Chapter 1

CHFIv9 STUDY GUIDE

Computer Forensics- deals with the process of finding evidence related to a digital crime
Cybercrime refers to “any illegal act that involves a computer, its systems, or its applications.”

Internal Attacks:

Insider attacks, considered as a primary threat, refer to attacks by disgruntled individuals working in the same firm or household as the victim. Examples of internal attacks include espionage, theft of intellectual property, manipulation of records, and Trojan horse attack.

External attacks:

External attacks originate from outside of an organization or can be remote in nature. Such attacks occur when there are inadequate information security policies and procedures.

Rules of Forensics Investigation

A forensic examiner must keep in mind certain rules to follow during a computer forensic examination, as well as to handle and analyze the evidence. This will safeguard the **integrity** of the evidence and render it **acceptable** in a court of law. The forensic examiner must **make duplicate copies** of the original evidence and start by **examining only the duplicates.** The duplicate copies must **be accurate** replications of the originals, and the forensic examiner must also **authenticate the duplicate copies** to avoid questions about the **integrity** of the evidence. The computer forensic examiner **must not continue** with the investigation if the examination is **going to be beyond his or her knowledge level** or skill level.

Forensic investigators should memorize the rules listed below.

- Limit access and examination of the original evidence
- Record changes made to the evidence files
- Create a chain of custody document
- Set standards for investigating the evidence
- Comply with the standards
- Hire professionals for analysis of evidence
- Evidence should be strictly related to the incident
- The evidence should comply with the jurisdiction standards
- Document the procedures applied on the evidence
- Securely store the evidence
- Use recognized tools for analysis

Enterprise Theory of Investigation (ETI) -ETI is a methodology for investigating criminal activity. It adopts a holistic approach toward any criminal activity as a criminal operation rather than as a single criminal act.

Understanding Digital Evidence

Digital evidence includes all such information that is either stored or transmitted in digital form and has probative value. Investigators should take utmost care while gathering digital evidence as it is fragile in nature. According to Locard's Exchange Principle, “anyone or anything, entering a crime scene takes something of the scene, and leaves something of themselves behind.”

Digital Forensics Challenge

Forensic investigators face many challenges during forensics investigation of a digital crime, such as extracting, preserving, and analyzing the digital evidence. For example, system data that an intruder can easily change or destroy should have priority while assembling the evidence.

Volatile Data: Volatile data refers to the temporary information on a digital device that requires a constant power supply and is deleted if the power supply is interrupted. Important volatile data includes **system time, logged-on user(s), open files, network information, process information, process-to-port mapping, process memory, clipboard contents, service/driver information, command history, etc**.

Non-volatile Data: Non-volatile data refers to the permanent data stored on secondary storage devices, such as hard disks and memory cards. Information stored in non-volatile form includes **hidden files, slack space, swap file, index.dat files, unallocated clusters, unused partitions, registry settings, and event logs.**

Characteristics of Digital Evidence

Admissible Evidence relevant to the case, act in support of the client presenting it, and be well communicated and non-prejudiced.

Authentic investigators must provide supporting documents regarding the authenticity, accuracy, and integrity of the evidence with details such as source and its relevance to the case. If necessary, they must also furnish details such as author of the evidence or path of transmission.

Complete must either prove or disprove the consensual fact in the litigation

Reliable extract and handle the evidence while maintaining a record of the tasks performed during the process to prove that the evidence is dependable. Forensic investigation is conducted only on the copies of evidence.

Believable present evidence in a clear manner to the jury and obtain expert opinions where necessary

Best Evidence Rule

The best evidence rule is to prevent any alteration of digital evidence, either intentionally or unintentionally.

Duplicate will also suffice as evidence under the following conditions:

- Original evidence is destroyed due to fire and flood.
- Original evidence is destroyed in the normal course of business.
- Original evidence is in possession of a third party.

Types of approaches to manage cybercrime investigations

Civil cases involve disputes between two parties, which may include an individual versus a company, an individual versus another individual, or a company versus another. They relate to **violation of contracts and lawsuits, where a guilty verdict generally results in monetary damages to plaintiff.**

Criminal Cases criminal cases involve actions that are against the norms of society. DID YOU KNOW WHAT YOU DID? IF SO, IT IS CRIMINAL.

- Investigators must follow a set of standard forensic processes accepted by law in the respective jurisdiction.
- Investigators, under court's warrant, have the authority to seize the computing devices.
- A formal investigation report is required.
- The law enforcement agencies are responsible for collecting and analyzing evidence.
- Punishments are harsh and include fine, jail sentence or both.
- Standard of proof needs to be very high.
- Difficult to capture certain evidence, e.g., GPS device evidence

Administrative Investigation refers to an internal investigation by an organization to discover if its employees, clients and partners are abiding by the rules or policies. Violation of company policies.

- Involves an agency or government performing inquiries to identify facts with reference to its own management and performance
- Non-criminal in nature and related to misconduct or activities of an employee that includes but are not limited to:
  - Violation of organization's policies, rules, or protocols. Resource misuse or damage or theft
  - Threatening or violent behavior. Sexual Exploitation, harassment and abuse
  - Improper promotion or pay raise, corruption and bribery

Scientific Working Group on Digital Evidence (SWGDE)

Principle 1 To ensure that digital evidence is collected, preserved, examined, or transferred in a manner that safeguards the accuracy and reliability of the evidence, law enforcement and forensic organizations must establish and maintain an effective system for quality control.

Standards and Criteria

1.1 All agencies that seize and/or examine digital evidence **must maintain an appropriate SOP** document.

1.2 Agency mgmt. must review SOPs on an annual basis to ensure their continued suitability and effectiveness.
1.3 SOPs must be generally accepted or supported by data gathered and recorded in a scientific manner.
1.4 The agency must maintain written copies of the appropriate technical procedures.
1.5 The agency must use hw and sw that is appropriate and effective for the seizure/examination procedure.
1.6 All activities related to the seizure, storage, examination, or transfer of digital evidence must be recorded in writing and be available for review and testimony.

Forensic Readiness refers to an organization's ability to make optimal use of digital evidence in a limited period and with minimal investigation costs. It includes technical and nontechnical actions that maximize an organization's competence to use digital evidence.

A forensic investigator performs the following tasks:

- Evaluates the damages of a security breach
- Identifies and recovers data required for investigation
- Extracts the evidence in a forensically sound manner
- Ensures proper handling of the evidence
- Acts as a guide to the investigation team
- Creates reports and documents about the investigation required to present in a court of law
- Reconstructs the damaged storage devices and uncovers the information hidden on the computer
- Updates the organization about various methods of attack and data recovery techniques, and maintains a record of them (following a variant of methods to document) regularly
- Addresses the issue in a court of law and attempts to win the case by testifying in court
- **Fourth Amendment** states that government agents may not search or seize areas or things in which a person has a reasonable expectation of privacy, without a search warrant. **Note:** Private intrusions not acting in the color of governmental authority do not come under the Fourth Amendment.

CHAPTER 1 SUMMARY

- Computer forensics refers to a set of procedures and techniques to identify, gather, preserve, extract, interpret, document and present evidence from computing equipment that is acceptable in court
- Cybercrime is defined as any illegal act involving a computing device, network, its systems, or its applications. Categorized into two types based on the line of attack: internal attacks and external attacks
- Computer crimes pose new challenges for investigators due to their speed, anonymity, volatile nature of evidence, global origin and difference in laws, and limited legal understanding
- Approaches to manage cybercrime investigation include: civil, criminal, and administrative
- Digital evidence is "any information of probative value that is either stored or transmitted in a digital form". It is of two types: volatile and non-volatile
- Forensic readiness refers to an organization's ability to make optimal use of digital evidence in a limited period of time and with minimal investigation costs
- Organizations often include computer forensics as part of incident response plan so as to track and prosecute perpetrators of an incident

Chapter 2 CHFIv9 STUDY GUIDE

The computer forensics investigation process includes a methodological approach for preparing for the investigation, collecting and analyzing evidence, and managing the case from reporting to the conclusion.

Phases Involved in the Computer Forensics Investigation Process

Pre-investigation Phase: all the tasks performed prior to the commencement of the actual investigation

- setting up a computer forensics lab(CFL), toolkit, and workstation
- the investigation team and getting approval from the relevant authority
- planning the process, defining mission goals, and **securing the case perimeter and devices involved.**
- **Investigation Phase:** Main phase of the computer forensics investigation performed by professionals
- acquisition, preservation, and analysis of the data to identify the source of crime and the culprit.

- implementing the technical knowledge to find evidence, examine, document, and preserve the findings.
- **Post-investigation Phase:** Reporting and documentation of all the actions undertaken and the findings during the course of an investigation.
- Ensure that the target audience can easily understand the report
- ensure report provides adequate and acceptable evidence.
- report should comply with all local laws and standards
- it should be legally sound and acceptable in the court of law.
- **Setting up a CFL:**
- Planning and budgeting
- Location and structural concerns. Work area considerations (50-63 sqft per station) no windows
- HR Considerations (certifications and experience)
- Physical security recommendations. Have the lab forensically licensed
    - ASCLD/Lab Accreditation
    - ISO/IEC 17025

TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations. Compromising emanations are unintentional intelligence-bearing signals that if intercepted and analyzed will disclose classified information when it is transmitted, received, handled, or otherwise processed by any information processing equipment."

A **search warrant** is a written order issued by a judge that directs a law enforcement officer to search for a particular piece of evidence at a particular location

Forensic Hardware Tools

- **FRED** systems are optimized for stationary laboratory acquisition and analysis. FRED will 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.
- **Paraben's StrongHold** Faraday Bags block out wireless signals to protect evidence.
- **PC-3000 Data Extractor** diagnoses and fixes file system issues, so that the client's data can be obtained.
- **Paraben's Chat Stick** is a thumb drive device that will search the entire computer and scan it for chat logs
- **RAPID IMAGE 7020 X2** designed to copy one "Master" hard drive to up to 19 "Target" hard drives
- **RoadMASSter-3 X2** is a forensic ruggedized portable lab for hdd data acquisition and analysis.
- **Image MASSterTM Wipe PRO** is a hard Drive Sanitization Station.
- **PC-3000 Flash** is a hardware and software suite for recovering flash- based storage
- **ZX-Tower** provides secure sanitization of hard disk
- **WriteProtect-DESKTOP** provides secure, read-only write-blocking of suspect hard drives.
- **Data Recovery Stick** can recover deleted files.
- **Tableau T8-R2 Forensic USB Bridge** offers secure, hw-based write blocking of USB storage devices.
- **Forensic Software Tools**
- **Cain & Abel** pw recovery for MS OS. Uses sniffing, dictionary, brute-force, and cryptanalysis attacks. Also record VoIP, decode scrambled passwords, recover wireless keys, reveal password boxes, uncover cached passwords and analyze routing protocols.
- **Recuva** recover lost pictures, music, docs, video, email, or other file type from all types of media
- **Capsa** sniffer with support for over 300 network protocols
- **R-Drive Image** utility that provides creation of disk image files for backup or duplication purposes.
- **FileMerlin** converts word processing, xls, ppt and database files between a wide range of file formats.
- **AccessData FTK** court-cited digital investigations platform that provides processing and indexing up front, so filtering and searching is fast. FTK can be setup for distributed processing and incorporate web-based case management and collaborative analysis.

- **Guidance Software's EnCase** Rapidly acquire data from variety of devices and unearth potential evidence with disk-level forensic analysis. Produce comprehensive reports on your findings and maintain the integrity of your evidence in a format the courts have come to trust
- **Nuix Corporate Investigation Suite** used to collect, process, analyze, review, and report evidence.
- **PALADIN** is a modified "live" Linux distribution based on the PALADIN Toolbox.
- **The Sleuth Kit** cmd line tools and a C library to analyze disk images and recover files from them.
- **Autopsy** digital forensics platform and gui to The Sleuth Kit® and other digital forensics tools.
- **Oxygen Forensic Kit** is a ready-to-use and customizable mobile forensic solution for field and in-lab usage. Allows extraction of data from the device but also creates reports and analyzes data in the field.
- **L0phtCrack** is a password auditing and recovery software.
- **Ophcrack** is a free GUI driven Windows password cracker based on rainbow tables
- **NIST has launched the Computer Forensic Tool Testing Project (CFTT), which establishes a "methodology for testing computer forensic software tools by development of general tool specifications, test procedures, test criteria, test sets, and test hardware."**

Forensic Investigation Team

- **Attorney:** legal advice about the investigation, and legal issues involved in the forensics investigation process.
- **Photographer**: Photographs the crime scene and all evidence. Should have an authentic certification.
- **Incident Responder:** Responsible for the measures taken when an incident occurs, securing the incident area and collecting the evidence that is present at the crime scene. He or she should disconnect the system from other systems to stop the spread of an incident
- **Decision Maker:** The person responsible for authorization of a policy or procedure during the investigative process. Based on the incident type, makes decision about the policies and procedures to handle the incident.
- **Incident Analyzer:** Analyzes the incidents based on their occurrence. He or she examines the incident with regard to its type, how it affects the systems, different threats and vulns associated with it
- **Evidence Examiner/Investigator:** Examines the evidence acquired and sorts the useful evidence.
- **Evidence Documenter:**gathers info and documents it from incident occurrence to the end of the investigation.
- **Evidence Manager:** has all the information about the evidence:name, evidence type, time, source of evidence, etc. manages and maintains a record of the evidence such that it is admissible in the court of law.
- **Expert Witness**: Offers a formal opinion as a testimony in a court of law.

Forensic Laws

- **18 USC §1029** - Fraud and related activity in connection with access devices
- **18 USC §1030** - Fraud and related activity in connection with computers
- **18 USC §1361-2** - Prohibits malicious mischief
- **18 USC §2252A** -law about child pornography
- **18 USC §2252B** -misleading domains on Internet
- **18 USC §2702** - voluntary disclosure of contents to government and non-government entities
- **42 USC §2000AA** -Privacy Protection Act, special steps to take during seizure that don't prevent freedom of expression
- **Rule 402** - General Admissibility of Relevant Evidence
- **Rule 502** - Attorney-Client privilege and work product; Limitations on waiver
- **Rule 608** - Evidence of character and conduct of witness
- **Rule 609** - Impeachment by evidence of a criminal conviction
- **Rule 614** - Calling and interrogation of witnesses by court
- **Rule 701** - Opinion testimony by lay witnesses
- **Rule 705** - Disclosure of facts or data underlying expert opinion
- **Rule 801** - hearsay
- **Rule 901** - Authenticating or Identifying Evidence

- **Rule 1002** - Requirement of original
- **Rule 1003** - Admissibility of duplicates
- **Rule 1004** - Admissibility of other evidence of Content

<u>Checklist to Prepare for a Computer Forensics Investigation</u>

1. Do not turn the computer off or on, run any programs, or attempt to access data on the computer.
2. Secure any relevant media including hard drives, cell phones, DVDs, USB drives, etc subject may have used
3. Suspend document destruction and recycling that may pertain to relevant media or users at the time of issue
4. 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
5. Once the machine is secured, obtain info about the machine, the peripherals, and network where connected
6. If possible, obtain passwords to access encrypted or password-protected files
7. Compile a list of names, e-mails, and other info of those with whom the subject might have communicated
8. 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 accessed, and when access occurred. If possible, find out why the pc was accessed
9. 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.
10. Create a list of key words or phrases to use when searching for relevant data

<u>Best Practices</u>

- Get authorization to conduct the investigation, from an authorized **decision maker**
- **Document all the events** and decisions at the time of the incident and incident response
- Depending on the scope of the incident and presence of any national security issues or life safety issues, the **first priority is to protect the organization from further harm**
- **The following are the Computer Forensics Investigation Methodology:**
- First Response
- Search and Seizure
- Collect the Evidence
- Secure the Evidence
- Data Acquisition
- Data Analysis
- Evidence Assessment
- Documentation and Reporting
- Testify as an Expert Witness

Documentation of the electronic crime scene is a **continuous process** during the investigation, making a permanent record of the scene. It includes photographing and sketching of the scene.

- If the evidence gathered by the CFP suggests that the suspect has committed a crime, he or she will produce that evidence in court. If the evidence suggests that the suspect has breached company policy, the CFP will hand over the evidence at the corporate enquiry.
- If the **suspect is present** at the time of the search and seizure, the **incident manager or the laboratory manager** may consider asking some questions. However, they must comply with the relevant human resources or legislative guidelines with regard to their jurisdiction

<u>Warrants</u>

Electronic storage device warrant allows the first responder to search and seize the victim's computer components such as HW/SW, Storage devices, Documentation

Service Provider search warrant allows first responders or investigators to consult the service provider and obtain the available **victim's computer information and** Service records, Billing records, Subscriber information

“**When destruction of evidence is imminent**, a **warrantless seizure** of that evidence is justified if there is probable cause to believe that the item seized constitutes evidence of criminal activity.” United States v. David, 756 F. Supp. 1385, 1392 (D. Nev. l991). Agents **may search** a place or object without a warrant or probable cause, if a person with authority has consented. Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973).

Dealing with Powered Off Computers

At this point of the investigation, do not change the state of any electronic devices or equipment:

- If it is switched OFF, leave it OFF
- If a monitor is switched OFF and the display is blank:
- Turn the monitor ON, move the mouse slightly, observe the changes from a blank screen to another screen, and note the changes and photograph the screen.
- If a monitor is switched ON and the display is blank
- Move the mouse slightly. If the screen does not change, do not perform any other keystroke.
- Photograph the screen.

Dealing with Networked Computer If the victim’s computer has an Internet connection, the first responder must follow the following procedure in order to protect the evidence:

- Unplug the network cable from the router and modem internet can make it vulnerable to further attack
- Don’t use the pc for evidence search because it may alter or change the integrity of the existing evidence
- Unplug all the cords and devices connected to the computer and label them for later identification
- Unplug the main power cord from the wall socket
- Pack the collected electronic evidence properly and place it in a static-free bag
- Keep the collected evidence away from magnets, high temperature, radio transmitters, and other elements that may damage the integrity of the evidence
- Document all the steps that involved in searching and seizing the victim’s computer for later investigation

Preserving Electronic Evidence

- Document the actions and changes observed on the monitor, system, printer, or other electronic devices
- Verify that the monitor is ON, OFF, or in sleep mode
- Remove the power cable, depending on the power state of the computer, i.e., ON, OFF, or in sleep mode
- Do not turn ON the computer if it is in the OFF state
- Take a photo of the monitor screen if the computer is in the ON state
- Check the connections of the telephone modem, cable, ISDN, and DSL
- Remove the power plug from the router or modem
- Remove any portable disks that are available at the scene to safeguard potential evidence
- Keep the tape on drive slots and the power connector
- Photograph the connections between the computer system and the related cables, and label them
- Label every connector and cable connected to the peripheral devices

Chain of Custody legal document that demonstrates the progression of evidence as it travels from the original evidence location to the forensic laboratory. It is a roadmap that shows how investigators collected, analyzed, and preserved the evidence. It ensures accurate auditing of the original data evidence, imaging of the source media, tracking of the logs, and so on. The chain of custody shows the technology used and the methodology adopted in the forensic phases as well as the persons involved in it. The chain of custody administers the collection, handling, storage, testing, and disposition of evidence. It helps to ensure protection of evidence against tampering or substitution of evidence. Chain of custody documentation should list all the people involved in the collection and preservation of evidence and their actions, with a stamp for each activity.

Exhibit numbering the process of tagging evidence with sequential number, which includes case and evidence details. This will allow the investigator to easily identify the evidence and know its details.

The investigators should mark all the evidence in a pre-agreed format, such as: **aaa/ddmmyy/nnnn/zz.**

- ***aaa*** are the initials of the forensic analyst or law enforcement officer seizing the equipment.
- ***dd/mm/yy*** is the date of seizure.
- ***nnnn*** is the sequential number of the exhibits seized by aaa, starting with 001 and going to nnnn.
- ***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.)

Image Integrity Tools:

- HashCalc-created MD5 hash for files, text and hex strings; 13 different algorithms
- MDF Calculator-view MD5 hash to compare to provided hash value
- HashMyFiles-calculate MD5 hash on one or more files. Can also display MD5 hashes of files or folders
- **Recover Lost or Deleted Data**
- Recover My Files-recover deleted files emptied from recycle bin, accidental format, hard disk crash, etc.
- Recuva-recover all types of lost files from disk or removable media
- Advanced Disk Recovery-quick or deep scan for lost or deleted files
- UndeletePlus-same as above
- **Data Analysis Tools**
- **FTK Imager**- data preview and imaging tool that enables analysis of files and folders on local hard drives, CDs/DVDs, network drives, and examination of the content of forensic images or memory dumps. FTK Imager can also create MD5 or SHA1 hashes of files, review and recover files deleted from the Recycle Bin, export files and folders from forensic images to disk and mount a forensic image to view its contents in Windows Explorer.
- **EnCase Forensic**- popular multi-purpose forensic platform that includes many useful tools to support several areas of the digital forensic process. It also generates an evidence report. EnCase Forensic can help investigators acquire large amounts of evidence, as fast as possible from laptops and desktop computers to mobile devices. EnCase Forensic directly acquires the data and integrates the results into the cases.
- **The Sleuth Kit (TSK)** -library and collection of command line tools that allows investigating disk images. The core functionality of TSK allows analyzing volume and filing system data. The plug-in framework also allows incorporating additional modules to analyze file contents and build automated systems. The library can be incorporated into larger digital forensics tools and the command line tools can be directly used to find evidence.

Tools to obtain information from different common social media websites:

- Netvizz, twecoll, divud, Digitalfootprints, Netlytic, X1 Social Discovery, Facebook Forensic Software
- H&A forensics, Geo360, Navigator by LifeRaft Social, Emotive, etc.

Chapter 2 Summary

- 3 phases in Computer Forensics Investigation Process, Pre-investigation, Investigation and Post-Investigation
- A CFL is a location designated for conducting a computer-based investigation on the collected evidence
- Search warrant is an order from a judge that directs LE to search for a particular piece of evidence at a particular location
- Make a duplicate of the collected data so as to preserve the original
- To preserve the integrity of the physical evidence, all evidence collected should be handled carefully
- All digital evidence must be stored in a container, which must be secured to prevent unauthorized access
- Documentation of the electronic crime scene is a continuous process during the investigation that creates a permanent record of the scene
- Final report should include what the investigator did during the investigation, and what he or she found

Chapter 3 CHFIv9 STUDY GUIDE

Hard Disks and Filesystems

- **Platters** circular metal disks mounted into a drive enclosure

- **Tracks** are concentric rings on the platters that store data; each track has smaller partitions called **disk blocks or sectors.** Track numbering starts at 0 and goes to 1023.
- **Sectors** are the **smallest physical storage** units located on a hard disk platter and are 512bytes long. New format sectors are 8 512B sectors to make one 4096B or 4KB sector; which is more efficient
- **Clusters** are the **smallest accessible/logical storage units** on the hard disk. Clusters form by combining sectors in order to ease the process of handling files. Also called allocation units, the clusters are sets of tracks and sectors ranging from 2 to 32, or more, depending on the formatting scheme
- **Slack space** is the wasted area of the disk cluster lying between end of the file and end of the cluster when the file system allocates a full cluster to a file, which is smaller than the cluster size.
- **Bad sectors** refer to the portions of a disk that are unusable due to some flaws in them and do not support the read or write operations. The data stored in bad sectors is not completely accessible. Bad sectors might be due to configuration problems or any physical disturbances to the disk.
- **Master Boot Record (MBR)** refers to a hard disk's first sector or **sector zero** that specifies the location of an operating system for the system to load into the main storage. Also called as, partition sector or master partition table contains a table, which locates partitioned disk data. **HOW BIG IS IT? 512BYTES**
- A **sparse file** is a type of computer file that attempts to use file system space more efficiently when blocks allocated to the file are mostly empty.
- **Cylinders, Heads, and Sectors (CHS)**determine the sector addressing for individual sectors on a disk
- **Logical Block Addressing (LBA)** addresses data by allotting a sequential number to each sector
- **BIOS Parameter Block (BPB)** data at sector 1 in the volume boot record and explains the layout
- **Master Boot Code** loads into BIOS and initiates system boot process

Master Boot Record (MBR)

- 512bytes long
- contains four 16-byte master partition records
- MBR starts @ sector 0
- volume boot sector is present in cylinder 0, head 0, and sector 1 of the default drive
- MBR signature or end of sector is always **0x55AA**

Back up the MBR:

dd if=/dev/xxx of=mbr.backupbs=512 count=1

Restore the MBR:

dd if=mbr.backup of=/dev/xxx bs=512 count=1

Globally Unique Identifier (GUID)

- 128-bit unique number generated by windows used to identify COM DLLs, primary key values, browser sessions, and usernames
- contains four 16-byte master partition records

GUID Partition Table (GPT)

- allows for disks larger than 2T and allows users to have 128 partitions on windows
- partition and boot data is more secure than MBR
- uses CRC to ensure data integrity and CRC32 checksum for header and partition table

<u>Windows Boot Process</u>

1. System switches ON, CPU sends a Power Good signal to mboard and checks for computer's BIOS firmware.
2. BIOS starts a POST and load all the firmware settings from nonvolatile memory on the mboard.
3. If POST is successful, add-on adapters perform a self-test for integration with the system.
4. The pre-boot process will complete with POST, detecting a valid system boot disk.
5. After POST, the computer's firmware scans boot disk and loads the master boot record (MBR), which search for basic boot information in Boot Configuration Data (BCD).

6. MBR triggers Bootmgr.exe, which locates Windows loader (Winload.exe) on the Windows boot partition and triggers Winload.exe.
7. Windows loader loads the OS kernel ntoskrnl.exe.
8. Once the Kernel starts running, the Windows loader loads HAL.DLL, boot-class device drivers marked as BOOT_START and the SYSTEM registry hive into the memory.
9. Kernel passes the control of boot process to the Session Manager Process (SMSS.exe), which loads all other registry hives and drivers required to configure Win32 subsystem run environment.
10. Session Manager Process triggers Winlogon.exe, which presents the user logon screen for user authorization.
11. Session Manager Process Initiates Service control manager, which starts all the services, rest of the non-essential device drivers, the security subsystem LSASS.EXE and Group policy scripts.
12. Once user logs in, Windows creates a session for the user.
13. Service control manager starts the Explorer.exe and initiates the Desktop Window Manager (DMW) process, which set the desktop for the user.

Deleted and Overwritten GUID Partitions

Case 1: In hard disks, the conversion or repartition of the MBR disk to GPT will generally overwrite the sector zero with a protective MBR, which will delete all the information about the old partition table. The investigators should follow the standard forensics methods of searching the filesystems to recover data about the previous MBR partitioned volumes.

Case 2: When conversion or repartition of the GPT to MBR disk takes place, then the GPT header and tables may remain intact based on the tool used. Investigators can easily recover or analyze data of such disk partitions. Implementation of general partition deletion tools for deletion of partition on the GPT disk will delete the protective MBR only, which investigators can easily recreate by simply reconstructing the disk.

Mac Boot Process

1. Activation of BootROM, which initializes system hardware and selects an operating system to run.
2. BootROM performs POST to test some hardware interfaces required for startup.
3. On PowerPC-based Macintosh computers, Open Firmware initializes the rest of the hardware interfaces.
4. On Intel-based Macintosh computers, EFI initializes the rest of the hardware interfaces.
5. After initializing the hardware interfaces, the system selects the operating system.
6. If the system contains multiple operating systems, it allows the user to choose the particular operating system by holding down the Option key.
7. Once the BootROM operation is finished, the control passes to the BootX (PowerPC) or boot.efi (Intel) boot loader, which is located in the /System/Library/CoreServices directory.
8. The boot loader loads a pre-linked version of the kernel, which is located at /System/Library/Caches /com.apple.kernelcaches .
9. Once the essential drivers are loaded, the boot loader starts initialization of the kernel, Mach and BSD data structures, as well as the I/O kit.
10. The I/O kit uses the device tree to link the loaded drivers to the kernel.
11. The launchd, which has replaced the mach_init process, runs startup items and prepares the system

Linux Boot Process

1. **BIOS stage**

a. It initializes the system hardware.
b. The BIOS retrieves the information, stored in the CMOS chip and then performs a POST test.
c. BIOS starts searching for the drive or disk which contains the operating system in a standard sequence.

2. **Bootloader Stage**

a. Load the Linux kernel and optional initial RAM disk.
b. Load pre-cursor software in a virtual file system called the initrd image or initial RAMdisk
c. System prepares to deploy the actual root file system.
d. System detects the device that contains the file system and loads the necessary chapters.

e. Lastly, load the kernel into the memory.

3. Kernel Stage

a. Virtual root file system executes the Linuxrc program. This generates the real file system for the kernel and later removes the initrd image.

b. Kernel searches for new hardware and loads any suitable device drivers found.

c. mounts the actual root file system and then performs the init process.

d. init reads the file "/etc/inittab" and uses this file to load the rest of the system daemons. This prepares the system and the user can log in and start using it.

e. Bootloaders for Linux are LILO (Linux Loader) and GRUB (Grand Unified Bootloader). These bootloaders allow the user to select which OS kernel to load during boot time.

Types of File Systems

- Disk File System-used to store data on disks or other media
- Network File System-used to access files on other computers or a NAS. NFS, CIFS, or GFS
- Database File System-used to store and manage files stored on a computer or server
- Flash File System-stores files or data in flash memory devices
- Tape File System-stores data/files on tape in self-describing form; very slow
- Shared Disk File System-external disk array or SAN accessed by servers or workstations
- Special Purpose File System-organizes files during run time and uses them for tasks. UNIX uses this.

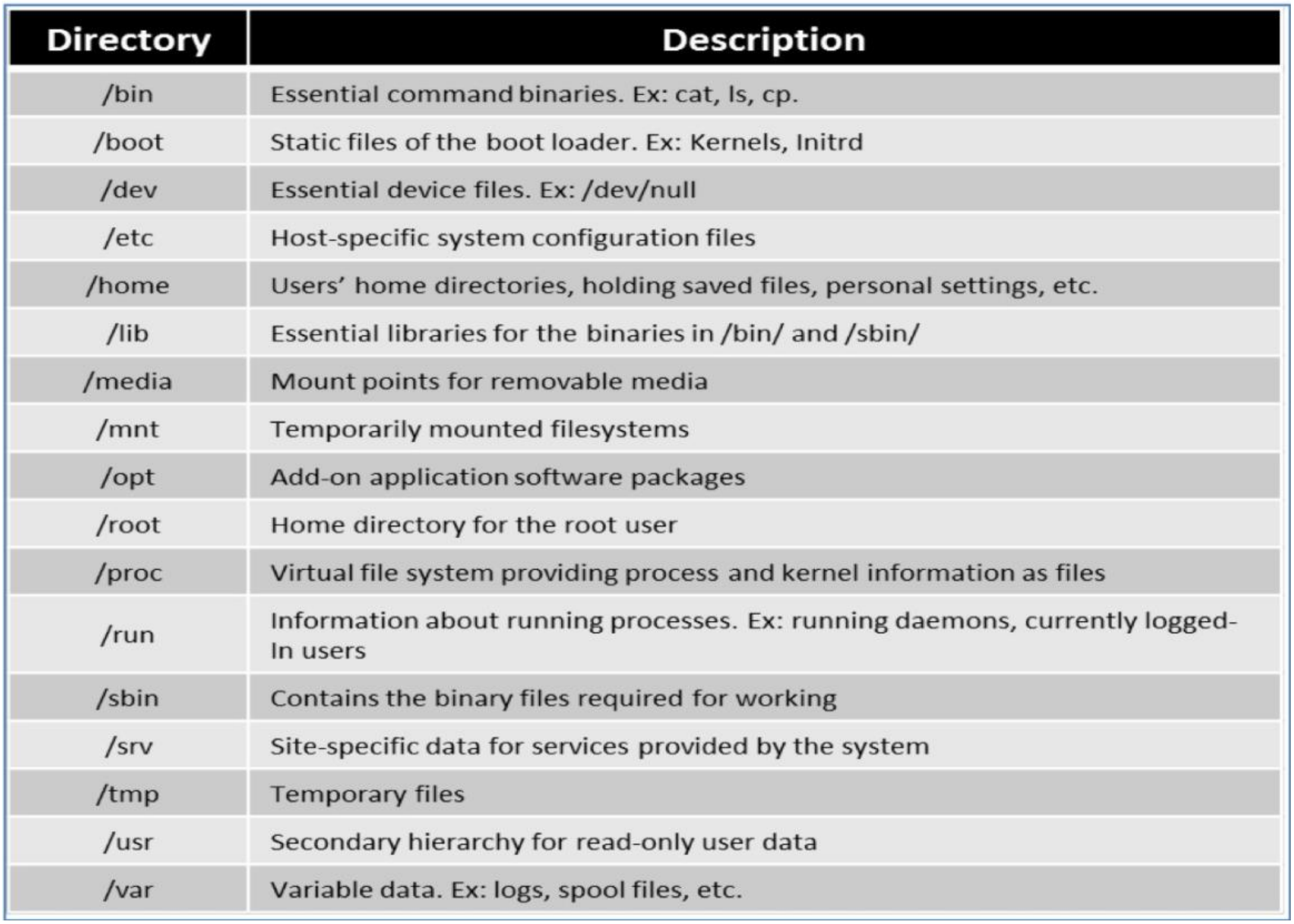
Windows File Systems

- FAT (file allocation table-16)
  - Designed for small disks with simple folder structures. Stores all files at beginning of volume
  - Creates two copies of allocation table for damage recovery
  - Flash, digital cameras, and other portable devices
- FAT32
  - Utilizes space 10-15% more effectively due to use of smaller clusters
  - Very robust and has lesser failure rate than FAT16 devices
  - No restriction on number of root folder entries
- New Technology File System (NTFS)
  - High-performance, self-repairing with advanced features like file-level security, compression, and auditing
  - Supports larger and more powerful volume storage solutions like RAID
  - Can encrypt/decrypt data, uses 16-bit Unicode for multi-language support, maintains fault tolerance via a backup log file
  - Introduces concept of metadata and master file tables
  - Supports files up to 16GB
  - Uses MFT (relational database) for file attributes like size, time, date, permissions, and contents

Linux File System

- User Space: The protected memory area where the user processes run and this area contains the available memory.
- Kernel Space: The memory space where the system supplies all kernel services through kernel processes. The users can access this space through the system call only. A user process turns into kernel process only when it executes a system call.
- The GNUC Library (glibc) sits between the User Space and Kernel Space and provides the system call interface that connects the kernel to the user-space applications.

Filesystem Hierarchy Standard (FHS)



Directory	Description
/bin	Essential command binaries. Ex: cat, ls, cp.
/boot	Static files of the boot loader. Ex: Kernels, Initrd
/dev	Essential device files. Ex: /dev/null
/etc	Host-specific system configuration files
/home	Users' home directories, holding saved files, personal settings, etc.
/lib	Essential libraries for the binaries in /bin/ and /sbin/
/media	Mount points for removable media
/mnt	Temporarily mounted filesystems
/opt	Add-on application software packages
/root	Home directory for the root user
/proc	Virtual file system providing process and kernel information as files
/run	Information about running processes. Ex: running daemons, currently logged-In users
/sbin	Contains the binary files required for working
/srv	Site-specific data for services provided by the system
/tmp	Temporary files
/usr	Secondary hierarchy for read-only user data
/var	Variable data. Ex: logs, spool files, etc.

Extended File System (EXT)

- First filesystem developed for Linux in 1992
- Metadata structure similar to UFS

Second Extended File System (EXT2)

- Most successful file system for linux and basis for all linux distros
- Data is stored in blocks of the same length during creation

Third Extended File System (Ext3)

- Journaling file system used in GNU/Linux OS; enhanced version of EXT2
- Main advantage is journaling and improves reliability/integrity and speed
- Can convert from ext2 to ext3 or vice or versa

Fourth Extended File System (EXT4)

- Better scale and reliability than EXT3
- Replaces block mapping scheme of EXT2/3 to increase performance and reduce fragmentation

Hierarchical File System (HFS) Developed to replace MFS or Mac File System

HFS Plus (HFS+) successor of HFS and is a primary file system in Macintosh.

UFS (UNIX File System) used by UNIX and UNIX-like OS

ZFS-used by Sun. High storage capacity, data protection, compression, volume management, integrity checks, deduplication, encryption, and auto repair.

ISO 9660 a standard that defines uses for file systems of CD-ROM and DVD media.

ISO 13490

- POSIX attributes and multi-byte characters
- efficient format that allows incremental recording and also permit the ISO 9660 format and the ISO/IEC 13490 format to exist on the same media
- specifies using multicasting properly.

CD File System (CDFS)

- file system for the Linux operating system
- transfers all tracks and boot images on a CD, as normal files. These files can then be mounted (for example, for ISO and boot images), copied, and played. Goal was to unlock information in old ISO images.

Universal Disk Format File System (UDF)

- defined by Optical Storage Technology Association (OSTA) to replace the ISO9660 file system on optical media and also FAT on removable media.
- 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.

RAID Level 0: Disk Striping

It is the simplest RAID level, which does not involve any redundancy and fragments the file into user-defined stripe size of the array. Then it sends these **stripes** to every disk in the array. As **RAID 0** does not have redundancy, it allows this RAID level to offer the **best overall performance** characteristics of the single RAID levels. Requires at **least two** drives

RAID 1 generally executes **mirroring** as it duplicates or copies the drive data on to two different drives using a hardware RAID controller or a software. If one of the drives fail, the other will function as a single drive until a user replaces the failed drive with a new one. Requires minimum of **2 drives**.

RAID 2 is the only level among all the RAID levels that does not implement even one of the standard techniques of parity, mirroring or striping. It uses a technique similar to striping with parity. It includes splitting of data at the bit level and distributing it to numerous data disks and redundancy disks.

RAID 3 uses byte-level striping with a dedicated parity disk, which stores checksums. It also supports a special processor for parity codes calculation. This RAID **cannot cater multiple data requests simultaneously**. If a failure occurs, it enables data recovery by an applicable calculation of the parity bytes, and the remaining bytes which relate with them.

RAID 5

Uses byte level data striping across multiple drives, and distributes the parity information among all member drives. Data writing process is slow. It **requires a minimum of three drives** to set up. The RAID stripes and distributes the error detection and correction code or Data and parity code across three or more drives.

RAID 10, also known as RAID 1+0, is a combination of RAID 0 (Striping Volume Data) and RAID 1 (Disk Mirroring) to protect data. It **requires at least four drives** to implement. It has same fault tolerance as RAID level 1 and the same overheads as mirroring alone. It allows mirroring of disks in pairs for redundancy and improved performance, and then stripes data across multiple disks for maximum performance. The user retrieves data from the RAID if one disk in each mirrored pair is working; however, if two disks in the same mirrored pair fail, the data is not available.

American Standard Code for Information Interchange (ASCII)

- 128 specified characters coded into 7-bit integers.
- Source code of a program, batch files, macros, scripts, HTML and XML documents
- 0 to 9, a-z, A-Z, Basic punctuation symbols, Control codes that originated with teletype machines
- ASCII table has 3 divisions namely, non-printable (system codes between 0 and 31), lower ASCII (codes between 32 and 127), and higher ASCII (codes between 128 and 255). The graphics files and documents use non-ASCII characters made in word processers, spreadsheet or database programs and sent as email file attachments.

Unicode computing standard developed with the Universal Coded Character Set (UCS) standard for encoding, representation, and management of texts, which most of the world's writing systems use.

- more than 128,000 characters from about 135 modern and historic scripts
- Technologies such as modern operating systems, XML, Java, and the Microsoft .NET Framework have adopted the Unicode standards.

OFFSET In computing, an offset usually refers to either the start of a file or the start of a memory address. Example: If "A" denotes address 80, then the expression A+20 implies the address 100, where 20 in the expression is the offset

File carving is a technique to recover files and fragments of files from unallocated space of the hard disk in the absence of file metadata

JPEG- lossy compression file type for images, can achieve 90% compression. The first bits of a file represent the file type and JPEG **files start with hex value ff d8 ff**

BMP- device independent bitmap (DIB) file format or a bitmap, is a standard graphics image file format used to store images on Windows operating systems. Bitmap images can include animations. The size and color of these images can vary from 1 bit per pixel (black and white) to 24-bit color (16.7 million colors). **RGBQUAD array:** A color table that comprises the array of elements equal to the colors present in the bitmap; this color table does not support bitmaps with 24 color bits, as each pixel is represented by24-bit RGB values in the actual bitmap. **BMP** Files **start with hex value 42 4d or BM in ASCII**

GIF is a file format that contains 8 bits per pixel and displays 256 colors per frame. GIF uses lossless data compression techniques, which maintain the visual quality of the image. The hex value of a GIF image file **starts with the values 47 49 46**, which represent the GIF file name.

PNG, short for Portable Network Graphics, is a lossless image format intended to replace the GIF and TIFF formats. Supports 24-bit true color, transparency in both the normal and alpha channels as well as indexed/palette-based images of 24-bit RGB or 32-bit RGBA colors and grayscale images. PNG file hex values **begin with 89 50 4e**, which is the hex value for GIF.

PDF device independent and support different systems like MAC, Linux, etc. Support different compression algorithms and several multimedia elements. Allows password protection

Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools. Law enforcement, military, and corporate examiners use it to investigate what happened on a computer. You can even use it to recover photos from your camera's memory card

The Sleuth Kit® (TSK) is a library and collection of command line tools that allow you to investigate disk images. The core functionality of TSK allows you to analyze volume and file system data. The plug-in framework allows you to incorporate additional chapters to analyze file contents and build automated systems. The library can be incorporated into larger digital forensics tools and the command line tools can be directly used to find evidence. **To perform analysis, create a forensics image .dd or. E01**

- **'fsstat'** displays the details associated with a file system. The output of this command is file system specific.
- **istat** - Display details of a meta-data structure (inode)
- **fls** - List file and directory names in a disk image.
- **img_stat** - Display details of an image file

Chapter 3 Summary

- The disk drive is a hardware device that reads data from a disk and writes onto another computer disk.
- Types of disk drives include: magnetic storage devices, optical storage devices, and flash memory devices
- The HDD is a non-volatile, random access digital data storage device used in any computer system
- SSD is a data storage device that uses solid state memory to store data and provides access to the stored data in the same manner as an HDD drive
- Slack space is the area of a disk cluster between the end of the file and cluster

- A master boot record (MBR) is the first sector ("sector zero") of a data storage device such as a hard disk
- Booting refers to the process of starting or resetting operating systems when the user turns on a computer system. It is of two types: Cold boot (Hard boot) and Warm boot (Soft boot)
- The file system is a set of data types, which is employed for storage, hierarchical categorization, management, navigation, access, and recovering the data
- File carving is a technique to recover files and fragments of files from unallocated space of the hard disk in the absence of file metadata

Chapter 4 CHFIv9 STUDY GUIDE

Data acquisition is the first pro-active step in the forensic investigation process. The aim of forensic data acquisition is to extract every bit of information present on the victim's hard disk and create a forensic copy to use it as evidence in the court. In some cases, data duplication is preferable instead of data acquisition to collect the data. Investigators can also present the duplicated data in court.

Live Data Acquisition

It is the process of acquiring volatile data from a working computer (either locked or in sleep condition) that is already powered on. Volatile data is fragile and lost when the system loses power or the user switches it off. Such data reside in registries, cache, and RAM. Since RAM and other volatile data are dynamic, a collection of this information should occur in real time.

Static Data Acquisition

It is the process of acquiring the non-volatile or unaltered data remains in the system even after shutdown. Investigators can recover such data from hard drives as well as from slack space, swap files, and unallocated drive space. Other sources of non-volatile data include CD-ROMs, USB thumb drives, smartphones, and PDAs. The static acquisition is usually applicable for the computers the police had seized during the raid and include an encrypted drive.

Volatile Data Collection Methodology

1. **Incident Response Preparation**
    a. **The following should be ready before an incident occurs:**
        1. **A first responder toolkit (responsive disk)**
        2. **An incident response team (IRT) or designated first responder**
        3. **Forensic-related policies that allow forensic data collection**
2. **Incident Documentation**
    a. Document all information about incident
    b. Use logbook to record all actions during collection
3. **Policy Verification**
    a. Read and examine all polices signed by the user of suspect computer
    b. Determine forensic capabilities and limitations of the investigator by determining legal rights of user
4. **Volatile Data Collection Strategy**

a. Devise strategy based on type of data, source(s) of data, type of media, etc..

5. **Volatile Data Collection Setup**

a. Establish trusted command shell to minimize footprint and any malware triggers
b. Establish transmission and storage method
c. Ensure integrity of tool output with MD5 hash for admissibility

6. **Volatile Data Collection Process**

a. Record time, date, command history and do so when using tools/commands
b. Document forensic activities and do not restart or shutdown until complete
c. Maintain a log of all actions performed, photo the screen, identify OS
d. Check system for use of encryption, dump RAM to sterile storage
e. Complete full report of steps taken and evidence gathered

A chain of custody document is a written record consisting of all the processes involved in the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence. It also includes the details of people, time and purpose involved in the investigation and evidence maintenance processes.

Media sanitization is the process of permanently deleting or destroying data from storage media.

NIST SP 800-88 Guidelines= Clear, Purge, Destroy

Enable Write Protection on the Evidence Media

If hardware write blocker is used:

- Install a write blocker device
- Boot the system with the examiner's controlled operating system
- Examples of hardware devices: CRU® WiebeTech® USB WriteBlockerTM, Tableau Forensic Bridges, etc.
- If software write blocker is used:
- Boot the system with the examiner's controlled operating system and activate write protection
- Examples of software applications: SAFE Block, MacForensicsLab Write Controller, etc.

Determine Data Acquisition Format

Raw Format creates simple, sequential, flat files of a data set or suspect drive.

Advantages:

- Data transferring is fast
- Can ignore minor data read errors on the source drive
- A Universal acquisition format that most of the forensic tools can read

Disadvantages:

- Takes same storage space as that of original disk or data set
- Some tools like freeware versions may not collect bad sectors on the source drive

Proprietary Format Raw format and advanced forensics format are open source formats, and these are the only proprietary format.

- These formats can change from one vendor to another based on features they offer.
- Saves space on target drive and allows to compression of image files of a suspect drive
- Allows splitting an image into smaller segmented files
- Ensures data integrity by applying data integrity checks on each segment while splitting
- It can integrate metadata into image file by adding metadata such as date and time of the acquisition, examiner or investigator name, the hash value of the original medium or disk and case details or comments

Advanced Forensics Format (AFF)

- Open source format w/no size restrictions and Space for metadata

Advanced Forensic Framework 4 (AFF4)

- Supports more file formats than AFF and much larger capacities
- Image signing and cryptography and is transparent to clients

Generic Forensic Zip (gfzip)

- Open format for compressed and signed files that uses SHA-256
- Embeds user metadata with file metadata and signs with x.509

Data Acquisition Methods:

Bit-stream disk-to-image

- ProDiscover, EnCase, FTK, TSK, X-Ways, ILook

Bit-stream disk-to-disk

- EnCase, SafeBack, Norton Ghost

Acquiring Data on Linux: dd Command

The syntax for the dd command is as follows:

dd if <source> of<target> bs<byte size> skip seekconv<conversion>

- source: from where to read the data
- target: where to write the data
- Bs: byte size ***(usually some power of 2, not less than 512 bytes [i.e., 512, 1024, 2048, 4096, 8192])***
- skip: number of blocks to skip at the start of the input
- seek: number of blocks to skip at the start of the output
- conv: conversion options

An investigator may use the following commands for the respective tasks:

Suppose a 2GB hard disk is seized as evidence. Use DD to make a complete physical backup of the hard disk, use

dd if=/dev/ hda of=/dev/case5img1

To copy one hard disk partition to another hard disk, use

dd if=/dev/sda2 of=/dev/sdb2 bs=4096 conv=notrunc,noerror command

Following are the important functions **dcfldd** offers that are not possible with dd:

1. Hashing on-the-fly - dcfldd can hash the input data, helping to ensure data integrity
2. Status output - dcfldd can update the user of its progress in terms of time or data left
3. Flexible disk wipes - dcfldd can be used to wipe disks quickly, and with a known pattern if desired
4. Image/wipe Verify - dcfldd can verify that a target drive is a bit-for-bit match
5. Multiple outputs - dcfldd can output to multiple files or disks at the same time
6. Split output - dcfldd can split output to multiple files with more configurability than the split command
7. Piped output and logs - dcfldd can send all its log data and output to commands as well as files natively

Acquiring Data on Linux: dcfldd Command

An advanced dcfldd command look like:

dcfldd if=/dev/sdb hash=md5,sha256 hashwindow=2G md5log=md5.txt sha256log=sha256.txt \ hashconv=after bs=4k conv=noerror,sync split=2G splitformat=aa of=sdb_image.img

Acquiring Data on Windows: AccessData FTK Imager

CRC-32: Cyclic Redundancy Code algorithm-32 is a hash function based on polynomial division idea. The resulting hash value or checksum which is 32 bits.

MD5: It is an algorithm used to check the data integrity by creating 128-bit message digest from the data input of any length. Every MD5 hash value is unique to that particular data input.

SHA-1: Secure Hash Algorithm-1 is a cryptographic hash function developed by the NSA and it is a US Federal Information Processing Standard issued by NIST. It creates a 160-bit (20-byte) hash value called a message digest. This hash value is a hexadecimal number, 40 digits long.

SHA-256: It is a cryptographic hash algorithm that creates a unique and fixed-size 256-bit (32-byte) hash. Hash is a one-way function which means, decryption is impossible. Therefore, it is apt for anti-tamper, password validation, digital signatures and challenge hash authentication.

Chapter 4 Summary

- Data acquisition is the use of established methods to extract the ESI from the suspect computer or storage media to gain insight into a crime or an incident
- Live data acquisition involves collecting volatile information that resides in registries, cache, and RAM
- When collecting volatile information, the collection should proceed from the most volatile to the least volatile
- Static data acquisition is defined as acquiring data that resides in the disk drive, USB, DVD, etc., which remains unaltered when the system is powered off or shutdown
- Select the data acquisition tool that accomplishes the tasks described as mandatory requirements
- Contingency plans must be made in the case the hardware or software does not work, or in case there is any type of failure during acquisition
- Digital evidence validation involves using a hashing algorithm utility to create a binary or hexadecimal number that represents the uniqueness of a data set such as a disk drive or file

What Happens When a File is Deleted in Windows?

When a user deletes a file, the OS does not actually delete the file, but marks the file name in the Master File Table (MFT) with a special character. This character represents that the space once occupied by the file is ready for use.

FAT- the OS replaces the first letter of the deleted filename with **E5H**. Corresponding clusters of that file are **marked unused, even though they are not empty.** Until these clusters are overwritten, the file can still be recovered.

NTFS- marks the index field in the MFT with a **special code.** The computer now looks at the clusters occupied by that file **as being empty**. Until these clusters are overwritten, the file can be recovered

Recycle Bin- place to store files that are marked for deletion. The exceptions are large files and files from removable media.

Windows 98 and earlier (FAT)

- C:\Recycled (4GB limit)
- Files are named **Dxy.ext** "x" is drive, "y" is sequence number(0-??) and "ext" is original extension.
- For the first document file deleted on C: drive would be: **Dc0.doc**

Windows Vista, 7,8, and 10

- C:\$Recycle.Bin
- Files are named $Ry.ext "y" is sequence number and "ext" is original extension
- For the first document file deleted on C: drive would be: **$R0.doc**

Windows 2000, XP, NT (NTFS)

- C:\Recycler\S- (based on windows SID)

When a user deletes a file or folder, the **OS stores** all the details of the file such as its complete path, including the original file name, in a special hidden file **called "Info" or "Info2**" in the Recycle Bin folder.

In Windows **newer than Vista and XP**, the **OS stores the complete path** and file or folder name in a hidden file called **INFO2.**

INFO2 contains various details of deleted files such as: **original file name, original file size, the date and time of deletion, unique identifying number, and the drive number that the file came from.**

File Recovery Tools for Windows- Recover My Files, EaseUS, DiskDigger, Handy Recovery, Quick Recovery, Stellar Phoenix, Total Recall, Advanced Disk Recovery, Windows Data Recovery Software, R-Studio, Orion File Recovery, Data Rescue PC, Smart Undeleter, DDR Professional, GetDataBack, UndeletePlus, File Scavenger, VirtualLab, Active@UNDELETE, WinUndelete, R-Undelete, Recover4all, Recuva, Active@ File Recovery, Pandora Recovery, Ontrack EasyRecovery, Wise Data Recovery, Glary Undelete, Disk Drill, PhotoRec,

Recover files on Mac

- Put back from trash
- Time Machine
- 3rd party software

File Recovery Tools for Mac- AppleXsoft File Recovery, Disk Doctor Mac Data Recovery, R-Studio for mac, Data Rescue 4, Stellar Phoenix, FileSalvage, 321Soft, Disk Drill, Mac Data Recovery Guru, Cisdem

Recovering Deleted Partition Windows

1. Restart system with Windows install DVD then select repair. When DOS comes up type "fixboot"
2. Slave the drive to another and try to recover that way
3. 3rd Party tool like: Active@ Partition Recovery, Acronis Recovery Expert, DiskInternals, GetDataBack, EaseUS, 7-Data

Password Cracking

Brute Force Attack

In a brute force attack, the attacker tries **every possible combination of characters** until the correct password is found including using different hashes for encrypted passwords.

Dictionary Attack

In a dictionary attack, a dictionary file is loaded into the cracking application that runs against user accounts. The program uses every word present in the dictionary file to find the password. Dictionary attacks can be considered more useful than brute force attacks, although they do not work against systems that use passphrases.

Syllable Attack

A syllable attack is the **combination of both a brute force attack and a dictionary attack**. This is often used when the password is a nonexistent word. The attacker takes syllables from dictionary words and combines them in every possible way to try to crack the password.

Rule-Based Attack

This type of attack is used when an **attacker already has some information about the password.** He or she can then write a rule so that the password-cracking software will generate only passwords that meet this rule. For example, if the attacker knows that all passwords on a system consist of six letters and three numbers, he or she can craft a rule that generates only these types of passwords. This is considered the most powerful attack

Hybrid Attack

This type of attack is **based on the dictionary attack and brute force.** Often, people change their passwords by just adding numbers to their old passwords. In this attack, the program adds numbers and symbols to the words from the dictionary. For example, if the old password is “system”, the user may have changed it to “system1” or “system2.”

Password Guessing

Sometimes users set passwords that **can be easily remembered, such as a relative’s name, a pet’s name, or an automobile license plate number.** This can make the password easily guessed. Unlike other methods of password cracking, guessing requires only physical access or an open network path to a machine running a suitable service.

Rainbow Attack

In a rainbow attack, a password hash table called a rainbow table is created in advance and stored into memory. This rainbow table is a table of password hashes created by hashing every possible password and variation thereof to be used in a rainbow attack to recover a plaintext password from a captured ciphertext.

L0phtCrack Helps to recover lost Microsoft Windows passwords by using dictionary attacks, hybrid attacks, rainbow tables, and brute-force attacks

Ophcrack is a Windows password cracker based on rainbow tables. GUI and runs on multiple platforms.

Cain & Abel is a password recovery tool for Microsoft OSs. It sniffs the network, cracks encrypted passwords using dictionary, brute-force, and cryptanalysis attacks. It covers some security aspects/weaknesses present in a protocol’s standards, caching mechanisms, and authentication methods. This offers a simplified recovery of passwords and credentials from various sources. It consists of an Arp Poison Routing (APR) that enables sniffing on switched LANs and man-in-the-middle attacks. The sniffer in this tool is also capable of analyzing encrypted protocols, such as HTTP and SSH-1, and contains filters to capture credentials from a wide range of authentication mechanisms.

RainbowCrack is a hash cracker. It uses a time-memory tradeoff algorithm to crack hashes. It pre-computes all possible plaintext–ciphertext pairs in advance and stores them in the “rainbow table” file.

PWdump7 is an application that dumps the password hashes (OWFs) from NT’s SAM database. It extracts LM and NTLM password hashes of local user accounts from the SAM database. T

Fgdump is basically a utility for dumping passwords on Windows NT/2000/XP/2003/Vista machines.

Bypass/reset BIOS password

- manufacturer’s backdoor password
- password-cracking software (CmosPwd, DaveGrohl)

- reset CMOS or remove battery
- professional service
- keyboard buffer overload

Resetting Admin passwords- Active@ Password changer, Windows Recovery Bootdisk, Windows Password Recovery Lastic,

Application Password Cracking-Passware Kit, SmartKey, Advanced Office Password Recovery(all versions of Office), Office password recovery,

PDF password recovery- PDF Password recovery, PDF Password Genius, SmartKey, Tenorshare, Guaranteed

Steganography- the art of hidden writing, has been in use for centuries. It involves embedding a hidden message in some transport or carrier medium and mathematicians, military personnel, and scientists have been using it.

Steganalysis is the process of discovering the existence of the hidden information within a cover medium. Steganalysis is the reverse process of steganography.

Steganalysis tools- Gargoyle, StegAlyzerAS/RTS, StegExpose, StegAlyzerSS, Steganography Studio, Virtual Steganographic Lab (VSL), ImgStegano

Setting Windows registry key

"HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate" **to 1 disables** updating of the last-accessed timestamp

Following are the steps to detect rootkits by examining the registry:

1. Run regedit.exe from inside the potentially infected OS.
2. export HKEY_LOCAL_MACHINE\SOFTWARE and HKEY_LOCAL_MACHINE\SYSTEM hives in text file format.
3. Boot into a clean CD (such as WinPE).
4. Run regedit.exe.
5. Create a new key such as HKEY_LOCAL_MACHINE\Temp.
6. 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 \system32\config\system.
7. 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.)
8. 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).

In a **buffer overflow attack**, attackers use buffer overflows in order to inject and run code in the address space of a **running program**, thereby successfully altering the victim program's behavior.

Privacy Eraser is an anti-forensic solution to protect the privacy of the user by deleting the browsing history and other computer activities. The software implements and **exceeds the US Department of Defense and NSA clearing and sanitizing standards**, giving you the confidence that once erased, your file data is gone forever and can never be recovered.

Chapter 5 Summary

- Intruders implement anti-forensics techniques to hinder or prevent proper forensics investigation process
- Anti-forensics techniques include file deletion, password protection, steganography, trail obfuscation, artifact wiping, overwriting data/metadata, encryption, program packers, rootkits, exploiting forensics tool bugs, etc.
- Intruders may use anti-forensics tools such as Privacy Eraser, QuickStego, CryptaPix, etc. to hide their malicious activities from being caught
- Strictly implementing countermeasures against anti-forensics may enable an investigator to successfully deal with a case

Chapter 6 CHFIv9 STUDY GUIDE

The **first step** while investigating an incident is the **collection of the system time**.

The next step is to figure out who was logged on and who is currently logged on to a system.

Some of the tools and commands used to determine logged-on users:

- **PsLoggedOn-** displays both the locally logged on users and users logged on via resources for either the local computer, or a remote one.
- **net sessions –** displays information about all logged in sessions of the local computer.
- **LogonSessions-** It lists the **currently active logged-on sessions** and, if you specify the -p option, it can provide you the information of processes running in each session.

Open files

- **net fil**e displays the names of **all open shared files** on a server and the **number of file locks**, if any, on each file. You can also close files and remove file locks
- **PsFile** is a command-line utility that can **retrieve the list of remotely opened files** on a system and allows investigator to close open files
- **Openfiles** This command queries or **displays open files and also queries, displays, or disconnects files opened by network users.**

Nbtstat helps to troubleshoot NetBIOS name resolution problems. When a network is functioning normally, NetBIOS over TCP/IP (NetBT) resolves NetBIOS names to IP addresses. –a remote name, -A ip address, –c cache, -n names, -r resolved, -S sessions.

Netstat tool helps in collecting information about network connections operative in a Windows system. The **most common way to run Netstat is with the -ano switches.** These switches tell the program to display the TCP and UDP **network connections**, listening **ports**, and the identifiers of the processes **(PIDs).** –r routing table, -e ethernet stats, -p *Protocol*

Process Information

- **Tasklist** tool displays the list of applications and services along with the Process IDs (PID) for all tasks that running on either a local or a remotely connected computer.
- **Pslist.exe** displays basic information about the already running processes on a system, including the amount of time each process has been running. –x details about threads and memory, -t task tree, -d detail, -m memory, -e exact match for process name
- **ListDLLs** reports DLLs loaded into processes. Processname, Pid, Dllname, -r relocated, -u unsigned, -v version
- **Handle** displays information about open handles for any process. –a all types, -c close, -l sizes, -y no prompt, -s print count, -u username, -p processes, name

Process Memory

- **Process Explorer** shows the information about the handles and DLLs of the processes which have been opened or loaded.
- **PMDump** is a tool that lets you dump the memory contents of a process to a file without stopping the process. This tool is highly useful in forensic investigations.
- **ProcDump** monitor applications for CPU spikes and generating crash dumps during a spike so that an administrator or developer can determine the cause of the spike.
- **Process Dumper (PD)** forensically dumps the memory of a running process.

The system stores the information about **shared files and folders** in the following registry root key:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Shares

Important Registry Entries:

- ClearPageFileAtShutdown-will clear the page file at system shutdown; possibly deleting valuable data
- DisableLastAccess-used to disable the updating of last access time on files
  - Can invoke using the “fsutil” command
- AutoRuns Tool-used to identify tasks or programs that run at startup or on a regular schedule

Fsutil-performs tasks related to file allocation table (FAT) and NTFS file systems, such as managing reparse points, managing sparse files, or dismounting a volume.

Microsoft Security ID refers to a unique identification number that Microsoft assigns to a Windows user account for granting the user access to a particular resource.

PsLogList allows users to login to remote systems in situations when current set of security credentials would not permit access to the Event Log. It retrieves message strings from the computer on which the event log resides. It shows the contents of the System Event Log on the local computer and allows formatting of Event Log records.

Extensible Storage Engine (ESE) is a data storage technology from MS to store and retrieve data sequential access. This helps the server to store various files, messages etc. and access folders, text messages, attachments, etc. for email service provision. These files have the extension .edb and can provide valuable case evidences in forensic investigations. The database is in the form of a B-Tree structure and has a hexadecimal file signature.

Common artifact locations of Microsoft Edge include:

ESE database:

\Users \username\AppData\Local\Packages \Microsoft.MicrosoftEdge_xxxxx\AC\MicrosoftEdge\User\Default\DataStore\Data\nouser1\xxxxx\DBStore\spartan.eb

Edge cached files location:

\Users \user_name\AppData\Local\Packages \Microsoft.MicrosoftEdge_xxxx\AC\#!001\MicrosoftEdge\Cache\

Edge last active browsing session data location:

\Users\user_name\AppData\Local\Packages\Microsoft.MicrosoftEdge_xxxx\AC\MicrosoftEdge\User\Default\Recovery\Active\

Edge stores history records, Cookies, HTTP POST request header packets and downloads in:

\Users \user_name\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat

If the last browsing session open was in PrivacIE mode then the browser stores these records in: \Users \user_name\AppData\Local\Packages\Microsoft.MicrosoftEdge_xxxx\AC\MicrosoftEdge\User\Default\Recovery\Active\{browsing-session-ID}.dat

DevCon or Device Console, is a command-line tool that displays detailed information about devices on computers running Windows operating system. DevCon can be used to enable, disable, install, configure, and remove devices.

Slack space - the space generated between the end of the file stored and the end of the disk cluster.

Use **X-Ways** Forensics tool to scan **virtual memory**.

Linux operating system allocates certain amount of storage space on a hard disk called **Swap Space**. OS uses as the virtual memory extension of a computer's real memory (RAM). In Windows, this is called a **Page File**. Found in: Found in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management

Windows Power Management

- Sleep Mode keeps the system running in a low power state so that the user can instantaneously get back where he/she has paused working
- Hibernate mode completely writes the memory as a hiberfil.sys file in HDD.
  - Found in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power

Passware Search Index Examiner - It makes all the data indexed by Windows Search accessible. Requires only one file from the target PC, a **Windows Desktop Search Database (.edb)**

DumpChk (the Microsoft Crash Dump File Checker tool) is a program that performs a quick analysis of a crash dump file.

Handle is a utility that displays information about open handles for any process in the system. You can 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.

ListDLLs.exe utility that reports the DLLs loaded into processes.

There are five root folders in the Registry Editor:

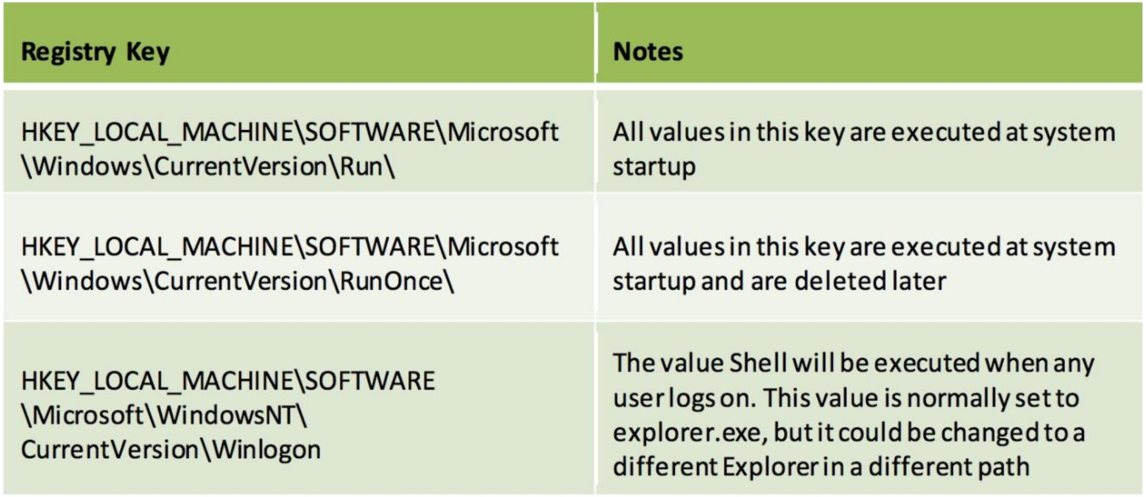
- **HKEY_CLASSES_ROOT** – subkey of HKEY_LOCAL_MACHINE\Software and contains file extension association information and also programmatic identifier (ProgID), Class ID (CLSID), and Interface ID (IID) data.
- **HKEY_CURRENT_USER** - contains the configuration information related to the user currently logged on. Wallpaper, screen colors, display settings, etc..
- **HKEY_LOCAL_MACHINE** - contains most of the configuration information for installed software which includes the Windows OS as well, and the information about the physical state of the computer which includes bus type, installed cards, memory type, startup control parameters and device drives.
- **HKEY_USERS** - contains information about all the currently active user profiles on the computer.
- **HKEY_CURRENT_CONFIG** - stores information about the current hardware profile of the system. It is also a pointer to: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\CurrentControlSet\HardwareProfiles\Current

Registry Tools

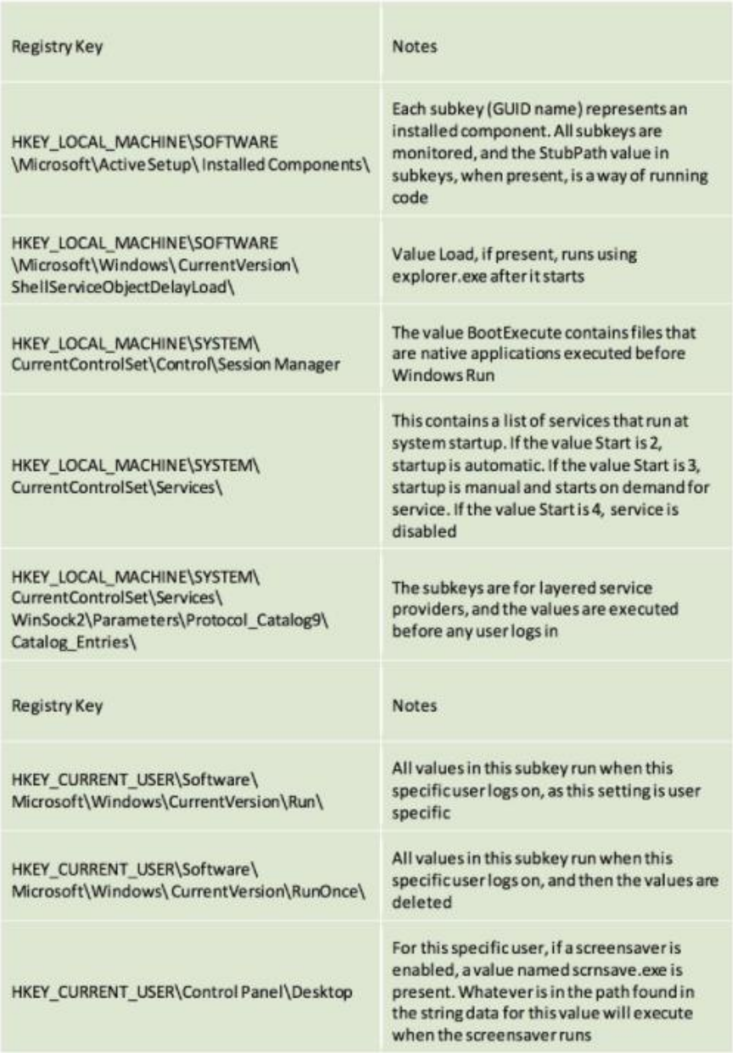
- RegRipper
- ProDiscover
- Process Monitor
- RegScanner
- RegEdit
- Registry Viewer

What else is in the registry?

- HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares=**Share Names**
- HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation=**Time Zones**
- HKLM\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces\{GUID}=**Wireless SSIDs**
- HKLM\SYSTEM\ControlSet00x\Control\SessionManager\Memory Management\PrefetchParameters=**Prefetching**
- Registry keys that track **user's activities** can be found in the **NTUSER.DAT** file
- The Most Recently Used list registry key is the RecentDocs key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs



Registry Key	Notes
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft \Windows\CurrentVersion\Run\	All values in this key are executed at system startup
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft \Windows\CurrentVersion\RunOnce\	All values in this key are executed at system startup and are deleted later
HKEY_LOCAL_MACHINE\SOFTWARE \Microsoft\WindowsNT\ CurrentVersion\Winlogon	The value Shell will be executed when any user logs on. This value is normally set to explorer.exe, but it could be changed to a different Explorer in a different path



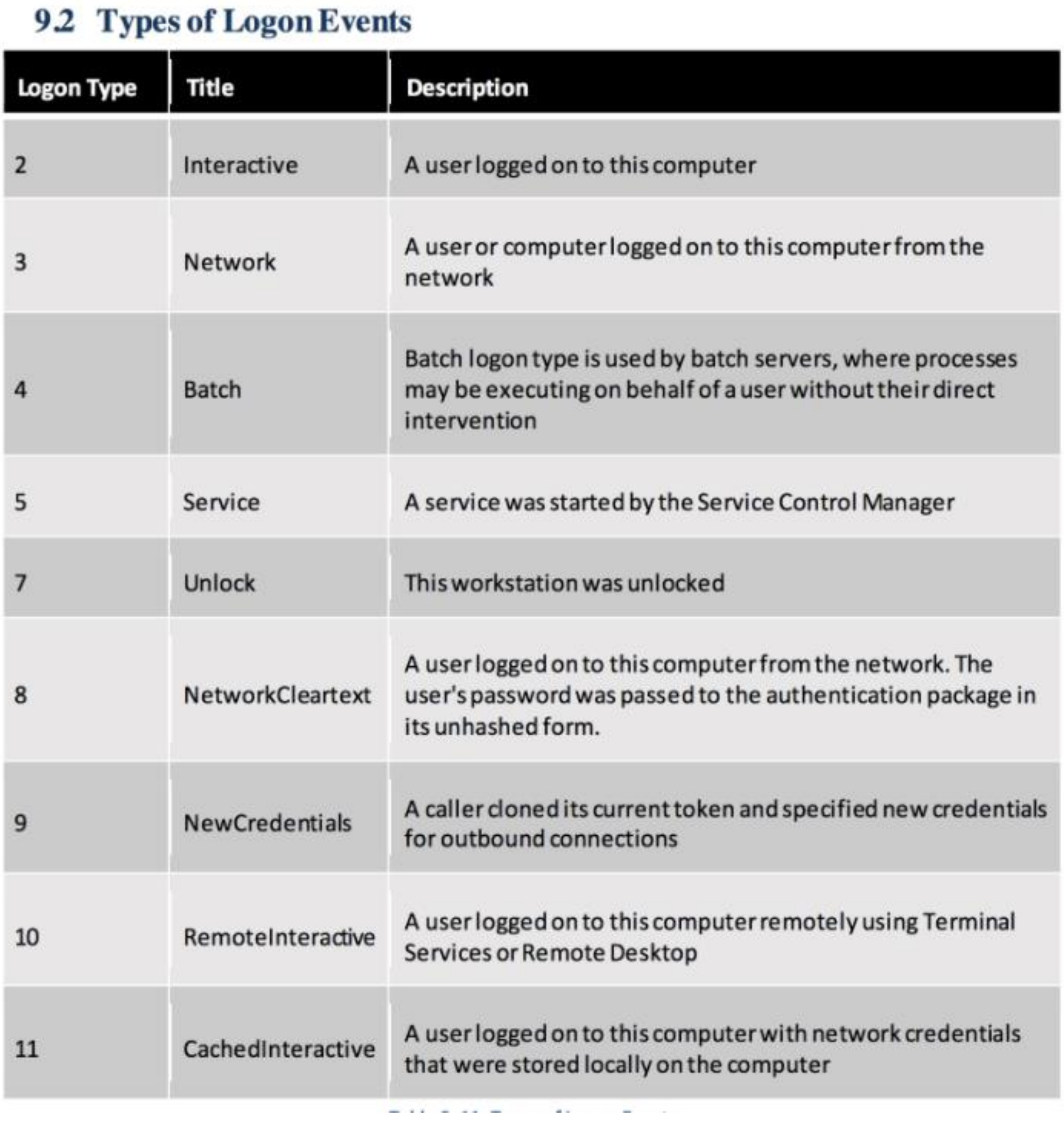
Registry Key	Notes
HKEY_LOCAL_MACHINE\SOFTWARE \Microsoft\ActiveSetup\Installed Components\	Each subkey (GUID name) represents an installed component. All subkeys are monitored, and the StubPath value in subkeys, when present, is a way of running code
HKEY_LOCAL_MACHINE\SOFTWARE \Microsoft\Windows\CurrentVersion\ ShellServiceObjectDelayLoad\	Value Load, if present, runs using explorer.exe after it starts
HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\Session Manager	The value BootExecute contains files that are native applications executed before Windows Run
HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\	This contains a 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
HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\ WinSock2\Parameters\Protocol_Catalog9\ Catalog_Entries\	The subkeys are for layered service providers, and the values are executed before any user logs in
Registry Key	Notes
HKEY_CURRENT_USER\Software\ Microsoft\Windows\CurrentVersion\Run\	All values in this subkey run when this specific user logs on, as this setting is user specific
HKEY_CURRENT_USER\Software\ Microsoft\Windows\ CurrentVersion\RunOnce\	All values in this subkey run when this specific user logs on, and then the values are deleted
HKEY_CURRENT_USER\Control Panel\Desktop	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

Cache, Cookies, and History

- **Mozilla Firefox** - Cache, Cookies, and History are stored in the following system locations:
  Cache Location:
  C:\Users\<Username>\AppData\Local\Mozilla\Firefox\Profiles \XXXXXXXX.default\cache2
  Cookies Location:
  C:\Users\<Username>\AppData\Roaming\Mozilla\Firefox\Profiles\XXXXXXXX.default\cookies.sqlite
  History Location:
  C:\Users\<Username>\AppData\Roaming\Mozilla\Firefox\Profiles\XXXXXXXX.default\places.sqlite
- **Google Chrome**
  History, Downloads, Cookies Location: C:\Users\{user}\AppData\Local\Google\Chrome\User Data\Default
  Cache Location: C:\Users\{user}\AppData\Local\Google\Chrome\User Data\Default\Cache
- **Microsoft Edge**
  Cache Location:
  C:\Users\Admin\AppData\Local\Microsoft\Windows\WebCache
  Cookies Location:
  C:\Users\Admin\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\MicrosoftEdge\Cookies
  History Location:
  C:\Users \Admin\AppData\Local\Microsoft\Windows \History

Prefetch Information:

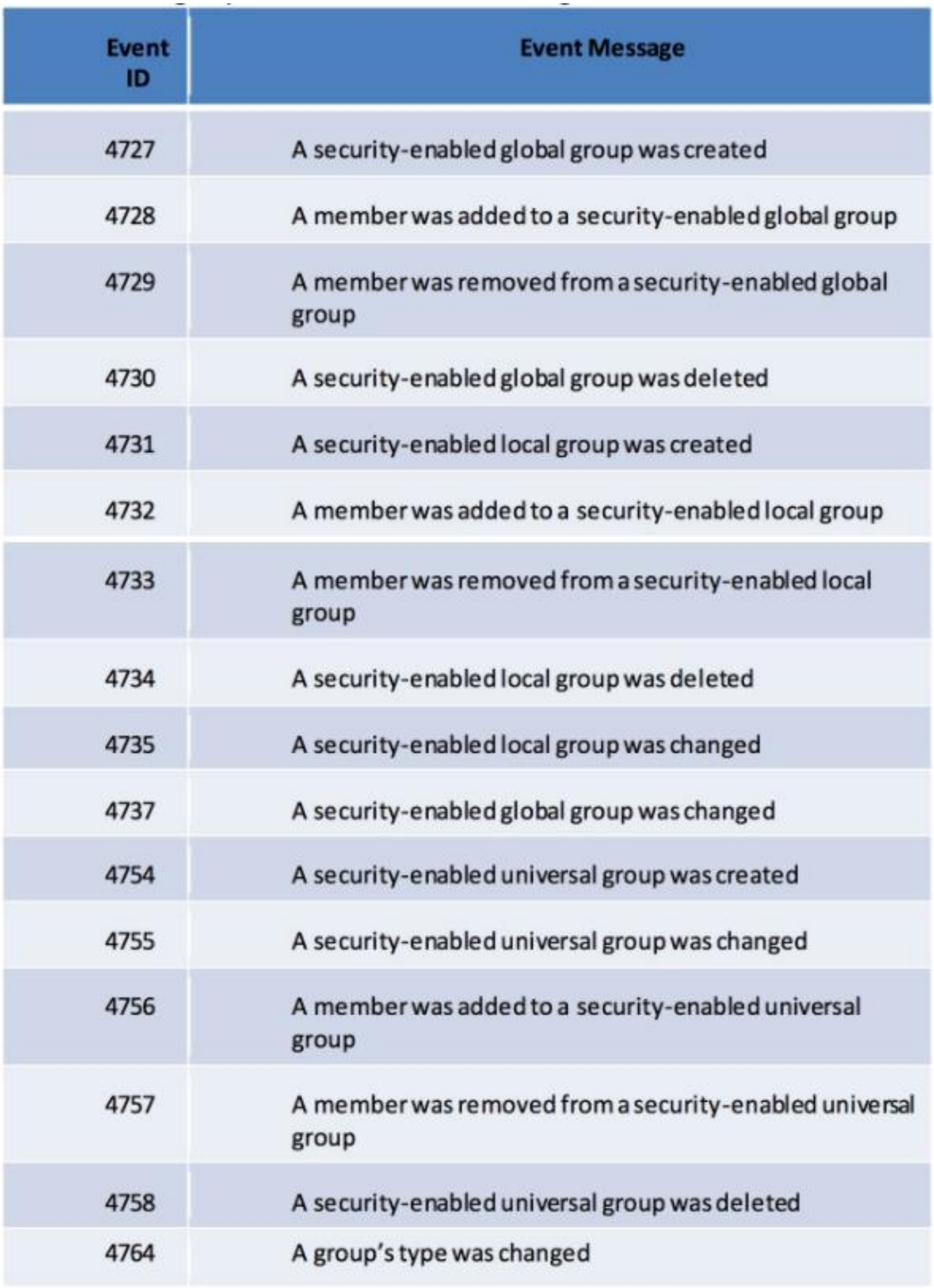
- DWORD value at the offset **120** within the file corresponds to the **last time of the application run**, this value is stored in UTC format
- DWORD value at the offset **144** within the file corresponds to the **number of times** the application is launched
- 0:prefetch disabled 1:application prefetch enabled 2:boot prefetch enabled 3:application and boot prefetch enabled



9.2 Types of Logon Events

Logon Type	Title	Description
2	Interactive	A user logged on to this computer
3	Network	A user or computer logged on to this computer from the network
4	Batch	Batch logon type is used by batch servers, where processes may be executing on behalf of a user without their direct intervention
5	Service	A service was started by the Service Control Manager
7	Unlock	This workstation was unlocked
8	NetworkCleartext	A user logged on to this computer from the network. The user's password was passed to the authentication package in its unhashed form.
9	NewCredentials	A caller cloned its current token and specified new credentials for outbound connections
10	RemoteInteractive	A user logged on to this computer remotely using Terminal Services or Remote Desktop
11	CachedInteractive	A user logged on to this computer with network credentials that were stored locally on the computer

Event ID 624-account created
Event ID 642-information about changes made to an account



Event ID	Event Message
4727	A security-enabled global group was created
4728	A member was added to a security-enabled global group
4729	A member was removed from a security-enabled global group
4730	A security-enabled global group was deleted
4731	A security-enabled local group was created
4732	A member was added to a security-enabled local group
4733	A member was removed from a security-enabled local group
4734	A security-enabled local group was deleted
4735	A security-enabled local group was changed
4737	A security-enabled global group was changed
4754	A security-enabled universal group was created
4755	A security-enabled universal group was changed
4756	A member was added to a security-enabled universal group
4757	A member was removed from a security-enabled universal group
4758	A security-enabled universal group was deleted
4764	A group's type was changed

13. Shell Commands

Investigators use the shell commands in Linux for collecting information from the system. Some of the frequently used commands include:

dmesg

The command **dmesg** is the short for display message or 'Driver Message'. The command 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. These messages are helpful in resolving the restoring the device's driver issues.

Syntax: dmesg options

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

fsck

The command **fsck**, is meant for File System Consistency Check. It is a tool to check the consistency of Linux file system and repair.

Syntax: **fsck –A** (Checks all configured filesystems)

Stat

Displays file or file system status.

Syntax: stat [OPTION]... FILE...

history

The command **history** checks and lists the Bash shell commands used. This command helps the users for auditing purposes.

Syntax: **history n** (Lists the last n commands)

mount

The command **mount causes** mounting of a file system or a device to the directory structure, making it accessible by the system.

Syntax: **mount -t type device dir** (Requests kernel to attach the file system found on device of type type at the directory dir)

14. Linux Log files

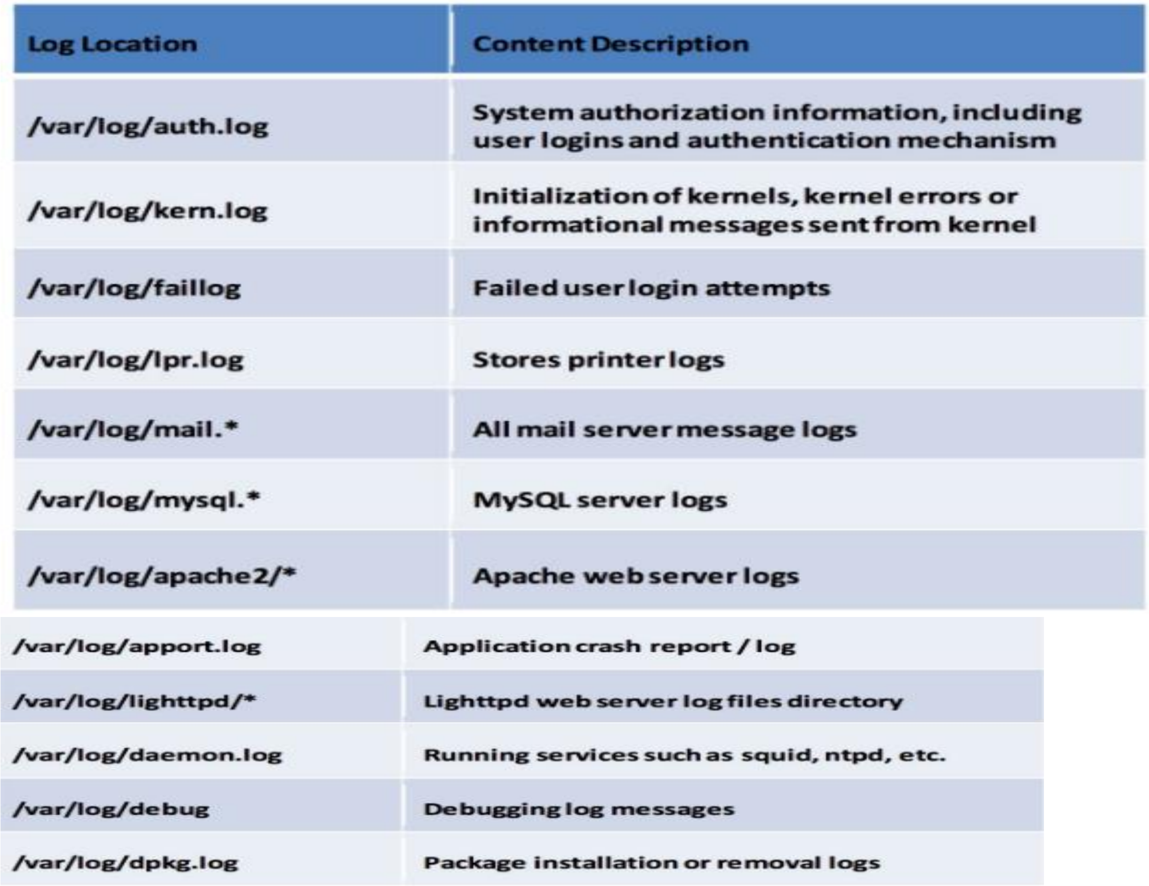
Log files are records of all the activities performed over an operating system. Linux log files store information about the system's kernel and the services running in the system. In Linux OS, different log files hold different information, which helps the investigators to analyze various issues during a security incident.

Investigators should learn and understand about the contents of various log files, which will help them during security incidents and help them understand the locations they might have to look for finding potential evidences.

Below mentioned are some locations for Linux log files which can help the investigators to find out the required data and resolve the issues. Additional log locations include:

/var/log/messages	Global system messages
/var/log/dmesg	Kernel ring buffer information
/var/log/cron	Information about the cron job in this file
/var/log/user.log	All user level logs
/var/log/lastlog	Recent login information
/var/log/boot.log	Information logged on system boots

Table 6. 15: Linux log files



Log Location	Content Description
/var/log/auth.log	System authorization information, including user logins and authentication mechanism
/var/log/kern.log	Initialization of kernels, kernel errors or informational messages sent from kernel
/var/log/faillog	Failed user login attempts
/var/log/lpr.log	Stores printer logs
/var/log/mail.*	All mail server message logs
/var/log/mysql.*	MySQL server logs
/var/log/apache2/*	Apache web server logs
/var/log/apport.log	Application crash report / log
/var/log/lighttpd/*	Lighttpd web server log files directory
/var/log/daemon.log	Running services such as squid, ntpd, etc.
/var/log/debug	Debugging log messages
/var/log/dpkg.log	Package installation or removal logs

Table 6. 16: Linux log Location

lsof

The command lsof is the short for ‘list open files’. The command is used to list all the open files and the active processes that opened them.

Lsmod-The command lsmod displays the information about the loaded modules.

last -F:-The command last –F displays the activities of each user in detail such as number of login and logout attempts along with dates of the system.

Aureport-is used to produce summary reports of the audit system logs.

readelf is the short notation for ‘Read Executable and Linking Format’. The command is used to analyze the file headers and section of the ELF files.

command ss -l -p -n | grep is used to check if that particular process running on the system is suspicious

The following are the most widely used **MAC Forensics Tools:**

- OS X Auditor
- Mac Forensics Tool
- MacForensicLab
- Macintosh Forensic Software
- Memoryze for the Mac
- Mac Marshal
- F-Response
- Mac OS X Memory Analysis Toolkit
- Volatility 2.5
- Avast Free Mac Security
- OS X Rootkit Hunter for Mac

<u>Chapter 6 Summary</u>

- In live response, collect the data about to change in a short time span Registry analysis provides more information to the investigator during live response

- The RAM contents analysis will help the investigator to find hidden things
- Gather more information about a suspicious process by dumping the used memory Collect information regarding network connections to and from the affected system
- Investigate the processes running on compromised system and collect info from the Task Manager

Federal Information Security Management Act of 2002 (FISMA):

Federal Information Security Management Act of 2002 that states several key security standards and guidelines, as required by Congressional legislation. FISMA emphasizes the need for each Federal agency to develop, document, and implement an organization-wide program to provide information security for the information systems that support its operations and assets. NIST SP 800-53, Recommended Security Controls for Federal Information Systems, was developed in support of FISMA. NIST SP 800-53 is the primary source of recommended security controls for Federal agencies.

Gramm-Leach-Bliley Act (GLBA): requires financial institutions to protect their customers' information against security threats. Log management can be useful in identifying possible security violations and resolving them effectively.

Health Insurance Portability and Accountability Act of 1996 (HIPAA): includes security standards for health information. NIST SP 800-66

Sarbanes-Oxley Act (SOX) of 2002: protect investors from the possibility of fraudulent accounting activities by corporations, applies primarily to financial and accounting practices, it also includes IT functions that support these practices.

Payment Card Industry Data Security Standard (PCI DSS): standard for organizations that handle cardholder information for the major debit, credit, prepaid, ATM, and POS cards.

Event correlation has four different steps, as follows:

Event aggregation called event de-duplication. It compiles the repeated events to a single event and avoids duplication of the same event.

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

Event filtering the event correlator filters or discards the irrelevant events.

Root cause analysis is the most complex part in event correlation. During a root cause analysis, the event correlator identifies all the devices that became inaccessible due to network failures.

Types of Event Correlation

- Same-Platform; same OS
- Cross-Platform; different OS for desktop, server, and network gear
- Transmission of Data; transmitting securely with authentication and encryption
- Normalization; after data is transmitted, return to common format for use
- Data Reduction; reducing or removing data for faster correlation

Event Correlation Approaches

- Neural Network approach
- Codebook-Based; stores sets of events in codes
- Rule-Based; uses rules to correlate events
- Field-Based; uses and compares fields in the data for correlation
- Automated Field correlation; compares some or all fields and determines correlation across these fields
- Packet Parameter/Payload Correlation; compares packets with signatures (IPS/IDS)
- Profile/Fingerprint; collect data to see if system was used as a relay or comp'd host
- Vulnerability-based; helps map IDS events to vulnerability scanner output
- Open-Port based; determine risk of attack by evaluating list of open ports

- Bayesian Correlation; predicts next steps based on statistics and probability
- Time or role-based approach; monitors computer and user behavior for anomalies
- Route correlation; extracts attack route info to single out other attack data

IIS centralized binary logging is a process where most of the websites transmit binary and scattered log data to a single log file. IIS centralized binary logging reduces system resources that are used for logging and provides complete log data for organizations that need it.

FSUM command line utility for file integrity verification. It offers a choice of 13 hash and checksum functions for file message digest and checksum calculation.

Swatch tool used for monitoring log files produced by UNIX's syslog facility

Logcheck utility that allows system administrators to view the log files, which are produced by hosts under their control. This is done by mailing summaries of the log files to the hosts, after first filtering out "normal" entries. Normal entries are entries that match one of the many regular expression files contained in the database.

Network Forensics Analysis Mechanism

Analyst Interface provides visualization of the evidence graph and reasoning results to the analyst, who passes the feedback to the graph generation and reasoning components.

Evidence Collection the collection of intrusion evidence from networks and hosts under investigation.

Evidence Preprocessing the analysis of assertive types of evidence, such as IDS alerts, into the appropriate format and reduces the repetition in low-level evidence by aggregation.

Evidence Depository collected intrusion evidence is stored in the evidence depository.

Evidence Graph Generation generates and updates the evidence graph using intrusion evidence from the depository.

Attack Reasoning process of automated reasoning based on the evidence graph.

Attack Knowledge Base includes knowledge of prior exploits.

Asset Knowledge Base includes knowledge of the networks from the fundamentals and hosts under investigation.

TOOLS: GFI EventsManager, Eventlog Analyzer, Kibana, Syslog-ng, RSYSLOG, Firewall Analyzer, SEC, OSSEC, Ipswitch Log Management, Snare, Loggly, Sumo Logic, ArcSight, Logscape, LogRhythm, Sawmill, McAfee log manager, LogMeister, Sentinel, TripWire, etc.

Sniffing Tools WireShark, SteelCentral Packet Analyzer, Tcpdump, Windump, Capsa, Omnipeek, Observer,

Fundamentals of Reconstruction

Temporal analysis

It produces a sequential event trail, which sheds light on important factors such as what happened and who was involved

Relational analysis

It correlates the actions of suspect and victim

Functional analysis

It provides a description of the possible conditions of a crime. It testifies to the events responsible for a crime in relation to their functionalities

Chapter 7 Summary

- Network forensics is the capturing, recording, and analyzing network traffic and event logs to discover the source of security attacks
- Network Addressing Schemes are of two types, LAN and Internetwork Addressing
- Log files are the primary recorders of a user's activity on a system and of network activities
- Routers store network connectivity logs with details such as date, time, source and destination IPs and Ports used that help investigators in verifying the timestamps of an attack and correlate various events to find the source and destination IP

- Investigators analyze network traffic to locate suspicious traffic, find the network generating the troublesome traffic, and identify network problems
- Gathering evidence on a network is cumbersome for the following reasons since the evidence is not static and not concentrated at a single point on the network

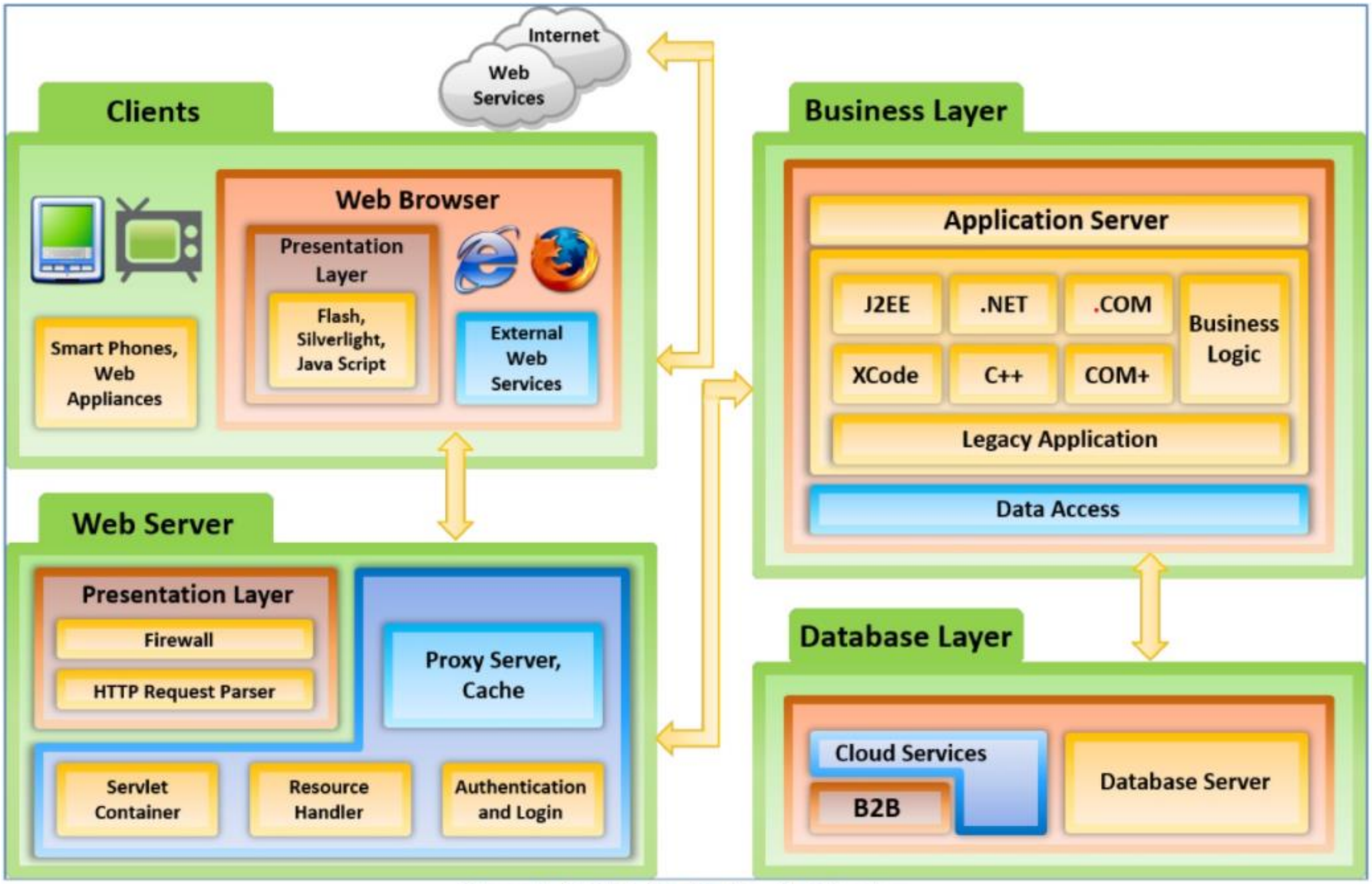


Figure 8. 1: Web Application Architecture

Data to collect from a website attack:

1. Date and time at which the request was sent
2. IP Address from where the request has initiated
3. HTTP method used (GET/POST)
4. URI
5. HTTP Query
6. A full set of HTTP headers
7. The Full HTTP Request body
8. Event Logs (non-volatile data)
9. File listings and timestamps (non-volatile data)

Types of Web Application Threats

- Buffer Overflow-overwrites adjacent memory locations
- Cookie Poisoning-modification of information in cookies
- Insecure Storage-lack of controls around data storage
- Information leakage-unintentional leakage of sensitive information
- Improper error handling-information is returned due to improper internal error handling
- Broken account mgmt.-poor controls around passwords, accounts in general
- Directory traversal-technique using http exploits to access outside http root directory
- SQL injection-injection of SQL commands via input data; no data checking

- Form tampering-manipulates communication parameters to change data
- DoS-targeted attack to produce a loss of service or availability
- Log tampering-an attempt to cover your tracks
- Unvalidated input-input strings to solicit XSS or SQL injection
- Cross site scripting-bypassing client security and injecting malicious code
- Injection flaws-injecting of malicious code that returns sensitive information
- Cross site request forgery-similar to phishing, user is made to click on a link
- Busted access control-flaws related to access control are exploited
- Platform exploits-vulnerability exploits based on java, .Net, etc..
- Insecure direct object references
- Insufficient transport layer protection
- SSL/TLS downgrade attacks-constant failure to negotiate TLS, so browser goes back to SSL and a MiTM attack can occur
- Failure to restrict URL access
- Insecure or improper cryptographic storage
- Cookie snooping
- Obfuscation application
- DMZ attacks

When an attack occurs, what to do?

- Run Event Viewer to look at the logs:
  - **C:\> eventvwr.msc**
- Check if the following suspicious events have occurred:
  - Event log service ends
  - Windows File Protection is inactive on the system
  - The MS Telnet Service is running
- Find if the system has failed login attempts or locked-out accounts
- Review file shares to ensure their purpose
  - **C:\> net view <IP Address>**
- Verify the users using open sessions
  - **C:\> net session**
- Check if the sessions have been opened with other systems
  - **C:\> net use**
- Analyze at NetBIOS over TCP/IP activity
  - **C:\> nbtstat –S**
- Find if TCP and UDP ports have unusual listening
  - **C:\> netstat –na**
- Find scheduled and unscheduled tasks on the local host
  - **C:\> schtasks.exe**
- Check for creation of new accounts in administrator group
  - **C:\> lusrmgr.msc**
- See if any unexpected processes are running in Task Manager
  - **Start -> Run -> taskmgr -> OK**
- Look for unusual network services
  - **C:\> net start**
- Check file space usage to look for a sudden decrease in free space
  - **C:\> dir**

Internet Information Server (IIS), a Microsoft-developed application, is a Visual Basic code application that lives on a Web server and responds to requests from the browser. It supports HTTP, HTTPS, FTP, FTPS, SMTP, and NNTP.

On Windows Server 2012, by default the log files are stored at **%SystemDrive%\inetpub\Logs\LogFiles**

The **Deep Log Analyzer** is a web analytics solution for small and medium size websites. It analyzes web site visitors' behavior and gets the complete website usage statistics in easy steps. Other tools: **Apache Logs Viewer, WebLog Expert, AWStats, Nagios, Splunk, Webalizer**

• MSSQL forensics take 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.

• Mysqldump is command line utility is used to take a backup of the database.

• Mysqldbexport is used to export metadata or data, or both from one or more databases

Apache web server comprises of a modular approach. It consists of two major components, the Apache Core and the Apache Modules.

Apache core elements are http_protocol, http_main, http_request, http_core, alloc, and http_config.

Apache Log provide very important information during auditing and forensic investigations about all the operations performed on the web server. This information includes:

- Client IP address
- ident of the client machine
- time
- **client user ID**
- Request line from a client
- Status code
- Size of the object returned to the client.

The default location of error logs:

- RHEL/Red Hat/CentOS/Fedora Linux: **/var/log/httpd/error_log**
- Debian/Ubuntu Linux: **/var/log/apache2/error.log**
- FreeBSD: **/var/log/httpd-error.log**

The default location of access logs:

- RHEL/Red Hat/CentOS/Fedora Linux**: /var/log/httpd/access_log**
- Debian/Ubuntu Linux: /**var/log/apache2/access.log**
- FreeBSD Linux: **/var/log/httpd-access.log**

Apache configuration file location:

- RHEL/Red Hat/CentOS/Fedora ````Linux: **/usr/local/etc/apache22/httpd.conf**
- Debian/Ubuntu Linux: **/etc/apache2/apache2.conf**
- FreeBSD: **/etc/httpd/conf/httpd.conf**

LOG FORMAT

%h %l %u %t \"%r\" %>s %b is the common percent directive log format

%h client's IP address.

%l Remote log name. Returns a dash unless mod_ident is there and IdentityCheck is set on.

%u is the client user ID.

%t represents the time when the server received the request.

\"%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).

%>s represents the status code which the server sends back to the client.

%b represents the size of the object which the server sends to the client.

IP Address Locating Tools: SmartWhois, ActiveWhois, LanWhois, CallerIP, HotWhois

Chapter 8 Summary

- Web applications provide an interface between the end users and web servers through a set of web pages that are generated at the server end or contain script code to be executed dynamically within the client Web browser
- An attack vector is a path or means by which an attacker can gain access to computer or network resources in order to deliver an attack payload or cause a malicious outcome
- Web defacement occurs when an intruder maliciously alters the visual appearance of a web page by inserting or substituting provocative and frequently offensive data
- Computer security logs contain information about the events occurring within an organization's systems and networks
- Injection flaws are web application vulnerabilities that allow untrusted data to be interpreted and executed as part of a command or query
- Intrusion detection is the art of detecting inappropriate, incorrect, or anomalous activity

Chapter 9 **CHFIv9 STUDY GUIDE**

MSSQL Forensics

Data and Logs in SQL servers are stored in three different files:

- **Primary Data Files (MDF)**
  The primary data file is the **starting point of a database** and points to other files in the database. Every database has an MDF. The **MDF stores all the data in the database objects** (tables, schema, indexes, etc.).
- **Secondary Data Files (NDF)**
  The secondary data files are **optional**. While a database contains only one primary data file, it can contain zero/single/multiple secondary data files.
- **Transaction LOG Data Files (LDF)**
  The transaction log files **hold the entire log information** associated with the database. The transaction log file helps a forensic investigator to examine the transactions occurred on a database, and even recover data deleted from the database.

Location of Files to Restore the Evidence

- Database & logs files: \\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\ DATA*.MDF | *.LDF
- Trace files: \\Microsoft SQL Server\MSSQL11.MSSQLSERVER \MSSQL\ LOG\LOG_#.TRC
- SQL Server error logs: \\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\ LOG\ERRORLOG

Investigators can track the volatile database information like login sessions of an account and the transactions using **ApexSQL DBA's ApexSQL Audit application**. Pretty much this is the only tool mentioned.

To initialize connection with the server (WIN-CQQMK62867E), the following
command is used in the application

sqlcmd -S WIN-CQQMK62867E -e -s"," –E

-e is used to echo input

-s is used for column separation

-E is used for trusted connection

Collecting Primary Data File and Transaction Logs

Collect the database files (.mdf) and log files (.ldf) from:

C:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER \MSSQL\DATA

Database Consistency Checker (DBCC) commands may give the investigator valuable insight into what is happening within the Server system. The DBCC LOG command allows investigators to view and retrieve the active transaction log files for a specific database.

Collecting SQL Server Trace Files

- To collect the trace files (.trc) or SQL Server error logs navigate to
  - C:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\LOG
  - The SQL Server error logs contain user defined events and specific system events

- The trace files contain the events that occurred on a SQL server and the host databases

MySQL

The architecture of MySQL is based on a tiered architecture, which is the combination of subsystems and support components interacting with one another to read, analyze and execute the queries made to the database server, and return the results. MySQL is an open source relational database. Data entered in a MySQL database is duplicated and stored in multiple locations.

ACID (Atomicity, Consistency, Isolation, Durability)

The default path to the data directory is mentioned below for the windows based machines

C:\ProgramData\MySQL\MySQL Server 5.n\
(or)
C:\mysql\data

Chapter 9 Summary

- Database Forensics is the examination of the databases and related metadata in a forensically precise manner to make the findings presentable in the court of law
- MSSQL Server stores data and logs in Primary Data Files (MDF), Secondary Data Files (NDF) and Transaction Log Data Files (LDF), respectively
- SQL server data is stored natively within SQL Server, and externally in windows machine hosting the server
- MySQL is based on a tiered architecture containing subsystems and support components, which work together in order to respond to the queries made to the database server
- MySQL server stores all the databases, status and log files; along with the data managed by the server under the data directory
- The database structure varies depending on the storage engine (MyISAM/InnoDB) used by MySQL

Chapter 10 **CHFIv9 STUDY GUIDE**

Infrastructure-as-a-Service (IaaS) This cloud computing service enables subscribers to use fundamental IT resources such as computing power, virtualization, data storage, network, and so on, on demand.

Platform-as-a-Service (PaaS)offers the platform for the development of applications and services. Subscribers need not buy and manage the software and infrastructure underneath it but have authority over deployed applications and perhaps application hosting environment configurations.

Software-as-a-Service (SaaS) This cloud computing service offers application software to subscribers' on-demand, over the Internet. The provider charges for it on a pay-per-use basis, by subscription, by advertising, or by sharing among multiple users.

Cloud computing

On-demand self-service

A type of service rendered by cloud service providers that 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.

Distributed storage

Offers better scalability, availability, and reliability of data. However, cloud distributed storage does have the potential for security and compliance concerns.

Rapid elasticity

The cloud offers instant provisioning of capabilities, to rapidly scale up or down, according to demand.

Automated management

By minimizing the user involvement, cloud automation speeds up the process, reduces labor costs, and reduces the possibility of human error.

Broad network access

Cloud resources are available over the network and accessed through standard procedures, via a wide-variety of platforms, including laptops, mobile phones, and PDAs.

Resource pooling

The cloud service provider pools all the resources together to serve multiple customers in the multi-tenant environment, with physical and virtual resources dynamically assigned and reassigned on demand by the cloud consumer.

Measured service

Cloud systems employ "pay-per-use" metering method. Subscribers pay for cloud services by monthly subscription or according to the usage of resources such as storage levels, processing power, bandwidth, and so on. Cloud service providers monitor, control, report, and charge consumption of resources by customers with complete transparency.

Virtualization technology

Enables rapid scaling of resources in a way that non- virtualized environments could not achieve.

Limitations of Cloud Computing:

- Organizations have limited control and flexibility
- Prone to outages and other technical issues
- Security, privacy, and compliance issues
- Contracts and lock-ins
- Depends on network connections

Types of clouds:

- Private
- Public
- Hybrid
- Community(multi-tenant, common computing concerns)

Types of DNS Attacks

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

Cloud Crime

- Cloud as a subject It refers to a crime in which the attackers try to compromise the security of a cloud environment to steal data or inject a malware. Ex: Identity theft of cloud user's accounts, unauthorized modification or deletion of data stored in the Cloud, installation of malware on the cloud, etc.
- Cloud as an object when the attacker uses the cloud to commit a crime targeted towards the CSP. The main aim of the attacker is to impact cloud service provider. Ex: DDoS attacks that can bring the whole cloud down.
- Cloud as a tool when the attacker uses one compromised cloud account to attack other accounts. In such cases, both the source and target cloud can store the evidence data.

Cloud Computing Threats

- Data Breach or Loss
- Abuse of Cloud Services to perpetrate attacks
- Insecure Interfaces and APIs
- Insufficient Due Diligence
- Shared Technology Issues (PaaS/IaaS; shared HW)
- Unknown Risk Profiles
- Inadequate Infrastructure Design and Planning
- Conflicts between Client Hardening Procedures and Cloud Environment
- Loss of Operational and Security Logs

- Malicious Insiders
- Illegal Access to the Cloud
- Privilege Escalation, etc..

Cloud Computing Attacks

- Service Hijacking using Social Engineering
- Session Hijacking
- DNS Attacks
- SQL Injection
- Wrapping(SOAP/TLS exploit)
- Side Channel or Cross-guest VM attacks
- Cryptanalysis
- DoS/DDoS

Artifacts Left by Dropbox Client

When a user installs Dropbox the files are saved at **C:\Program Files (x86)\Dropbox**
Configuration is stored **C:\Users\<username>\AppData\Local\Dropbox\instance(n)**
The system uses **C:\Users\<username>\Dropbox** as the default folder to sync files.
YOU CAN USE "WhatChanged" as a tool to see what programs add to the registry or Magnet IEF for other data gathering on pcs, phones, and tablets**

Artifacts Left by Google Drive Client

When a user installs Google Drive the files are saved at **C:\Program Files (x86)\Google\Drive**
Configuration and Logs are stored **C:\Users\<username>\AppData\Local\Google\Drive\user_default**
The system uses **C:\Users\<username>\Google Drive** as the default folder to sync files.
Cellebrite UFED Cloud Analyzer tool provides forensic practitioners with instant extraction, preservation, and analysis of private social media accounts -- Facebook, Twitter, Kik, Instagram -- file storage and other cloud-based account content that can help speed investigations.

Chapter 10 Summary

- Cloud computing is an on-demand delivery of IT capabilities where IT infrastructure and applications are provided to subscribers as a metered service over a network
- Cloud services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS)
- Cloud forensics is the application of digital forensic investigation process in the cloud computing environment
- Crime committed with cloud as a subject, object, or tool is a cloud crime
- Forensic investigations in cloud involve a minimum of CSP and the client. But, the scope of the investigation extends when the CSP outsources services to third parties
- According to the NIST, cloud forensics challenges are categorized into nine major groups - architecture, data collection, analysis, legal, training, anti-forensics, incident first responders, role management, standards, etc.
- Cloud storage services such as Dropbox, Google Drive, etc. create artifacts on a system they are installed upon that may provide relevant information to investigation

Chapter 11 **CHFIv9 STUDY GUIDE**

Malware Forensics

Malware programs include viruses, worms, Trojans, rootkits, adware, spyware, etc., that can delete files, slow down computers, steal personal information, send spam, and commit fraud.
Static Analysis- analysis of malware without executing the code or instructions. Includes file fingerprinting(HashMyFiles), local and online scanning(VirusTotal), string searches(Strings, ResourcesExtract, Bintext), obfuscation methods(PEiD), finding portable executables(Anubis), identify file dependencies, malware disassembly.

Dynamic analysis involves execution of malware to examine its conduct, operations and identifies technical signatures that confirm the malicious intent.

Other Tools: Dr. Web Online Scanner, Metascan Online, Bitdefender QuickScan, ThreatAnalyzer, Jotti, IDA Pro, OllyDbg, ESET SysInspector, YAPM, MONIT, OpManager, FCIV, SIGVERIF, Tripwire, FileVerifier++, CSP File Integrity Checker,

Different Ways Malware Can Get into a System

- IM applications
- IRC
- Removable Devices
- Email and attachments
- Browser and software bugs
- File Downloads
- Network File Sharing
- Bluetooth and wireless networks

Malware Distribution Techniques

- Blackhat SEO
- Social Engineering click jack
- Spearphishing
- Malvertising – malware laden advertisements
- Compromise legitimate websites
- Drive-by Download – browser exploits that install malware

Malware Components

- **Crypter:** Refers to a software program that can conceal existence of malware.
- **Downloader:** Type of Trojan that downloads other malware (or) malicious code and files from the Internet on to the PC.
- **Dropper:** Attackers need to install the malware program or code on the system to make it run and this program can do the installation task covertly.
- **Exploit**: Part of the malware that contains code or sequence of commands that can take advantage of a bug or vulnerability in a digital system or device.
- **Injector:** Program that injects the exploits or malicious code available in the malware into other vulnerable running processes and changes the way of execution to hide or prevent its removal.
- **Obfuscator:** A program to conceal the malicious code of a malware via various techniques.
- **Packer:** It is software that compresses the malware file to convert the code and data of malware into an unreadable format.
- **Payload:** Part of the malware that performs desired activity when activated.
- **Malicious Code:** It is a piece of code that defines basic functionality of the malware and comprises commands that result in security breaches.

netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]

- -a: Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.
- -e: Displays Ethernet statistics, such as the number of bytes and packets sent and received. This parameter can be combined with -s.
- -n: Displays active TCP connections, however, addresses and port numbers are expressed numerically, and no attempt is made to determine names.
- -o: Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the Processes tab in Windows Task Manager. This parameter can be combined with -a, -n, and -p.

- -p Protocol: Shows connections for the protocol specified by Protocol. In this case, the Protocol can be tcp, udp, tcpv6, or udpv6. If this parameter is used with -s to display statistics by protocol, Protocol can be tcp, udp, icmp, ip, tcpv6, udpv6, icmpv6, or ipv6.
- -s: Displays statistics by the protocol. By default, statistics are shown for the TCP, UDP, ICMP, and IP protocols. If the IPv6 protocol for Windows XP is installed, statistics are shown for the TCP over IPv6, UDP over IPv6, ICMPv6, and IPv6 protocols. The -p parameter can be used to specify a set of protocols.
- -r: Displays the contents of the IP routing table. This is equivalent to the route print command.

NETSTAT -an to look for suspicious connections AND -ano for also Process ID

Chapter 11 Summary

- Malware is a malicious software that damages or disables computer systems, and gives limited or full control of the systems to the malware creator for the purpose of theft or fraud
- Components of a malware software relies on the requirements of the malware author who designs it for a specific target to perform the intended tasks
- Malware forensics deals with identifying and capturing malicious code, and evidences of its effect on the infected system
- To analyze malware, a dedicated laboratory system is required, which can be infected keeping the production environment safe
- Performing malware analysis enables you to know the type of malware, how it works, its behavior, and impact on the target system
- Static analysis/code analysis involves going through the executable binary code without actually executing it to have a better understand of the malware and its purpose
- Dynamic analysis/behavioral analysis involves executing the malware code to know how it interacts with the host system and its impact on it

Chapter 12 **CHFIv9 STUDY GUIDE**

SMTP (Simple Mail Transfer Protocol, port 25) is an outgoing mail server, which allows a user to send emails to a valid email address.

POP3 (Post Office Protocol, v3, port 110) is a simple protocol for retrieving emails from an email server. When the POP server receives emails, they are stored on the server until and unless the user requests it.

IMAP(port 143 or 993) 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. This enables the users to organize all the mails depending on their requirement.

-For an organization, any information in the form of electronic documents or records is a proprietary asset. Electronic Records Management makes sure that the organization has all the documents or records it needs when they are required.

- It helps to the organizations to tackle any legal mandates pertaining to the protection of the organization.
- It protects against unauthorized access or manipulations of electronic data
- It reduces the retrieval costs of the records that are no longer required to be maintained on the system and also reduces the burden of keeping paper records
- It helps to produce data on demand and withhold it for inspection.
- It helps in capacity management for effective usage of the IT resources such as servers and disk storages.
- Helps in preserving original form of email messages, thereby ensuring consistent mail forms.

E-mail crime can be categorized in two ways:

Crimes committed by sending e-mails

- Spamming
- Phishing
- Mail bombing - primary objective behind mail bombing is to overload the email server and degrade the communication system by making it unserviceable.

- Mail storms - occurs when computers start communicating without human intervention.

Crimes supported by e-mails

- Identity Fraud
- Cyber-stalking
- Child pornography
- Child abduction

Email crimes and violations depend on the cyber laws created by the government of the place from where the email originates. We can categorize email crime in two ways: one committed by sending emails and the other supported by emails. When criminals use emails for selling narcotics, stalking, fraud, child pornography, or child abduction, spamming, fake email, mail bombing, or mail storms then we can say that emails support cybercrime.

Steps involved in investigating e-mail crimes and violations

- Obtain a Search Warrant
- Examine e-mail messages
- Copy and print the e-mail messages
- View the e-mail headers
- Analyze the e-mail headers
- Trace the e-mail
- Acquire e-mail archives
- Examine e-mail logs
- Types of encoding in emails

MIME

It is an Internet standard that extends the email format for supporting the following:

- Text in non-ASCII character sets
- Attachments like application programs, images, audio, video, etc. other than text
- Multiple part message bodies
- Non-ASCII character set header information

Uuencode

also known as UNIX-to-UNIX encoding or Uuencode/Uudecode, is a utility for encoding and decoding files shared between users or systems using the UNIX operating systems. It is also available for all other operating systems, and many e-mail applications offer it as an encoding alternative, especially for e-mail attachments. While sending e-mails with attachments, if the recipient(s) do not have an MIME-compliant system, the Uuencode should be used to send the attachment as an e-mail note.

BinHex is the short form for "binary-to-hexadecimal." It is a binary-to-text encoding system used on Mac OS to send binary files via e-mails. This system is similar to Uuencode, but BinHex combines both "forks" of the Mac file system including extended file information.

Stellar Phoenix Deleted Email Recovery is a software that safely recovers lost or deleted emails from MS Outlook data (PST) files and Outlook Express data (DBX) files.

Forensic Toolkit (FTK) is a court-cited digital investigations platform built for speed, stability and ease of use. It provides comprehensive processing and indexing up front, so that filtering and searching is fast.

Paraben's Email Examiner examines email formats including Outlook (PST and OST), Thunderbird, Outlook Express, Windows mail and more. It allows to analyze message headers, bodies and attachments. It recovers email in the deleted folders, supports advanced searching, reporting and exporting to PST and other formats and supports all major email types that are stored on local computers for analysis, reporting, and exporting/conversion.

Kernel for PST Recovery is able to repair corrupted PST file and recover all email items from them. It successfully fixes errors resulted due to damaged or corrupted PST file, virus attacks, deleted emails, broken PST files, header corruption, disk corruption, errors due to large PST file size and others.

The **CAN-SPAM Act** (Controlling the Assault of Non-Solicited Pornography and Marketing Act) is a law that sets the rules for sending e-mails for commercial purposes, establishes the minimum requirements for commercial messaging, gives the recipients of e-mails the right to ask the senders to stop e-mailing them, and spells out the penalties in case if the rules are violated.

CAN-SPAM's main requirements meant for senders:

- Do not use false or misleading header information
- Do not use deceptive subject lines
- The commercial e-mail must be identified as an ad
- The email must have your valid physical postal address
- The email must contain the necessary information regarding how to stop receiving e-mails from the sender in future
- Honor recipients opt-out request within 10 business days
- 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

Chapter 12 Summary

- An e-mail system consists of e-mail servers and e-mail clients
- An e-mail client, also known as a mail user agent (MUA), is a computer program for accessing and managing emails
- An e-mail server connects to and serves several e-mail clients
- Headers contain significant information regarding the mail, such as sent time, unique identifying numbers, IP address of the sending server, etc.
- "Received" headers maintain a record of the detailed log history of message history, and they help to find out the origin of an e-mail, even when other headers have been forged
- Online e-mail programs such as AOL, Gmail, and Yahoo! leave the files containing e-mail messages on the computer in different folders such as History, Cookies, Temp, Cache, and Temporary Internet Folder

Chapter 13 CHFIv9 STUDY GUIDE

Mobile Forensics-includes extraction, recovery, and analysis of data from the internal memory, SD cards, and **SIM cards** of mobile devices. Forensics experts analyze the phone by examining the incoming and outgoing text messages, pictures stored in the memory of the phone, call logs, email messages, SIM data, deleted data, etc., in an attempt to trace the perpetrators of crimes that involve the use of mobile phones.

Top Threats

- Web/network based attacks
- Malware
- Social Engineering
- Resource Abuse
- Data Loss
- Data Integrity threats

Communication API simplifies the process of interacting with web services and other applications such as email, internet, and SMS.

The GUI API responsible for creating menus and sub-menus in designing applications. It acts as an interface where the developer has a chance of building other plugins.

Phone API provides telephony services related to the mobile carrier operator such as making calls, receiving calls, and SMS. All phone APIs appear at the application layer.

Operating system: scheduling multiple tasks, memory management tasks, synchronization, and priority allocation. It also provides interfaces for communication between application layers, middleware layers, and hardware.

Hardware: hardware such as a display device, keypad, RAM, flash, embedded processor, and media processor, which are responsible for mobile operation.

Radio interface, gateway, and network interface: A mobile device communicates with the network operator with some interfaces, such as radio interface, gateway, and network interface, to establish safe and secure communication.

Network: To communicate with the network, the data must pass through various layers to reach the destination. The data travels over network layers to reach its destination.

Android Libraries native library that permits the device to manage various types of data

Surface Manager: windows owned by different applications on different processes

Media framework: media codecs that allow the record and playback of all the media

SQLite: SQLite is the database engine that stores data in Android devices

OpenGL/ES and SGL: used to render 2D (SGL) or 3D (OpenGL/ES) graphics to the screen

FreeType: It renders the bitmap and vector fonts

WebKit: It is the browser engine used to display web pages

Libc: It is a C system library tuned for embedded Linux-based devices

Core Java provides almost all the functionalities stated in Java software edition libraries

Dalvik Virtual Machine (DVM) is a type of the Java virtual machine responsible for power management and memory management.

Android Boot Process

1. Boot ROM is activated and loads Boot Loader into RAM
2. Boot Loader initializes and then starts the Kernel
3. Kernel initializes interrupt controllers, memory protections, caches, and scheduling. System can use virtual memory and launch the user space process (init)
4. Init process launches and is first process on device, parent process. Next init initializes Zygote, runtime, and daemon processes; the Android logo appears
5. Zygote is used to spin up new VMs for each app that is started; a new DVM with code sharing across the vms.
6. Runtime requests Zygote launch system server; which includes: power manager, battery service, and Bluetooth

iOS Architecture

1. No access directly to hardware
2. OS contains 4 abstraction layers (500MB+)
3. Core OS-low-level services-
4. Core services-foundation to upper layers. iCloud, dispatch, in-app purchases, etc
5. Media services-audio, video, animation, graphics, etc. OpenGL ES, AL, etc
6. Cocoa Touch layer-framework for app development UIKit
7. Uses C-based libSystem libraries like BSD sockets, POSIX threads, and DNS

iOS Boot Process

1. BootRom initializes some components and checks signature of LLB (lower level bootloader)
2. LLB is loaded and checks signature of iBoot (stage-2 boot loader)
3. iBoot is loaded and checks kernel and device tree signatures (Not booted in Device Firmware Upgrade DFU mode)
4. Kernel and device trees load. Kernel checks signatures of all user applications

Mobile Storage/Evidence

Internal Phone Memory: It includes data stored in RAM, ROM, or flash memory. It stores the Mobile phone's OS, applications, and data. The investigator can extract information from internal phone memory using AT commands with the help of a USB cable, infrared, or Bluetooth.

SIM Card Memory: data stored in the SIM card memory like address books, messages, and service-related information.

External Memory: data stored in SD card, MiniSD Card, MicroSD, etc. It stores personal information such as audio, video, and images.

The investigator must follow the steps before performing a forensic investigation:

Build a Forensics Workstation

Investigators build forensic workstations to perform forensic investigation on mobile devices. The workstation includes hardware and software tools in the lab such as laptop or desktop computer, USB connector, FireWire, mobile forensics toolkit, cables (including Bluetooth and IR), SIM card reader, and micro-SD memory card reader.

Build the Investigation Team

The investigation team consists of persons who have expertise in responding, seizing, collecting, and reporting evidences from the mobile devices. Includes the expert witness, evidence manager, evidence documenter, evidence examiner/investigator, attorney, photographer, incident responder, decision maker, and incident analyzer.

Review Policies and Laws

Before starting the investigation process, investigators need to understand the laws pertaining to the investigation. They must also be aware of the potential concerns associated with Federal laws, State statutes, and local policies and laws before beginning the investigation.

Notify Decision Makers and Acquire Authorization

Decision makers are authorities who implement the policies and procedures for handling an incident. The decision maker must be notified for the authorization when written incident response policies and procedures do not exist.

Risk Assessment

Risk assessment measures the risk associated with the mobile data, estimating the likelihood and impact of the risk. Risk assessment is an iterative process and it assigns priorities for risk mitigation and implementation plans.

Build a Mobile Forensics Toolkit

Investigators require a collection of hardware and software tools to acquire data during the investigation. The investigator needs to use different tools to extract and analyze the data, depending on the make and model of the phone seized.

The **best practices** to get authorization and define the course of action are as follows:

- An authorized decision maker should be chosen to obtain authorization for conducting the investigation.
- All the events occurring and decisions taken at the time of the incident and incident response should be documented. Investigators can use these documents in court proceedings to determine the course of action.
- Depending on the scope of the incident and absence of any national security issues or life safety issues, the first priority is to protect the organization from further harm.
- After securing the organization, the services are reinstated, and the investigation is carried out for the incident.

Here are some of the tools a forensic investigator requires as a part of a forensic toolkit:

Hardware Tools:

- Cellebrite UFED System
- Secure ViewKit for Forensics
- DS-Device Seizure & Toolbox
- USB reader for SIM cards
- iGo

- DC Lab Power Supply 0-15V/3A
- Digital Display with Backlight
- Paraben's Phone Recovery Stick

Software Tools:

- SEARCH Investigative Toolbar
- SIMiFOR ASC
- 001Micron Data Recovery
- *SIM Explorer
- BitPim
- *Oxygen Forensics Analyst
- Paraben's Sim Card Seizure
- *MOBILedit! Forensic
- TULP2G
- iDEN Phonebook Manager
- SUMURI's PALADIN
- floAt's Mobile Agent
- XRY Logical & XRY Physical
- Forensic Explorer- for file carving
- Scalpel – file carving for iphone
- Phone Image Carver
- *Blade Professional
- Autopsy
- FTK Imager/EnCase/Smart for imaging
- IExplorer – to bypass iPhone passcode
- *ViaExtract ADB – bypass Android passcode
- SIMIS 2.0
- SIMulate
- SIMXtractor
- Last SIM
- USIM Detective
- SIM Query
- SQLite Database extraction
- Andriller

Rooting Tools

- Android
    - OneClickRoot
    - Kingo Android ROOT
    - Towelroot
    - RescuRoot
- iOS
    - PANGU JAIL BREAK
    - Redsn0w
    - Sn0wbreeze
    - GeekSn0w

Cellular Components

SIM – Subsciber Indentity Module can store data such as contacts, messages, and time stamps. It also contains technical info like: Integrated Circuit Card Id (ICCID), International Mobile Subscriber Identity (IMSI), last dialed numbers, service provider name, etc.

Mobile Switching Center (MSC): processes calls and messages within a network and routes them between landline and wireless networks.

Base Transceiver Station (BTS): equipment that facilitates the user with wireless communication between the mobile phone and a network.

Base Station Controller (BSC): It manages the transceiver's equipment and performs channel assignment. It is part of the GSM architecture, which controls one or more base transceiver stations and the cell site's radio signals in order to reduce the load on the switch.

Base Station Subsystem (BSS): This is one of the major sections of a cellular network. It controls the BSC and BTS units. It is responsible for handling traffic, network switching system and signaling between cell phones.

Home Location Register (HLR): This is the database at the MSC. It is the central repository system for subscriber data and service information.

Visitor Location Register (VLR): This is the database used in conjunction with the HLR for mobile phones roaming outside of their service area. It contains the current location of the mobile user as well as the Temporary Mobile Subscriber Identity (TMSI).

Authentication Center (AuC): stores the user's IMSI, encryption, and authentication keys.

Equipment Identity Register (EIR): database that contains a list of devices with their IMEI numbers. 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, if required.

Cellular Networks

Code Division Multiple Access (CDMA): dominant cellular network used. It employs spread-spectrum technology where channels for communication are defined in terms of codes.

Enhanced Data Rates for GSM Evolution (EDGE): Improved data transmission rates are possible through backward-compatible digital mobile phone technology. It delivers high bit-rates per radio channel that is used for any of the packet-switch applications.

Integrated Digital Enhanced Network (iDEN): developed by Motorola, is the mobile communication technology that provides its users with the benefit of a trunked radio and cellular telephone.

General Packet Radio Service (GPRS): packet-oriented mobile data service available to the users of GSM and IS-136 mobiles.

Global System for Mobile communications(GSM): popular cellular network.

High-Speed Downlink Packet Access (HSDPA): This third generation mobile telephony communication protocol allows high data transfer speed for networks based on UMTS.

Time Division Multiple Access (TDMA): single- frequency channel provided to multiple users over a divided time slot.

Universal Mobile Telecommunications System (UMTS): This is a 3-G mobile phone technology (upgrade to 4-G) that use W-CDMA as the underlying interface.

Unlicensed Mobile Access (UMA): UMA or the Generic Access Network (GAN) enables mobile services such as voice, IP Multimedia Subsystem/Session Initiation Protocol (IMS/SIP applications), and data to access IP networks.

SIM File System

- Master File – root of filesystem and contains or more DF's and/or one or more EF's. Identified by 3F00
- Dedicate File (DF) - directories that can contain one or more EF's and holds only the header that contains information related to file structure and security
- Elementary Files (EF) – contains both header and body; which hold actual data. Contains serial number of SIM.

International Mobile Equipment Identifier (IMEI) 15-digit GSM-based unique number on handset that identifies mobile equipment.

Obtained with *#06# **Format is AA BBBBBB CCCCCC D**

AA: Reporting body ID that allocated the Type Allocation Code (TAC)

BBBBBB: remainder of the TAC (FAC)
CCCCCC: Serial sequence of the Model (SNR)
D: Luhn check digit of entire model or 0 (CD)

Electronic Serial Number (ESN) **unique, 32-bit number** attached on a chip inside a **CDMA** phone by manufacturer. There are **two formats**:

8 bits manufacturer code and 24 bits for serial number **OR**
14 bits for manufacturer code and 18 bits serial number

Integrated Circuit Card Identifier (ICCID) is a **19 or 20-digit** unique identification/serial number printed on the SIM to identify each SIM internationally.

89	44	245252	001451548
Industry Identifier	**Country**	**Issuer ID**	**Individual Account ID**

International Mobile Subscriber Identity (IMSI) **15-digit** subscriber identification number that defines a subscriber in the wireless world, including the country and mobile network to which the subscriber belongs.

Service Provider Network (SPN) defines SIM card Service Provider

Mobile Country Code (of a SIM user internationally on a GSM network.

Mobile network code (MNC) **two-digit** network identification number used along with the MCC printed on SIM. It used to identify the SIM user on a mobile phone network.

Mobile subscriber identification number (MSIN): It is a **10-digit** number MIN (mobile identification number) that helps identify the mobile phone service provider within a mobile carrier network.

Mobile international subscriber directory number (MSISDN): **15-digit number** used for international identification of mobile phone numbers, and it contains the country code and nation-wide destination code.

Abbreviated dialing numbers (ADN): These are **three-digit dialing numbers**. communication in emergency

Chapter 13 Summary

- Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions
- Diversity in the mobile OS architecture may impact forensics analysis process
- Knowledge of mobile OS booting process helps investigators to gain lower level access
- Mobile storage and evidence locations include: internal memory, SIM card, and external memory
- Identifying cell phone brand, model, OS, and network service provider assists in choosing an appropriate forensics tool for data acquisition
- Rooting/Jailbreaking provides privileged control (known as "root access") within device's subsystem, enabling data acquisition
- Standard tools such as Cellebrite UFED Touch can be used to prepare mobile forensics report

Chapter 14 **CHFIv9 STUDY GUIDE**

Forensics Investigation Reports

A forensic investigation report is a statement of allegations and conclusions drawn from the computer forensics investigation. It contains all the findings of the investigator in written form, thereby making it a concise, precise, accurate, and organized report. It represents all the aspects of an investigation, which is unbiased, organized, and understandable.

Reports can be categorized as:

- Verbal – board, jury, managers=formal
- Written – court, under oath = formal

Further division of the previous categories includes:

- Formal
- Informal

It is advisable to include the contents of an informal written report in an informal verbal report and the essentials such as the subject system, tools used, and findings should be summarized in it. If the produced

informal written report is destroyed then it is **considered as destruction or concealing of evidence**, which in legal terms is known as **spoliation.**

Expert witnesses recognized by the court of law as trustworthy for taking an opinion or verify a process by virtue of their education, skills, expertise, knowledge, and experience in a specific field. In this case, expert witnesses are the technically sound persons, who understand the working, process of attacks, investigative methods and the results obtained. Curriculum vita (CV) of an expert witness is helpful in qualifying his/her testimony by acknowledging his/her previous professional experiences.

- **Consulting Expert:** To offer technical explanations for a complex situation during court trials.
- **Court's Expert:** To advise the court on technical issues that the court fails to comprehend.
- **Testifying Expert:** To present testimony whenever required during the trial.

Technical witnesses' testimony may only provide facts found during the investigation to showcase an incident or a crime. He/she explains what exactly the evidence leads to in the process of acquisition; however, they cannot draw conclusions or offer opinion. They only conduct the fieldwork and submit the findings or facts of the investigation.

On the other hand, expert witnesses can give opinions based on their observation and experiences. They can also perform a deductive analysis with facts found during an investigation. Since computer forensics is a comparatively new field and does not follow any standards of practice, the expert witnesses must provide a clear opinion to the jury who may not be fully aware of the latest developments in the field of computer forensics.

The **Daubert Standard**, the **rule of evidence regarding the admissibility of the expert witnesses' testimony** during the federal legal proceedings. The trial judges should analyze the proffered expert witnesses to decide whether their testimony is **both "relevant" and "reliable".**

The **Frye Standard** related to **the admissibility of scientific examinations or experiments** in legal cases. According to this act, any kind of expert opinion based on scientific techniques is admissible, if the technique involved is acceptable by the relevant scientific community.

International Organization of Computer Evidence (IOCE) is an organization formed in 1995. This organization provides an **international forum for law enforcement** agencies around the world for **exchanging information** that are related with computer investigation and digital forensic issues.

The standard order of trial proceedings includes:

- **Motion in Limine (Motion in Beginning):** This is a handwritten list of objections to a certain testimony. It is a special hearing on the acceptability of evidence or restriction of evidence. It is usually done a day or two before the beginning of the trial proceedings. This allows the judge to determine if the evidence should be allowed without the jury's presence.
- **Opening Statement:** An opening statement is important because it offers an outline of the case.
- **Plaintiff and Defendant**: A plaintiff is a person who initiates the lawsuit, claiming for damages; whereas the defendant is the person who is answerable to the plaintiff's complaints or claims. The attorney and the opposing counsel presents the case, explains what, when, where, and how it happened.
- **Rebuttal Session**: The rebuttal session is the cross-examination of the expert witness by both the plaintiff and the defendant.
- **Jury Orders:** The judge educates the jury about the law points related to the case. They can be presented either before or after the closing statements. These are intended to assist the jury with the application of certain specific laws to the details involved in the case, which is then read and approved by the jury.
- **Closing Arguments:** After the presentation of all the evidence, both the plaintiff and defendant have the chance to present the summarized closing statements of the case. The attorney and the opposing counsel can suggest solutions for the case but must leave the verdict to be decided by the jury.

Chapter 14 Summary

- An investigation report provides detailed information on the complete forensics investigation process

- 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
- Direct examination is the process of a witness being questioned by the attorney who called him or her to the stand
- Cross-examination is providing the opposing side in a trial the opportunity to question a witness
- Deposition is the process of questioning witnesses prior to a trial, and it is used in the pretrial stages of both civil and criminal cases
- Deposition differs from a trial as:
    - Both attorneys are present
    - No jury or judge present
    - Opposing counsel asks questions
- Purpose of a deposition:
    - Enables opposing counsel to preview your testimony at trial