. 50 4B 03 04 14 00 08 00 08 00 – JAR
xi. 50 4b 03 04 – ZIP
xii. 52 61 72 21 1a 07 – RAR
xiii. 30 26 b2 75 8e 66 cf 11 – WMV
xiv. 41 56 49 20 – AVI
xv. 47 49 46 - GIF
xvi. D0 CF 11 E0 A1 B1 1A E1 – DOC or PPT or XLS
xvii. https://www.garykessler.net/library/file_sigs.html

18. Forensic File System Tools Demo
a. Sluthkit
b. WinHex
c. Kali
d. Autopsy
i. Windows

19. Hard Disks and File Systems – info not in videos
a. Kernel space

TOOLS Methodologies, Frameworks and Processes Term

i. Memory space where the system supplies all kernel services through kernel processes
ii. Users can access this space only through the system call
iii. A user process turns into kernel process only when it executes a system call

b. VFS
i. Virtual Files System
ii. Abstract layer residing on top of a complete file system
iii. Allows client applications to access various file systems
iv. Consists of a dispatching layer which provides file system abstraction and numerous caches to enhance the files system operations performance

c. Super Block
i. Linux
ii. Holds data that the file system uses to access the partition or volume
iii. Analogous to the FAT Partition Boot Sector
iv. The revision level is information held by the super block that allow the mounting code to determine whether or not supported features are available to the file system.

d. HFS
i. Hierarchical File System
ii. Divides the volume into logical blocks of 512 bytes and groups the logical blocks into allocation blocks
iii. HFS uses a 16-bit value to address allocation blocks
iv. Max number of allocation blocks is 65,535

e. JPEG (Page 251)
i. Joint Photographic Experts Group
ii. method of lossy compression for digital images
iii. most significant bit of marker is set to 0xff

f. Common mistakes while collecting data from the system that result in the loss of critical evidence
i. Choosing wrong resolution for data acquisition
ii. Poor knowledge of the instrument

g. The Sleuth Kit (TSK) (Page 271)
i. library and collection of command line tools
ii. Allows you to
1. investigate disk images
2. analyze volume and file system data
3. incorporate additional chapters to
a. analyze file contents
b. build automated systems
iii. To perform analysis, create a forensics image .dd or. E01 using disk imaging tools such as AccessData FTK Imager

TOOLS Methodologies, Frameworks and Processes Term

iv. fsstat
    1. **displays the details associated with a file system**
    2. The output of this command is file system specific
v. Istat
    1. Display details of a meta-data structure (inode)
vi. Fls
    1. List file and directory names in a disk image.
vii. img_stat
    1. Display details of an image file

4. Data Acquisition and Duplication

20. Data Acquisition and Duplication Part 1
    a. Data Acquisition (Page 294)
        i. The use of established methods to extract the Electronically Stored Information (ESI) from suspect computer or storage media to gain insight into a crime or an incident
        ii. Forensic data acquisition
            1. Process of imaging or collecting information from various media in accordance with certain standards for analyzing its forensic value.
        iii. Live Data Acquisition
            1. **Process of acquiring volatile data from a working computer (either locked or in sleep condition) that is already powered on**.
            2. Order of Volatility
                a. Registers/Caches – Always changing
                b. Routing tables/process table/memory – ten nanoseconds
                c. Temporary files – seconds or minutes
                d. Disk and storage media - minutes
                e. Remote logging and monitoring data – hour to week
                f. System configuration / topology
                g. Archival media – Does not change
            3. Common mistakes in volatile data collection
                a. Assuming that some parts of the suspicious machine may be reliable and usable
                b. Shutting down or rebooting the suspicious computer
                c. Not having access to baseline documentation about the suspicious computer
                d. Not documenting the data collection process
            4. Live Data Collection Methodology
                a. Incident Response Preparation
                b. Incident Documentation
                c. Policy Verification
                d. Data collection strategy

e. Data collection setup
    i. Record the time, date, and command history of the system to establish an audit trail generate dates and times while executing each forensic tool or command.
    ii. Start a command history to document all the forensic collection activities. Collect all possible volatile information from the system and network.
    iii. Do not shut down or restart a system under investigation until all relevant volatile data has been recorded.
    iv. Maintain a log of all actions conducted on a running machine.
    v. Photograph the screen of the running system to document its state.
    vi. Identify the operating system (OS) running on the suspect machine.
    vii. Note system date, time and command history, if shown on screen, and record with the current actual time.
    viii. Check the system for the use of whole disk or file encryption.
    ix. Do not use the administrative utilities on the compromised system during an investigation; exercise caution when running diagnostic utilities.
    x. Dump the RAM from the system to a forensically sterile removable storage device.
    xi. Collect other volatile OS data and save to a removable storage device.
    xii. Complete a full report documenting all steps and actions taken.

iv. Static Data Acquisition

1. **Process of acquiring the non-volatile or unaltered data remains in the system even after shutdown.**

21. Data Acquisition and Duplication Part 2
    a. Static Data
        i. Temporary (temp) files
        ii. System registries
        iii. Event/system logs
        iv. Boot sectors
        v. Web browser cache
        vi. Cookies
        vii. Hidden files
    b. Static Data Acquisition

TOOLS Methodologies, Frameworks and Processes Term

i. Prepare a Chain of Custody document (Page 302)
ii. Sanitize the Target Media - (NIST SP800-88) (Page 304)
iii. Determine the Best Acquisition Method
iv. Enable Write Protection on the Evidence Media (Page 303)
v. Determine the Data Acquisition Format (Page 305)
vi. Select the Data Acquisition Tool
vii. Plan for Contingency
viii. Acquire the Data
ix. Validate Data Acquisitions

c. Data acquisition methods
    i. Bit-stream disk to image (Page 308)
        1. flexible method which allows creation of one or more copies or bit-for-bit replications
        2. Tools used to read the disk-to-image files
            a. ProDiscover
            b. EnCase
            c. FTK
            d. The Sleuth Kit
            e. X-Ways Forensics
            f. ILook Investigator
    ii. Bit-stream disk to disk
        1. Performed when creating an image is not possible
        2. Tools that can modify the target disk's geometry to match the data copied from original suspect drive
            a. EnCase
            b. SafeBack
            c. Norton Ghost
        3. Logical – collection of only the files required
        4. Sparse – collecting only fragments of deleted data

d. Data acquisition formats
    i. Raw - understood by everything
    ii. Proprietary - (by tool vendor)
    iii. Advanced Forensics Format (AFF) - open source
        1. file extensions include .afm for AFF metadata and .afd for segmented image files.
        2. Supports two compression formats: zlib and LZMA
    iv. Advanced Forensics Framework 4 (AFF4) - AFF4 supports image signing and cryptography. Adopts a scheme of globally unique identifiers for identifying and referring to all evidence.

e. Data acquisition tools
    i. The tool must not alter or make any changes to the original content

ii. The tool must log I/O errors in an accessible and readable form, including the type and location of the error
iii. The tool must be able to compare the source and destination and alert the user if the destination is smaller than the source
iv. The tool must have the ability to pass scientific and peer review. Results must be repeatable and verifiable by a third party, if necessary
v. The tool shall completely acquire all visible and hidden data sectors from the digital source
vi. The tool should create a bit stream copy of the original content when there are no errors in accessing the source media
vii. The tool should create a qualified bit stream copy (A qualified bit-stream copy is defined as a duplicate except in identified areas of the bit-stream)when I/O errors exist in accessing the source media

f. Hardware data acquisition tools
   i. UltraKit (Page 312)
      1. portable kit of UltraBlock hardware write blockers to acquire a forensically sound image of virtually any hard drive or storage device
   ii. Forensic Falcon
      1. Image and verify from 4 source drives to 5 destinations
      2. Preview suspect drive contents directly on the Falcon
      3. Image to/from a network location
      4. Remote operation with a web-based browser interface
   iii. T3iu Forensic SATA Imaging Bay (Page 313)
      1. SATA write blocker
      2. A suspect drive cooler
      3. Suspect drive tray
   iv. Triage-Responder (Page 314)
      1. scan, analyze and extract evidence from a digital device.
   v. XRY Office (Page 315)
      1. software based solution
      2. hardware to recover data from mobile devices
   vi. Atola Insight Forensic (Page 316)
      1. data retrieval functionalities with utilities for accessing hard drives at the lowest level
      2. Includes built-in write blocker
   vii. US-LATT PRO (Page 317)
      1. Live acquisition and triage of Microsoft® Windows systems (XP – Windows 8)
   viii. IM Solo-4 G3 Forensic Enterprise Super Kit (Page 317)
      1. Drive data acquisition unit
      2. Extract data from suspect to evidence hard drives at SATA-3 speed
   ix. ROADMASSTER-3 X2 (Page 317)

TOOLS Methodologies, Frameworks and Processes Term

1. Portable drive data capture and analysis workstation

x. TD2u Forensic Duplicator (Page 317)

xi. Disk Imager Forensic Edition

1. Portable forensic imaging tool

xii. Disk Jockey PRO(Page 317)

1. Disk copy and write blocking tool
2. Copies the Drive Configuration Overlay (DCO) areas and Host Protected Area (HPA) of a hard disk drive
3. Windows or Macintosh systems

xiii. RAPID IMAGE 7020 X2 IT (Page 317)

1. Hard Drive Duplicators
2. Can and sanitize drives simultaneously

xiv. ZClone®Xi (Page 318)

xv. HardCopy 3P (Page 318)

xvi. Forensic Tower IV Dual Xeon (Page 318)

xvii. FREDDIE (Page 318)

xviii. PC-3000 PRO Data Extractor (Page 318)

xix. Project-A-Phone (Page 318)

xx. Mobile Field Kit (Page 319)

xxi. iRecovery Stick (Page 319)

xxii. UFED Touch (Page 319)

xxiii. UFED Pro Series (Page 319)

xxiv. FRED (Page 319)

xxv. Ditto Forensic FieldStation (Page 319)

xxvi. Forensic UltraDock (Page 319)

g. Software data acquisition tools

i. EnCase Forensic (Page 320)

ii. DriveSpy (Page 321)

iii. ProDiscover Forensics (Page 321)

iv. Data Acquisition Toolbox (Page 322)

v. RAID Recovery for Windows (Page 322)

vi. R-Tools R-Studio (Page 322)

vii. X-Ways Forensics (Page 322)

viii. F-Response Imager (Page 322)

ix. R-Drive Image Flash (Page 323)

x. Retriever Forensic Edition (Page 323)

xi. Forensic Replicator (Page 323)

xii. MacQuisition (Page 323)

xiii. Belkasoft Live RAM Capturer (Page 323)

xiv. Magnet RAM Capture (Page 323)

xv. OSFClone (Page 323)

xvi. FDAS - Fast Disk Acquisition System (Page 324)

TOOLS Methodologies, Frameworks and Processes Term

xvii. SMART for Linux (Page 324)
xviii. Paragon Hard Disk Manager 15 Suite (Page 324)
xix. Macrium Reflect Free (Page 324)
xx. DAEMON Tools Pro 7 (Page 324)
xxi. Active@ Disk Image (Page 325)

22. Data Acquisition and Duplication Part 3
    a. Tools/commands to collect information
        i. systeminfo /fo list
        ii. psinfo
        iii. Cat (l)
        iv. Uname (l)
            1. **Returns the computer name and Linux version**
        v. psuptime
        vi. net statistics
        vii. Uptime (l)
        viii. top (l)
        ix. w (l)
        x. ps (l)
        xi. ls (l)
        xii. lsof (l)
        xiii. lsof -np +L1 (l)
        xiv. chkconfig (l)
        xv. inittab (l)
        xvi. netusers
        xvii. psloggedon
        xviii. who (l)
        xix. last (l)
        xx. lastlog (l)
        xxi. passwd (l)
        xxii. shadow (l)
        xxiii. ldd (l)
        xxiv. listdlls
        xxv. ifconfig (l)
        xxvi. psservice
        xxvii. dd (l) (Page 325)
            1. **To copy one hard disk partition to another hard disk, use dd**
            2. **if=/dev/sda2 of=/dev/sdb2 bs=4096 conv=notrunc,noerror c**
        xxviii. dcfldd(l) (Page 326)
            1. **dcfldd if=/dev/sda split=2M of=usbimg hash=md5.**
            2. **This command generates segmented volumes of 2MB each**
    b. Data Acquisition Mistakes
        i. Choosing the wrong resolution for data acquisition

TOOLS Methodologies, Frameworks and Processes Term

ii. Using the wrong cables and cabling techniques
iii. Taking insufficient time for system development
iv. Making the wrong connections
v. Having poor knowledge of the instrument

c. Validating Data Acquisition:
    i. CRC-32
        1. Cyclic Redundancy Code algorithm32 (CRC-32)
        2. A hash function based on the idea of polynomial division
        3. The number 32 indicates the size of the resulting hash value or checksum, which is 32 bits
        4. The checksum identifies errors after data transmission or storage
    ii. MD5
        1. Message Digest 5
        2. algorithm used to check data integrity by creating a 128-bit message digest from data input of any length.
    iii. SHA-1
        1. Secure Hash Algorithm-160
        2. Cryptographic hash function developed by the United States National Security Agency (NSA)
        3. A US Federal Information Processing Standard (FIPS) issued by NIST
        4. It creates a 160-bit (20-byte) hash value called a message digest
        5. This hash value is a hexadecimal number, 40 digits long.
    iv. SHA-256
        1. A cryptographic hash algorithm that creates a unique and fixed-size 256-bit (32-byte) hash

5. Defeating Anti-Forensic Techniques

23. Defeating Anti-Forensic Techniques Part 1
    a. NTFS Disk explorer
    b. Anti-forensic or counter forensics
        i. A set of techniques used by attackers to break the forensic cycle and hide, obfuscate, modify, manipulate, data and activities
    c. Forensics goal is to not to stop every attack. It is to prevent the most common attacks, minimize, and mitigate the risks. 8:35 – 12:55
        i. Delay and deter as much as possible
            1. As in defense in depth
        ii. Make it as difficult as possible for the attacker to act and navigate that the attacker must leave evidence and make the attacker easier to find
    d. Goals of anti-forensics: 12:55 – 13:58 (Page 344)
        i. Interrupt and prevent information collection
        ii. Toughen the investigator's task in finding the evidence
        iii. Hide traces of crime or illegal activity

iv. Compromise the accuracy of a forensic report or testimony
v. Force the forensic tool to reveal its presence
vi. Use a forensic tool itself for attack purposes
vii. Delete evidence that an anti-forensic tool has been used

e. Anti-forensics techniques 18:38 -
i. Data/File Deletion
ii. Password Protection
1. Adding passwords to files
iii. Steganography
iv. Data Hiding in File System Structures
1. Using slack space, file system structures, or white space
v. Trail Obfuscation
1. Using proxies, onion routing, nat-ing
vi. Artifact Wiping
1. Deletion of data and trace data
vii. Overwriting Data/Metadata
viii. Encryption
ix. Encrypted Network Protocols
1. Tunneling or VPNs
2. Use of TLS (Transport layer security), L2TP/IPsec, SSTP (secure socket tunneling protocol)
x. Program Packers
1. Hiding and obfuscating files and executables
2. Trojans
xi. Rootkits
1. Allows burrowing into the OS
2. Types of rootkits (Page 432)
a. Hypervisor Level Rootkit
b. Hardware/Firmware Rootkit
c. Kernel Level Rootkit
d. Boot Loader Level Rootkit
e. Application Level Rootkit
f. Library Level Rootkits
xii. Minimizing Footprint
xiii. Exploiting Forensics Tool Bugs
xiv. Detecting Forensics Tool Activities
1. Understand how the tools work and what they leave behind to identify them

24. Defeating Anti-Forensic Techniques Part 2
a. What happens when a file is deleted in Windows 2:25 – 9:25 (Page 345)
i. Shift+del – file deleted and bypasses recycle bin
ii. The data is still on the hard drive

TOOLS Methodologies, Frameworks and Processes Term

1. The reference point has been removed.
2. The referenceable metadata has been removed.
3. The data can now be overwritten
4. If the data is not overwritten, then I can be salvages

iii. FDK disk editor to recover a file

iv. FAT file system

1. **The OS marks the file name in the Master File Table (MFT) with a special character**
    a. **replaces the first letter of a deleted file name with a hex byte**
    b. **code: E5h**
    c. (E5h is a special tag that indicates that the file has been deleted)
2. The corresponding **cluster of that file in FAT is marked as unused**, although it will continue to contain the information until it is overwritten

v. NTFS file system

1. OS marks the index field in the master file table (MFT)
    a. $MFT
    b. $MFT Mirror
2. The clusters allocated to the deleted file are marked as free in the $BitMap
    a. ($BitMap file is a record of all used and unused clusters)
3. The computer now notices those empty clusters and avails that space for storing anew file
    a. The deleted file can be recovered if the space is not allocated to any other file
4. Note: On a Windows system, performing normal Delete operation sends the files to the Recycle Bin. Whereas performing the Shift+Delete operation bypasses the Recycle Bin.

b. Windows Recycle Bin 9:25

i. Deleted files are stored

1. Older FAT file system
    a. Windows 98 and prior
    b. Drive:\RECYCLED in older FAT file system
2. NTFS file system
    a. Windows 2000, XP, NT
    b. Drive:\RECYCLER folder

ii. Recycled files

1. FAT system
    a. Dumped into a single **C:\RECYCLED** directory
2. NTFS system
    a. Prior to Windows Vista
        i. Categorized into directories named **C:\RECYCLER\S-**

b. Post Vista
i. **C:\$Recycle.Bin\S-....** based on the user's SID

iii. Limits
1. **Up to XP and before, recycle bin had a limit of 3.99GB**
2. Windows Vista and after, recycle bin had no limit

iv. Files in the bin have names changed
1. Vista and later (Page 348)
a. Files stored in bin as $Ry.ext
b. Where y is a sequential number
c. Ext is the original files extension
d. New file name: $R7.doc=(eighth file deleted, a doc file)
e. INFO file path: $I<#>.<original extension>): $I7.doc
2. XP and earlier
a. Files stored in bin as Dxy.ext
b. Where x is the drive name
c. INFO file path: E:\Winword\Letter to Rosemary.doc
d. New file name: De7.doc = (E drive, eighth file deleted, a .doc file)

c. INFO2 file (Page 348)
i. When a user deletes a file or folder, the OS stores info of the deleted file in this file. Info includes
1. Its complete path
2. including the original file name

ii. The info in this file is used to restore the deleted file to its original location

d. To repair a damaged or corrupted recycle bin
i. Delete the hidden INFO file from the Recycled folder and restart Windows to re-create the INFO file; this will enable you to access the deleted files in the Recycle Bin.

e. Damaged files in the Recycle Bin folder (C:\RECYCLER, C:\RECYCLER\S- or C:\$Recycle.Bin\S -) do not appear in the Recycle Bin
i. Create a copy of the Desktop.ini file in the Recycle Bin folder and save it in another folder, and then delete the entire contents of the Recycle Bin folder
ii. Delete all files in the Recycle Bin then Restore the Desktop.ini file to the Recycled folder
iii. If there is no Desktop.ini file or if it is damaged, then re-create it by adding the information to blank Desktop.ini file: [.ShellClassInfo]CLSID={645FF040-5081-101B-9F08-00AA002F954E}

f. In Windows 10, follow the steps below to repair a damaged or corrupted recycle bin folder:
i. Open a command prompt with administrative privileges
ii. Run rd /s /q C:\$Recycle.bin command
iii. Restart the computer

iv. Perform the same operation to repair the Recycle Bin of every partition on the hard disk separately, by replacing C with the respective drive letter

g. Recover My Files data recover tool (Page 351 not in videos)
   i. Recovers deleted files emptied from the Windows Recycle Bin
   ii. Recovers files lost due to
      1. **format or corruption of a hard drive**
      2. **virus or Trojan infection**
      3. **unexpected system shutdown**
      4. **software failure**
      5. Recovers files even
         a. if emptied from the Recycle Bin data
         b. After accidental format, even after Windows is reinstalled
         c. Performs disk recovery after a hard disk crash
         d. Recovers files after a partitioning error
         e. Recovers data from RAW hard drives
         f. Recovers documents, photos, videos, music, and email
         g. Recovers from a hard drive, camera card, USB, Zip, floppy disk, or other media

h. EaseUS Data Recovery Wizard data recovery tool (Page 352 not in videos)
   i. **Performs format recovery**
   ii. Unformat and recover deleted files
      1. **Emptied from the Recycle Bin**
      2. **Data lost due**
         a. partition loss or damage
         b. Software crash
         c. Virus infection
         d. unexpected shutdown
         e. Any other unknown reasons under Windows 10, 8, 7, 2000/XP/Vista/2003/2008 R2 SP1/Windows 7 SP1.

i. DiskDigger data recovery tool (Page 353 not in videos)
   i. Undeletes and recovers lost files from
      1. **hard drives**
      2. **memory cards**
      3. **USB flash drives.**
   ii. Windows 10, 8, 7, Vista, and XP OSs
   iii. Shows recoverable files as a list or as thumbnail previews
   iv. Previews of ZIP files will show a list of files contained in the archive.
   v. https://diskdigger.org

j. Handy Recovery data recovery tool (Page 353 not in videos)
   i. Restores files accidentally deleted from
      1. hard disks
      2. memory cards

ii. Can recover files damaged by:
    1. virus attacks
    2. power failures
    3. software faults
    4. files from deleted and formatted partitions.
iii. Can restore files if a program does not use the Recycle Bin when deleting files
iv. It can also recover files moved from the Recycle Bin after it has been emptied.

k. Quick Recovery data recovery tool (Page 354 not in videos)
    i. Recovers files that have been
        1. Lost
        2. Deleted
        3. Corrupted
        4. Deteriorated
    ii. The application searches, scans, and recovers files that are encrypted and password protected and restores them.
    iii. Repairs and recovers Disk bad sectors

l. Stellar Phoenix Windows Data Recovery data recovery tool (Page 354 not in videos)
    i. Recovers
        1. Lost due to
            a. hard drive corruption
            b. formatting
            c. virus attack.
        2. Deleted
        3. Inaccessible data
    ii. Windows OS HDDs and other storage media.

m. Total Recall data recovery tool (Page 354 not in videos)
    i. Recovers lost data from
        1. Hard drives
        2. RAID
        3. Photos
        4. deleted files
        5. iPods
        6. removable disks connected via FireWire or USB.
    ii. Advanced Disk Recovery data recovery tool (Page 354 not in videos)
        1. Scans the entire system for deleted files and folders and recovers them
        2. Scans
            a. hard drives
            b. partitions
            c. external devices
            d. CDs and DVDs
        3. Provides two types of scans:

a. Quick Scan that uses MFT
b. Deep Scan that uses file signatures

iii. Windows Data Recovery Software data recovery tool (Page 354 not in videos)
1. Recover accidentally deleted files and files emptied from the Recycle Bin and from Windows Explorer with Shift + Delete.
2. Recover data from
a. Reformatted partition (to any file system)
b. a corrupted, deleted, or missing partition.
3. Two scanning methods: Quick Scan and Thorough Scan

iv. Other Windows data recovery tools not in the videos
1. R-Studio data recovery tool (Page 355 not in videos)
2. Data Rescue PC data recovery tool (Page 355 not in videos)
3. Smart Undeleter
4. DDR Professional Recovery Software
5. Data Recovery Pro
6. GetDataBack (Page 356)
7. Undelete Plus (Page 356)
8. File Scavenger (Page 356)
9. VirtualLab (Page 357)
10. Active@ UNDELETE (Page 357)
11. WinUndelete (Page 357)
12. R-Undelete (Page 357)
13. Recover4all Professional (Page 357)
14. Recuva (Page 357)
15. Active@ File Recovery (Page 358)
16. Pandora Recovery (Page 358)
17. Ontrack EasyRecovery (Page 358)
18. Seagate File Recovery Software (Page 358)
19. Wise Data Recovery (Page 358)
20. Glary Undelete (Page 359)
21. Disk Drill (Page 359)
22. PhotoRec (Page 359)

n. MAC OS X file recovery 18:40 -19:50
i. Files move to trash folder if you delete them.
ii. If Shift+delete is used, you bypass trash, but files can still be recovered using local or forensic tools such as TIMEMACHINE or REMO Recover or MacKeeper

o. Other MAC data recovery tools no in the videos (Page 361)
i. AppleXsoft File Recovery for Mac (Page 361)
ii. Disk Doctors Mac Data Recovery (Page 361)
iii. R-Studio for Mac (Page 361)
iv. Data Rescue 4 (Page 361)
v. Stellar Phoenix Mac Data Recovery (Page 361)

TOOLS Methodologies, Frameworks and Processes Term

vi. FileSalvage (Page 362)
    1. **Recovers files from a crashed or virus corrupted hard drive**
vii. 321Soft Data Recovery (Page 362)
viii. Disk Drill for Mac (Page 362)
ix. Mac Data Recovery Guru (Page 362)
x. Cisdem DataRecovery 3 (Page 362)
xi. File Recovery for Linux (Page 362)

p. Linux file recovery 19:50 – 21:20
    i. Files deleted using /bin/rm remain on the disk, and are recoverable.
    ii. If an executable is deleted, its contents can be retrieved from /proc memory image; the command "cp /proc/$PID/exe/tmp/file"
    iii. This creates a copy of a file in /tmp

q. Knoppix
    i. A bootable Linux distro
    ii. Can be used to recover data from Windows environments

r. Disk Partition 21:53 – 29:30
    i. Partition is just the logical reference of how the hard drive is carved up
    ii. What happens when a partition is deleted
        1. Reference are removed from the file allocation table, MBR, all of the protected sectors
        2. When a hard drive partition is deleted, what really happens is that the parameters that specify how the partition is setup are deleted, but the data stays intact
        3. To recover, use a tool can create and layout the entire drive
    iii. Partition Recovery in Windows
        1. Recovery console through the install media
        2. Remove HD from source machine, mount it as a slave in another machine
        3. Use third-party recovery software (Pages 364-369)
            a. Active@ Partition Recovery
            b. 7-Data Partition Recovery
            c. Acronis Disk Director Suite
            d. RS Partition Recovery
            e. Partition Find & Mount
            f. Advance Data Recovery Software Tools for NTFS
            g. NTFS Data Recovery Toolkit
            h. GetDataBack
            i. Partition Recovery (Disk Internals)
            j. TestDisk for Windows
            k. Stellar Phoenix Windows Data Recovery
            l. EaseUS Partition Master
            m. Hetman Partition Recovery

n. MiniTool Power Data Recovery Free
o. ZAR Windows Data Recovery (Page 369)

iv. Partition Recovery tools in MAC
1. Mac Data Recovery Software
2. Remo Recover (Mac) – Pro (Page 368)
3. TestDisk for Mac (Page 368)
4. Starus Partition Recovery (Page 369)
5. Disk Drill (Page 369)
6. Stellar Phoenix Mac Data Recovery (Page 369)

v. Partition Recovery tools in Linux
1. Quick Recovery for Linux (Page366)
2. Stellar Phoenix Linux Data Recovery Software (Page 367)

25. Defeating Anti-Forensic Techniques Part 3
a. Password types 2:30 - 4:40
i. Cleartext
ii. Obfuscated
1. Randomized or pseudo randomized to be presented in an encrypted form
iii. Hashed
1. Not the actual password, but a cryptographic representation of the password
b. Rainbow table cracking 4:40 – 6:05
i. A word list is created and then hashed to present a "pre-compiled" listing for use in the software
ii. The hashed word list is used to compare against "target" passwords that we want to decrypt
iii. If we get a match, we know the hash value and the corresponding clear-text equivalent, i.e., the password !!
iv. Possible tools to do this
c. List of rainbow tables 6:05 – 11:22
i. http://project-rainbowcrack.com/table.htm
d. Rainbow table creation tools (Page 376)
i. Rtgen
ii. Winrtgen
e. Password cracking software (Tools) is a program that can decrypt passwords 11:25 – 12:30
i. John the ripper
ii. Lophcrack
iii. PWDump
iv. Ophcrack
v. RainbowCrack (Page 409)

TOOLS Methodologies, Frameworks and Processes Term

1. pre-computes all possible plaintext–ciphertext pairs in advance and stores them in the rainbow table

vi. Wfuzz (Page 412)
1. http://www.edge-security.com/
2. Designed to brute force Web applications.

vii. LSASecretsView (Page 413)
1. displays a list of all LSA secrets stored in the Registry on a computer
2. may contain VPN/RAS passwords, Autologon passwords, and other system keys/passwords.
3. just requires copy of the executable file in any of the folder and run it

viii. Password Cracker (Page 413)
1. restore forgotten passwords, including Internet Explorer.

ix. Kon-Boot (Page 413)

x. THC-Hydra (Page 414)
1. dictionary or brute-force attacks
2. Linux, *BSD, Solaris, Mac OS X, and any Unix and Windows

f. Password Cracking Techniques 12:30 – 13:35 (Page373)
i. Dictionary Attacks
1. The program uses every word present in the dictionary to find the password

ii. Brute Force Attacks (Page 374)
1. Testing all possible keys is an attempt to recover the plaintext

iii. Hybrid Attacks
1. 2 or more techniques combined

iv. Syllable Attacks = Brute force + dictionary

v. Rule-Based Attacks = use of information about structure or make-up of password to narrow down search parameters

g. Password Attack Categories 13:35 – 17:00
i. Passive on-line
1. Wire sniffing
2. Man-in-the-Middle (MitM)
a. Masquerading
3. Replay
a. Using the victim's session ID

ii. Active on-line
1. Guessing
2. Malware
3. Hash Injection

iii. Offline
1. Pre-computed/Rainbow Tables - http://projectrainbowcrack.com/table.htm
2. Distributed Network (grids !!)

TOOLS Methodologies, Frameworks and Processes Term

iv. Non-electronic
    1. Shoulder surfing
    2. Dumpster diving

h. System Hacking / Password recovery @ the O/S level 20:15 – 21:00
    i. Bypassing BIOS passwords
        1. Using a manufacturers' backdoor password to access the BIOS password
        2. Using password-cracking software
            a. CmosPwd
                i. works and compiles under Dos - Win9x, Windows NT/W2K/XP/2003, Linux, FreeBSD, and NetBSD
            b. DaveGrohl
                i. Brute- forcing OS X user passwords
                ii. used since OS X Lion
        3. Resetting the CMOS using the jumpers or solder beads
        4. Removing the CMOS battery for at least 10 minutes
        5. Using a professional service
        6. Overloading the keyboard buffer

i. Tools for resetting Windows Admin Passwords
    i. Active@ Password Changer (Page 383)
        1. designed for resetting local administrator and user passwords on Windows XP/Vista/2008/2003/2000, and Windows 7 systems
    ii. Windows Password Recovery Bootdisk (Page 385)
        1. Windows Key creates a password reset CD or USB Flash Drive
        2. works during the boot process
        3. instantly resets Administrator or other account passwords and Windows security settings that prevent you from logging in.
    iii. Windows Password Recovery Lastic (Page 386)
        1. For Windows OS
        2. requires rebooting into another OS
        3. Run the tool on another computer to create a bootable USB stick or CD/DVD disk
        4. Boot from it on the computer and the program lists all user accounts it finds
        5. Offers a choice to either remove a password of a Windows user account or to save its hash
    iv. PWdump7 (Page 410)
        1. extracts LM and NTLM password hashes of local user accounts from the SAM database.
    v. Fgdump (Page 411)
        1. dumps passwords on Windows NT/2000/XP/2003/Vista machines.
        2. has all the capabilities of PWdump
        3. Can also execute a remote executable

TOOLS Methodologies, Frameworks and Processes Term

4. Can also dump the protected storage on a remote or local host
5. Can also grab cached credentials

vi. Offline NT Password & Registry Editor (Page 412)
1. Resets the password of any user that has a valid local account on the Windows system

vii. Password Unlocker Bundle (Page 412)
1. resets or recovers passwords for different file types
2. Windows OS, MS SQL Severs, RAR/PDF/Word/Excel/PPT files.

viii. Windows Password Unlocker (Page 413)

ix. LCP (Page 413)
1. Recovers passwords from Windows NT/2000/XP/2003.

x. Windows Password Recovery Tool (Page 413)

xi. iSunshare Windows Password Genius (Page 414)
1. Windows 10/8/7/Vista/XP/NT/2000
2. Windows server 2000/2003/2008/2011/2012.

xii. THC-Hydra (Page 414)
1. dictionary or brute-force attacks
2. Linux, *BSD, Solaris, Mac OS X, and any Unix and Windows

xiii. Windows Password Breaker Enterprise (Page 415)
1. creates a bootable password reset CD/DVD or USB flash drive to reset the lost Windows password
2. works for Windows 7/Vista/XP/2000 and server 2003(R2)/2008(R2).

j. Application Password Cracking Tools

i. Passware Kit Forensic (Page 388)
1. Recovers passwords for 200+ file types and decrypts hard disks providing an all-in-one user interface

ii. SmartKey Password Recovery Bundle Standard (Page 389)
1. Windows
2. PDF
3. ZIP
4. RAR
5. Office Word/Excel/PowerPoint documents
6. instant messengers
7. email clients
8. web browsers
9. FTP clients and more

iii. Microsoft Office password recovery tools
1. Advanced Office Password Recovery (Page 390)
    a. unlocks documents created with all versions of Microsoft Office.
2. Office Password Recovery
3. Office Multi-document Password Cracker (Page 391)
4. Stellar Phoenix Office Password Recovery (Page 401)

TOOLS Methodologies, Frameworks and Processes Term

5. Online Password Recovery
6. Office Password Genius
7. Office Password Recovery Lastic
8. SmartKey Office Password Recovery (Page 403)
9. Proactive System Password Recovery (Page 412)
10. Password Unlocker Bundle (Page 412)
    a. Resets or recovers passwords for different file types
    b. Windows OS, MS SQL Severs, RAR/PDF/Word/Excel/PPT files

iv. Word Password recovery tools
1. Word Password Recovery Tools
    a. Crack password-protected documents created in MS Word 97/2000/XP/2003/2007/2010/2013.
2. Accent WORD Password Recovery
    a. recovers lost Microsoft Word passwords.

v. Power Point password recovery tools
1. SmartKey PowerPoint Password Recovery (Page 394)
2. PowerPoint Password

vi. Excel Password Recovery tools
1. PDS Excel Password Recovery (Page 396)
    a. crack password-protected documents created in MS Excel 97/2000/XP/2003/2007/2010
2. Accent EXCEL Password Recovery (Page 397)

vii. PDF Password recovery tools
1. Advanced PDF Password Recovery
2. PDF Password Cracker
3. PDF Password Recovery
4. PDF Password Genius
5. SmartKeyPDF Password Recovery
6. Tenorshare PDF Password Recovery
7. Guaranteed PDF Decrypter (Page 404)
8. Password Unlocker Bundle (Page 412)
    a. resets or recovers passwords for different file types
    b. Windows OS, MS SQL Severs, RAR/PDF/Word/Excel/PPT files.

viii. ZIP/RAR password recovery tools
1. Advanced Archive Password Recovery (Page 401)
2. Accent ZIP Password Recover
3. ZIP Password Genius
4. SmartKey ZIP Password Recovery (Page 405)
5. KRyLack ZIP Password Recovery (Page 405)
6. Stellar Phoenix Zip Password Recovery (Page 405)
7. Accent RAR Password Recovery (Page 405)
8. cRARk 5.1 (Page 406)

TOOLS Methodologies, Frameworks and Processes Term

9. SmartKey RAR Password Recovery (Page 406)
10. KRyLack RAR Password Recovery (Page 406)
11. Proactive System Password Recovery (Page 412)
12. Password Unlocker Bundle (Page 412)
    a. resets or recovers passwords for different file types
    b. Windows OS, MS SQL Severs, RAR/PDF/Word/Excel/PPT files

k. Default Vendor password sites: 18:30 – 20:10
   i. http://www.defaultpassword.com
   ii. http://www.cirt.net/passwords
   iii. http://default-password.info

l. How Hashed Passwords Are Stored in the Windows SAM file: 23:20 – 24:20
   i. The SAM file is stored at %SystemRoot%/system32/config/SAM in Windows systems
   ii. Windows mounts it in the registry under the HKLM/SAM registry hive.
   iii. It stores LM or NTLM hashed passwords.
   iv. HKLM
      1. H Key Local Machine
   v. LM
      1. LanMan
      2. New versions of Windows still support LM hashes for backward compatibility; however, Vista and later Windows versions disable the LM hash by default.
      3. The LM hash is blank in newer Windows versions. The SAM file stores a "dummy" value in its database, which bears no relationship to the user's actual password and is the same for all user accounts.
      4. It is not possible to calculate LM hashes for passwords exceeding 14 characters in length. Thus, the LM hash value is set to a "dummy" value when a user or administrator sets a password of more than 14 characters.
   vi. NTLM
      1. NT LanMan
      2. The use of NTLM has replaced the LM hash, which is susceptible to cracking.

m. Steganography: 24:20 – 25:20
   i. Steganography is a technique of hiding a secret message within an ordinary message and extracting it at the destination to maintain confidentiality of data

n. Steganography Techniques 25:48 – 34:10
   i. Substitution - substitutes redundant part of the cover object with a secret message
   ii. Transform - embed secret message in a transform space of the signal (e.g. in the frequency domain)
      1. Tools

a. http://www.Vulnhub.com has the frequency lab where you can capture the flag in the mp3
b. Mpstego
c. Whitenoise

iii. Statistical - embed messages by altering statistical properties of the cover objects and use hypothesis methods for extraction
iv. Distortion - Store information by signal distortion and in the extraction step measure the deviation from the original cover
v. Cover Generation - Encode information that ensures creation of cover for secret communication
vi. Technical - use of physical or chemical means to hide information
vii. Linguistic - use of natural language to hide message in non-obvious ways
viii. Image - replaces redundant bits of image data with message
    1. Types:
        a. Least Significant Bit Insertion
            i. The right most bit of a pixel is called the Least Significant Bit (LSB).
            ii. The binary data of the hidden message is broken up and inserted into the LSB of each pixel in the image file in a deterministic sequence.
            iii. Modifying the LSB does not result in a noticeable difference
        b. Masking & Filtering
            i. Mostly used on 24 bit and grayscale images.
            ii. The masking technique hides data using a method similar to watermarks on actual paper, and it can be done by modifying the luminance of parts of the image.
            iii. Masking techniques hide information in such a way that the hidden message is inside the visible part of the image.
        c. Algorithms & Transformation - The data is embedded in the cover image by changing the coefficients of a transform of an image
            i. Types of techniques:
                1. Fast fourier
                2. Discrete cosine
                3. Wavelet
ix. Audio - refers to hiding secret information in audio files. Information can be hidden in an audio file by using LSB or by using frequencies that are inaudible to the human ear (>20,000 Hz)
    1. Types of techniques:

a. Echo data hiding - the secret message is embedded into a cover audio signal as an echo. The parameters of the echo, amplitude, decay rate and offset from the original signal, are varied to represent an encoded secret binary message
b. Spread Spectrum – encodes data as a binary sequence that sounds like noise but can be recognized by a receiver with the correct key
    i. Two approaches are used in this technique:
        1. Direct Sequence Spread Spectrum (DSSS) – secret message is spread out by chip rate (constant) and then modulated with a pseudo-random signal that is then interleaved with the cover signal
        2. Frequency Hopping Spread Spectrum (FHSS) - audio file's frequency spectrum is altered so that it hops rapidly between frequencies
c. LSB Coding - replaces the LSB of information in each sampling point with a coded binary string
d. Tone Insertion - depends on the inaudibility of low power tones in the presence of significantly higher spectral components
e. Phase Decoding – It encodes the secret message bits as phase shifts in the phase spectrum of a digital signal, achieving a soft encoding in terms of signal-to-noise ratio

x. Video - hiding secret information or any kind of files with any extension into a carrier video file. Discrete Cosine Transform (DCT) manipulation is used to add secret data

o. Issues with Steganography 34:10
    i. Levels of visibility - embedding cannot distort cover image to point that it is noticeable
        1. There needs to be enough coverage left behind to conceal the hidden data
    ii. File format dependence - image and sound files are either lossless or lossy.
        1. Lossy compression reduces file size by permanently eliminating certain information, especially redundant information (even though the user may not notice it). JPEG is an example of a format using lossy compression. Does not maintain data integrity. Vector Quantization is used.
        2. Lossless compression retains raster values during compression and file size is also reduced. For example, LZ77 is a lossless compression file type. Maintains data integrity. Huffman Coding algorithm & Lempel-Ziv Coding algorithm are used.

iii. The conversion of lossless information to compressed lossy information destroys the hidden information in the cover.

p. Steganography Detection Tools
   i. Gargoyle InvestigatorTM Forensic Pro (Page 421)
   ii. Xstegsecret (Page 423)
      1. java-based multiplatform steganalysis tool
   iii. StegSecret (Page 423)
      1. Open source
      2. java-based multiplatform
   iv. StegAlyzerAS (Page 424)
   v. StegAlyzerRTS (Page 424)
   vi. StegExpose (Page 424)
   vii. StegAlyzerSS (Page 424)
   viii. Steganography Studio (Page 424 and 439)
      1. Java tool for the detection of hidden information
   ix. Virtual Steganographic Laboratory (VSL) (Page 424)
   x. Stegdetect (Page 424)
   xi. ImgStegano (Page 425)

26. Defeating Anti-Forensic Techniques Part 4
   a. Image terminology 1:00 – 4:35
      i. Pixel - a single point in an image
      ii. Bit Depth - number of colors available for each pixel
      iii. Resolution - sharpness and clarity of an image
         1. HD, 4k, etc.
      iv. File Formats - particular ways to encode information
         1. PNG, JPG, etc.
      v. Image File Size - measured in bytes
      vi. Compression - method used to make an image smaller
         1. Lossy vs Lossless
      vii. Vector images - use geometrical primitives such as points, lines, curves, and polygons, which are all based upon mathematical equations to represent images in the computer
      viii. Raster images - a data file or structure representing a generally rectangular grid of pixels, or points of color, on a computer monitor.
         1. A colored raster image has pixels with eight bits of information for each of the red, green, and blue components.
         2. Quality of a raster image is determined by the total number of pixels and the amount of information in each pixel
   b. Steganalysis 4:44
      i. The art of discovering and rendering covert messages using steganography
   c. Attacks on Steganography 5:20 – 9:14
      i. Attacker is the investigator or stego-analyst

TOOLS Methodologies, Frameworks and Processes Term

ii. Steganographic attacks work according to the type of information available to perform steganalysis. This information may include the hidden message, carrier (cover) medium, stego-object, steganography tools, or algorithms used to hide information.
iii. Stego-only attack
    1. The investigator has knowledge of
        a. the stego-medium (medium with hidden object)
    2. Investigator needs to try all possible steganography algorithms and related attacks
    3. Goal: recover the hidden information.
iv. Known-stego attack
    1. The investigator has knowledge of
        a. The steganographic algorithm
        b. The original cover medium
        c. The stego-object (medium with hidden object)
    2. Goal: Extract the hidden information with the information at hand.
v. Known-message attack
    1. The investigator has knowledge of
        a. The message
        b. The stego-medium
    2. Goal: Detect the technique used to hide the message.
vi. Known-cover attack
    1. The investigator has knowledge of
        a. the stego-object (medium with hidden object)
        b. the original cover-medium
    2. Goal: This will enable a comparison between both the mediums in order to detect the changes in the format of the medium to find the hidden message.
vii. Chosen-message attack
    1. The investigator has knowledge of
        a. The message
    2. Investigator uses known message to generate a stego-object by using some steganography tool in order to find the steganography algorithm used to hide the information.
    3. Goal: to determine patterns in the stego-object that may point to the use of specific steganography tools or algorithms.
viii. Chosen-stego attack
    1. The investigator has knowledge of
        a. The stego-object
        b. steganographic tool or algorithm used to hide the message.
    2. Goal: find the hidden information

d. Standard Image File Formats 9:14 – 15:22

TOOLS Methodologies, Frameworks and Processes Term

i. Joint Photographic Experts Group (JPEG) - .jpg
ii. JPEG 2000 - .jp2
iii. Graphics Interchange Format (GIF) - .gif
iv. Tagged Image File Format (TIFF) - .tif
v. Windows Bitmap - .bmp
vi. Portable Network Graphics (PNG) - .png

e. Nonstandard Image File Formats 9:29 – 9:50
i. Targa - .tga
ii. Raster Transfer Language - .rtl
iii. Photoshop - .psd
iv. Illustrator - .ai
v. Freehand - .h9
vi. Scalable Vector Graphics - .svg
vii. Paintbrush - .pcx

f. Rootkit detection techniques: 10:18
i. signature based (Page 433)
1. **rootkit fingerprint**
2. The sequences of bytes from a file are **compared with another sequence of bytes belonging to a malicious program**
3. mostly scans the system files
4. It can easily detect invisible rootkits by scanning the kernel memory
5. The success of signature-based detection is less due to the rootkit's tendency to hide files by interrupting the execution path of the detection software

ii. heuristic / behavior based (Page 433)
1. identifies deviations in normal OS patterns or behaviors
2. Capable of identifying new, previously unidentified rootkits
3. Recognizes deviants in "normal" system patterns or behaviors.
4. Execution path hooking is one such deviant that causes heuristic- based detectors to identify rootkits.
5. AI
6. Start that nothing is acceptable and learn was is acceptable

iii. integrity based (Page 433)
1. substitute to both signature- and heuristic-based detection
2. Initially, the attacker runs tools such as Tripwire, AIDE, etc. on a clean system
3. These tools create a baseline of clean system files and store them in a database
4. Compares current file system, boot records, or memory snapshot with the trusted baseline
5. Notifies on evidence or presence of malicious activity based on the dissimilarities between the current and baseline snapshots

TOOLS Methodologies, Frameworks and Processes Term

iv. Runtime execution path profiling (Page 433)
    1. Compares runtime execution path profiling of all system processes and executable files
    2. The rootkit adds new code to a routine's execution path to destabilize it
    3. The method hooks instructions executed before and after a certain routine, as it can be significantly different
    4. Looks at runtime execution and what path the file is being executed from
    5. Looks at the calls that are made
    6. Takes time because normal actions must be learned
v. cross-view based (Page 433)
    1. Function by assuming that the attackers have disrupted the OS in some way.
    2. Detects for tainted data returned by the OS APIs caused by the API hooking (APIs being used) or manipulation of kernel data structure using the same information, free from DKOM or hook manipulation, output from low-level mechanisms
vi. Process for manual detection of rootkits (Page 434)
    1. Examine the file system and registry of the system
    2. Run regedit.exe from inside the potentially infected OS.
    3. Export HKEY_LOCAL_MACHINE\SOFTWARE and HKEY_LOCAL_MACHINE\SYSTEM hives in text file format.
    4. Boot into a clean CD (such as WinPE).
    5. Run regedit.exe.
    6. Create a new key such as HKEY_LOCAL_MACHINE\Temp
    7. Load the Registry hives named Software and System from the suspect OS. The default location will be c:\windows\system32\config\software and c:\windows \s ys tem32\config \s ys tem.
    8. Export these Registry hives in text file format. (The Registry hives are stored in binary format and Steps 6 and 7 convert the files to text.)
    9. Launch WinDiff from the CD, and compare the two sets of results to detect file-hiding malware (i.e., invisible inside, but visible from outside).

g. Anti-Forensics Techniques that Minimize Footprint (Page 434)
    i. Userland Execve Technique
        1. lets programs on the victim computer load and run without using the Unix execve() kernel call, thereby letting the attacker overcome kernel-based security systems that might deny access to execve().
    ii. Syscall proxying
        1. Rather than uploading the entire exploit program, the attacker can upload a system call proxy to accept the remote procedure calls from

the attacker's machine. The victim's machine executes the requested system call and sends the result back to the attacker.

iii. Using Bootable Live CD's
iv. Using Bootable USB devices
v. Using Virtual Machines

h. Anti-Forensics Countermeasures 16:43 – End (Page 436)
   i. Train and educate the forensic investigators about anti-forensics
   ii. Validate the results of examination using multiple tools
   iii. Impose strict laws against illegal use of anti-forensics tools
   iv. Understand the anti-forensic techniques and their weaknesses
   v. Use latest and updated CFTs, and testing them for vulnerabilities
   vi. Save data where the attacker can't get at it, such as log hosts, CD-ROMs, etc.
   vii. Use intelligent decompression libraries to defend against compression bombs
   viii. Replace weak file heuristics with stronger ones

i. Anti-Forensics Challenges (Page 437)
   i. Decrypting a strong encryption
   ii. Obtaining obscured information
   iii. Steganography in Social Networks
   iv. Encrypting cryptographic choices for MAC and Windows

j. Anti-Forensics Tools
   i. Privacy Eraser (Page 438)
      1. Used to protect the privacy of the user by deleting the browsing history and other computer activities.
      2. Erases all digital footprints:
         a. web browser cache
         b. cookies
         c. browsing history
         d. address bar history
         e. typed URLs
         f. autocomplete form history
         g. saved passwords
         h. index.dat files
         i. Windows' run history
         j. search history
         k. open/save history
         l. recent documents
         m. temporary files
         n. recycle bin
         o. clipboard
         p. DNS cache
         q. log files
         r. error reporting, etc.

3. Windows 10/8.x/7/Vista/2012/2008 (32/64-bit), and also supports Windows FAT16/FAT32/exFAT/NTFS file systems.

ii. Azazel Rootkit (Page 438)
1. Userland rootkit written in C based off of the original LD_PRELOAD technique from Jynx rootkit

iii. QuickCrypto (Page 438)
1. Windows-based privacy and encryption software
2. Will hide and encrypt files, emails, and passwords

iv. CyptaPix (Page 439)
1. image file management and encryption program for Windows
2. organizes prints and secures digital photos and downloaded image files
3. secures proprietary images from unauthorized access with 256-bit AES encryption or hides sensitive text, data, or other images into an image with the secure steganography feature

v. GiliSoft File Lock Pro (Page 439)
1. locks folders on an internal hard drive, flash drive, external USB drive, thumb drive, memory card, pendrive, and network drive
2. It restricts access to files, folders, and drivers
3. encrypts files and folders
4. hides files and folders and drives to make them invisible
5. makes files, folders, and drives read only
6. or password protects files, folders, and drives

vi. DBAN (Page 440)
1. Automatically deletes the contents of any hard disk that it can detect. This method prevents identity theft before recycling a computer

vii. Ontrack Eraser Degausser (Page 441)
1. Deletes data securely with a certificate of erasure for each tape confirming the validity of the process

viii. BatchPurifier (Page 441)
1. Removes hidden data and metadata from multiple files.
2. Removes more than 60 types of hidden data from 25 file types

ix. Steganos Privacy Suite 17 (Page 441)
1. Stops tracking anonymous browser and blocks ads
2. Accesses your passwords with or without using a cloud
3. Erases data tracks and stops the acquisitiveness of the computer

x. Blancco Flash (Page 441)
1. Permanently erase flash memory from USB drives, SD cards, micro drives, CompactFlash cards, and other flash memory storage devices

xi. Blancco 5 (Page 442)
1. Erase data from drives, including complex SSDs
2. acknowledged by DIPCOG

xii. Secure IT (Page 442)

TOOLS Methodologies, Frameworks and Processes Term

1. Protects files individually through file encryption.
2. allows the user to send encrypted emails.

xiii. ParetoLogic Privacy Controls (Page 442)
1. Allows the users to delete all the data related to internet activity.
2. The tool erases all privacy files pertaining to Instant Messaging and Voice Over Internet Protocol
3. Finds and deletes unwanted history items from third-party applications
4. Removes all traces of your desktop search history from applications

xiv. Exiv2 (Page 443)
1. C++ library and a command line utility to manage image metadata
2. Provides read and write access to the EXIF, IPTC, and XMP metadata of digital images in various formats
3. Sets and deletes methods for EXIF thumbnails
4. Extracts previews from RAW images and thumbnails from the EXIF metadata
5. Inserts and deletes the thumbnail image embedded in the EXIF metadata
6. Prints, sets, and deletes the JPEG comment of JPEG images
7. Fixes the EXIF ISO settings of picture taken with Canon and Nikon cameras

k. Steganography Tools

i. wbStego (Page 439)
1. Used to hide sensitive data in a carrier file

ii. Data Stash (Page 439)
1. Hides files within files (Steganography)
2. Receptacle file remains fully functional
3. Provides password protection using Blowfish encryption

iii. OmniHide PRO (Page 439)
1. Hides files within common image/music/video/document formats
2. The output file would work just as the original source file would

iv. Masker (Page 440)
1. Encrypts files so that a password will be needed to open the files
2. The carrier file will remain fully functional
3. Hidden files can be previewed and modified in hidden mode

v. DeepSound (Page 440)
1. Audio converter that hides secret data into audio files
2. DeepSound supports encrypting secret files.

vi. Universal Shield (Page 440)
1. Hides files, folders, and drives

vii. Invisible Secrets 4 (Page 443)
1. Encrypts data and files.
2. Hides files in picture or sound files or web pages

TOOLS Methodologies, Frameworks and Processes Term

3. It allows file encryption to hide files from Windows Explorer and transfers them by email or via Internet.

27. Defeating Anti-Forensic Techniques Demo
    a. Tools
        i. Password Cracking
            1. John the Ripper
            2. Kane and Abel
            3. Lophcrack
            4. Offcrack
            5. Passware Password Recovery Kit Forensic
            6. APDFRP
        ii. Steganography
            1. StegSpy
                a. http://www.spy-hunter.com
                b. Extracts hidden data
            2. OpenStego
                a. Create stego images
                b. Extracts hidden data
            3. Image Steganography
                a. Extracts hidden data

6. Operating System Forensics

28. Operating System Forensics Part 1
    a. Windows O/S Forensics Methodology
        i. **Volatile Information**
            1. Dynamic data
            2. Memory
                a. Active ram
                b. Perform a memory dump
            3. Register data
            4. Caches
                a. Arp cache
                    i. Windows comman
                        1. Arp
                            a. Arp –a shows IP mapped to MAC
                b. NetBIOS
                c. Nbtstat cache
                d. Netstat cache
                    i. Shows current network statistics
                        1. Ports being used
                        2. Info about inbound and outbound connections
                        3. Protocols being used

TOOLS Methodologies, Frameworks and Processes Term

4. State of each connection
5. IP address being connected to

e. Ipconfig
f. Display DNS
g. Name resolver cache
h. Logged on users
i. Network information

5. Linux - IFconfig

ii. Collecting Non-Volatile Information
1. Machine name
2. Registry keys
3. Winver command
4. Baseline info
5. Product licensee
6. Host name
7. MAC address
8. File structure
9. HDD size
10. Information not affected by power cycling

iii. Windows Memory Analysis
1. OSForensics tool
a. Windows
b. Can be used to:
i. Open a case
ii. Analyze memory
2. Edge web browser stores it data in the ESC format

iv. Windows Registry Analysis
1. Use Regedit or Regedit32

v. Cache, Cookie & History Analysis

vi. Windows File Analysis

vii. Metadata Investigation

viii. Event Logs Analysis 18:00
1. Event log explorer tool
a. Can mount all the logs from the local machine

b. Volatile Information Collection (Page 453)
i. System Time / Date
1. GetSystemTime
2. Windows command: time /t
3. Windows comman: date /t
4. Net statistics server

ii. Logged-On Users
1. PSloggedon (Page 456)

TOOLS Methodologies, Frameworks and Processes Term

a. applet displays both the locally and remotely logged on users

2. LogonSessions –p (Page 457)
   a. lists the currently active logged-on sessions
   b. can provide info of processes running in each session
3. net session (Page 457)
   a. Command is used for managing server computer connections
   b. Can also show if users have any open files and how long each user's session has been in the idle mode

iii. Open Files

1. net file (Page 459)
   a. Shows the names if all open shared files on a server
   b. Shows number of file locks on each file
2. Psfile (Page 459)
   a. Can retrieve the list of remotely opened files
   b. Can close the opened files either by name or by a file identifier
3. Openfiles (Page 460)
   a. displays open files
   b. displays or disconnects files opened by network users

iv. Network Information

1. nbtstat –c (Page 462)
   a. Displays info from the NetBIOS name table cache
   b. Other switches
      i. –n
      ii. –r
      iii. -S
2. netstat -a | -r (Page 464) (Page 910)
   a. collects info about network connections in Windows
   b. –r shows routing table and persistent routes
   c. –a shows all active connections and the TCP and UPD listening ports
   d. Other switches
      i. –e shows Ethernet statistics
      ii. –n shows active TCP connections
      iii. –o shows active TCP connections with process ID (PID) for each
      iv. -p Shows connections for the protocol specified
      v. –s shows stats by protocol

v. Process information
vi. Process-to-port mapping
vii. Process memory
viii. Mapped drives
ix. Shares

x. Clipboard contents
xi. Service/driver information
xii. Command history

29. Operating System Forensics Part 2
    a. Volatile Information Collection (Con't)
        i. Process Information (Page 465)
            1. The full path to the executable image (.exe file)
            2. The command line used to launch the process, if any
            3. The amount of time that the process has been running
            4. The security/user context that the process is running in
            5. Which modules the process has loaded
            6. The memory contents of the process
                a. tasklist /v
                    i. shows all running processes
                    ii. /v Displays verbose task info
                    iii. /S specifies the remote system to connect to
                    iv. /SVC Displays services hosted in each process
                    v. /APPS Displays store apps and their associated processes
                    vi. /FI displays a set of tasks that match a filter
                    vii. /FO Specifies output format
                    viii. Valid values are "TABLE" and "CSV"
                    ix. /NH removes column header from Table or csv
                b. pslist -x
                c. listdlls (Page 469)
                    i. reports the DLLs loaded into processes
                    ii. can also display full version information for DLLs
                        1. including their digital signature
                    iii. can also scan processes for unsigned DLLs
                d. handle (Page 470)
                    i. displays info about the open handles for any process
                    ii. find out if user has specified any cmd-line parameters
        ii. Process to port mapping
            1. netstat –o (Page 472)
                a. shows the PIDs of processes that establish network connections
            2. netstat -fport
        iii. Process Memory Tools
            1. process explorer (Page 472) (Page 570)
                a. shows the information about the handles and DLLs of the processes which have been opened or loaded
                b. on technet
                c. sysinternals tool

2. pmdump (Page 472)
    a. dumps the memory contents of a process to a file without stopping the process
3. ProcDump (Page 473)
    a. monitors applications for CPU spikes and generating crash dumps during a spike so that an administrator or developer can determine the cause of the spike.
    b. command line interface tool
4. Process Dumper (PD) (Page 473)
    a. dumps the memory of a running process
    b. command line interface tool
5. userdump

iv. Network Status

1. Arp -a
2. **Ipconfig /all**
3. promqry (Page 475)
    a. checks if the network adapter is running in promiscuous mode
4. promisdetect (Page 475)
    a. checks if the network adapter is running in promiscuous mode
    b. command line interface tool

b. Print Spool files

i. The temporary files can store print details such as owner, document, printer, printing processor - format, number of copies printed and the print method

ii. The windows printing process supports two data types: RAW -.SPL file consists of data to be printed EMF - .SPL file consists the metadata and can be printed on any printer

iii. By default, the path of (the temp files) .SPL and .SHD in windows is C:\Windows\System32\spool\PRINTERS

iv. SPL and .SHD files contain metadata stored as Unicode and require Unicode capable tools to explore:

1. Hex editors
2. UCCHECK

c. Other Information: (Page 478)

i. Cilpboard contents –

1. free clipboard viewer

ii. Service/Driver Information

1. Wmic service list brief | more (Page 479)
    a. Command line tool in Windows
    b. Shows the list of running services, their PIDs, startmode, state and status.

iii. Command History

1. doskey /h

        a. Shows the commands run during a cmd prompt session
    iv. Mapped Drives
    v. Shares (Page 480)
        1. maintained by a machine in registry key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lanmanserver\Shares key
d. Non-Volatile Information Collection
    i. Examining the file system - dir /o:d
        1. Lists the directories most recently accessed (date and time)
    ii. FSUTIL
    iii. Disable LAST ACCESS UPDATE on files:
        1. HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem\Disablelastacess
        2. HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem\NTFSDisablelastacessupdate
    iv. AutoRUNS
        1. List what runs automatically
    v. Microsoft Security ID's for users with active accounts
        1. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList
        2. **Unique ID numbers assigned to user accounts for granting user access to particular resources**

30. Operating System Forensics Part 3
    a. Non-Volatile Information Collection (Con't)
        i. Event Logs
            1. PsLogList (Page 484)
                a. shows the contents of the System Event Log on the local computer and allows formatting of Event Log records
            2. Index.dat files for I.E. cache info can be found here: (up through Windows 7/Windows Vista)
                a. http://www.forensicswiki.org/wiki/Internet_Explorer_History_File_Format
            3. Windows 8/Windows 10:
                a. http://www.thewindowsclub.com/index-dat-file-Windows
        ii. Edge browser ESE database Files
            1. Uses Extensible Storage Engine (ESE) format to store browsing records, including history, cache, and cookies
            2. .edb extension
            3. The database store tables - FileCleanup, Folder, ReadingList, RowId, MSysObjids, MSysObjects, FolderStash, MSysLocales, and MSysObjectsShadow
            4. Common data locations include:

a. ESE database:
b. \Users\user_name\AppData\Local\Packages\Microsoft.MicrosoftEdge_xxxxx\AC\MicrosoftEdge\User\Default\DataStore\Data\nouser1\xxxxx\DBStore\spartan.eb

5. Edge cached files location:
    a. \Users\user_name\AppData\Local\Packages\Microsoft.MicrosoftEdge_xxxx\AC\#!001\MicrosoftEdge\Cache\
6. Edge last active browsing session data location:
    a. \Users\user_name\AppData\Local\Packages\Microsoft.MicrosoftEdge_xxxx\AC\MicrosoftEdge\User\Default\Recovery\Active\
7. Edge stores history records, Cookies, HTTP POST request header packets and downloads in:
    a. \Users\user_name\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat
8. If the last browsing session was opened in InPrivate mode then the browser stores these records in:
    a. \Users\user_name\AppData\Local\Packages\Microsoft.MicrosoftEdge_xxxx\AC\MicrosoftEdge\User\Default\Recovery\Active\{browsing-session-ID}.dat

b. Device information using DevCon tool:
    i. https://msdn.microsoft.com/en-us/windows/hardware/drivers/devtest/devcon
c. Finding Drive slack space using DRIVESPY Tool:
    i. https://www.digitalintelligence.com/software/disoftware/drivespy/
d. How do I scan Virtual Memory?
    i. http://www.x-ways.net/forensics/
e. Hibernate files
    i. Windows has two power management modes.
        1. The Sleep Mode, which keeps the system running in a low power state so that the user can quickly resume where he/she has paused working. The Hibernate Mode, which completely writes the contents of memory to a hiberfil.sys file in the HDD.
        2. The hiberfil.sys file is an important source of evidence, as it consists of the crucial information from all programs, applications, files and processes that were running in memory at the time the system was put into hibernation.
    ii. You can check if the user had enabled the hibernate option by searching for the
        1. following registry key:
        2. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power
f. Connected devices
    i. In the Device Manager window, click on View in the toolbar and select “Show hidden devices”
    ii. Devcon (Page 486)

1. Device Console
2. Command line tool
3. Displays detailed information about devices in Windows
4. Can change device settings
5. Can restart the device or computer

g. Virtual memory aka logical memory
   i. X-Ways Forensics tool (Page 488)
      1. Scans virtual memory
      2. Access logical memory of running processes
      3. Gather slack space, free space, inter-partition space, and generic text from drives and images
      4. Ability to read partitioning and file system structures
      5. Memory analysis for local RAM or memory dumps
      6. Disk cloning and imaging
h. Hibernate file (Page 491)
   i. Completely writes the memory as a hiberfil.sys file
   ii. Consists of the crucial information of all programs, applications, files and processes that were running on the RAM at a given time
   iii. Registry key to check if the user had enabled hibernate option
      1. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ Power
i. Pagefile.sys file (Page 493)
   i. Used as virtual memory to expand the physical memory of a system
   ii. Stores information about inactive processes, recently opened files and docs
   iii. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
j. Windows Search Index information access
   i. Maintaining a record of all the documents
   ii. http://www.lostpassword.com/search-index-examiner.htm
   iii.
   iv. Passware Search Index Examiner
      1. makes all the data indexed by Windows Search accessible
k. Hidden partition information
   i. may contain files, folders, confidential data, or backups of the system
   ii. http://partitionlogic.org.uk/
   iii. Partition Logic (Page 494)
      1. hard disk partitioning and data management tool
      2. Can create, delete, erase, format, defragment, resize, copy, and move partitions and modify their attributes
      3. Can copy entire hard disks from one to another
   iv. Partition Find & Mount
      1. deleted or lost partition recovery tool
l. Web Browser Caches

TOOLS Methodologies, Frameworks and Processes Term

i. Cookies
ii. Temp files

m. Windows Thumbnail caches
   i. In Windows 10 thumbcache.db file stores the thumbnails in the same location as Windows 7:
   ii. C:\Users\<USERNAME>\AppData\Local\Microsoft\Windows\Explorer
   iii. **the thumbnail of an image remains on a computer even after deleting the file itself**
   iv. helps the investigators to find if the suspect had deleted any files and it also gives a brief detail about the file that has been deleted
   v. Thumbcache Viewer (Page 497)
      1. Extracts thumbnail images from the thumbcache_*.db and iconcache_*.db database files found on Windows Vista, Windows 7, Windows 8, Windows 8.1, and Windows 10.

n. Windows Memory Analysis
   i. Memory Dump Files
   ii. https://support.microsoft.com/en-us/kb/969028
   iii. Dumpchk
      1. the Microsoft Crash Dump File Checker tool
      2. Performs a quick analysis of a crash dump file
      3. See summary information about what the dump file contains

o. Windows Kernel Opaque Structures -
   i. https://technet.microsoft.com/en-us/library/ff544273(v=vs.85).aspx

p. Executive Process (EProcess) Block Structure (Page 501)
   i. The basic data structure that stores various attributes of the process and the pointer to the other attributes and data structures related to the process
   ii. Important elementsof the EProcess
      1. PPEB_LDR_DATA (pointer to the loader data) structure that includes pointers or references to DLLs used by the process
      2. A pointer to the image base address, where the beginning of the executable image file can be found
      3. A pointer to the process parameters structure, which maintains the DLL path, the path to the executable image, and the command line used to launch the process

q. Parsing Memory Contents
   i. Lsproc.pl (Page 502)
      1. Locates processes but not threads
   ii. Lspd.pl (Page 503)
      1. Perl script that will allow the user to list the details of the process
      2. command-line Perl script that
      3. relies on the output of lsproc.pl to obtain its information.

r. Parsing Process Memory

i. Lspm.pl (Page 503)
    1. Takes the same arguments as lspd.pl
    2. Extracts the available pages from the dump file, and writes them to a file within the current working directory.

s. Extracting the process image
    i. Lspi.pl (Page 503)
        1. Locates the beginning of the executable image for the process.
        2. If the Image Base Address Offset leads to an executable image file, Lspi.pl parses the values contained in the PE header to locate the pages that make up the rest of the executable image file

t. Collecting process pemory
    i. Volatility Framework (page 504)
        1. **A completely open collection of tools, implemented in Python under the GNU General Public License, for the extraction of digital artifacts from volatile memory (RAM) samples.**
    ii. BinText (Page 505)
        1. Can extract text from a file and find plain ASCII text, Unicode (double byte ANSI) text, and Resource strings, providing useful information
    iii. Handle (Page 505)
        1. Displays info about open handles for any process in the system
        2. Use it to see the programs that have open files or to see the object types and names of all the handles of a program.
    iv. ListDLLs.exe (Page 505)
        1. Reports the DLLs loaded into processes
        2. It lists all DLLs loaded into all processes, or into a specific process. It can also list the processes that have a particular DLL loaded

31. Operating System Forensics Part 4
    a. Windows registry analysis Page (506)
        i. five root folders in the Registry Editor
            1. **HKEY_CLASSES_ROOT** (Page 507)
                a. sub-key of HKEY_LOCAL_MACHINE\Software
                b. contains file extension association information and also programmatic identifier (ProgID), Class ID (CLSID), and Interface ID (IID) data
                c. **This hive stores the necessary information which makes sure that the correct program opens when the user opens a file through the windows explorer**
            2. HKEY_CURRENT_USER (Page 507)
                a. config info related to the user currently logged on
                b. This hive controls the user level settings associated with user profile such as desktop wall paper, screen colors, display settings etc.

3. HKEY_LOCAL_MACHINE (Page 508)
    a. Contains most of the configuration information for installed software which includes the Windows OS
    b. The information about the physical state of the computer which includes bus type, installed cards, memory type, startup control parameters and device drives
    c. HKEY_LOCAL_MACHINE\System
        i. File path: Windows\System32\config\SYSTEM
    d. HKEY_LOCAL_MACHINE\SAM
        i. File Path: Windows\System32\config\SAM
        ii. Contains information about the system users
    e. HKEY_LOCAL_MACHINE\Security
        i. File Path: Windows\System32\config\SECURITY
    f. HKEY_LOCAL_MACHINE\Software
        i. File Path: Windows\System32\config\SOFTWARE
    g. HKEY_USERS\.Default
        i. File Path: Windows\System32\config\DEFAULT
4. HKEY_USERS (Page 507)
    a. Contains information about all the currently active user profiles
    b. Each registry key under HKEY_USERS hive relates to a user on the computer, which is named after the user's security identifier (SID)
    c. The registry keys and registry values under each SID control the user specific mapped drives, installed printers, environmental variables and so on.
5. HKEY_CURRENT_CONFIG (Page 507)
    a. Stores info about the current hardware profile of the system
    b. Explains the differences between the current hardware configuration and the standard configuration.
    c. A pointer to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\CurrentControlSet\Hardware Profiles\Current registry key, which contains the information about the standard hardware configuration that is stored under the Software and System keys

b. Registry Analysis
    i. RegRipper (Page 509)
    ii. ProDiscover (Page 509)
    iii. Process Monitor
    iv. RegScanner (Page 570)
        1. scan the registry, find the desired registry values that match the specified search criteria, and display them in one list
    v. RegEdit

TOOLS Methodologies, Frameworks and Processes Term

vi. Registry Viewer

c. System Information
    i. last system shut down in the following key (Page 511)
        1. HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Windows
    ii. ProductName, CurrentBuildNumber, and CSDVersion in the following key
        1. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
    iii. Find the time zone settings in the following key
        1. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInf orma tion
    iv. Find information about shares in the following key
        1. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Sha res
    v. registry entries for wireless network connections are in the following key
        1. HKLM|SOFTWARE\Micros oft\WZCSVC\Parameters \Interfaces \{GUID}
    vi. Registry keys accessed and parsed when a user logs in to a system (Page 517)
        1. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
        2. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
        3. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
        4. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
    vii. Look for malware in these locations
        1. HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\shell\open\command
        2. HKEY_CLASSES_ROOT\exefile\shell\open\Command
    viii. Notifications are handled by the Registry key
        1. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Notify
    ix. Shows mounted USB Devices
        1. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses
    x. UserAssist key gives information on what types of files or applications have been accessed on a particular system
        1. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
        2. Value name is ROT-13 encrypted. Unencrypting provides the application loaded under this key
    xi. MRU Lists (Page 524)
        1. Most Recently Used lists

2. lists of recently visited web pages, opened documents, etc.
3. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

xii. Volumes the user added to the system will appear in the following key
1. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2

xiii. Restore points are stored in the following registry key (Page 526)
1. HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\SystemRestore

xiv. All values in this key are executed at system startup
1. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\

xv. All values in this key are executed at system startup and are deleted later
1. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\

xvi. The value Shell will be executed when any user logs on.
1. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon

xvii. Each subkey (GUID name) represents an installed component.
1. HKEY_LOCAL_MACHINE\SOFTWARE \Microsoft\Active Setup\ Installed Components\

xviii. BootExecute contains files of native applications executed before Windows Run
1. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager

xix. List of services that run at system startup. If the value Start is 2, startup is automatic. If the value Start is 3, startup is manual and starts on demand for service. If the value Start is 4, service is disabled
1. HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\

xx. Values in this subkey run when this specific user logs on
1. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\

xxi. All values in this subkey run when this specific user logs on, and then the values are deleted
1. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\

xxii. For this specific user, if a screensaver is enabled, a value named scrnsave.exe is present. Whatever is in the path found in the string data for this value will execute when the screensaver runs
1. HKEY_CURRENT_USER\Control Panel\Desktop

xxiii. The string specified in the value run executes when this user logs on (Page 529)
1. HKEY_CURRENT_USER\Software\Microsoft\Windows NT\ CurrentVersion\Windows\

32. Operating System Forensics Part 5
    a. Mozilla Cache, Cookie, and History Analysis
        i. Firefox - Cache stored in the system locations
            1. C:\Users\<Username>\AppData\Local\Mozilla\Firefox\Profiles\XXXXXXX X.default\cache2
        ii. Firefox - Cookies stored in the system locations
            1. C:\Users\<Username>\AppData\Roaming\Mozilla\Firefox\Profiles\XXXX XXXX.default\cookies.sqlit
        iii. Firefox - History stored in the system locations
            1. C:\Users\<Username>\AppData\Roaming\Mozilla\Firefox\Profiles\XXXX XXXX.d efault\places.sqlite
        iv. Analysis tools
            1. MZCacheView (Page 531)
            2. MZCookiesView (Page 532)
            3. MZHistoryView (Page 533)
    b. Google Chrome Cache, Cookie, and History Analysis
        i. History, Downloads and Cookies Location:
            1. C:\Users\{user}\AppData\Local\Google\Chrome\User Data\Default
        ii. Cache Location:
            1. C:\Users\{user}\AppData\Local\Google\Chrome\User Data\Default\Cache
        iii. Analysis tools
            1. ChromeCacheView (Page 534)
            2. ChromeCookiesView (Page 535)
            3. ChromeHistoryView (Page 536)
    c. Microsoft Edge Cache, Cookie, and History Analysis
        i. Cache Location
            1. C:\Users\Admin\AppData\Local\Microsoft\Windows\WebCache
        ii. Cookies Location
            1. C:\Users\Admin\AppData\Local\Packages\Microsoft.MicrosoftEdge_8w ekyb3d8bbwe\AC\MicrosoftEdge\Cookies
        iii. History Location:
            1. C:\Users\Admin\AppData\Local\Microsoft\Windows\History
        iv. Analysis tools
            1. IECacheView (Page 537)
            2. IECookiesView (Page 538)
                a. http://www.nirsoft.net/utils/iecookies.html
            3. BrowsingHistoryView (Page 537)
                a. http://www.nirsoft.net/utils/browsing_history_view.html
    d. Prefetch Files
        i. Prefetch directory

TOOLS Methodologies, Frameworks and Processes Term

1. **When a user installs an application, runs it, and deletes it , traces of that application can be found here**

ii. DWORD value at the offset 120 within the file corresponds to the last time of the application run, this value is stored in UTC format

iii. DWORD value at the offset 144 within the file corresponds to the number of times the application is launched

iv. Prefetching is to improve system performance

v. Prefetching is controlled by the Registry key

1. HKEY_LOCAL_MACHINE\SYSTEM\ControlSet00x\Control\SessionManager\Memory Management\PrefetchParameters
2. Data associated with value EnablePrefetcher tells which form of prefetching the system uses (Page 541)
    a. **0: Prefetching is disabled**
    b. **1: Application prefetching is enabled**
    c. **2: Boot prefetching is enabled**
    d. **3: Both application and boot prefetching are enabled**

e. Metadata investigation (Page 543)

i. Types of metadata

1. Descriptive metadata
    a. describes discovery and identification purposes
    b. includes info such as title, abstract, author, and keywords
2. Structural metadata
    a. facilitates information of navigation and presentation of electronic resources
    b. Describes relationship among materials
3. Administrative metadata
    a. It provides info to manage a resource
    b. When and how it was created, file type, access permissions and other technical information

ii. Metadata analysis tools

1. Metashield Analyzer (Page 549)
    a. online tool to analyze the metadata contained in a file

f. Types of logon events (Page 551)

i. 2 – Interactive

1. A user logged on to this computer

ii. 3 – Network

1. A user or computer logged on to this computer from the network

iii. 4 – Batch

1. Batch logon type is used by batch servers, where processes may be executing on behalf of a user without their direct intervention

iv. 5 – Service

1. A service was started by the Service Control Manager

TOOLS Methodologies, Frameworks and Processes Term

v. 7 – Unlock
    1. This workstation was unlocked
vi. 8 – NetworkCleartext
    1. A user logged on to this computer from the network. The user's password was passed to the authentication package in its unhashed form.
vii. 9 – NewCredentials
    1. A caller cloned its current token and specified new credentials for outbound connections
viii. 10 – RemoteInteractive
    1. A user logged on to this computer remotely using Terminal Services or Remote Desktop
ix. 11 – CachedInteractive
    1. A user logged on to this computer with network credentials that were stored locally on the computer

g. Log file format
    i. ELF_LOGFILE_HEADER
        1. Header of fixed size
    ii. EVENTLOGRECORD structures
        1. Variable number of event records
    iii. ELF_EOF_RECORD structure
        1. End-of-file record
    iv. Event log record structure (Page 554)
        1. Length
            a. Event record size in bytes
        2. NumStrings
            a. Number of the stings in the log
        3. EventID
            a. used to identify an event.
        4. EventType
            a. Error: It denotes an issue or problem like data loss
            b. Warning: It is an indication of future occurrence of error
            c. Information: details of the occurrence of a successful operation
            d. Success Audit: successful audited security access attempt
            e. Failure Audit: failed audited security access attempt
        5. EventCategory
            a. the category of an event

h. Windows 10 event logs
    i. Wevtutil (Page 557)
        1. Command line tool
        2. **used to retrieve information about event logs and publishers** that is not readily apparent via the Event Viewer user interface

3. wevtutil el
    a. displays a list of available Event Logs on the system
4. wevtutil gl <log name>
    a. lists configuration information about a specific Event Log

i. Account management events (Page 559)
    i. used to record the changes in accounts and group membership
    ii. The first line of the description summarizes the type of action.
    iii. The account that performed the action is listed in the Caller User Name field
    iv. The account added or removed is shown in the Member ID field
    v. The group affected is listed as the Target Account Name
    vi. Various Event IDs are associated with changes in the accounts
        1. 4727 - A security-enabled global group was created
        2. 4728 - A member was added to a security-enabled global group
        3. 4729 - A member was removed from a security-enabled global group
        4. 4730 - A security-enabled global group was deleted
        5. 4731 - A security-enabled local group was created
        6. 4732 - A member was added to a security-enabled local group
        7. 4733 - A member was removed from a security-enabled local group
        8. 4734 - A security-enabled local group was deleted
        9. 4735 - A security-enabled local group was changed
        10. 4737 - A security-enabled global group was changed
        11. 4754 - A security-enabled universal group was created
        12. 4755 - A security-enabled universal group was changed
        13. 4756 - A member was added to a security-enabled universal group
        14. 4757 - A member was removed from a security-enabled universal group
        15. 4758 - A security-enabled universal group was deleted
        16. 4764 - A group's type was changed

j. Log Types
    i. Application (Page 563)
        1. contains messages from both the operating system and various programs
        2. logevent.exe (page 563)
            a. Microsoft tool used to send custom messages
        3. Event ID 1
    ii. Security
        1. stores data pertaining to login/logout activities or any other events related to security, as specified by the system's audit policy
    iii. Setup
    iv. System (page 562)
        1. contains events logged by Windows system components including
            a. Changes to the OS
            b. Changes to the hardware configuration

c. Device driver installation
d. Starting and stopping of services

2. Event ID 7035 – Service stopped or to be started again
3. Event ID 7036 – Service starts

v. Forwarded events

k. Windows event log file internals (Page 567)
   i. **System.evtx – System log files**
   ii. Security.evtx – Security log files
   iii. Application.evtx – Application log files
   iv. Stored at C:\Windows\System32\winevt\Logs

l. Windows forensics tools
   i. OS Forensics (Page 568)
      1. system information gathering software
      2. extracts forensic data from computers
      3. uncovers everything hidden inside a PC
      4. identifies suspicious files and activities with hash matching
      5. makes drive signature comparisons
      6. looks into emails, memory, and binary data
      7. analyzes the results in the form of a file listing, a thumbnail view, or a timeline view, which allows you to determine at what point some significant file change activity has occurred
   ii. Belkasoft Evidence Center (Page 569)
      1. search, analyze, and store digital evidences found in Instant Messenger histories, Internet browser histories, and Outlook mailboxes
   iii. MultiMon (Page 571)
      1. system monitoring tool for Windows OS
      2. displays system activities in real time
      3. shows registry activity in real time
      4. monitor clipboard, keyboard, and task activities
   iv. Security Task Manager (Page 571)
      1. Shows information about programs and processes running
      2. detects unknown malware and rootkits hidden from av software
   v. Proc Heap Viewer (Page 571)
      1. Enumerates process and service heaps on Windows
      2. Can be used to discover heap-related vulnerabilities
   vi. Memory Viewer (Page 571)
      1. View system memory configuration
      2. Shows the type of memory: SDRAM, DDR, etc.
   vii. Word Extractor (Page 572)
      1. converts binary files (like Windows EXE applications, DLLs, and encrypted files) to text files, allowing you to look inside.

2. separate the strings that contain human text or words from binary code It is suitable for many purposes
    a. Finding cheats in games
    b. Finding hidden text in any files (EXE applications, binary, DLL)
    c. Finding hidden passwords in any files
    d. Recovering corrupted documents
    e. Checking suspicious files against viruses and malware

viii. Belkasoft Browser Analyzer (Page 572)
1. search and analyze various Internet browser histories
2. can retrieve URLs, passwords, and cookies

ix. Metadata Assistant (Page 572)
1. The Metadata Assistant analyzes Word/Excel/PowerPoint (2000 and higher) files to determine the type and amount of metadata (hidden information) that exists within
2. Remove unwanted metadata

x. HstEx (Page 572)
1. recover browser artifacts and Internet history
2. It finds deleted Internet history from:
    a. Unallocated clusters
    b. Cluster slack
    c. live memory, memory dumps, and crash dumps

xi. XpoLog Log Management (Page 573)

xii. Event Log Explorer (Page 573)

xiii. LogMeister (Page 574)

xiv. System Explorer (Page 574)
1. free software for exploration and management of system internals

xv. ProDiscover Forensics (Page 574)

xvi. Helix3 Pro (Page 575)

xvii. ThumbsDisplay (Page 575)
1. tool for examining and reporting on the contents of Thumbs.db files

xviii. Registry Viewer (Page 576)

xix. Windows Forensic Toolchest (WFT) (Page 576)

33. Operating System Forensics Part 6
    a. Linux forensics shell commands
        i. Dmesg (Page 577)
            1. Short for display message or 'Driver Message'
            2. **Displays the kernel ring buffers**, which contains the **information about the drivers loaded into kernel** during boot process and error messages produced at the time of loading the drivers into kernel.
            3. Helpful in resolving the device's driver issues.
            4. Syntax: dmesg options

a. dmesg | grep -i eth0 (Displays hardware information of the Ethernet port eth0)

ii. fsck (Page 577)
1. File System Consistency Check
2. Checks the consistency of Linux file system and repair
3. Syntax: fsck –A (Checks all configured filesystems)

iii. Stat (Page 577)
1. Displays file or file system status.
2. Syntax: stat [OPTION]... FILE...

iv. history (Page 577)
1. Checks and lists the Bash shell commands used
2. Helps users for auditing purposes
3. Syntax: history n (Lists the last n commands)

v. mount (Page 577)
1. Causes mounting of a file system or a device to the directory structure, making it accessible by the system.
2. Syntax: mount -t type device dir (Requests kernel to attach the file system found on device of type type at the directory dir)

b. Linux log locations (Page 578)
i. /var/log/messages - Global system messages
ii. /var/log/dmesg - Kernel ring buffer information
iii. /var/log/cron - Information about the cron job in this file
iv. /var/log/user.log - All user level logs
v. /var/log/lastlog - Recent login information
vi. /var/log/boot.log - Information logged on system boots
vii. /var/log/auth.log - System authentication information
viii. /var/log/kern.log – Messages sent from kernel
ix. /var/log/faillog - Failed user login attempts
x. /var/log/lpr.log - Stores printer logs
xi. /var/log/mail.* - All mail server message logs
xii. /var/log/mysql.* - MySQL server logs
xiii. /var/log/apache2/* - Apache web server logs
xiv. /var/log/apport.log - Application crash report / log
xv. /var/log/lighttpd/* - Lighttpd web server log files directory
xvi. /var/log/daemon.log - Running services such as squid, ntpd, etc.
xvii. /var/log/debug - Debugging log messages
xviii. /var/log/dpkg.log - Package installation or removal logs

c. Collecting volatile data in Linux (Page 579)
i. Netstat
1. displays info about network connections, routing tables, network interfaces and network protocol stats

ii. Last –F

TOOLS Methodologies, Frameworks and Processes Term

1. displays the activities of each user in detail

iii. hostname
1. displays the hostname of a system

iv. ifconfig –a
1. view the configuration of all network, both up and downed interfaces

v. lsof (Page 582)
1. short for 'list open files'
2. list all the open files and the active processes that opened them

vi. lsmod
1. displays the information about the loaded modules

vii. xclip -o
1. interact with the X clipboard instead of using a mouse to copy paste
2. –o to output contents onto the command line

viii. Aureport
1. Used to produce summary reports of the audit system logs

ix. id
1. determines the user ID and group information for a specified user

x. ausearch
1. command to track all events of a specific user ID

xi. readelf
1. short notation for 'Read Executable and Linking Format'
2. Used to analyze the file headers and section of the ELF files
3. ELF is the format for executables, shared libraries, kernel modules and the kernel

xii. Cron
1. schedules tasks to run at a specific point of time
2. Cron tasks are located in /var/spool/cron/ and /etc/cron.daily

xiii. .bash_history
1. stores the command history

xiv. /proc
1. Directory of special files that represent the current state of a kernel

xv. ps
1. short notation for 'process status'
2. Used to view the list of processes running

xvi. arp (Page 588)
1. short notation for Address Resolution Protocol.
2. Used to clear, add to or extract the kernel's ARP cache

xvii. ss -l -p -n | grep <PID>
1. used to check if particular process (PID) running is suspicious

d. Collecting non-volatile data in Linux (Page 591)
i. Check for auto-start services
1. Ls /etc/rcl.d

ii. Review recently modified files
iii. Collect login and system Logs
    1. Cat /var/log/kern.log
iv. Search for files with strange names in /dev directory
    1. [name] –check –rwo
v. Check security settings of the system for anomalies
    1. Chkrootkit

e. MAC forensics tools (Page 599)
    i. OS X Auditor- Mac Forensics Tool
    ii. MacForensicLab
    iii. Macintosh Forensic Software
    iv. Memoryze for the Mac
    v. Mac Marshal
    vi. F-Response
    vii. Mac OS X Memory Analysis Toolkit
    viii. Volatility 2.5
    ix. Avast Free Mac Security
    x. OS X Rootkit Hunter for Mac

7. Network Forensics

34. Network Forensics Part 1
    a. Network forensics
        i. the implementation of sniffing, recording, acquisition, and analysis of network traffic and event logs to investigate a network security incident
    b. Postmortem and Real-Time Analysis
        i. Postmortem
            1. detect something that has already occurred in a network/device and determine what it is
        ii. Real-Time Analysis
            1. Ongoing process, which returns results simultaneously, so that the system or operators can respond to the attacks immediately
    c. Network Vulnerabilities
        i. Only thing that a user can do is minimize these vulnerabilities
        ii. Complete removal of the vulnerabilities is not possible
        iii. Internal network vulnerabilities (Page 610)
            1. Occur due to the overextension of bandwidth and bottlenecks
                a. Overextension of bw occurs when user need exceeds total resources
                b. Bottlenecks occur when user need exceeds resources in particular network sectors
        iv. External network vulnerabilities

1. Occur due to threats such as DoS/DDoS attacks and network data interception
    a. DoS and DDoS attacks result from one or numerous attacks
    b. Attacks are responsible for slowing down or disabling the network
    c. Data interception is a common vulnerability among LANs and WLANs
        i. Attacker infiltrates a secure session and thus monitors or edits the network data to access or edit the network operation.

d. Network Attacks (Page 610)
    i. Eavesdropping
        1. Technique used in intercepting the unsecured connections in order to steal personal information
    ii. Data Modification (Page 611)
        1. Intruder alters the data
    iii. IP Address Spoofing (Page 611)
        1. The attacker sends messages to the computer with an IP address that indicates the messages are coming from a trusted host
    iv. **Denial of Service (DoS)** (Page 611)
        1. The attacker floods the target with huge amount of invalid traffic
        2. Leads to exhaustion of the resources available on the target
        3. The target then stops responding to further incoming requests
        4. Leads to denial of service to the legitimate users
    v. Man-in-the-Middle Attack (Page 611)
        1. Attacker makes independent connections with the users/victims and relays messages between them, making them believe that their conversation is direct
    vi. Packet Sniffing (Page 611)
        1. Process of capturing traffic flowing through a network
        2. Aims at gaining sensitive information such as usernames and passwords
        3. Software tools known as Cain&Able are used to server this purpose.
    vii. Enumeration (Page 611)
        1. Process of gathering the following information about a network
            a. Topology of the network
            b. List of live hosts
            c. Architecture and the kind of traffic (for example, TCP, UDP, IPX)
            d. Potential vulnerabilities in host systems
    viii. Session Hijacking (Page 611)
        1. Exploitation of a session-token generation mechanism or token security controls

TOOLS Methodologies, Frameworks and Processes Term

2. Done so the attacker can establish an unauthorized connection with a target server

ix. Buffer Overflow (Page 612)
    1. If the data count exceeds the original capacity of a buffer, then the extra information may overflow into neighboring buffers, destroying or overwriting the legal data

x. Email Infection (Page 612)
    1. Uses emails as a means to attack a network
    2. Email spamming and other means are used to flood a network and cause a DoS attack

xi. Malware Attacks (Page 612)
    1. Installation of malicious code on the targeted system
    2. Once installed, it damages the system

xii. Password-based attacks (Page 612)
    1. attacker performs numerous login attempts on a system or an application to duplicate the valid login and gain access to it

xiii. Router attacks (Page 612)
    1. It is the process of an attacker attempting to compromise the router and gaining access to it

e. Wireless network Attacks (Page 612)

i. Rogue Access Point Attack (Page 612)
    1. Attackers or insiders create a backdoor into a trusted network by installing an unsecured access point inside a firewall

ii. Client Mis-association (Page 612)
    1. The client may connect or associate with an AP outside the legitimate network either intentionally or accidentally
    2. Can lead to access control attacks

iii. Misconfigured Access Point Attack (Page 612)
    1. Easiest vulnerability to exploit
    2. Upon successful exploitation, the entire network could be open to attacks
    3. One of the means of causing the misconfiguration is to apply default usernames and passwords to use the access point

iv. Unauthorized Association (Page 613)
    1. attacker takes advantage of WLAN radios present in some laptops
    2. attacker can activate these access points in the victim's system through a malicious program and gain access to the network

v. Ad Hoc Connection Attack (Page 613)
    1. uses a USB adapter or wireless card
    2. Host connects with an unsecured station to attack a particular station or evade access point security

vi. HoneySpot Access Point Attack (Page 613)

1. Occurs when multiple WLANs co-exist in the same area and a user can connect to any available network
2. An attacker sets up a rogue AP, aka honeypot AP, using high-power (high gain) antennas and uses the same SSID of the target network
3. Users who regularly connect to multiple WLANs may connect to the rogue AP
4. NICs searching for the strongest available signal may connect to the rogue AP
5. If an authorized user connects to a honeypot AP, it reveals sensitive user information such as identity, user name, and password to the attacker

vii. **AP MAC Spoofing** (Page 613)
1. the attacker can reconfigure the MAC address in such a way that it appears as an authorized access point to a host on a trusted network
2. The tools for carrying out this kind of attack are changemac.sh, SMAC, and Wicontrol.

viii. **Jamming Signal Attack** (Page 613)
1. The attacker jams the WiFi signals to stop all legitimate traffic from using the access point by sending huge amounts of illegitimate traffic to the access point

35. Network Forensics Part 2
a. TCP/IP
i. Transmission Control Protocol/Internet Protocol
ii. Communication protocol used to connect different hosts in the Internet
iii. TCP/IP program has two layers
1. Higher layer
a. manages the information sent and received in the form of small data packets sent over Internet and joins all those packets as a main message
2. Lower layer
a. handles the address of every packet so that they all reach the right destination
iv. Model
1. Layer 1: Network Access Layer
a. Defines how to use the network to transfer data
b. Includes protocols which help the machine deliver the desired data to other hosts in the same network
i. Frame Relay
ii. SMDS
iii. Fast Ethernet
iv. SLIP
v. PPP
vi. FDDI

TOOLS Methodologies, Frameworks and Processes Term

vii. ATM
viii. Ethernet
ix. L2TP
x. ARP, etc.,

2. Layer 2: Internet Layer
    a. Handles the movement of data packet over a network, from source to destination
    b. Contains protocols
        i. Internet Protocol (IP) – Main protocol used
        ii. Internet Control Message Protocol (ICMP)
        iii. Address Resolution Protocol (ARP)
        iv. Internet Group Management Protocol (IGMP), etc
3. Layer 3: Transport Layer
    a. Serves as the backbone for data flow between two devices in a network.
    b. Allows peer entities on the source and destination devices to carry on a communication.
    c. Uses many protocols
        i. Transmission Control Protocol (TCP)
            1. Reliable connections
        ii. User Datagram Protocol (UDP)
            1. non-reliable connections.
4. Layer 4: Application Layer
    a. Includes all processes to deliver data.
    b. Protocols
        i. HTTP
        ii. Telnet
        iii. FTP
        iv. SMTP
        v. NFS
        vi. TFTP
        vii. SNMP
        viii. DNS

b. Law and regulations
    i. Federal Information Security Management Act of 2002 (FISMA):
        1. Key security standards and guidelines, as required by Congressional legislation.
        2. **Requires Federal agencies to develop, document, and implement an organization-wide program to provide information security** for the information systems that support its operations and assets.
        3. NIST SP 800-53 - recommended security controls for Federal agencies.

a. Describes controls related to log management, including the generation, review, protection, and retention of audit records, as well as the actions to be taken because of audit failure.

ii. Gramm-Leach-Bliley Act (GLBA) (Page 617)
1. **Requires financial institutions**—companies that offer consumers financial products or services such as loans, financial or investment advice, or insurance—**to protect their customers' information against security threats**

iii. Health Insurance Portability and Accountability Act of 1996 (HIPAA)
1. Security standards for health information
2. NIST SP 800-66, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security
a. Lists HIPAA-related log management needs
b. The need to perform regular reviews of audit logs and access reports
c. Specifies that documentation of actions and activities need to be retained for at least six years.

iv. Sarbanes-Oxley Act (SOX) of 2002
1. Act passed by the U.S. Congress in 2002 to protect investors from the possibility of fraudulent accounting activities by corporations
2. Encompasses IT functions that support financial and accounting practices
3. Requires review of logs regularly to look for signs of security violations, including exploitation
4. Requires log retention and records of log reviews for future review by auditors

v. Payment Card Industry Data Security Standard (PCI DSS)
1. Proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards
2. PCI DSS applies to organizations that "store, process, or transmit cardholder data" for credit cards
3. One of the requirements of PCI DSS is to "track...all access to network resources and cardholder data"

c. U.S. Federal Rule of Evidence Rule 803 – Records of Regularly Conducted Activity as Evidence 22:30-26:15 (Page 618)
i. Business records would be accurate in representing the timeline of events as long as they are created as a normal course of business

d. Steps of Event correlation 26:15-27:13 (Page 619)
i. Event aggregation
1. AKA event de-duplication

TOOLS Methodologies, Frameworks and Processes Term

2. Compiles the repeated events to a single event and avoids duplication of the same event

ii. Event masking
1. Missing events related to systems that are downstream of a failed system. It avoids the events that cause the system to crash or fail.

iii. Event filtering
1. Event correlator filters or discards the irrelevant events

iv. Root cause analysis
1. Identifies all the devices that became inaccessible due to network failures – Why did something happen

e. Types of event correlation 27:13-31:00 (Page 620)
i. Same-Platform Correlation
1. When one common OS is used throughout the network

ii. Cross-Platform Correlation
1. Different OS and network hw platforms used throughout the network

f. Prerequisites of event correlation (Page 620)
i. Transmission of Data
1. Transmitting data from one security device to another until it reaches a consolidation point in the automated system

ii. Normalization (Page 621)
1. After the data is gathered, it must be formatted again from different log formats to a single or polymorphic log that can be easily inserted into the database

iii. Data Reduction (Page 621)
1. After collecting the data, repeated data must be removed so that the data can be correlated more efficiently
2. Removing unnecessary data can be done by compressing the data, deleting repeated data, filtering or combining similar events into a single event and sending that to the correlation engine

36. Network Forensics Part 3
a. Event Correlation Approaches 1:11-8:20 (Page 621)
i. Graph-Based Approach
1. Constucts a graph with each node as a system component and each edge as a dependency among two components

ii. Neural Network-Based Approach
1. uses a neural network to detect the anomalies in the event stream, root causes of fault events, etc.

iii. Codebook-Based Approach
1. Groups all events together
2. It uses a codebook to store a set of events and correlates them

iv. Rule-Based Approach
1. correlates events according to a specified set of rules as follows

TOOLS Methodologies, Frameworks and Processes Term

a. condition → action

v. Field-Based Approach
    1. compares specific events with single or multiple fields in the normalized data

vi. Automated Field Correlation
    1. checks and compares all the fields systematically and intentionally for positive and negative correlation with each other to determine the correlation across one or multiple fields

vii. Packet Parameter/Payload Correlation for Network Management
    1. Used for correlating particular packets with other packets. C
    2. Can make a list of possible new attacks by comparing packets with attack signatures

viii. Profile/Fingerprint-Based Approach
    1. Gathers a series of data sets from forensic event data to compare and link attack data to other attacker profiles

ix. Vulnerability-Based Approach
    1. Maps IDS events that target a particular vulnerable host with the help of a vulnerability scanner
    2. This approach deduces an attack on a particular host in advance, and it prioritizes attack data in order to respond to the trouble spots quickly

x. Open-Port-Based Correlation
    1. The open-port correlation approach determines the chance of a successful attack by comparing it with the list of open ports available on the host

xi. Bayesian Correlation
    1. Advanced correlation method that assumes and predicts what a hacker can do next after the attack by studying statistics and probability

xii. Time (Clock Time) or **Role-Based Approach**
    1. Monitors computers' and computer users' behavior and alerts if some anomaly is found

xiii. Route Correlation
    1. Extract an attack route information and use that information to single out other attack data

b. Network Forensic Readiness
    i. Ensure log file accuracy
        1. Log Everything (Page 623) - Configure to log all fields available
        2. Keeping Time (Page 623) - synch IIS servers using Windows Time service with an external time source
            a. NTP (page 624)
                i. HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\
                    1. Value name: Type

TOOLS Methodologies, Frameworks and Processes Term

2. Type: REG_SZ
3. Value data: NTP

ii. HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\
1. Value name: NtpServer
2. Type: REG_SZ
3. Value name: tock.usno.navy.mil

iii. HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\
1. Value name: Period
2. Type: REG_SZ
3. Value data: 24

3. Use multiple sensors (Page 625) - combine logs from different devices
4. Avoid missing logs (Page 625) - schedule a few hits to the server using a scheduling tool and then keep a log of the outcomes of these hits to determine when the server was active

ii. 3 tiers of log management (Page 625)
1. **Log generation**
2. **Log analysis and storage**
3. **Log monitoring**

iii. Functions of log management infrastructure (Page 626)
1. Log parsing - extracting data from a log so that the parsed values can be used as input for another logging process.
2. Event filtering - suppression of log entries through analysis, reporting, or long-term storage because their characteristics indicate that they are unlikely to contain information of interest.
3. Event aggregation - similar entries are consolidated into a single entry
4. Log rotation - closes a log file and opens a new log file on completion of the first file performed according to a schedule or when a log file reaches a certain size
5. Log archival and retention - retaining logs for an extended time period,
6. **Log compression** - storing a log file in a way that reduces the amount of storage space needed
7. **Log reduction** - removing unneeded entries from a log
8. **Log conversion** - parsing a log in one format and storing its entries in a second format
9. Log normalization - log data fields are converted to a particular data representation and categorized consistently.
10. Log file integrity checking - calculation of a message digest for each file and storing the message digest securely to ensure detection of the changes made to the archived logs.
11. Event correlation - determining relationships between log entries

12. Log viewing - displays log entries in a human-readable format
13. Log reporting - displaying the results of log analysis
14. Log clearing - removes all entries from a log

iv. Challenges – **Major concerns with log management** (Page 627)
   1. **Log creation and storage**
   2. **Log protection**
   3. **Log Analysis**
      a. lack of tools and skillful professionals for log analysis

v. Meeting the challenges (Page 628)
   1. Define requirements for performing log management
   2. Generate policies and procedures to ensure a consistent method
   3. Create and maintain secure infrastructure
   4. Provide training to all staff regarding their responsibilities

vi. Centralized logging (Page 628)

vii. Syslog
   1. de-facto standard for logging system events
   2. client/server protocol used for forwarding log messages across an IP network to the syslog receiver
   3. Port 514
   4. Syslogd (Page 630)
      a. Logging daemon
      b. reads messages from file, consults its configuration file, and dispatches message to appropriate destination
      c. Writes its process ID to the file /etc/syslog.pid:
      d. Restart syslogd by
         i. kill -HUP '/bin/cat /etc/syslog.pid'
      e. Controlled by the file /etc/syslog.conf
   5. Swatch (Page 631)
      a. Tool used to generate real-time alerts, which help to continuously monitor the log files

viii. IIS centralized binary logging (Page 631)
   1. Process where most of the websites transmit binary and scattered log data to a single log file
   2. Other IIS logging processes generate a separate log file collectively for all websites
   3. Reduces system resources that are used for logging and provides complete log data

c. Network forensic steps (Page 632)
   i. Ensure log file authenticity
      1. Use signatures, encryption, and checksums
      2. FSUM

TOOLS Methodologies, Frameworks and Processes Term

a. command line utility for file integrity verification.
b. 13 hash and checksum functions for file message digest and checksum calculation

ii. Work with copies
iii. Maintain Chain of Custody
iv. Condense log files (Page 635)

1. Tools used to filter log files depending on requirements
   a. Swatch
   b. Logcheck
2. Network Forensics Analysis Mechanism
   a. Presenting the evidence
   b. Manipulating
   c. Automated reasoning

d. Log Capturing and Analysis Tools

i. GFI EventsManager (Page 637)
ii. Kibana
iii. Syslog-ng
iv. RSYSLOG
v. Firewall Analyzer
vi. Simple Event Correlator (SEC)
vii. OSSEC
viii. Ipswitch Log Management
ix. Veriato Server Manager
x. Log Management Utility
xi. Snare
xii. Splunk Enterprise
xiii. Loggly
xiv. vRealize Log Insight
xv. Sumo Logic
xvi. TIBCO LogLogic
xvii. Logscape
xviii. ArcSight ESM
xix. XpoLog Log Management
xx. LogRhythm
xxi. Sawmill
xxii. McAfee Enterprise Log Manager
xxiii. Log and Event Manager
xxiv. Papertrail
xxv. EventReporter
xxvi. Kiwi Log Viewer
xxvii. Event Log Explorer
xxviii. WebLog Expert

TOOLS Methodologies, Frameworks and Processes Term

xxix. ELM Enterprise Manager
xxx. EventSentry
xxxi. LogMeister
xxxii. InTrust
xxxiii. Alert Logic Log Manager
xxxiv. Sentinel Log Manager
xxxv. Tripwire Log Center
xxxvi. AlienVault Unified Security Management
xxxvii. MyEventViewer
xxxviii. WinAgents EventLog Translation Service
xxxix. EventTracker Enterprise
xl. Logstash
xli. SecurityCenter CV
xlii. The Elastic Stack
xliii. CorreLog
xliv. Assuria Log Manager
xlv. BlackStratus LOGStorm
xlvi. PowerBroker Event Vault
xlvii. Logsene
xlviii. SaaS Log Management
xlix. ApexSQL Log
l. FortiSIEM
li. Graylog

37. Network Forensics Part 4
    a. Analyzing router logs 3:58
        i. Arp -a
        ii. Cisco routers
            1. 0 – Emergency – System unusable
            2. 1 – Alert – Immediate action required
            3. 2 – Critical
            4. 3 – Error
            5. 4 - Warning
        iii. DHCP logging
            1. saved in the C:\Windows\System32\dhcp folder on DHCP servers
            2. C:\Windows\system32\dhcp\backup folder contains a backup dhcp
    b. Network Traffic Investigation (Page 664)
        i. Sniffing tools
            1. Wireshark
                a. Follows the TCP stream
            2. SteelCentral Packet Analyzer (Page 670)
            3. Tcpdump
            4. Windump (Page 674)

TOOLS Methodologies, Frameworks and Processes Term

5. Capsa Network Analyzer (Page 675)
6. OmniPeek Network Analyzer (Page 676)
7. Observer (Page 677)
8. Colasoft Packet Builder (Page 678)
9. RSA NetWitness Investigator (Page 679)
10. Ace Password Sniffer (Page 680)
    a. password recovery utility that captures the forgotten passwords.
11. IPgrab – Sniffer for UNIX (Page 680)
12. Big Mother (Page 680)
13. EtherDetect Packet Sniffer (Page 680)
14. dsniff (Page 681)
15. EffeTech HTTP Sniffer (Page 681)
16. Ntopng (Page 681)
17. Ettercap (Page 682)
18. SmartSniff (Page 682)
19. EtherApe (Page 682)
20. Network Probe (Page 682)
21. WebSiteSniffer (Page 682)
22. ICQ Sniffer (Page 683)
23. MaaTec Network Analyzer (Page 683)
24. Alchemy Network Monitor (Page 683)
25. CommView (Page 683)
26. NetResident (Page 684)
27. Kismet (Page 684)
    a. wireless network detector, sniffer, and intrusion detection system
28. AIM Sniffer (Page 684)
29. NetworkMiner (Page 685)

c. Fundamentals of evidence reconstruction for investigating a crime 27:22- (Page 686)
    i. Temporal analysis
        1. It produces a sequential event trail, which sheds light on important factors such as what happened and who was involved
    ii. Relational analysis
        1. It correlates the actions of suspect and victim
    iii. Functional analysis
        1. It provides a description of the possible conditions of a crime
        2. It testifies to the events responsible for a crime in relation to their functionalities

8. Web Forensics

38. Web and database forensics Part 1

TOOLS Methodologies, Frameworks and Processes Term

a. Attacks on web applications
    i. SQL injection
    ii. cross-site scripting
    iii. session hijacking
    iv. local and remote file inclusions
    v. remote code execution
b. Web application forensics
    i. examination of web applications
    ii. its contents to trace back the attack
    iii. identify the origin of the attack
    iv. and determine how the attack was propagated
        1. along with the devices used
        2. and the persons involved to perform the attack
c. Web application architecture layers
    i. Clients or Users Layer (Page 697)
        1. **Web appliances, such as smartphones and PCs, which a user interacts with a web application deployed on a web server**
        2. External web services and web browsers
        3. Presentation layer
            a. Flash, Silverlight, and Java Script
    ii. Web Server Layer (Page 698)
        1. **components that parse the request (HTTP Request Parser) coming from the clients and forwards the response to them**
        2. holds all the business logics and databases that are responsible for building websites and store data in them
        3. In some cases, the users access the application through the presentation layer, which serves as an intermediary between the user and the Web Server
        4. This layer includes the user interface components.
        5. Proxy server, cache
        6. Authentication and login take place
        7. Resource handler and serlet container
        8. Firewall
    iii. Business Layer
        1. **Responsible for the core functioning of the system and includes business logic and applications, such as .NET**, .COM, COM+
        2. **Used by the developers to build websites according to the clients' requirements**
        3. This layer also holds a legacy application, an older system integrated as an internal or external component
        4. Data access is done at this layer
    iv. Database Layer

1. **Comprises of cloud services**
2. B2B layer that **holds all the commercial transactions and**
3. A Database **Server that supplies an organization's production data in a structured form**. Example: MS SQL Server, MySQL server, etc.

d. Challenges in Web Application Forensics
   i. forensic investigators must have good knowledge of various servers
   ii. Web applications are often business-critical,
   iii. difficult for the investigators to capture volatile data
   iv. Most of the web applications restrict access to HTTP information
   v. impossible for investigators to differentiate valid HTTP requests from malicious ones

e. Most common indications of a web attack (Page 700)
   i. Customers being unable to access services
   ii. Suspicious activities in user accounts
   iii. Leakage of sensitive data
   iv. Correct URLs redirecting to incorrect sites
   v. Web page defacements
   vi. Unusually slow network performance
   vii. Frequent rebooting of the server
   viii. Anomalies in log files
   ix. Error messages such as 500 errors, "internal server error," and "problem processing your request"

39. Web and database forensics Part 2, 3, and 4
    a. Web application threats (Page 700)
       i. Buffer Overflow
          1. **Occurs when the application fails to guard memory properly and allows writing beyond maximum size**
       ii. Cookie poisoning
          1. **Modification of a website's remnant data for bypassing security measures or gaining unauthorized information**
       iii. Insecure storage
          1. **Occurs when an attacker is allowed to gain access as a legitimate user to a web application or data such as account records, credit card numbers, passwords, or other authenticated information**
       iv. Information Leakage
          1. **Refers to a drawback in a web application where it unintentionally reveals sensitive data to an unauthorized user**
       v. Improper Error Handling
          1. **Arises when a web application is unable to handle technical issues properly and the website returns info, such as database dumps, stack traces, and codes**
       vi. Broken Account Management

1. **Refers to vulnerable management functions, including user updates, recovery of passwords, or resetting passwords**

vii. **Directory Traversal**
   1. **Occurs when attackers exploit HTTP, gain access to unauthorized directories, and execute commands outside the web server's root directory**

viii. **SQL Injection**
   1. **Occurs when attackers insert commands via input data nd are able to tamper with the data**

ix. **Parameter/Form Tampering**
   1. **Occurs when attackers intend to manipulate the communication exchanged between the client and server to make changes in application data**

x. **Denial of Service (DoS)**
   1. **Intended to terminate website or server operations by making resources unavailable to clients**

xi. Log Tampering

xii. **Unvalidated Input**
   1. **Occurs when attackers tamper with the URL, HTTP requests, headers, hidden fields, form fields, or query strings**

xiii. **Cross Site Scripting**
   1. **Occurs when attackers bypass the client's ID security mechanism, gain access privileges, and inject malicious scripts into specific fields in web pages**

xiv. **Injection Flaws**
   1. **Occurs when attackers insert malicious code commands, or scripts into the input gates of web applications, enabling the applications to interpret and run the newly supplies malicious input**

xv. **Cross Site Request Forgery**
   1. **Occurs when an authenticated user is forced to perform certain tasks on the web application chosen by the attacker**

xvi. **Broken Access Control**
   1. **Occurs when attackers identify a flaw, bypass authentication, and compromise the network**

xvii. Platform Exploits

xviii. Insecure Direct Object References

xix. Insufficient Transport Layer Protection

xx. SSL/TLS Downgrade Attack

xxi. Failure to Restrict URL Access

xxii. Cookie Snooping

xxiii. Obfuscation Application

xxiv. Demilitarized Zone (DMZ) Protocol Attacks

TOOLS Methodologies, Frameworks and Processes Term

xxv. Security Management Exploits
xxvi. Authentication Hijacking
xxvii. Network Access Attacks
xxviii. Web Services Attacks
xxix. Hidden Manipulation
xxx. Un validated Redirects and Forwards
xxxi. Session Fixation Attack
xxxii. CAPTCHA Attacks

40. Web and database forensics Part 5
    a. Investigating a Web Attack (page 704)
        i. The steps involved in an investigation of web attacks
        ii. Confirmation of the Attack and Identification of its Nature
        iii. Capturing Volatile Data
        iv. Taking Snapshot or Shutting down the System
        v. Making Forensic Image/Mounting Snapshot
        vi. Understanding the Flow of an Application
        vii. Analysis of the Log Files
        viii. Collection of Application and Server Configuration Files
        ix. Identification of Abnormal Activities
        x. Corroboration with Firewall and IDS Logs
        xi. Blocking the Attack
        xii. Tracing Back Attack IPs
        xiii. Full-proof Documentation (Page 706)
    b. Investigating web attacks in Windows-Based servers (Page 706)
        i. Run Event Viewer to look at the logs
            1. C:\> eventvwr.msc
            2. Check if the following suspicious events have occurred:
                a. Event log service ends
                b. Windows File Protection is inactive on the system
                c. The MS Telnet Service is running
            3. Find if the system has failed login attempts or locked-out accounts
        ii. Review file shares to ensure their purpose
            1. C:\> net view <IP Address>
        iii. Verify the users using open sessions
            1. C:\> net session
        iv. Check if the sessions have been opened with other systems
            1. C:\> net use
        v. Analyze at NetBIOS over TCP/IP activity
            1. C:\> nbtstat –S
        vi. Find if TCP and UDP ports have unusual listening (Page 707)
            1. C:\> netstat –na
        vii. Find scheduled and unscheduled tasks on the local host

TOOLS Methodologies, Frameworks and Processes Term

1. C:\> schtasks.exe

viii. Check for creation of new accounts in administrator group
1. C:\> lusrmgr.msc

ix. See if any unexpected processes are running in Task Manager
1. Start -> Run -> taskmgr -> OK

x. Look for unusual network services (Page 708)
1. C:\> net start

xi. Check file space usage to look for a sudden decrease in free space
1. C:\> dir

c. IIS Web server architecture
i. Visual Basic code application that lives on a Web server and responds to requests from the browser
ii. supports HTTP, HTTPS, FTP, FTPS, SMTP, and NNTP
iii. Components
1. Protocol listeners (HTTP.sys)
2. Web services like World Wide Web Publishing Service (WWW service
3. Windows Process Activation Service (WAS)
iv. Components responsibilities
1. Listening to the requests coming from the server
2. Managing processes
3. Reading configuration files

d. Web server log files have HTTP status codes specific to certain activities.

e. On Windows Server 2012, the log files are stored by default in the %SystemDrive%\inetpub\logs\LogFiles

f. IIS Time
i. Records logs using UTC
ii. The admin should verify the process IIS is set to roll over logs using the local time.
iii. The server's time zone setting can be verified by looking at the first entries in the log file. If the server is set to UTC -08:00, then the first log entries should appear around 16:00 (00:00 - 08:00 = 16:00)
iv. UTC does not follow daylight savings
v. The administrator must also consider the date. For example, UTC -8:00 will be -7:00 half the year.

g. IIS logs
i. Stored in ASCII format

h. The elements of the Apache core are: (Page 713)
i. http_protocol - responsible for managing the routines, which interacts with the client and takes care of all the data exchange and socket connections between the client and the server.
ii. http_main - handles the server startups and timeouts. It also consists of the main server loop that waits for the connections and accepts them.

iii. http_request - controls the step by step procedure involved between the modules to complete a client request and is also responsible for error handling.
iv. Alloc.c - handles allocation of resource pools.
v. http_config - responsible for reading and handling of the configuration files.
    1. One of the main tasks of http_config is that it arranges all the modules, which the server will call during various phases of the request handling.

41. Web and database forensics Part 6
    a. Apache Access log
        i. Requests processed by the Apache server
        ii. Format(Page 714)
            1. %h %l %u %t \"%r\" %>s %b is the common percent directive log format.
            2. EXAMPLE
                a. 10.10.10.10 - jason [17/Aug/2016:00:12:34 +0300] "GET /images/content/bg_body_1.jpg HTTP/1.0" 500 1458
            3. Where:
                a. %h represents the client's IP address 10.10.10.10
                b. %l represents the Remote log name. This will return a dash unless mod_ident is present and IdentityCheck is set on -
                c. %u is the client user ID jason
                d. %t represents the time when the server received the request. It is displayed in the format [day/month/year:hour:minute:second zone] [17/Aug/2016:00:12:34 +0300]
                e. \"%r\" indicates the methods used for a request-response between a client and server, the resource requested by a client (apache_pb.gif), and the protocol used (HTTP/1.0)
                f. %>s represents the status code which the server sends back to the client 500
                g. %b represents the size of the object which the server sends to the client 1458
        iii. The default location of access logs:
            1. RHEL/Red Hat/CentOS/Fedora Linux: /var/log/httpd/access_log
            2. Debian/Ubuntu Linux: /var/log/apache2/access.log
            3. FreeBSD Linux: /var/log/httpd-access.log
    b. Apache error logs
        i. Location where the server records all the errors that occurred during the client request processing
        ii. Example
            1. [Mon Sep 16 14:25:33.812856 2016] [core:error] [pid 12485:tid 8589745621] [client 10.10.255.14] File does not exist: /images/content/bg_body_1.jpg
            2. Where

a. Mon Sep 16 14:25:33.812856 2016 This is the first element in the log entry. It contains the timestamp (day, month, date, time, and year) of the log.
b. core:error The second element in the log describes the module producing the message. In this case, the Apache core is producing the message describing the security level (error).
c. pid 12485:tid 8589745621 The next element in the log contains the process ID and its corresponding thread ID.
d. client 10.10.255.14 The fourth element in the log is the client address that made the request.
e. File does not exist: /images/content/bg_body_1.jpg The final element in the log displays the status of the file,

iii. The default location of error logs:
1. RHEL/Red Hat/CentOS/Fedora Linux: /var/log/httpd/error_log
2. Debian/Ubuntu Linux: /var/log/apache2/error.log
3. FreeBSD: /var/log/httpd-error.log

c. Apache configuration file
i. find the exact location of the log files
ii. RHEL/Red Hat/CentOS/Fedora Linux: /usr/local/etc/apache22/httpd.conf
iii. Debian/Ubuntu Linux: /etc/apache2/apache2.conf
iv. FreeBSD: /etc/httpd/conf/httpd.conf

d. Web attack detections tools and log viewers
i. Deep Log Analyzer (Page 722)
1. Web analytics solution for small and medium size websites
ii. WebLog Expert (Page 723)
iii. Apache Logs Viewer (ALV) (Page 724)
iv. AWStats (Page 725)
v. Nagios Log Server (Page 725)
vi. Splunk (Page 725)
vii. Web Log Storming (Page 725)
viii. LogCruncher (Page 725)
ix. GoAccess (Page 725)
x. HTTP-ANALYZE (Page 725)
xi. Active LogView (Page 725)
xii. Webalizer (Page 725)

e. IP Address locating tools (Page 726)
i. SmartWhois
ii. ActiveWhois

f. WHOIS lookup tools
i. LanWhoIs (Page 728)
ii. Batch IP Converter
iii. CallerIP

TOOLS Methodologies, Frameworks and Processes Term

iv. Sobolsoft
v. WhoIs Analyzer Pro
vi. HotWhois
vii. ActiveWhois
viii. WhoisThisDomain
ix. SoftFuse Whois
x. Whois
xi. Domain Dossier (Page 729)
xii. BetterWhois
xiii. Whois Online
xiv. Web Wiz
xv. Network-Tools.com
xvi. Whois
xvii. DNSstuff
xviii. Network Solutions Whois
xix. WebToolHub
xx. UltraTools (Page 729)

9. Database Forensics

42. Database Forensics Part 1
    a. Databases
        i. Store the entire data pertaining to a web application and allow users to view, access, manage, and update the information
        ii. Act as the primary source of electronic evidence for every organization irrespective of its size and complexity
    b. MSSQL
        i. SQL server is a Relational Database Management System
        ii. This type of forensics takes action when a security incident has occurred and detection and analysis of the malicious activities performed by criminals over the SQL database file are required
    c. SQL Server databases have three types of files (Page 737)
        i. Primary data file (MDF)
            1. Startup point of the database
            2. Points to the other files in the database
            3. Stores all the data in the database objects
            4. Every database has one primary data file
        ii. Secondary data file (NDF)
            1. Optional
            2. Database can contain none or more than one
        iii. Transaction log files (LDF)
            1. **holds the log information** that is used to recover the database
            2. Must be at least one log file for each database

3. These are divided into smaller parts called virtual log files

d. Location of Files to Restore Evidence: Along with the volatile database data, Windows logs and Database plan cache, you can examine the following files to have an insight of the activities occurred on the database: (Page 739)
    i. Database & logs files:
        1. \Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\DATA*.MDF | *.LDF
    ii. Trace files:
        1. \Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\LOG\LOG_#.TRC
    iii. SQL Server error logs:
        1. \Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\LOG\ERRORLOG
e. Collecting Volatile Database data
    i. ApexSQL Audit Application
        1. View login history for a given date and time of a database
    ii. SQLCMD
        1. Can collect primary data file and active transaction logs
        2. sqlcmd -S WIN-CQQMK62867E -e -s"," –E
            a. Load and establish a connection with the server WIN-CQQMK62867E
        3. :out E:\ForensicTest.txt
            a. create a new text file with name ForensicTest and save the output to E drive:
        4. sp_helpdb
            a. outputs the information related to the specified database
f. SQL Server Management Studio (SSMS) (Page 743 & 751
    i. Integrated environment for accessing, configuring, managing, administering, and developing all components of SQL Server and Azure SQL Database
    ii. combines a group of graphical tools with script editors
    iii. fn_dblog(a,z)
        1. function allows you to retrieve the active portion of the transaction log file
    iv. fn_dump_dblog(a,z)
        1. function allows view of transaction logs
    v. Select * from ::fn_dblog(NULL, NULL)
        a. Displays the active portion of the transaction log file
        b. Values in the (a,z) are the start and end points
        c. Assigning NULL values implies that the start and end points for the log sequence numbers (LSNs) are not specified
    vi. DBCC LOG
        1. view and retrieve the active transaction log files for a specific database

vii. DBCC DBTABLE
    1. Returns the structure of the selected database table
viii. DBCC DBINFO
    1. Returns information related to the database metadata
ix. DBCC PROCBUF
    1. Returns the contents of the SQL Server Procedure Buffer.
    2. The buffer contains SQL Server cached executable statements such as stored procedures and SQL queries
x. DBCC BUFFER
    1. Returns the buffer headers and pages from SQL Server's buffer cache, where SQL Server stores results.
xi. DBCC SHOWFILESTATS
    1. Returns information related to the space occupied by the data files in the active database.
xii. DBCC PAGE
    1. Returns the data page structure of the selected database
xiii. Select * from sys.dm_exec_cached_plans cross apply sys.dm_exec_sql_text(plan_handle)
    1. Command to collect the database plan cache and retrieves the SQL text of all cached entries
    2. sys.dm_exec_cached_plans returns a row for each query plan that the SQL server had cached to speed up query execution
    3. This dynamic management view will help users to find cached query plans, cached query text, the amount of memory taken by cached plans, and the reuse count of the cached plans.
    4. plan_handle uniquely identifies a query plan for a batch that the server had cached or is currently executing
xiv. https://docs.microsoft.com/en-us/sql/relational-databases/system-dynamic-management-views/sys-dm-exec-cached-plans-transact-sql

43. Database Forensics Part 2
    a. Collecting SQL Server Trace Files
        i. C:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\LOG
        ii. Record all events occurred on a SQL server and the host databases
        iii. .trc files
        iv. View with SQL Server Profiler
    b. Collecting SQL Server Error Logs
        i. record user-defined events and specific system events
        ii. contain the IP Address of SQL Server client connections
        iii. C:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\LOG
    c. Other database management and monitoring tools
        i. SQLite Database Browser (Page 751)
        ii. Adminer (Page 751)

TOOLS Methodologies, Frameworks and Processes Term

d. Methodology for Database Forensics Using SQL Server Management Studio (SSMS)

i. Examine Windows Logs (Page 752)
    1. to obtain info related to SQL Server authentication, startup and shutdown instances, and the IP addresses of client connections

ii. Examine Error Logs
    1. to see the record of user defined events such as user logins

iii. Examine Trace Files (Page 753)
    1. Navigate to C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\LOG
    2. Open log_n.trc file in a SQL Server Profiler
    3. Examine for suspicious activity
    4. Make a note of the SPID and the start time of the instance

iv. Examine Active Transaction Logs
    1. Launch SQL Server Management Studio and connect to the SQL Server
    2. Execute the command dbcc log(a, z) in the query window to view the transaction log file
    3. Convert hexadecimal value of the page ID to decimal
        a. locate the page containing the updated record

v. Examine Data Page (Page 755)
    1. find the object ID where the data has been modified
    2. Execute the commands: dbcc traceon()dbcc page()
    3. Note down the Object ID

vi. View the Object(s) that have been modified (Page 756)
    1. use the object ID to find the name of the object/table in the database
    2. Execute the command Select * from sysobjects where id = [metadata ObjectId]

vii. Gather the Object Schema (Page 757)
    1. use the object ID, collect the object schema (table) associated with the User_Profile
    2. Execute the command: SELECT sc.colorder , sc.name, st.name as 'datatype', sc.length FROM syscolumns sc, systypes st WHERE sc.xusertype = st.xusertype and sc.id = [metadata ObjectId] ORDER BY colorder

viii. View the Modified Record
    1. issue the commands dbcc trace () and dbcc page()

ix. Identify the Data Type (Page 758)
    1. Using slot ID and row offset , which were obtained previously from the transaction log, the specific point within the data row was identified in which the transaction began

x. Compare the Row Logs (Page 759)
    1. Note down the hex values of RowLog Contents 0 and RowLog Contents 1 and convert them to their equivalent decimal values

e. Methodology for Database Forensics Using ApexSQL Audit
    i. Collect volatile database data using Logon activity history (Page 760)
    ii. Collect volatile database data from the Security configuration history (Page 761)
    iii. Examine the Database Transaction Log File by connecting to the db (Page 763)
    iv. Examine the Database Transaction Log File by selecting the log file (Page 764)
    v. Examine the Database Transaction Log File by outputting the results (Page 765)
    vi. Examine the Database Transaction Log File by configuring the options (Page 766)
    vii. Examine the Database Transaction Log File by displaying the transactions (Page 767)
f. MySQL (Page 768)
    i. Open source relational database
    ii. Data is duplicated and stored in multiple locations
    iii. Any users deleting data in the database will not completely delete the data
    iv. Can examine all the files containing a copy of the deleted data and recover it
    v. Database structure depends on the storage engine (Page 792)
        1. MyISAM
        2. InnoDB
    vi. Tiered architecture
        1. SQL Interface layer accepts the SQL statements and delivers the result
        2. Parser validates the SQL queries entered by a user.
        3. Optimizer validates the tables, and the level of access for a user
        4. Caches and Buffers ensure that commonly used data are made available
        5. Storage engines create, read, and update data within a database
    vii. Data directory (Page 772)
        1. Stores all databases, status and log files, along with the data managed by the server
        2. C:\ProgramData\MySQL\MySQL Server 5.n\ in Windows based machines.
        3. Databases are stored as folders in the data directory
            a. The files within these folders (databases) correspond to the tables, views, and triggers within that database
        4. Organized in tree-like structures by following the hierarchical structure of the Unix or Windows file systems:
            a. Every database corresponds to a directory under the data directory
            b. The tables of a database, correspond to the files of the database directory
        5. Contains the auto.cnf file containing the server_uuid which is used to uniquely identify a server.
        6. Status and log files stored in data directory

a. Status and log files generated by the server, which store information related to the operations performed on the server. These files include:
b. Process ID file (HOSTNAME.pid), contains the process ID created when the server starts
c. Error log (HOSTNAME.err), contains the information associated with the startup and shutdown events, and errors
d. General query log (HOSTNAME.log), logs the client connections and activities
e. Binary log (HOSTNAME-bin.nnnnnn), contains the events that describe the changes occurred in the database
f. Binary log index (HOSTNAME-bin.index), contains the list of all the binary log files currently available in the data directory
g. Relay log (HOSTNAMErelay-bin.n), contains the events that describe the changes occurred in the database
h. Relay log index (HOSTNAMErelay-bin.index), contains the list of all the relay log files currently available in the data directory
i. Master info file (master.info) created by a replication slave server, that contains the essential parameters used for connecting to the master slave
j. Relay log info file (relay-log.info) created by a replication slave server, that contains the status of relay log processing
k. Slow query log (HOSTNAMEslow.log), a text file that contains statements which take longer processing time

viii. The InnoDB storage engine contains two types of logs:
    1. Undo logs, help you to roll back the transactions
    2. Redo logs, help you to re-execute the transactions (ib_logfile0 and ib_logfile1)
ix. Ibdata1, stores InnoDB's permanent table records
    1. https://dev.mysql.com/doc/refman/5.7/en/innodb-storage-engine.html
x. MySQL Utility Programs for Forensic Analysis (Page 775)
    1. **Mysqldump**
        a. **Command line utility used to take a backup of the database**
    2. Mysqlaccess
        a. Checks and validates the access privileges
    3. Myisamlog
        a. Processes the contents of MyISAM log file and perform recovery operation, display version information, etc., depending on the situation
    4. Myisamchk
        a. Views, checks, repairs, or optimizes the MyISAM table
    5. Mysqlbinlog

TOOLS Methodologies, Frameworks and Processes Term

a. Reads the binary log files and displays them in text format

6. **mysqldbexport** (Page 776)
    a. **used to export metadata or data, or both from one of more databases**

10. Cloud Forensics

44. Cloud Forensics Part 1
    a. Cloud computing (Page 796)
        i. on-demand delivery of IT capabilities in which IT infrastructure and applications are provided to subscribers as metered services over network
    b. NIST SP 800-145
        i. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
    c. Characteristics of Clouds (Page 796)
        i. On-Demand Self Service
            1. Allow provisions for cloud resources such as computing power, storage, network, and so on, always on demand, without the need for human interaction with service providers.
        ii. Distributed storage
        iii. Automated management
        iv. Broad Network Access
        v. Resource Pooling
        vi. Rapid Elasticity
        vii. Measured Service
        viii. Virtualization technology (Page 797)
    d. Limitation of Cloud computing (Page 797)
        i. Limited control and flexibility
        ii. Prone to outages and other technical issues
        iii. Security, privacy, and compliance issues
        iv. Contracts and lock-ins
        v. Depends on network connections
    e. 3 Cloud Service Models
        i. IaaS – Infrastructure-as-a-Service
            1. enables subscribers to use fundamental IT resources such as computing power, virtualization, data storage, network, and so on, on demand
            2. CSPs are responsible for managing the underlying cloud-computing infrastructure
            3. Provides virtual machines, hardware, and operating systems which may be controlled through a service API.
        ii. PaaS – Platform-as-a-Service (Page 798)
            1. Offers a platform for the development of applications and services

2. Subscribers need not buy and manage the software and infrastructure underneath it but have authority over deployed applications and perhaps application hosting environment configurations

iii. **SaaS – Software-as-a-Service** (Page 799)

1. **offers application software to subscribers' on-demand, over the Internet.**

f. 4 Cloud Deployment Models

i. **Public** (Page 802)

1. **provider makes services such as applications, servers, and data storage available to the public over the Internet**
2. provider is liable for the creation and constant maintenance of the public cloud and its IT resources
3. Advantages
    a. Simplicity and efficiency
    b. Low cost
    c. Reduced time
    d. No maintenance
    e. No Contracts
4. Disadvantages
    a. Security is not guaranteed
    b. Lack of control
    c. Slow speed

ii. **Private** (Page 800)

1. **AKA internal or corporate cloud**
2. **cloud infrastructure that a single organization operates solely**
3. Advantage
    a. Enhance security
    b. More control over resources
    c. Greater performance
    d. Customizable hardware, network, and storage performances
    e. Sarbanes-Oxley, PCI DSS, and HIPAA compliance data are much easier to attain
4. Disadvantage
    a. Expensive
    b. On-site maintenance

iii. **Hybrid** (page 801)

1. **comprised of two or more clouds**
2. Advantages
    a. More scalable
    b. Offers both secure resources and scalable public resources
    c. High level of security
    d. Allows to reduce and manage the cost as per the requirement

3. Disadvantages
    a. Communication at the network level may differ as it uses both public and private clouds
    b. Difficult to achieve data compliance
    c. Organization has to rely on the internal IT infrastructure for support to handle any outages
    d. Complex Service Level Agreements

iv. **Community** (Page 801)

1. **Multi-tenant infrastructure shared among organizations from a specific community with common computing concerns such as security, regulatory compliance, performance requirements, and jurisdiction**
2. Advantages
    a. Less expensive compared to the private cloud
    b. Flexibility to meet the community's needs
    c. Compliance with legal regulations
    d. High scalability
    e. Organizations can share a pool of resources and from anywhere via the Internet
3. Disadvantages
    a. Competition between consumers in usage of resources
    b. No accurate prediction on required resources
    c. Who is the legal entity in case of liability?
    d. Moderate security
    e. Trust and security concern between the tenants

g. Cloud computing threats

i. Data Breach/Loss (Page 802)
    1. Illegal access to the data

ii. Abuse of Cloud Services (Page 803)
    1. weak registration systems in the cloud-computing environment

iii. Insecure Interfaces and APIs
    1. risks include circumvention of user defined policies

iv. Insufficient Due Diligence
    1. Ignorance of CSP's cloud environment

v. Shared Technology Issues
    1. Rutkowska's Red and Blue Pill exploits
    2. Kortchinsky's CloudBurst presentations

vi. Unknown risk profile
    1. Unable to have a clear picture of internal security practices

vii. Inadequate Infrastructure Design and Planning (Page 804)
    1. shortage of computing resources and/or poor network design

viii. Conflicts between Client Hardening Procedures and Cloud Environment

TOOLS Methodologies, Frameworks and Processes Term

1. customers' security requirements are likely to diverge from one another

ix. Loss of Operational Security Logs
    1. Loss of security logs may occur in case of under-provisioning of storage
x. Malicious Insiders
    1. Malicious insiders could compromise organization's information
xi. Illegal Access to the Cloud
    1. Weak authentication and authorization controls
xii. Privilege Escalation (Page 804)
    1. A mistake in the access allocation systems
xiii. Loss of Business Reputation due to Co-Tenant Activities (Page 805)
    1. Lack of resource isolation, lack of reputational confinement, etc.
xiv. Natural Disasters
    1. Based on geographic location and climate
xv. Hardware Failure
    1. failure of switches, servers, routers, APs, hdd, network cards, and CPUs
xvi. Supply Chain Failure
    1. Cloud providers outsource certain tasks to third parties
xvii. Modifying Network Traffic
    1. user provisioning and de-provisioning vulnerabilities may alter traffic
xviii. Isolation Failure (Page 805)
    1. Lacking isolation of storage, memory, routing, and reputation
xix. Cloud Provider Acquisition Countermeasure (Page 806)
    1. Acquisition of the cloud provider
xx. Management Interface Compromise Countermeasures
    1. Customer management interfaces are accessible via the Internet
xxi. Network Management Failure Countermeasures
    1. Poor network management leads to network congestion, etc.
xxii. Authentication Attacks Countermeasures
    1. Weak authentication mechanisms and inherent limitations of 1FA
xxiii. VM-Level Attacks
    1. vulnerabilities in the hypervisors
xxiv. Lock-in
    1. Unable to shift from one cloud service provider to another or in-house
xxv. Licensing Risks
    1. Huge fees if the CSP charges for software on a per-instance basis
xxvi. Loss of Governance (Page 806)
    1. CSPs have more control over security issues compared to the customers
xxvii. Loss of Encryption Keys (Page 807)
    1. poor management of keys and poor key generation techniques
xxviii. Risks from Changes of Jurisdiction (Page 807)
    1. Cloud service provider may have cloud databases in multiple locations
xxix. Undertaking Malicious Probes or Scans (Page 807)

TOOLS Methodologies, Frameworks and Processes Term

1. allows attackers to collect sensitive information

xxx. Theft of Computer Equipment (Page 807)
1. Results from poor controls on physical parameters

xxxi. Cloud Service Termination or Failure (Page 807)
1. Termination of cloud service because of non-profitability, etc

xxxii. Subpoena and E-Discovery (Page 807)
1. data and services are subpoenaed from authorities or third parties

xxxiii. Improper Data Handling and Disposal
1. Limited access makes it hard to determine data handling

xxxiv. Loss/Modification of Backup Data
1. Lack of data restoration procedures in case of data loss

xxxv. Compliance Risks (Page 808)
1. Lack of governance over audits and industry standard assessments.

xxxvi. Economic Denial of Service (EDoS) (Page 808)
1. Account holder has to pay for resources used from malicious code

45. Cloud Forensics Part 2
    a. Cloud Computing Attacks (Page 808)
        i. Service Hijacking using Social Engineering Attacks (Page 808)
            1. An attacker steals CSP's or client's credentials and gains access to the cloud computing services.
            2. Attackers might target cloud service providers to reset passwords, or IT staff to access their cloud services to reveal passwords.
        ii. Session Hijacking using XSS Attack (Page 809)
            1. An attacker implements cross-site scripting (XSS) to steal cookies used in user authentication process thereby gaining unauthorized access
            2. Attacker can also predict or sniff session IDs.
            3. The attacker hosts a web page with the malicious script onto the cloud server. When the user views the page hosted by the attacker, the HTML containing malicious script runs on the user's browser. The malicious script will collect browser cookies and redirects the user to the attacker's server; it also sends the request with the collected cookies.
        iii. Domain Name System (DNS) Attacks (Page 809)
            1. The attacker directs users to a fake website to gather the authentication credentials.
            2. Here, the user queries the internal DNS server for DNS information. The internal DNS server then queries the respective cloud server for DNS information. At this point, attacker blocks the DNS response from the cloud server and sends DNS response with IP of a fake website to the internal DNS server. Thus, the internal DNS server cache updates itself with the IP of fake website and automatically directs the user to the fake website.
            3. Types of DNS Attacks

a. DNS Poisoning: Involves diverting users to a spoofed website by poisoning the DNS server or the DNS cache on the user's system
b. Cybersquatting: Involves conducting phishing scams by registering a domain name that is similar to a CSP
c. Domain Hijacking: Involves stealing a CSP's domain name
d. Domain Snipping: Involves registering an elapsed domain name

iv. SQL Injection Attacks (Page 809)
    1. Attackers insert malicious code (generated using special characters) into standard SQL code to gain unauthorized access to a database and ultimately to other confidential information.
    2. Attackers can manipulate the database contents, retrieve sensitive data, remotely execute system commands, or even take control of the web server for further criminal activities
v. Wrapping Attacks (Page 810)
    1. When users send a request from their VM through a browser, the request first reaches a web server, which generates a SOAP message containing structural information, which it will exchange with the browser during message passing. Before message passing occurs, the browser needs to sign the XML document and authorize it. In addition, it should append the signature values to the document. Finally, the Simple Object Access Protocol (SOAP) header should contain all the necessary information for the destination after computation.
    2. For a wrapping attack, the adversary does its deception during the translation of the SOAP message in the TLS (transport layer service) layer. The attacker duplicates the body of the message and sends it to the server as a legitimate user. The server checks the authentication by the Signature Value (which is also duplicated) and checks its integrity. As a result, the adversary can intrude in the cloud and can run malicious code to interrupt the normal functioning of the cloud servers.
vi. Service Hijacking using Network Sniffing (Page 810)
    1. Interception and monitoring of network traffic sent between two cloud nodes to capture sensitive data such as passwords, session cookies, and other web-based services security configuration such as the UDDI (Universal Description Discovery and Integrity), SOAP, and WSDL (Web Service Description Language) files
vii. Session Hijacking using Session Riding
    1. cross-site request forgeries to transmit unauthorized commands. In session riding, attackers "ride" an active computer session by sending an email or tricking users to visit a malicious web page, during login, to an actual target site. When the user clicks the malicious link, the website executes the request as if the user had already authenticated it.

Commands used include modifying or deleting user data, performing online transactions, resetting passwords, and others.

viii. Side Channel Attacks or Cross-guest VM Breaches (Page 810)
    1. Attackers run VMs on the same physical host of the victims' VM and take advantage of shared physical resources (processor cache) to launch side- channel attacks (timing attack) to extract cryptographic keys/plain text secrets to steal the victim's credentials. The attackers then use the stolen credentials to impersonate the victim.

ix. Cryptanalysis Attacks
    1. Insecure or obsolete encryption or Critical flaws in cryptographic algorithm implementations might turn strong encryption to weak or broken; also there exist novel methods to break the cryptography.
    2. Attackers can obtain partial information from encrypted data by monitoring clients' query access patterns and analyzing accessed positions.

x. DoS and DDoS Attacks
    1. If attackers gain access to the cloud, they generate fake data requests or a type of code that can run applications of legitimate users.
    2. Malware requests consume server's CPU, memory, and all other devices
    3. Once the server reaches its threshold limit, it starts offloading its jobs to another server. The same happens to other inline servers, and finally, the attackers will succeed in engaging the whole cloud system just by interfering the usual processing of one server.
    4. A DDoS attack involves a multitude of compromised systems attacking a single target, thereby causing the denial of service for users of the targeted system.

b. Cloud Crime (Page 813)
    i. Any criminal activity that involves a cloud environment
    ii. Cloud as a subject
        1. When attackers try to compromise the security of a cloud environment to steal data or inject malware
    iii. Cloud as an object
        1. When attackers uses the cloud to commit a crime against the CSP
        2. In this case, the main aim of the attacker is to impact cloud service provider rather than cloud environment
    iv. Cloud as a tool
        1. When attackers uses a compromised cloud account to attack other
        2. In such cases, both source and target cloud can store the evidence data

c. Cloud Forensics stakeholders (Page 819)
    i. IT Professionals
        1. professionals responsible for managing and maintaining all aspects of the cloud

ii. **Investigators**
    1. **Responsible for conducting forensic examinations against allegations made**
    2. Work in collaboration with the external investigators, law enforcement agencies for forensic investigations on the internal assets
iii. **Incident Handlers**
    1. **First responders for all the security incidents taking place on a cloud**
    2. First line of defense against cloud security attacks
    3. Primary role is to respond against any type of security incident
iv. **Law Advisors**
    1. **Make sure all forensic activities are within the jurisdiction and not violating any regulations or agreements**
v. External Assistance
    1. Used to perform any task apart from the ones which they have already performed, such as investigation of civil cases, e-discovery, etc.

46. Cloud Forensics Part 3
    a. Cloud Forensic Challenges (Page 820)
        i. Architecture and identification
            1. Deletion of data
            2. Recovering overwritten data (Page 821)
            3. Interoperability of CSP's
            4. Single Point of Failures (SPOF)
            5. No single point of failure for criminals
            6. Detection of malicious activity
            7. Criminals access to low cost computing power
            8. Real-time investigation not always possible
            9. Malicious code may break VM isolation
            10. Multiple locations for data
            11. Lack of transparency (Page 821)
            12. Criminals can hid in cloud (Page 822)
            13. Confiscation and resource seizure in multi-tenant environments
            14. Errors in management portal configuration
            15. Evidence segregation in multi-tenant environments
            16. Boundaries
            17. Secure provenance
            18. Evidence chain of custody (Page 822)
        ii. Data collection
            1. Decreased access and data control (Page 823)
            2. Chain of dependencies
            3. Locating evidence
            4. Data location
            5. Imaging and isolating data

6. Data availability
7. Locating storage media
8. Evidence identification (Page 823)
9. Dynamic storage (Page 824)
10. Live forensics
11. Imaging the cloud
12. Resource abstraction
13. Application details are not available (Page 824)
14. Additional collection is often infeasible in the cloud
15. Selective data acquisition
16. Cryptographic Key Management
17. Ambiguous trust boundaries (Page 824)
18. Data integrity and evidence preservation (Page 824)
19. Root of Trust (Page 825)

iii. Logs
1. Decentralization and evaporation of Logs (Page 825)
2. Multiple layers and tiers
3. Less evidently value of logs (Page 825)

iv. Legal
1. Missing terms in contract or SLA (Page 826)
2. Limited investigative power
3. Reliance on cloud providers
4. Physical data location
5. Port protection
6. Lack of international cloud services
7. Jurisdiction
8. International communication (Page 826)
9. Confidential Personally identifiable information (PII) (Page 827)
10. Reputation fate sharing (Page 827)

v. Analysis
1. Evidence correlation (Page 827)
2. Reconstructing virtual storage
3. Timestamp synchronization
4. Log format unification
5. Use of metadata (Page 827)
6. Log capture (Page 828)

vi. Role management
1. Identifying account ownership (Page 828)
2. Fictitious identities
3. Decoupling user credentials and physical location
4. Authentication and Access Control (Page 828)

vii. Standards

1. Testability, validation, and scientific principles not addressed (Page 829)
2. Lack of standard processes and models

viii. Training / Competence of CSP provider staff

47. Cloud Forensics Part 4
    a. Cloud storage services such as Dropbox, Google Drive, SkyDrive, iCloud, etc. create artifacts on a system they are installed upon that may provide relevant information to investigation. Some of the artifacts that you have to look at during cloud storage service investigation include:
        i. Artifacts created during the installation process
        ii. Artifacts left behind after the uninstallation process
        iii. Information present in the database files
        iv. Artifacts created when a file is uploaded or downloaded
        v. Artifacts left when a file is shared
        vi. Artifacts left behind after using anti-forensics software
        vii. Logs recorded and their accuracy
    b. DROPBOX
        i. feature called extended version history (EVH)
            1. saves all the deleted and previous versions of the files by default.
            2. two versions
                a. Free version will store deleted files for 30 days
                b. Pro version can access any version at any given time
            3. can view version history of each file and recover previous versions
            4. Steps to retrieve a deleted file from Dropbox (Page 832)
                a. Login into the web based application
                b. Select the Files option from the right side menu list
                c. Right-click over the file from the provided list
                d. Select Previous versions from the drop-down menu
                e. site will be redirected to the version history page of the selected file, which contains details of all the previous versions
                f. Select a version from the list and click the Restore button
        ii. Atrifacts left by Dropbox
            1. By default in Windows 10, the Dropbox client is installed at
                a. C:\Program Files (x86)\Dropbox
            2. The default folder used for syncing files is
                a. C:\Users\<username>\Dropbox
                b. contains all files uploaded or downloaded from the cloud
        iii. Tools
            1. WhatChanged Portable (Page 835)
                a. Scans for modified files and registry entries.
                b. First, take a snapshot to get the current state of the computer before installing Dropbox client;

    c. Second, run it again to check the differences since the previous snapshot, after installing Dropbox client.
    d. By comparing both screen shots, investigators can find out the list files modified in the registry and entries made to the registry
2. Magnet IEF (Page 838)
    a. processes the forensic image, or file dump and extracts the meaningful data for each supported artifact type
    b. Can recover artifacts from unallocated space by extracting data from the files that are not sequential, out of order, or missing entirely
3. DiskPulse (Page 840)
    a. disk change monitoring solution
    b. monitor changes in directories
    c. send E-Mail notifications
    d. save various types of reports
    e. generate statistical pie charts
    f. Export detected changes to an SQL database
    g. Send error messages to the system event log
    h. Execute custom commands when a user-specified number of changes detected
    i. Intercepts file system change notifications issued by the operating system and detects newly created files, modified files, deleted files and renamed files
    j. All file system changes are detected in real-time
4. Directory Monitor (Page 841)
    a. Used for surveillance of certain directories and network shares
    b. Will notify the investigator of file changes/access, deletions, modifications, and new files in real-time.
    c. Users and processes making the changes can also be detected.
    d. Provides text logs, automation via script/application execution, emailing, writing to a database, sound notifications, etc.
    e. Enable snapshots to ensure changes can be detected while the network is down and even during power outages
5. Ram Capturer (Page 842)
    a. Used to dump the RAM contents
    b. use a hex editor tool to analyze the captured RAM contents
6. HXD (Page 843)
    a. hex editor
    b. edit the raw binary content of a file or a disk of any size
    c. searching, replacing, exporting, checksums/ digests, insertion of byte patterns
    d. a file shredder

TOOLS Methodologies, Frameworks and Processes Term

e. concatenation or splitting of files
f. statistics
g. analyze malware
h. patch programmers
i. repair hard drive tables
j. perform file comparisons
k. track the logged in credentials of the required Dropbox account by searching the RAM dump using the string AUTHENTICATE and the logged in user's name can be obtained using the string DISPLAYNAME
l. trace the path of filecache.dbx by searching the RAM dump using hex editor with the string filecache.dbx
m. use the string server_time to trace the server time of a particular instance
n. Use string UPDATED/DELETED to find updated and deleted files
o. Find logged in Dropbox credentials of a web-based application by exploring RAM dump using strings login_email for the user's email ID and login_password for the password of the account

7. WebBrowserPassView (Page 845)
   a. http://www.nirsoft.net
   b. Password recovery tool for passwords stored in Internet Explorer (Version 4.0 - 11.0), Mozilla Firefox, Google Chrome, Safari, and Opera

iv. Registry keys created by Dropbox installation
1. HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules
2. HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\DropboxExt(n)
3. HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox
4. HKLM\SOFTWARE\Classes\DropboxUpdate.ProcessLauncher
5. HKLM\SOFTWARE\Dropbox\InstallPath
6. HKLM\SOFTWARE\Dropbox\Client\Version

v. config.db (Page 838)
1. Path-C:\Users\<Username>\AppData\Local\Dropbox\instance(n)
2. Contains info about local Dropbox installation and account
3. Lists the email IDs linked with the account, current version/build for the local application, the host_id, and local path information "config.dbx" is an encrypted variant of "config.db"

vi. filecache.db
1. Path -C:\Users\<Username>\AppData\Local\Dropbox\instance(n)
2. Consists of several columns of which, "file_journal" is important

a. Contains a list of all directories and files inside “Dropbox”. It appears as if they are existing files, not deleted ones.

vii. sigstore.db
1. Path -C:\Users\<Username>\AppData\Local\Dropbox\instance(n)
2. Records SHA-256 hash and each file’s size information

viii. host.db
1. Path -C:\Users\<Username>\AppDataLocal\Dropbox
2. Plain text file containing hash value(s) of usernames

ix. unlink.db
1. Path -C: \Users\<Username>\AppData\Local\Dropbox
2. binary/database file.

x. dropbox.cache
1. Path -C:\Users\<Username>\Dropbox
2. A hidden directory located at the root Dropbox folder that is used as a staging area for downloading and uploading files

c. Google Drive (Page 846)

i. By default the Google Drive client is installed at
1. C:\Program Files (x86)\Google\Drive

ii. The default folder used for syncing files is
1. C:\Users\<username>\Google Drive

iii. Configuration files are saved inside the installation folder in the user profile
1. C:\Us ers \<username>\AppData\Local\Google\Drive\us er_default

iv. Executable and libraries are stored at (Page 852)
1. C:\Program Files (x86)\Google\Drive

v. Files created during Google Drive client installation
1. C:\Users\<username>\Desktop\Google Drive.lnk
2. C:\Users\<username>\Links\Google Drive.lnk
3. C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Google Drive\Google Drive.lnk

vi. The Google Drive installation creates various keys and values inside the registry:
1. HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders
2. HKCU\SOFTWARE\Google\Drive
3. HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\GoogleDriveSync
4. HKCU\SOFTWARE\Classes

vii. Sync_config.db (Page 854)
1. Database file for the Google Drive Client
2. C:\Users\<Username>\AppData\Local\Google\Drive\user_default
3. Contains several records including
a. Google Drive version
b. local sync root path

c. user's email address.

viii. You can read the database files using the DB Browser for SQLite tools to extract the required information and also use the file to recreate the databases and search them for the data.

d. Tools

i. UFED Cloud Analyzer (Page 866)

1. Collects both existing cloud data and metadata and packages it in a forensically sound manner.
2. Extraction, preservation, and analysis of private social media accounts

11. Malware Forensics

48. Malware Forensics Part 1

a. Malware (Page 870)

i. Malicious software

b. Types of Malware 16:20- (Page 870)

i. Backdoor
ii. Rootkit
iii. Botnet
iv. Scareware
v. Downloader
vi. Spam-sending malware
vii. Launcher
viii. Worm or virus
ix. Trojans
x. Adware
xi. Spyware
xii. Credential-stealing program

c. Ways malware can get info a system (Page 871)

i. Instant Messenger Applications
ii. Internet Relay Chat
iii. Removable Devices
iv. E-mail and Attachments (Page 872)
v. Browser and Software Bugs
vi. File Downloads
vii. Network File Sharing (Using NetBIOS) (Page 873)
viii. Bluetooth and wireless networks

d. Ways to distribute malware across the Web (Page 873)

i. Blackhat Search Engine Optimization (SEO)

1. uses aggressive SEO tactics such as keyword stuffing, doorway pages, page swapping, and adding unrelated keywords in an effort to get higher search engine ranking for their malware pages

ii. Social Engineered **Click-jacking**

TOOLS Methodologies, Frameworks and Processes Term

1. Attackers **inject malware into legitimate- looking websites to trick users into clicking them**
2. When clicked, the malware embedded in the link executes without the knowledge or consent of the user

iii. Spearphishing Sites

1. Attacker mimicks legitimate institutions, such as banks, in an attempt to steal passwords, credit card and bank account data, and information

iv. Malvertising

1. Involves embedding malware-laden advertisements in authentic online advertising channels to spread malware

v. Compromised Legitimate Websites

1. When an unsuspecting user visits the compromised website, the malware secretly installs itself on the user's system and thereafter carries out malicious activities.

vi. Drive-by Downloads

1. The unintentional downloading of software via the Internet.
2. **Attackers exploit flaws in browser software to install malware just merely by visiting a web site**

49. Malware Forensics Part 2
    a. Components of Malware (Page 873)
        i. Crypter
            1. Program that can conceal existence of malware
            2. Used to elude antivirus detection.
            3. Encrypts the malicious file or complete malware itself to avoid detection
        ii. Downloader (Page 874)
            1. Type of Trojan that downloads other malicious code and files from the Internet on to the PC
            2. Attackers install the downloader when they first gain access to a system
        iii. Dropper
            1. Install the malware code covertly on the system to make it run
            2. Can contain unidentifiable code that antivirus scanners cannot detect
            3. Capable of downloading additional files needed to execute the malware on a target system
        iv. Exploit
            1. Part of the malware that contains code or sequence of commands that can take advantage of a bug or vulnerability in a system or device
            2. The code attackers use to breach the system's security through software vulnerabilities
        v. Injector

1. Program that injects the malicious code in the malware into other vulnerable running processes and changes the way of execution to hide or prevent its removal

vi. Obfuscator
1. A program to conceal the malicious code of malware making it hard for security mechanisms to detect or remove it

vii. Packer
1. Software that uses compression techniques to convert malware into an unreadable format

viii. Payload
1. Part of the malware that performs desired activity when activated.

ix. Malicious Code
1. Code that defines basic functionality of the malware

b. Tools to extract patterns from malicious files
i. Balbuzard (Page 875)
ii. Cryptam Malware Document Detection Suite (Page 875)

c. Two types of malware analysis
i. Static analysis
1. Basic analysis of the binary code and comprehension of the malware that explains its functions, **without running or executing the code**
2. Process of looking for known traces and values (malicious code, strings, executables, etc.) that represent presence of malware
3. Techniques include:
a. File fingerprinting (Page 880)
i. calculation of cryptographic hashes of the binary code to recognize its function and compare it to other binary codes
1. Tools
a. HashMyFiles (Page 881)
b. Local and Online malware scanning
i. calculates hash values of a suspect file and compare them to online and offline malware databases
c. Performing strings search
i. some strings are commands for performing specific functions
ii. Tools to extract all types of strings from executable files
1. Strings (Page 885)
2. ResourcesExtract (Page 885)
3. Bintext (Page 885)
4. Hex Workshop (Page 885)
d. Identifying packing/obfuscation methods

TOOLS Methodologies, Frameworks and Processes Term

i. find if the file includes packed elements and also locate the tool or method used for packing it
ii. Finding the packer will ease the task of selecting a tool for unpacking the code
iii. Tools to find if files have packed programs or obfuscated code
1. PEid (Page 886)
a. Displays
i. type of packers used
ii. entry point
iii. file offset
iv. EP Section and subsystem used

e. Finding the portable executables (PE) information (Page 881)
i. PE stores metadata about the program
ii. PE of the files contains (Page 886)
1. .text: instructions and program codes that the CPU executes
2. .rdata the import and export info as well as other read-only data used by the program
3. .data the program's global data, which the system can access from anywhere
4. .rsrc the resources employed by the executable, such as icons, images, menus, and strings
iii. PE analysis tools
1. PEview (Page 886)
2. PE Explorer (Page 886)
3. PEBrowse Professional (Page 886)

f. Identifying file dependencies
i. Find the libraries and file dependencies, as they contain info about the run-time requirements of an application
ii. Investigators should look for (Page 888)
1. dlls with different names or
2. misspelled dlls or
3. functions of the dlls to identify malicious dlls
iii. Most common dlls (Page 888)
1. Kernel32.dll
2. Advapi32.dll
3. User32.dll
4. Gdi32.dll
5. Ntdll.dll
6. WSock32.dll
7. Ws2_32.dll

TOOLS Methodologies, Frameworks and Processes Term

8. Wininet.dll

iv. Tools to identify file dependencies

1. Dependency Walker (Page 888)
    a. lists all the dependent modules
    b. builds a hierarchical tree diagram
    c. records all the functions each module exports and calls

g. Malware disassembly and analysis
    i. dismantling of a given executable into binary format to study its functionalities and features
    ii. find the language used for programming the malware, look for APIs that reveal its function, etc
    iii. Use debugging tools
        1. OllyDbg
        2. IDAPro (Page 889)
            a. disassembler and debugger
            b. explores binary programs, for which source code isn't always available, to create maps of their execution
            c. displays the internals of the file such as
                i. IDA view
                ii. hex view
                iii. enumerations
                iv. imports and exports,
                v. subroutines and their paths,
                vi. functions that call a subroutine

ii. Dynamic or behavior analysis

1. Scanning the behavior of the software program while running it in a controlled environment
2. Study of malware behavior during installation, on execution and while running
3. Steps
    a. Baseline the system (Page 890)
        i. capture system state and compare to the system's state after executing the malware file.
    b. Monitor host integrity (Page 891)
        i. Take a snapshot of the system before and after the incident or actions and analyze changes
    c. Monitor installation
        i. know the folders modified or created during the installation process and the files and folders which have not been modified by the uninstalling process

TOOLS Methodologies, Frameworks and Processes Term

ii. Tools to monitor installation
    1. Mirekusoft Install Monitor (Page 891)
    2. Advanced Uninstaller PRO (Page 891)
    3. Epsilon Squared's InstallWatch (Page 891)
    4. Revo Uninstaller Pro (Page 891)
    5. Comodo Programs Manager (Page 891)
    6. SysAnalyzer (Page 891)

d. Monitor processes (Page 892)
    i. observe the child processes, associated handles, loaded libraries, and functions
    ii. Tools to monitor processes
        1. Process Monitor (Page 892)
            a. shows real-time file system, Registry and process/thread activity
        2. What's Running (Page 893)
            a. explore processes, services, modules, IP- connections, and drivers, etc.
        3. Process Explorer (Page 894)
        4. System Explorer (Page 895)
        5. HijackThis (Page 895)
        6. Autoruns for Windows (Page 895)
        7. KillProcess (Page 895)
        8. Security Task Manager (Page 895)
        9. Yet Another (remote) Process Monitor (YAPM)
        10. MONIT (Page 896)
        11. ESET SysInspector (Page 896)
        12. ManageEngine OpManager (Page 897)

e. Monitor Files and Folders
    i. find the files and folders which malware creates and analyze them to collect any important information stored in them.
    ii. Tools
        1. The File Checksum Integrity Verifier (FCIV)
        2. SIGVERIF (Page 897)
        3. Tripwire (Page 898)
    iii. Files and Folder Integrity Checkers
        1. FastSum (Page 898)
        2. WinMD5 (Page 899)
        3. Directory Monitor (Page 899)
        4. FSUM Frontend (Page 900)
        5. Verisys (Page 900)
        6. AFICK (Another File Integrity Checker)

TOOLS Methodologies, Frameworks and Processes Term

7. FileVerifier++ (Page 900)
8. PA File Sight (Page 901)
9. CSP File Integrity Checker (Page 901)
10. ExactFile (Page 901)
11. OSSEC (Page 902)
12. Change Tracker Enterprise (Page 902)

f. Monitor the registry
   i. Tools
      1. Regedit (Page 903)
      2. RegScanner (Page 904)
      3. Reg Organizer (Page 906)
      4. Registry Viewer (Page 906)
      5. Comodo Cloud Scanner (Page 906)
      6. Buster Sandbox Analyzer (Page 906)
      7. SysTracer (Page 906)
      8. MJ Registry Watcher (Page 906)
      9. Active Registry Monitor (ARM) (Page 906)
      10. Regshot (Page 907)
      11. Whatchanged Portable (Page 907)
      12. Alien Registry Viewer (Page 907)

g. Monitor network activity
   i. Process of capturing the network traffic and investigating it to determine the malware activity
   ii. Tools
      1. Capsa Network Analyzer (Page 908)

h. Monitor ports (Page 909)
   i. find if malware is trying to access a particular port
   ii. Tools
      1. Netstat (Page 909)
      2. TCPView (Page 911)
      3. CurrPorts (Page 912)

i. Monitor DNS (Page 913)
   i. Check if malware is capable of changing DNS server settings
   ii. Tools
      1. DNSChange (Page 913)
         a. capable of changing the systems' DNS server settings
         b. Malicious
      2. DNSstuff (Page 913)
      3. DNSQuerySniffer (Page 913)

j. Monitor API Calls

TOOLS Methodologies, Frameworks and Processes Term

i. Gather APIs related to the malware programs and analyze them to reveal its interaction with the OS as well as the activities it has been performing over the system
ii. Tools
    1. API Monitor (Page 914)

k. Monitor device drivers (Page 915)
    i. for suspicious device drivers and verify if they are genuine
    ii. Tools
        1. DriverView (Page 916)
        2. Driver Detective (Page 917)
        3. Unknown Device Identifier
        4. DriverGuide Toolkit (Page 917)
        5. InstalledDriversList (Page 917)
        6. Driver Magician (Page 918)
        7. Driver Reviver (Page 918)
        8. ServiWin (Page 918)
        9. Driver Fusion (Page 918)
        10. My Drivers (Page 919)
        11. DriverEasy (Page 919)

l. Monitor Startup programs
    i. scanning for suspicious startup programs is essential
    ii. Open command prompt with administrator, type bcdedit command and press enter button to view all the boot manager entries
    iii. Run → Type services.msc →Sort by Startup Type
    iv. C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
    v. C:\Users\(User-Name)\AppData\Roaming\Microsoft\Windows\StartMenu\Programs \Startup
    vi. Press the Windows and r buttons simultaneously to open the run box then Type shell:startup in the box and click OK button to navigate to the startup folder
    vii. Tools
        1. Security AutoRun (Page 923)
        2. Autoruns for Windows (Page 923)
        3. WinTools.net 16.7.1 Premium (Page 924)
        4. StartEd Pro (Page 924)
        5. WhatInStartup (Page 925)
        6. PCTuneUp Free Startup Manager (Page 925)

7. Chameleon Startup Manager (Page 925)
8. Ccleaner (Page 926)
9. WinPatrol (Page 926)
10. Chameleon Startup Manager (Page 926)
11. Startup Booster (Page 926)

m. Monitor Windows services (Page 926)
   i. malicious services run as SYSTEM account or other privileged accounts
   ii. trace the malicious services initiated by the suspect file
   iii. Tools that can detect changes in services
      1. Windows Service Manager (SrvMan) (Page 927)
      2. Advanced Win Service Manager (Page 926)
      3. Netwrix Service Monitor (Page 926)
      4. PC Services Optimizer (Page 926)
      5. ServiWin (Page 930)
      6. Windows Service Manager Tray (Page 930)
      7. AnVir Task Manager (Page 930)
      8. Process Hacker (Page 930)
      9. Free Windows Service Monitor Tool (Page 931)
      10. Nagios XI (Page 931)
      11. Service+ (Page 931)

d. Malware analysis lab
   i. Multiple virtual systems running different operating systems
      1. VirtualBox (Page 876)
      2. VMware vSphere Hypervisor (Page 876)
      3. Microsoft Hyper-V (Page 876)
      4. Parallels Desktop 11 (Page 877)
      5. Boot Camp (Page 877)
   ii. Requirements
      1. Isolate the malware-analysis lab from the production network
      2. Use removable media, mainly DVDs to install tools and malware
      3. Virtualization snapshot and re-imaging tools to capture machine state
      4. Tools to wipe and rebuild the victim's machine quickly (Page 877)
         a. Imaging tool to get a clean image for forensics and prosecution purpose
         b. File/data analysis to perform static analysis of potential malware files
         c. Registry/configuration tools to identify the last saved settings
         d. Sandbox to perform dynamic analysis manually
         e. Log analyzers to extract log files
         f. Network capture to understand how the malware leverages the network

TOOLS Methodologies, Frameworks and Processes Term

iii. Network and internet simulation tools
    1. NetSim (Page 877)
        a. http://tetcos.com/netsim_gen.html
    2. ns-3 (Page 877)
        a. https://www.nsnam.org
    3. Riverbed Modeler (Page 878)
        a. http://www.riverbed.com
    4. QualNet (Page 878)
        a. http://web.scalable-networks.com
iv. Screen Capture and Recording Tools (Page 878)
    1. Snagit
        a. https://www.techsmith.com
    2. Jing
        a. https://www.techsmith.com
    3. Camtasia
        a. https://www.techsmith.com
    4. Ezvid
        a. http://www.ezvid.com
v. OS Backup and Imaging Tools (Page 878)
    1. Genie Backup Manager Pro
        a. http://www.genie9.com
    2. Macrium Reflect Server
        a. http://www.macrium.com
    3. R-Drive Image
        a. http://www.drive-image.com
    4. O&O DiskImage 10
        a. https://www.oo-software.com
vi. Rules for malware analysis (Page 878)
    1. pay great attention to key features
    2. gather a general overview
    3. Try different tools and approaches
    4. identify, understand, and defeat aversion techniques
vii. Documentation to prepare before analysis (Page 879)
    1. Full path and location of the file
    2. MAC-times tamp
    3. The system information where file was stored
        a. The operating system and version
        b. File system
        c. User accounts
        d. IP address
    4. References to that file within the file system or registry
    5. Who found the file and when?

TOOLS Methodologies, Frameworks and Processes Term

viii. Online malware testing tools
    1. VirusTotal (Page 882)
        a. http://www.virustotal.com
        b. Generates a report that provides
            i. total # of engines that marked the file as malicious
            ii. malware name
            iii. if available, additional information about the malware
        c. offers important details of the online file analysis such as
            i. target machine
            ii. compilation time stamp
            iii. type of file
            iv. compatible processors
            v. entry point
            vi. PE sections
            vii. data link libraries (DLLs)
            viii. used PE resources
            ix. different hash values
            x. IP addresses accessed or contained in the file
            xi. program code
            xii. type of connections established

ix. Online Malware analysis services
    1. Anubis: Analyzing Unknown Binaries (Page 883)
        a. analyzes the behavior of Windows PE-executables
        b. Generated report includes detailed data about
            i. modifications made to the Windows registry or file system,
            ii. interactions with Windows Service Manager or other processes
            iii. logs all generated network traffic
    2. Malware Protection Center
        a. service provided to protect computers from malware
        b. Users submit the file containing malware or potentially unwanted software
        c. Microsoft analyzes the file and generates a complete report
    3. Dr. Web Online Scanners
        a. online tool that allows file scan, link scan, and virus database search
        b. generates detailed report of detected viruses, worms, and various kinds of adware, and sends it to the requester
    4. Metascan Online
        a. online file scanning service powered by OPSWAT's Metascan technology, a multiple-engine malware scanning solution.

TOOLS Methodologies, Frameworks and Processes Term

5. Bitdefender QuickScan (Page 884)
    a. online virus scanner that detects hidden threats, malware, and keyloggers.
    b. It uses in-the-cloud scanning technology to detect active malware on a system
6. ThreatAnalyzer (Page 884)
    a. Analyzes malware samples, generates report analyses
7. Jotti
    a. online tool which uses many anti-virus vendors to scan malware

e. Malware analysis challenges (Page 933)
    i. Accuracy of the analysis process
    ii. Detection of malware pieces and traits
    iii. Amount of data to be analyzed
    iv. Changing technologies and dynamics of malware creation and propagation
    v. Anti-analysis procedures such as encryption, code obfuscation, and deletion of records

12. Investigating Email Crimes

50. Investigating Email Crimes Part 1
    a. Mail user agent (MUA) (Page 939)
        i. Email client
        ii. configuration includes issuing
            1. email ID
            2. password
            3. POP3/IMAP and SMTP address
            4. port number
            5. and other related preferences
        iii. email client becomes active only when a user runs it
        iv. Most commonly used email clients (Page 939)
            1. Standalone
                a. Microsoft Outlook
                b. Thunderbird
            2. Web-based
                a. Gmail
                b. Yahoo! Mail
    b. Mail transfer agent (MTA)
        i. Sends the emails stored in the users' mailbox to the users' inbox
        ii. agent that enables email transfer from one system to another (Page 948)
    c. Mail submission agent (MSA)
        i. Email client sends emails to the server using a Mail Submission Agent
    d. ESP (Page 939)
        i. Email Service Provider

ii. hosts and manages a mailbox that stores the users' emails

e. Email server (Page 939)
   i. computer within the network that works as a virtual post office
   ii. connects and serves several email clients
   iii. exchange email with the SMTP server
   iv. When a user sends an email, the client application first directs it to the email server
   v. email server checks for the validity of the username with the other email server
   vi. It contains the text file for each account
   vii. the email client connects to the email server and passes the name of the sender and the recipient with the body of the message to the email server
   viii. Comprise of 3 components (Page 940)
      1. PO3
      2. SMTP
      3. IMAP

f. **SMTP** server – Simple Mail Transfer Protocol server (Page 940)
   i. an outgoing mail server, which allows a user to send emails to a valid email address
   ii. internet protocol that's designed for transmitting email over IP networks
   iii. SMTP server is just a computer running SMTP, and it acts like a postman
   iv. Process
      1. Send button clicked, Outlook client connects to the sender's domain server xx.com on port 25
      2. Client sends sender info, recipient's address, and body of email to the sender's SMTP server
      3. The sender's SMTP breaks down the recipient's name and domain name
      4. The sender's SMTP server contacts the DNS server and inquires about the IP address of the recipient's SMTP server. The DNS replies and gives one or more IP addresses
      5. The sender's SMTP server connects with the recipient's SMTP server on port 25 and gives the message to it. The recipient's SMTP server gets the message and transfers it to the POP3 server

g. POP3 server – Post Office Protocol version 3 server (Page 941)
   i. Uses port 110
   ii. Protocol for retrieving emails from an email server.
   iii. When the POP server receives emails, they are stored on the server until and unless the user requests it
   iv. Messages automatically download from the mail server to the user's hard disk
      1. emails are no longer stored on the mail server unless the user specifies to keep a copy of it

h. IMAP server (Page 942)
   i. similar to POP3 servers

ii. IMAP handles the incoming mail
iii. IMAP server listens on port 143
iv. IMAPS (IMAP over SSL) listens on port 993
v. MAP stores emails on the mail server and allows users to view and manipulate their emails, as if the mails are stored on their local systems
vi. IMAP does not move mails from the mail server to the user's mailbox
vii. acts as a remote server that stores all the user's mails in the mail server

i. Email Crimes (Page 944)
    i. Crimes committed by sending e-mails
        1. **Spamming (Page 944)**
            a. **unsolicited commercial email (UCE) or junk mail**
            b. **Spammers hide their identities by forging the email header.**
        2. Phishing (Page 945)
            a. deceives and convinces the user with the fake content
        3. Mail bombing (Page 946)
            a. process of repeatedly sending an email message to a particular address at a specific victim's site
        4. Mail storms (Page 946)
            a. **flurry of junk mail sent by accident without human intervention**
    ii. Crimes supported by e-mails
        1. Identity Fraud (Page 946)
            a. illegitimate retrieval and use of others' personal data
        2. Cyber-stalking (Page 947)
            a. attackers harass using emails or IMs
        3. Child pornography (Page 947)
            a. a minor is depicted of engaging in a sexually explicit conduct
        4. Child abduction
            a. wrongfully removing, retaining, detaining or concealing a minor

j. RFC 5322 (Page 947)
    i. defines the Internet email message format

k. RFC 2045 through RFC 2049
    i. defines multi-media content attachments

l. MIME
    i. Multipurpose Internet Main Extensions

m. Message header
    i. consists of fields like From, To, CC, Subject, and Date, etc.
    ii. Metadata attached to every email
    iii. Common headers (Page 949 - 951)
        1. Apparently-To – Normally the sign of a mailing list
        2. BCC
        3. Comments - free-form header field

4. Content-Transfer-Encoding - way of enclosing non-text content (MIME)
5. Content-Type - states type of content to expect in the message (MIME)
6. Date
7. Errors-To - address for mailer-generated errors
8. From
9. Message-Id - unique ID associated with each message
10. In-Reply-To - message ID of the message to which it is replying
11. MIME-Version - specifies MIME protocol version used by sender (MIME)
12. Newsgroups - newsgroup(s) to which the user posted the message
13. Organization - free-form header holds name of the sender organization
14. References - identifies upstream posts to which message is a response
15. Priority - free-form header that assigns a priority to the mail
16. Reply-To - address for sending replies
17. Sender
18. Subject
19. To

iv. Common X-headers

1. X-Confirm-Reading – read receipt header
2. X-Distribution - identify if the received mail had numerous recipients
3. X-Errors-To - email address to which it can send the errors
4. X-Mailer - free-form header showing sender's mail software
5. X-PMFLAGS - Pegasus adds this header for users using it
6. X-Priority – defines priority
7. X-Sender - e-mail equivalent to the Sender
8. X-UIDL – used by POP for retrieving mail from a server

n. Message body

i. the message conveyed through the mail that sometimes includes a signature block in the end

o. Steps involved in investigating e-mail crimes and violations (Page 953)

i. Obtain a Search Warrant

ii. Examine e-mail messages (Page 954)

1. The primary information required for starting an email investigation is the unique IP address.

iii. Copy and print the e-mail messages (Page 955)

iv. View the e-mail headers (Page 955)

v. Analyze the e-mail headers (Page 962)

1. Examine additional files (Page 964)
    a. Microsoft Outlook
        i. Personal email file (.pst)
        ii. Offline email file (.ost)
2. Check the email validity
    a. See below

3. Examine the originating IP address
    a. Trace Email Analyzer tool (Page 966)
        i. Open the email to trace and find its header.
        ii. Copy the header and paste it in the box space in the Trace Email Analyzer tool webpage.
        iii. Press the "Get Source" icon.
        iv. Scroll down below the webpage to find a box containing the Trace Email results.

vi. Trace the e-mail origin (Page 967)
1. IP address
2. mail server
3. username
4. domain name, etc.
5. Validate header info
    a. Attackers can fake all email header information except the "Received" portion referencing the last receiver
6. Online websites such as Yahoo!, Hotmail, etc. maintain the IP address of each machine accessing their email services.
    a. Once the IP address is authenticated, examiners can contact an email provider to get the sender's information
7. Registry sites to determine email origin
    a. www.arin.net
        i. employs the American Registry for Internet Numbers (ARIN) to match the domain name for an IP address
        ii. Provides the point of contact for the domain name
    b. www.internic.com
        i. Provides the identical info given by www.arin.net
    c. www.freeality.com
        i. Provides options for searching such as email address, phone numbers, and names
        ii. can do a reverse email search, which could reveal the subject's real name
        iii. This site can do other searches such as reverse phone number searches and address searches

vii. Acquire e-mail archive (Page 969)
viii. Examine e-mail logs

p. Checking validity of an e-mail sender:
i. Email Dossier (Page 965)
1. http://centralops.net
2. online network scanning utility
3. initiates SMTP sessions to check address acceptance

ii. Email Address Verifier (Page 966)

1. connects to mailboxes to check whether an email address exists or not

iii. Email Checker (Page 966)
1. Free tool for verifying an email address
2. tells you whether the email address is real or not
3. Extracts the MX records from the email address and connect to mail server (over SMTP and also simulates sending a message) to make sure the mailbox really exists for that user/address

iv. G-Lock Software Email Verifier (Page 966)
1. Check every email address from a database or a mailing list and determine if the e-mails are still valid.

q. Email archives (Page 969)
i. Local archive
1. end user on the local computer deals with the local archive

ii. Server storage archive

iii. Email archives store received and sent emails, contacts, attachments, and other email client related data, and store them on the system hard drive

iv. Table of contents files (Page 969)
1. Directory of the details of the email message
2. Stores main status
3. unread and read
4. Forwarded
5. Redirected
6. Flagged
7. Deleted

r. Types of encoding in emails
i. MIME
1. Extends the email format to support the following:
a. Text in non-ASCII character sets
b. Attachments like application programs, images, audio, video, other than text
c. Multiple part message bodies
d. Non-ASCII character set header information

ii. Uuencode
1. AKA UNIX-to-UNIX encoding or Uuencode/Uudecode
2. Utility for encoding and decoding files shared between users or systems using the UNIX operating systems
3. It is also available for all other OSes, and many e-mail applications offer it as an encoding alternative, especially for e-mail attachments.

iii. BinHex
1. Short form for "binary-to-hexadecimal."
2. A binary-to-text encoding system used in the Mac OS
3. Used to send binary files via e-mails.

4. This system is similar to Uuencode, but BinHex combines both "forks" of the Mac file system including extended file information

s. Examining Linux E-mail Server Logs (Page 974)
   i. Sendmail is the command used to send emails via Linux or Unix system
   ii. Linux and Unix uses Syslog to maintain logs of what happened on the system
   iii. Configuration file, /etc/syslog.conf determines the location of syslog service logs
   iv. Syslog config file contains info on the logging priority, where logs are sent, and what other actions may be taken
      1. The syslog.conf provides the location of the log file for e-mail, which is usually /var/log/mailog
      2. /var/log/mailog file contains source and destination IP addresses, date and time stamps, and other information necessary to validate the data within an e-mail header

t. Examining Microsoft Exchange E-mail Server Logs (Page 975)
   i. Microsoft Exchange uses the Microsoft Extensible Storage Engine (ESE)
   ii. Focus on the following files:
      1. .edb database files (responsible for MAPI information)
      2. .stm database files (responsible for non-MAPI information)
      3. checkpoint files
         a. helps to find out if any data loss occurred after last backup
      4. temporary files
         a. Stores the info received by the server when it was too busy to process it immediately
      5. Transaction log preserves and processes modifications done in the database file
         a. it can be used to determine if the email has been sent or received by the server

u. Email forensics tools (Page 976)
   i. RecoverMyEmail
      1. Can recover deleted email messages from either Microsoft Outlook PST files or Microsoft Outlook Express DBX files
   ii. MailXaminer (Page 977)
      1. an e-mail searching, reporting, and exporting tool
   iii. Stellar Phoenix Deleted Email Recovery (Page 979)
      1. recovers lost or deleted emails from MS Outlook data (PST) files and Outlook Express data (DBX) files
   iv. Forensic Toolkit (FTK) (Page 979)
   v. Paraben's Email Examiner (Page 979)
      1. Analyze message headers, bodies and attachments
      2. Recovers email in the deleted folders, supports advanced searching, reporting and exporting to PST and other formats
   vi. Kernel for PST Recovery (Page 979)

TOOLS Methodologies, Frameworks and Processes Term

1. Repair corrupted PST file and recover all email items from them.

vii. MxToolBox Email Header Analyzer (Page 980)
   1. This tool will make email headers human readable by parsing them

viii. Wise Data Recovery (Page 980)
   1. Data recovery program for free

ix. EaseUS Email Recovery Wizard (Page 980)

x. DiskInternals Mail Recovery (Page 980)
   1. Locate, recover and fix broken email databases

xi. Aid4Mail Email Forensic software (Page 980)
   1. Migrate email accounts and transfer messages between email apps and web-based services.

xii. Paraben's Network E-mail Examiner (Page 980)
   1. Analyze and filter messages and output the results into PST files

xiii. Nuix Investigator Lab (Page 980)

xiv. EmailTrackerPro (Page 980)
   1. Trace an email using the email header
   2. Scans each email as it arrives and warns the user if it is suspected spam

xv. EnCase Forensic (Page 980)

xvi. OSForensics (Page 981)

xvii. Exchange Deleted Email Recovery (Page 981)

xviii. Kernel Email Recovery Software (Page 981)

xix. Intella TEAM (Page 981)

xx. EMail Detective - Forensic Software Tool (Page 981)

xxi. Lotus Notes Forensics Tool (Page 981)
   1. Recovers and extracts evidence from NSF Files

xxii. Stellar Phoenix Mailbox Exchange Recovery (Page 982)

xxiii. PST Outlook Repair (Page 982)

xxiv. Forensic Email Recovery Tools Kit (Page 982)

xxv. Repair PST - Outlook PST Recovery (Page 982)
   1. recover emails from corrupt PST files of Microsoft Outlook

xxvi. Kroll Ontrack Email Recovery (Page 982)

xxvii. Unistal Email Recovery Software (Page 982)
   1. Recover MS Outlook Files, Lotus Notes email files, Incredimail as well as MS Exchange email files

xxviii. InFixi® Email Recovery Tools (Page 982)
   1. "Email Recovery", "Email Conversion", "File Repair", "File Recovery" and "Password Recovery”

xxix. DataNumen Outlook Repair (Page 982)

xxx. Stellar Phoenix Outlook PST Repair Software (Page 983)

xxxi. Recovery Toolbox for Outlook (Page 983)

xxxii. MS Outlook PST Recovery Tool (Page 983)

v. U.S laws against E-mail related crimes: (Page 983)

TOOLS Methodologies, Frameworks and Processes Term

i. CAN-SPAM Act -(Controlling the Assault of Non-Solicited Pornography and Marketing Act)
    1. Sets the rules for sending e-mails for commercial purposes
    2. Establishes the min requirements for commercial messaging
    3. Gives the recipients of e-mails the right to ask the senders to stop e-mailing them
    4. Spells out the penalties in case the rules are violated
    5. Requirement for senders (Page 983)
        a. Do not use false or misleading header information
        b. Do not use deceptive subject lines
        c. The commercial e-mail must be identified as an ad
        d. The email must have your valid physical postal address
        e. The email must contain the necessary information regarding how to stop receiving e-mails from the sender in future
        f. Honor recipients' opt-out request within 10 business days
        g. Both the company whose product is promoted in the message and the e-mailer hired on contract to send messages must comply with the law
    6. Subject to financial penalties of up to $16,000
    7. Both the company whose product is being promoted in the message and the company that originally sent the message may be held legally responsible
    8. Criminal penalties and imprisonment may be sentenced for (Page 984)
        a. Accessing someone else's computer to send spam without permission
        b. Using false information to register for multiple email accounts or domain names
        c. Relaying or **retransmitting multiple spam messages through a computer to mislead others about the origin of the message**
        d. Harvesting email addresses or generating them through a dictionary attack (the practice of sending e-mails to addresses made up of random letters and numbers in the hope of reaching valid ones)
        e. Taking advantage of open relays or open proxies without permission

ii. 18 U.S.C. § 2252A -Transmission of Child Pornography
iii. 18 U.S.C. § 2252B -Manipulation of domain names or other means to provide access to Child Pornography
iv. Residents of Washington D.C. are governed by RCW 19.190.020

13. Mobile Forensics

51. Mobile forensics Part 1

TOOLS Methodologies, Frameworks and Processes Term

a. Mobile forensic (Page 990)
    i. Recover digital evidence from a mobile device in a forensically sound manner
    ii. Extraction, recovery, and analysis of data from the internal memory, SD cards, and SIM cards of mobile devices
b. Top Threats Targeting Mobile Devices
    i. Web-based and network-based attacks
        1. Web-based and network- based attacks attempt to install malware or steal confidential data flowing through the browser
    ii. Malware
        1. Traditional computer virus: Comes into force after attaching to a legitimate host program.
        2. Computer worms: Spreads from one device to another and tries to appear across the entire mobile network.
        3. Trojan horse programs: Performs malicious actions upon satisfying certain conditions.
    iii. Social Engineering Attacks
        1. The attacker entices the victim to share his/her sensitive information
        2. Phishing, Baiting, Pretexting, Quid Pro Quo, Tailgating
    iv. Resource Abuse
        1. Attackers aim at misusing mobile device
        2. Most common include sending phishing mails and denial of service attacks from a set of compromised machines/botnets
    v. Data Loss
        1. Unauthorized transfer of data on a mobile device unintentionally by a legitimate mobile user or by an attacker with remote access
        2. Data loss is the biggest threat to mobile devices.
    vi. Data Integrity Threats (Page 992)
        1. Modify or corrupt the data stored in mobile devices.
c. Architectural layers of mobile device environment (Page 993)
    i. **Client application** (Page 993)
        1. **Any android application that runs on the Android platform**
        2. The client application needs resources to function effectively. These include communication APIs, GUI API, phone API, and middleware components.
    ii. Communication APIs, GUI API, phone API, and middleware components
        1. Communication API simplifies the process of interacting with web services and other applications such as email, internet, and SMS
        2. GUI API is responsible for creating menus and sub-menus in designing applications and acts as an interface where the developer has a chance of building other plugins
        3. Phone API provides telephony services related to the mobile carrier operator such as making calls, receiving calls, and SMS

        a. All phone APIs appear at the application layer
    iii. **Operating system** (Page 994)
        1. **The mobile OS offers utilities for scheduling multiple tasks, memory management tasks, synchronization, and priority allocation**
        2. Provides interfaces for communication between application layers, middleware layers, and hardware.
    iv. **Hardware** (Page 994)
        1. **display device, keypad, RAM, flash, embedded processor, and media processor, which are responsible for mobile operation**
    v. Radio interface, gateway, and network interface (Page 994)
        1. A mobile device communicates with the network operator with some interfaces
    vi. **Network** (Page 994)
        1. To communicate with the network, the data must pass through various layers to reach the destination
        2. **Allows a mobile device to communicate with the network operator**
d. Android architecture stack (Page 995)
    i. Linux Kernel:
        1. **Android is a Linux kernel** that communicates with the hardware and comprises all the necessary hardware drivers.
        2. Operates as an intelligence layer between the hw and sw layers
    ii. Libraries:
        1. permits the device to manage various types of data
        2. The application developer generally writes libraries for all the available hardware separately in C or C++ language
        3. Important native libraries include
            a. Surface Manager: takes care of displaying windows owned by different applications running on different processes
            b. Media framework: allows recording and playback of all the media formats
            c. SQLite: the database engine that stores data in Android devices
            d. OpenGL/ES and SGL: used to render 2D (SGL) or 3D (OpenGL/ES) graphics content to the screen
            e. FreeType: renders the bitmap and vector fonts.
            f. WebKit: It is the browser engine used to display web pages
            g. Libc: C system library tuned for embedded Linux-based devices
    iii. Android Runtime (Page 996)
        1. transforms machine bytecode into normal instructions
        2. It is the successor of Dalvik
    iv. Dalvik Virtual Machine (DVM)
        1. Java virtual machine responsible for power and memory management

2. The Dalvik virtual machine runs only .dex files built from .class files during compilation to achieve better efficiency using few resources.
3. creates partitions in the virtual machine to provide security, isolation, memory management, and threading support simultaneously

v. Core Java Libraries:
1. Provides almost all functionalities stated in Java sw edition libraries

vi. Application Framework:
1. interact with application framework blocks to manage basic mobile functions such as resource management and voice call management
2. Important framework blocks are
a. Package Manager: tracks the apks installed in the mobile device
b. Activity Manager: controls the life cycle of applications running
c. Content Providers: allow apps to share data between them
d. Telephony Manager: controls/manages all calls made
e. Location Manager: manages the location using GPS or cell tower
f. Resource Manager: manages resources used in applications
g. Notifications Manager: allows apps to display alerts on screen

vii. Applications (Page 997)
1. Last stage of android architecture
2. Displays applications on the user screen
3. All the applications designed and developed fit into this portion
4. Basic applications are
a. Home, Contacts, Call Register, Browser
5. developer designs apps that replace default apps with better features

e. Android boot process (Page 997)
i. Boot ROM code is activated loading the Boot Loader into RAM
ii. Boot Loader sets up all the essential things start the kernel
iii. Android kernel initializes and sets up everything required for the system to run
iv. Init initializes Zygote, runtime, and daemon processes – Android logo appears
v. Zygote forks a new virtual machine and initializes the Dalvik virtual machine
vi. System triggers an “ACTION_BOOT_COMPLETED” standard broadcast

f. IOS Architecture
i. Cocoa Touch Layer (Page 1000)
1. First and the topmost layer in iOS architecture
2. The most important framework among the available frameworks is UIKit.
3. Defines simple application basics and offers advanced technologies such as multitasking and touch-based input

ii. Media Services Layer: (Page 1000)
1. takes care of media files such as audio and video.
2. handles important technologies such as OpenGL ES and OpenAL, Core Graphics, Core Media, and AV Foundation.

3. Contains the following frameworks:
    a. Assets Library Framework - To access photos and videos
    b. Core Image Framework – Image manipulation
    c. Core Graphics Framework – 2D drawing

iii. Core Services Layer: (Page 1000)
1. manages basic system services that an iOS application uses
2. Offers services such as iCloud Storage, Grand Central Dispatch, Block Objects, and In-App Purchase
3. The Automatic Reference Counting feature's purpose is to simplify the memory management in Objective C

iv. Core OS Layer: (Page 1000)
1. Core OS layer is the most important of all the layers
2. Provides the maximum features for the applications
3. Provides most of the frameworks needed for accurate functionality of the applications

g. IOS Boot Process
i. BootRom initializes some components and checks signature of LLB (lower level bootloader)
ii. LLB is loaded and checks signature of iBoot (stage-2 boot loader)
iii. iBoot is loaded and checks kernel and device tree signatures (Not booted in Device Firmware Upgrade DFU mode)
iv. Kernel and device trees load. Kernel checks signatures of all user applications

h. Mobile storage locations: (three) (Page 1002)
i. Internal Phone Memory:
1. Includes data stored in RAM, ROM, or flash memory.
2. Stores the Mobile phone's OS, applications, and data.

ii. The investigator can extract information from internal phone memory using AT commands with the help of a USB cable, infrared, or Bluetooth

i. SIM Card Memory:
i. SIM stores personal info, address books, messages, and service-related info

j. External Memory
i. Includes data stored in SD card, MiniSD Card, MicroSD, etc.
ii. Stores personal information such as audio, video, and images.

k. Mobile forensics tools (Page 1007)
i. SEARCH Investigative Toolbar
ii. BitPim
iii. Oxygen Forensics Analyst
iv. Paraben's Sim Card Seizure
v. MOBILedit! Forensic
vi. TULP2G
vii. iDEN Phonebook Manager
viii. SUMURI's PALADIN

TOOLS Methodologies, Frameworks and Processes Term

ix. floAt's Mobile Agent
x. XRY Logical & XRY Physical

l. Mobile device forensics process (Page 1008)
    i. Collect evidence (Page 1009)
        1. Protect the integrity of traditional and electronic evidence
        2. Prevent unauth users from entering scene and touching the evidence
        3. Collect all the electronic devices found at the crime scene
        4. Check whether the mobile device is connected to a computer
        5. Confirm the power status of the device(s) by checking for flashing lights
        6. Collect non-electronic evidence such as written passwords, handwritten notes, and computer printouts
    ii. Document scene and preserve evidence
        1. Crime location
        2. Power status of the evidence (ON/OFF)
        3. Condition of the device (Working/damaged)
        4. Document all the electronic devices found at the crime scene
        5. Take photographs of all evidence at the scene and write notes on what is seen on the screen
        6. Document the state of the device during seizure
        7. Document every activity on electronic devices found at the crime scene
        8. Phone Identification
            a. brand, model, and service provider
            b. Battery cavity or the SIM card or from the mobile phone board under the battery has this info
            c. The label under the battery contains the mobile phone model, type, code, IMEI, and FCC ID.
        9. Connection Identification
            a. Connect the mobile phone to the forensic station through a cable, Infrared, or Bluetooth.
        10. Preserve all the evidences and documents in a secure location.
        11. Take necessary actions to preserve hidden or trace evidence
        12. Pack the electronic devices in antistatic packaging
        13. Make sure all containers that hold evidence are labeled in properly
        14. Keep electronic evidence away from magnetic items while transporting
        15. Store evidence in a secure area and weather-controlled environment
        16. Maintain the chain of custody documents
    iii. Imaging & profiling
        1. FTK Imager, EnCase, and Smart
        2. Using SSH
            a. ssh -l <username> <your Linux box host address> dd of=/dev/disk0 | dd of=~/myiphoneback.img
    iv. Acquire information

1. Forensic Explorer and Autopsy
2. Extracting all possible evidence from mobile phones by using various techniques (Page 1020)
3. no standard process of collecting digital evidence in mobile forensics
4. The data acquisition methods are (Page 1021)
    a. Cellular Data Acquisition
    b. SIM File System Acquisition
    c. Logical Acquisition
    d. Physical Acquisition
    e. File System Acquisition

v. Report

m. Signal Containment Device/Bags (Page 1011)
    i. Faraday Bag Faraday bags
    ii. Signal Disruption Bag/ Wireless StrongHold Bag
    iii. Arson Cans
    iv. Aluminum Foil
    v. RF-shielded box
    vi. Cell Phone Signal Disruption Device

n. Bypassing Android phone lock password using ADB and ViaExtract (Page 1016)
    i. Connect the device to the forensics workstation through USB
    ii. Launch adb shell using ViaExtract
    iii. Remove password.key file from android directory

o. Bypassing the iPhone Passcode Using IExplorer (Page 1017)
    i. Only works or jailbroken devices
    ii. Connect the device to the workstation
    iii. Browse the iPhone file system with IExplorer
    iv. Navigate to the directory /var/mobile/Library/Preferences/ and delete
        1. com.apple.springboard.plist
    v. Navigate to the directory /var/Keychains/ and delete keychain-2.db
    vi. Reboot the iPhone

p. Enabling USB debugging mode in Android (Page 1017)
    i. Go to Settings→Developer Options→USB Debugging
    ii. In pop-up select the checkbox besides “Always allow from this computer”

q. Jailbreaking/Rooting (Page 1019)
    i. Jailbreaking, rooting, and unlocking to are used to bypass the preset limitations
    ii. Android Rooting Tools
        1. OneClickRoot (Page 1019)
            a. Allows the users to root their Android mobile devices without having a good understanding of its firmware and kernel
        2. Kingo Android ROOT (Page 1019)
            a. This is a simple and direct utility to root android devices and suitable for novice users.

TOOLS Methodologies, Frameworks and Processes Term

3. Towelroot (Page 1019)
    a. Provides one click root to most popular Android smart phones
    b. Download the towelroot.apk file to computer and transfer it to mobile
4. RescuRoot (Page 1019)
    a. One click utility to root most Android mobile devices from the brands Samsung, HTC, Motorola, LG, and Sony Ericsson

iii. iOS Jailbreaking Tools (Page 1020)

1. PANGU JAIL BREAK (Page 1020)
    a. allows the user to jailbreak iOS devices and removes the jailbreak by rebooting the iOS devices.
2. Redsn0w (Page 1020)
    a. jailbreak into an iPhone, iPod Touch, or iPad by running a variety of firmware versions.
3. Sn0wbreeze (Page 1020)
    a. developed by iH8sn0w for Apple devices running on iOS such as iPhone, iPad, and iPod Touch.
4. GeekSn0w (Page 1020)
    a. free tool developed by Andrea Bentivegna for jailbreaking iPhones running on iOS 7.1.

r. Terms (Page 1022)

i. SIM: Subscriber Identity Module

1. Stores sensitive data such as the user's contacts, messages, and time stamps associated with them
2. Contains technical information such as
    a. Integrated Circuit Card Identifier (ICCID)
    b. International Mobile Subscriber Identity (IMSI)
    c. last dialed numbers (LDNs)
    d. service provider name (SPN), etc.

ii. MSC: Mobile Services Switching Center

iii. HLR: Home Location Register

iv. BTS: Base Transceiver Station

v. AuC: Authentication Center

vi. VLR: Visitor Location Register

vii. BSC: Base Station Controller

viii. ME: Mobile Equipment

ix. EIR: Equipment Identity Register

s. Components of a cellular network (Page 1023)

i. Mobile Switching Center (MSC): the switching system for the cellular network

ii. Base Transceiver Station (BTS): radio transceiver equipment that communicates with mobile phones

TOOLS Methodologies, Frameworks and Processes Term

iii. Base Station Controller (BSC): manages the transceiver's equipment and performs channel assignment
iv. BSS: Base Station Subsystem is responsible for managing the radio network and is controlled by the Mobile service switching center (MSC). It consists of the elements BSC (Base Station controller), BTS (Base Transceiver Station), and TC (Transcoder)
v. Home Location Register (HLR): It is the database at MSC. It is the central repository system for subscriber data and service information
vi. Visitor Location Register (VLR): It is the database used in conjunction with the HLR for mobile phones roaming outside their service area
vii. Authentication Center (AuC): Stores the user's IMSI, encryption, and auth keys
viii. Equipment Identity Register (EIR): A database that contains a list of mobile devices along with their IMEI numbers.
    1. A mobile network operator (MNO) can go through the EIR to track the IMEI of a mobile device and check if it is valid (whitelisted) or (blacklisted) suspected or stolen/blocked (blacklisted) and take action

t. Cell network types
    i. Code Division Multiple Access (CDMA)
    ii. Enhanced Data Rates for GSM Evolution (EDGE)
    iii. Integrated Digital Enhanced Network (iDEN)
    iv. General Packet Radio Service (GPRS)
    v. Global System for Mobile Communications (GSM)
    vi. High-Speed Downlink Packet Access (HSDPA)
    vii. Time Division Multiple Access (TDMA)
    viii. Universal Mobile Telecommunications System (UMTS)
    ix. Unlicensed Mobile Access (UMA)

52. Mobile Forensics Part 2
    a. Service provider data
        i. contains info such as call history and text messages, including the date and time
        ii. can act as backup evidence when the user deletes content from a mobile device.
    b. Call Detail Record (CDR) (Page 1025)
        i. contains information about user activities with the mobile phone.
        ii. The call data record contains several categories of information:
            1. Called telephone number or numbers
            2. Names and addresses of the subscribers or registered users
        iii. Date and time of the start and end of the communication
        iv. Telephone service used, e.g. voice, conference call, Short Message Service (SMS), Multimedia Service (MMS)
        v. International Mobile Subscriber Identity (IMSI) of the calling and called party
        vi. International Mobile Equipment Identity (IMEI) of the calling and called party
        vii. Location label (Cell ID) at the start and end of the communication

viii. Data mapping between Cell IDs and their geographical location at the start and end of the communication

c. What are some of the things that get recovered?
   i. Call history
   ii. SIM card information
   iii. Phonebook information
   iv. Subscriber & equipment ID's
   v. SMS information
   vi. GPS and Internet settings
   vii. Photos | Videos
   viii. Web browsing history
   ix. E-mails

d. Subscriber Identity Module (SIM) (Page 1026)
   i. Authenticates the user of the cell phone to the network to gain access to subscribed service
   ii. Has both volatile and non-volatile memory
   iii. Has its own file system residing in non-volatile memory
   iv. The SIM file system is hierarchical in nature, consisting of three parts:
      1. Master File (MF) (Page 1027)
         a. the root of the file system
         b. Contains one or more DF's
         c. May contain one or more EF's
         d. A 2-byte file identifier of 3F00 identifies the master file
      2. Dedicated File (DF) (Page 1027)
         a. contains only the header that holds information related to file structure and security information
         b. A 2-byte identifier is useful for DF to identify the dedicated file
      3. Elementary File (EF) (Page 1027)
         a. contains both the header and body
         b. holds actual data in different forms, including the transparent, linear fixed, and cyclic forms
         c. Contains a unique serial number of the individual SIM card
         d. Contains various types of data as a sequence of data bytes, a sequence of fixed-size records, or as fixed-size records.

e. Data stored in the SIM (Page 1027)
   i. Integrated circuit card identifier (ICCID) (Page 1028)
      1. 19-digit unique identification number printed on the SIM to identify each SIM internationally
   ii. International mobile subscriber identity (IMSI)
      1. 15-digit subscriber identification number that defines a subscriber in the wireless world, including the country and mobile network to which the subscriber belongs

iii. Service provider name (SPN)
    1. It signifies a SIM card service provider (example: Idea, Airtel, etc.)
iv. Mobile country code (MCC)
    1. 2 to 3-digit identification number printed on the SIM
    2. Represents the country code of a SIM user internationally on a GSM network.
    3. Identifies a mobile phone operator.
v. Mobile network code (MNC)
    1. 2-digit network id number used with the MCC printed on SIM.
    2. Used to identify the SIM user on a mobile phone network
vi. Mobile subscriber identification number (MSIN)
    1. 10-digit number that identifies the mobile phone service provider within a mobile carrier network
vii. Mobile international subscriber directory number (MSISDN)
    1. number used for international identification of mobile phone numbers
    2. ontains the country code and nation-wide destination code
    3. This number has up to 15 digits after the exclusion of prefixes.
viii. Abbreviated dialing numbers (ADN)
    1. These are three-digit dialing numbers
    2. help create communication in emergency cases for public services by governments and offer fast dialing
    3. This number is accessible even if the mobile phones are on lock.
    4. Mostly private users rent these
ix. Last dialed numbers (LDN)
x. Short message service (SMS)
xi. Text Message parameters (SMSP)
xii. Text message status (SMSS) (Page 1029)
    1. status of the message that the sender gets.
xiii. Phase ID (Phase)
    1. It is a SIM identification number
    2. Stored in bytes in SIM and forensics tools help to extract this data.
xiv. SIM Service table (SST)
    1. A subscriber provides the service data stored in the SIM
    2. This data is stored in the form of a table where associated services are
xv. HPLMN search period (HPLMNSP)
    1. Home public land mobile network search period (HPLMNSP)
    2. Area location information of a mobile phone on a network.
xvi. PLMN selector (PLMNsel)
    1. Public land mobile network PLMN (PLMN)
    2. info used to identify the area location of the mobile phone on a network and its roaming information.
xvii. Forbidden PLMNs (FPLMN)

1. When a mobile station (MS) receives the 'PLMN not allowed' message in response to a location register (LR) request from a VPLMN, this VPLMN is added to the list of forbidden PLMN.

xviii. Capability configuration parameter (CCP)
1. Contains parameters regarding info about the required network calls dialed, emergency calls; last call dialed, and rejected dialed numbers

xix. Access control class (ACC)
1. This is the restriction imposed on the user access on a GSM network.
2. 2-byte information stored in the SIMs/USIMs
3. There are 15 classes inside this file
4. The first 10 classes are for normal subscribers, while the remaining five classes are for high-priority users.

xx. Broadcast control channels (BCCH)
1. These are point-to-multipoint downlink broadcast channels. The base transceiver station broadcasts the BCCH. It provides the mobile device with network information, such as its services, access parameters, and neighbor list.

xxi. Language preference (LP)

xxii. Cardholder verification (CHV1 and CHV2) (Page 1029)
1. Checks whether or not the cardholder is an authorized person.
2. This condition allows access to the files only after successful verification of the user's PIN.

xxiii. Ciphering key (Kc) (Page 1030)
1. Ciphering keys are used to encrypt or decrypt the data for security

xxiv. Ciphering key sequence number (CKSN) (Page 1030)
1. The user uses the ciphering keys and CKSN refers to the ciphering keys.

xxv. Emergency call code (Page 1030)
1. fast-dialing service used in emergencies

xxvi. Fixed dialing numbers(FDN) (Page 1030)
1. When FDN is ON; a user can call only those numbers listed in FDN list
2. The incoming calls are unaffected due to this feature

xxvii. Dialing Extension (EXT1 & EXT2) (Page 1030)
1. number assigned to a person or department in an organization or company used along with the phone number

xxviii. Groups (GID1 & GID2) (Page 1030)
1. These are the files in SIM. There are two groups, GID1 and GID2
2. Lock for this GID1 and GID2 files is changeable, but is non-removable,
3. GID1 does not allow the use to put a SIM from the main network into a phone on a virtual network
4. GID2 is the normal lock so that the user can put in any other SIM other than that of the same network.

xxix. Preferred network messages (CBMI) (Page 1030)

1. messages from the network prompted on the mobile phone such as network not registered, SIM card registration fails, and network not available

xxx. Calls per unit (PUCT) (Page 1030)
1. Price per unit and currency table in the SIM allows the mobile phone to calculate the cost of a call in a currency chosen

xxxi. Accumulated Call Meter (ACM) (Page 1030)
1. ACM is a call meter, which records the charges for both current and ongoing calls and proceeding calls

xxxii. Call Limit (CAMMmax) (Page 1030)
1. This is the restricted call time limit for the caller

xxxiii. Location Information (LOCI) (Page 1031)
1. Contains the temporary mobile subscriber identity and location update status.
2. MSs use it to trace the information about the location of the mobile handset and provide the information about the current and moving locations of mobile phones

xxxiv. Local area identity (LAI)
1. location area (LA) within in any PLMN.
2. Location area code has both the MNC and MCC.

xxxv. Own dialing number
1. Referred to as the phone number

xxxvi. Temporary mobile subscriber identity (TMSI)
1. temporary identification number is generated randomly when the mobile phone is turned on and works as the temporary identity between mobile and network.

xxxvii. Routing area identifier (RAI) Network Code (Page 1031)
1. In a network, there are different areas and they can be identified by the identifier called RIA.
2. RIA is comprised of location area (LA) code and routing area code (RAC).
3. The network code is useful for identification of a network on a large network.

xxxviii. Service dialing numbers (SDNs) (Page 1031)
1. to view these numbers, the following steps should be taken: Contacts > Menu key > Settings
2. In settings, select Service numbers and all the numbers of service provider will be on display

xxxix. Depersonalization control Keys (Page 1031)
1. The service provider provides this code to unlock the mobile phone device and access the network. These keys are also known as unlocking codes.

f. Integrated Circuit Card Identification - ICCID (Page 1031)

i. 19 or 20-digit serial number of the SIM card
ii. printed and stored in the SIM card
iii. Can be acquired using ForensicSIM if not printed on the card
iv. consists of
    1. industry identifier prefix (89 for telecommunications)
    2. followed by a country code
    3. an issuer identifier number
    4. and an individual account identification number

g. International Mobile Equipment Identifier – IMEI (Page 1032)
    i. GSM-based unique number
    ii. Used by GSM to identify the device and even to stop access to the mobile phone if stolen
    iii. Identifies mobile equipment in 15 digits representing
        1. the manufacturer
        2. model type
        3. country in which it is approved
    iv. first eight digits are known as the Type Allocation Code (TAC)
    v. IMEI can be obtained by keying in *#06# in GSM and UMTS phones

h. **Electronic Serial Number – ESN** (Page 1033)
    i. 32-bit identifier that is attached on a secure chip inside CDMA devices
        1. first 8 to 14 bits in the ESN represent the manufacturer code
        2. remaining 24 to 18 bits represent the manufacturer of the device

i. By altering Electronic Serial Number (ESN), Preferred Roaming List (PRL), and Mobile Identification Number, the hacker or an attacker can make fraudulent calls in the name of original subscriber. (Page 1034)
    i. GSM mobiles have IMEI number instead of an ESN number.
    ii. SIM Cloning tool
        1. MOBILedit
        2. SIMiFOR ASC - SIM Cloner
            a. http://www.forensicts.co.uk
        3. 001Micron Data Recovery
            a. http://www.simrecovery.com/
    iii. Prerequisites:
        1. SIM card Reader
        2. Blank SIM card or Super SIM card
        3. SIM cloning software

j. SIM Data Acquisition tools (Page 1036)
    i. MOBILedit
    ii. SIM Explorer
    iii. MOBILedit! Forensice (Page 1038)
    iv. EnCase Forensic (Page 1038)
    v. Paraben's SIM-Card Seizure (Page 1038)

TOOLS Methodologies, Frameworks and Processes Term

TOOLS Methodologies, Frameworks and Processes Term

iii. SecureView
iv. NowSecure Forensics
v. MOBILedit
vi. Lantern
vii. Aceso (Page 1053)
viii. Athena (Page 1053)
ix. Elcomsoft iOS Forensic Toolkit (Page 1053)
x. iXAM (Page 1053)

q. The mobile forensics report should contain (Page 1056)
i. Summary
ii. Objectives
iii. Date and time the incident allegedly occurred
iv. Date and time the incident was reported to agency personnel
v. Name of the person or persons reporting the incident
vi. Examination start date and time
vii. The physical condition of the phone
viii. Photos of the phone and individual components
ix. Phone status when received turned on or off
x. Make and Model
xi. Mobile Subscriber International ISDN Number (MSISDN)
xii. Integrated Circuit Card ID (ICCID)
xiii. Service Provider Name (SPN)
xiv. Abbreviated dialing numbers
xv. Last Numbers received
xvi. Last Numbers dialed
xvii. Missed calls
xviii. Short Message Services (SMS)
xix. Calendar entries
xx. Photographs stored in the handset
xxi. Video stored in the handset
xxii. Smart Media/ Compact Flash
xxiii. MMS
xxiv. International Mobile Subscriber Identity (IMSI)
xxv. Mobile Country Code (MCC)
xxvi. Mobile Subscriber Identification Number (MSIN)
xxvii. Preservation of the evidence
xxviii. Investigative techniques
xxix. Tools used for the acquisition
xxx. Tools used for the examination
xxxi. Data found during the examination
xxxii. Notes from peer review
xxxiii. Supporting expert opinion

TOOLS Methodologies, Frameworks and Processes Term

r. How do I acquire data from a SIM Card?
    i. To access the SIM, PIN code (Personal Identification Number) is required
    ii. Failure to enter a valid PIN in three attempts blocks the card and then an eight-digit PUK (Personal Unlock Number) must be entered
    iii. PUK is provided by the network operator and cannot be changed by the user
    iv. Failure to get correct PUK in 10 attempts disables the SIM permanently
    v. Investigator should ask the network operator for PUK to gain access to the SIM

14. Forensics Report Writing

53. Forensics Report Writing
    a. A computer forensics report provides detailed information on complete computer forensics investigation process
    b. Goals of an investigative report (Page 1066)
        i. Investigative report writing involves a well-structured documentation that should be truthful, timely, and understandable to the target audience.
    c. What does a sample report look like?
        i. http://www.academia.edu/12324822/Example_of_An_Expert_Witness_Digital_forensics_Report
    d. Aspects of a good report
        i. The main objective of a cybercrime investigation is to identify the evidence and facts.
        ii. Provide a detailed explanation of the
            1. approach to the problem.
            2. The examination procedures
            3. materials or equipment's used
            4. analytical or statistical techniques implemented
            5. data collection of sources
        iii. Present data in a well-organized manner.
            1. Better to record all the data and observations in a laboratory notebook
            2. All the data presented in tabular forms should be labeled properly
        iv. Include all calculations and algorithms done during the investigation in a summarized form.
            1. The algorithms denoted in the report should be coined with some specific names, such as Message Digest 5 (MD5) hash.
            2. Report should contain a brief description of the standard tools used in the investigation and their cited sources.
        v. Provide a statement of uncertainty and error analysis during the observation.
            1. Provide the limitations of knowledge to protect the integrity during a computer investigation.
            2. if an investigator retrieves a time stamp from a computer file, then one should state explicitly in the report that a time stamp can be reset easily.

vi. It should explain all the results in a logical order
    1. using subheadings, tables, and figures, to address the purpose of the report
    2. Results should be presented in such a way that any reader, irrespective of his/her knowledge of the case, can understand the whole investigation process
vii. Results and conclusions should be discussed.
    1. All the findings and their significances should be established in light of overall examination in the discussion section.
    2. questions on how the case developed
    3. what were the problems faced
    4. how the solutions were approached should also be answered.
viii. Enlist all the references in alphabetical order for providing sufficient details to track down the information used in drafting the report.
    1. It should follow a standard writing style for references including books, journal articles, leaflets, websites, and other materials mentioned
ix. Any extra materials used in the report should be included as appendix
    1. charts, diagrams, graphs, transcripts, and copies of materials with proper description of each particular
    2. They should be mentioned in their order of occurrence in the text of the report.
x. optional, a report can end up with an acknowledgment section
    1. It is not a dedication but a gesture of thanking people in general who helped during the research.
    2. people who contributed in analysis and proofreading of the report can be mentioned in this section

e. Report template
    i. Executive summary:
        1. Case number
        2. Names and Social Security Numbers of authors, investigators, and examiners
        3. Purpose of investigation
        4. Significant findings
        5. Signature analysis
    ii. Investigation objectives
    iii. Details of the incident
        1. Date and time the incident allegedly occurred
        2. Date and time the incident was reported to the agency's personnel
        3. Details of the person or persons reporting the incident
    iv. Investigation process
        1. Date and time the investigation was assigned
        2. Allotted investigators

3. Nature of claim and information provided to the investigators

v. Evidence information
    1. Location of the evidence
    2. List of the collected evidence
    3. Tools involved in collecting the evidence
    4. Preservation of the evidence

vi. Evaluation and analysis Process
    1. Initial evaluation of the evidence
    2. Investigative techniques
    3. Analysis of the computer evidence (Tools involved)

vii. Relevant findings

viii. Supporting Files
    1. Attachments and appendices
    2. Full path of the important files
    3. Expert reviews and opinion

ix. Other Supporting details
    1. Attacker's methodology
    2. User's applications
    3. Internet activity
    4. Recommendations

f. Spoliation (Page 1071)
    i. If the produced informal written report is destroyed then it is considered as destruction or concealing of evidence

g. Expert witness (Page 1073)
    i. An expert witness is a witness, who by virtue of education, profession, or experience, is believed to have special knowledge of his/her subject beyond that of the average person, sufficient that others legally depend upon his/her opinion
    ii. The opinion of an expert witness, authorized by a court, has legal status and can be accepted as evidence by the court of law

h. Technical witness vs. Expert witness (Page 1074)
    i. Technical --> Worker Bee
        1. May only provide facts found during the investigation
        2. they cannot draw conclusions or offer opinion
    ii. Expert --> Queen Bee
        1. can give opinions based on their observation and experiences
        2. Can perform a deductive analysis with facts found during an investigation

i. How do I qualify?
    i. According to US federal rules, to be present as an expert witness in a court, the following information must be furnished:
        1. Four years of previous testimony (indicates experience)

2. Ten years of any published literature
3. Previous payment received when giving testimony

j. The Daubert Standard (Page 1074)
   i. The rule of evidence regarding the admissibility of the expert witnesses' testimony during the federal legal proceedings.
   ii. Rule for federal trial judges to act as "gatekeepers" of scientific evidence
   iii. Standard used by a trial judge to make a preliminary assessment of whether an expert's scientific testimony is based on reasoning or methodology that is scientifically valid and can properly be applied to the facts at issue. Under this standard, the factors that may be considered in determining whether the methodology is valid are:
      1. (1) whether the theory or technique in question can be and has been tested;
      2. (2) whether it has been subjected to peer review and publication;
      3. (3) its known or potential error rate;
      4. (4) the existence and maintenance of standards controlling its operation; and
      5. (5) whether it has attracted widespread acceptance within a relevant scientific community.
      6. See Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).
   iv. https://www.law.cornell.edu/wex/daubert_standard#

k. Fry Standard (Page 1075)
   i. Related to the admissibility of scientific examinations or experiments in legal cases
   ii. Any kind of expert opinion based on scientific techniques is admissible, if the technique involved is acceptable by the relevant scientific community
   iii. Legal precedent regarding admissibility of scientific examinations or experiments in legal cases

l. Charactaristics of a good expert witness (Page 1075)
   i. Self-confidence
   ii. Politeness
   iii. Sincerity
   iv. Preparedness
   v. Awareness
   vi. Relaxed excellence

m. The order of a trial (Page 1077)
   i. Motion(s) in beginning
   ii. Opening statement
   iii. Presentation of the case | Cross examination & rebuttal
   iv. Closing arguments
   v. Jury orders

n. General ethics while testifying (Page 1078)

i. **Maintain a steady body expression**
ii. **Always be enthusiastic while giving testimony.**
iii. **Always pay a compliment to the jury.**
iv. **Avoid leaning, develop self-confidence and create personal space with a winning professional style in the courtroom.**

o. Deposition (Page 1082)
   i. A question and answer session in which both the attorney and the opposing counsel are present and are involved in the cross-examination of a witness
   ii. Testimony is admissible at trial
   iii. Informal atmosphere
   iv. attorney's office is the best location for conducting the deposition
   v. purpose of a deposition is to identify the facts and acquire evidence of the investigation
   vi. procedural rules during examination are direct examination, cross-examination, and redirect examination
   vii. Deposition differs from a trial (Page 1083)
      1. **Both attorneys are present**
      2. No jury or judge present
      3. Opposing counsel asks questions

p. Guidelines for dealing with media (Page 1084)
   i. Avoid contact with media during a case
   ii. Do not give opinions about the trial to media; simply refer to the attorney
   iii. Avoid conversing with the media because
      1. It is unpredictable what the journalists might publish
      2. The comments might influence the case
      3. It can create a record that could be used against you while your present future testimonies
   iv. Record your interviews, if any, with the media

54. EC-Council Assessment
   a. Identify Rule 901 of forensic laws
      i. Requirement of authentication and identification
   b. Federal Rules of Evidence for Admissibility and Duplicates
      i. Rule 1003
   c. "Evidence must be related to the fact being proved", defines which characteristic?
      i. Admissible
   d. Identify the nature of digital evidence
      i. Fragile
   e. The result of which analysis may indicate the additional steps that needs to be taken in the extraction and analysis processes?
      i. Application file and analysis
   f. A system's audit policy is maintained in the Security hive, below the PolicyPolAdtEv key. Its default value is REG_NONE data type and contains binary information into which the

audit policy is encoded. The first 4 bytes (DWORD) of the binary data gives the information about whether auditing was enabled. The value of DWORD explains the status of the audit policy. The value 02 means:

    i. Failure events are audited

g. What description does the FTP sc-status Error Code 1xx give?
    i. Positive preliminary replies
h. Which of the following pane represents a structured view of all gathered evidence in a Windows-like folder hierarchy?
    i. Tree Pane
i. By default, a backup copy of the case file is saved every 10 minutes. Selecting which option you can disable the autosave function?
    i. 0
j. “Once you select a role, you can change the role if needed”. Identify whether the above statement is true or false:
    i. False
k. In which of this files contain a collection of files, but lack the integration of metadata and compression hash values that the EnCase evidence file provides:
    i. Raw image files
l. Source Processor automates and streamlines common investigative tasks that collect, analyze, and report on evidence. Which of this source processor module obtains drives and memory from a target machine?
    i. Acquisition module
m. “EnCase have built-in capabilities to view all file types”. Identify whether the above statement is true or false:
    i. False
n. The file content of evidence files can be viewed using the View Pane. The View pane provides several tabs to view file content. Which of this tab provides native views of formats supported by Oracle outside in technology?
    i. Doc tab
o. When does a file group bookmark get created in EnCase?
    i. If more than one file is selected in the entries table

Size of partition table which stores info about the parititions present - 64 byte

Bits used by MBR for storing LBAs - 32 bits

Bits used by HFS to address allocation blocks - 16 bits

Size of a sector – 512 bytes

Bytes in each logical block in GPT – 512 bytes

TOOLS Methodologies, Frameworks and Processes Term

http://stop.zona-m.net/2018/01/spectre-explained-as-if-computer-were-banks/

TOOLS Methodologies, Frameworks and Processes Term