Study Guide

<u>Course Name</u>

Created By: Dereck Coleman, Teaching Assistant

Module 1: Computer Forensics Today

<u>Lesson 1.1</u>: Computer Forensics Today Part 1

Skills Learned From This Lesson: What is Computer Forensics, Types of crimes, Investigator challenges

- What is computer forensics?
  - Computer forensics is a set of procedures and techniques that help an investigator identify gather, extract, interpret, document and preserve evidence from a computer in a way that is legal and admissible for court. This includes hard drives, CDs, and Ram.
- Types of Computer Crimes
  - Phishing – Fraudulent attempt to obtain sensitive information from a user by computer
  - Malware/Ransomware – The use of malicious software
  - Identity Theft – Stealing someone's identity online.
  - Financial Fraud – Crimes committed against property, involving the unlawful conversation of the ownership of the property
  - Cyberterrorism – Computer used to further propaganda
  - Cyberextortion – Hacking webcams and then using that information as blackmail
  - Cyberwarfare – Different nations trying to hack each other
  - Cyberbullying – Bullying done online using social media
  - Drug Trafficking – Selling Drugs online
- Challenges investigators face
  - Encryption
  - Steganography
  - Data wiping / Anti-forensics
  - Legal challenges
  - Volume of data
  - Media formats

  - Time limitations
- Digital Forensics Investigative Processes
  - Assess
  - Acquire
  - Analyze
  - Report

Lesson 1.2: Computer Forensics Today part 2

Skills Learned from This Lesson: Type of Investigation, Evidence, Forensic rules

Notes

- Criminal Investigations
  - Violation of some type of law (international, state, country)
  - Need a digital forensics investigation processes before starting
  - A formal investigation report is REQURIED for a criminal Investigation
  - Beyond reasonable doubt is needed to prove a crime is committed
- Civil Investigation
  - Dispute between 2 parties
  - Monetary Damage
  - Preponderance >50% of truth
- Administrative Investigations
  - Could turn into a criminal Investigation if needed.
  - Internal investigation (within a company investigation)
  - Policy Violation
  - Threatening behavior
  - Corruption within possible
- Rules of a forensic Investigator
  - Limit access to original evidence
  - Make duplicate copies and examine those
  - Record Changes
  - Chain of custody
  - Standards
  - Know limitation of skills
  - Secure storage
  - Legal
  - Industry tools
- ETI (Enterprise Theory of Investigations)
  - *Holistic approach to criminal and civil investigations*

        - Ex. Trying to develop a pattern for a crime organization to get the bigger members.
- Types of Evidence
    - Volatile Evidence (gather before moving, closing, or shutting down the device)
        - System Time
        - Process Information
        - Open Files
        - Network Information
        - Process Memory
        - Clipboard
        - Service/Driver information
        - Command history
    - Non-Volatile Evidence (Data that stays present even when the device is turned off)
        - Slack Space
        - Hidden Files
        - Swap Files
        - Unallocated Clusters
        - Unused Partitions
        - Registry Settings
        - Event Logs

Lesson 1.3: Computer Forensics Today Part 3

Skills Learned From This Lesson: Law Types, Duties performed, SWGDE

- Federal Rules of Evidence (common ones not all)
    - Rule 101: Governs Proceedings in courts of the U.S. Department of Defense
    - Rule 103: Rulings on evidence
    - Rule 105: Limited admissibility
    - Rule 502: Attorney-client privilege
    - Rule 801-804: Hearsay
    - Rule 1002: Requirement of Original Evidence
    - Rule 1003: Admissibility of duplicate Evidence
    - Rule 1004: Admissibility of other evidence of content

- Laws
    - 18USC § 1030: Computer Fraud and Abuse Act

- ○ 18 USC § 2252A: Child Pornography
- ○ 18 USC § 2252B: Misleading domains
- ○ FISMA
    - ■ Federal Information Security Management Act
        - Requires Annual reviews of information security programs
- ○ GLBA
    - ■ Gramm-Leach-Bliley Act
        - Requires financial institutions to protect customer information against security threats
- ○ HIPPA
    - ■ Health Insurance Portability and Accountability Act
        - Safeguarding private medical information of patients
- ○ SOX
    - ■ Sarbanes-Oxley Act
        - Act against fraudulent financial reports
- ○ PCI-DSS
    - ■ Payment card industry
        - Security measures for the payment card industry

- Fourth Amendment
    - ○ Government agents may not search or seize things or areas, where a person has a reasonable expectation of privacy without a search warrant.
- Best Evidence Rule
    - ○ Prevent Alteration of digital evidence
    - ○ Duplicate digital evidence is admissible if:
        - ■ Original evidence is destroyed in fire/flood/any act of nature.
        - ■ Original evidence destroyed in the normal course of business.
        - ■ Original evidence in possession of third party such as website.
- SWGDE (scientific Working Group on Digital Evidence)
    - ○ Companies conducting forensic investigations must follow
        - ■ Standards
            - ○ 1.1: Maintain SOP document
            - ○ 1.2: Review SOP annually
            - ○ 1.3: SOP must be accepted
            - ○ 1.4: Written copies of technical procedures
            - ○ 1.5: Appropriate hardware/software
            - ○ 1.6: Record all actives for review and testimony

- Forensic Readiness
    - Optimal use of digital evidence in limited time, with limited investigation costs. Keep coast low
- Incident Response
    - Using Forensics to examine malware, data reaches, vulnerability and how someone got in

- What work does a forensic investigator do?
    - Evaluates damage
    - Identifies/recovers data
    - Extracts evidence in sound manner
    - Proper handling
    - Creates reports from finding.
    - Testifies
    - Stay current with forensic tools
- Ethics
    - Fairness
    - Integrity
    - Conflicts of interest – Not prosecuting someone you know such as a family member

Lesson 1.4: Analyze Photos Lab Part 1
Skills Learned From This Lesson: Hands on lab, Hex Calculator, Hex Editor

- For this portion move to the lab to follow how to set up your home lab
- Review the provided videos and lab documentation to complete the lesson

Lesson 1.5: Analyze Photos Lab Part 2
Skills Learned From This Lesson: Photo Altering, Tools needed

- Adding data and phrases to photos.
- Follow the video and the provided lab documentation to complete the lab.
        - Know what each image extension starts with in Hex.
            - (Ex) .jpeg hex starts with FF D8 FF

- Try to keep the files the same size if you alter the photo

Lesson 1.6: Analyze Photos Lab Part 3
Skills Learned From This Lesson: Photo Review, File size, Hash Calculator

- Review the modified and unmodified photos, are their any visual changes to them.

- Review the files with hash calculator and see if the hashes are different

Module 2: Computer Forensics Investigation Process

Lesson 2.1: Computer Forensics Investigation Process part 1

Skills Learned From This Lesson: Pre investigation, Investigation, Post Investigation

- Pre-Investigation Phase
  - Planning/budget – Initial work to begin the investigation
  - Lab setup/ Design – What equipment is needed for the job
  - Data Destruction – A plan to destroy the evidence when no longer needed
  - Evidence Locker – How many are needed for each piece of evidence
  - Workstations – Choose the correct hardware for the device needing to be analyzed
  - Certifications – Ensure the proper certifications are meet for the job conducted
  - QA – Following the proper chain of custody.
  - Auditing – Plan when Audits are conducted
  - Laws – Understanding the Laws in the area you're working

- Forensic Lab (what it entails)
  - Plan budget
  - Team
  - ISO/IEC 17025
  - Physical: floor to ceiling, walls, logs, secure containers, logs
  - Workstation: 50-63 square feet

- Investigation Phase
  - Consent/Warrant
    - Warrant
      - Electronic Storage Device – Hardware/Software components
      - Service Provider - Account information, Web browser, server internet provider
      - Search Warrant – Written by a judge that directs law enforcement to search for a particular piece of evidence at a particular location
  - Warrants not Needed
    - Warrantless Seizure – destruction of evidence is imminent AND the belief is the item being seized is evidence of criminal activity or from a person with authority consents
  - First Responder

        - Secures the scene when they arrive
        - System Administrator or IT member will be a part of the first responder
        - Non-Forensic staff such as police or paramedics
    - Photography/Document scenes
    - Collect evidence
    - Analyze evidence
- Post-Investigation Phase
    - Social media behavior – Do not inform of what is found during investigation
    - Collecting social media evidence
    - Tools: Facebook Forensic Software, Netlytic, Social Discovery, Navigator

Lesson 2.2: Computer Forensics Investigation Process Part 2
Skills Learned From This Lesson: Best Practice, Exhibit Numbers, Tools

- Best Practices
    - Authorization from decision maker such as a Judge or a Boss giving consent to open the investigation
    - First Response – Someone in IT capacity for forensic investigation
    - Search and Seize – Ensure proper producers in place to gather the evidence
    - Evidence collection- keep standards to follow by laws and regulation or organization
    - Secure - evidence found
    - Copy- create a copy without corrupting the evidence.
    - Acquire/Analyze
    - Report
    - Testify

- Powered off Computers
    - If it's off, leave it off
    - Photograph – the current state of the machine and its surroundings
    - Monitor on: move mouse slightly

- Networked Computers
    - Photograph/Document evidence
    - Unplug network cable from router/modem - purpose is to stop possible continued attack
    - Collect all cords and peripherals connected
    - Document

- Chain of Custody
  - Legal document
  - Demonstrates progression of evidence
  - Should list all people involved in evidence collection/preservation, their actions, and contain a time stamp.
- Exhibit Numbering
  - Aaa/ddmmyy/nnnn/zz
    - Aaa = name of investigator seizing
    - Dd/mm/yy= date of seizure
    - Nnnn=sequential number of exhibits, starting with 001
    - Zz=sequence number for parts of the same exhibit
- Common Data Recovery Tools
  - Recuva
  - Advanced Disk Recovery
  - Undelete Plus
  - The Sleuth kit (TSK) & Autopsy
  - EnCase
  - FTK Imager

Module 3: Computer Forensics Investigation Process

Lesson 3.1: Hard Disks and File Systems Part 1

Skills Learned From This Lesson: Hard Disk, components, Master Boot Record

- Hard Disk Drive (HDD)
  - Uses magnetic storage to store/retrieve data
  - Non-volatile storage
  - Platters
    - Circular metal disks mounted into a drive enclosure
    - 2 heads per platter
    - Can store information on both sides
    - Hard drive has several platters
  - Tracks
    - Concentric ring on platter
    - Stores data
    - Numbering 0-1023

        - Contains sectors (Disk blocks)

    - Sectors
        - Smallest physical storage on hard disk platter
        - 512 bytes long for HDD
        - Newer HDD = 4096 Bytes AF (advanced format)

    - Bad Sectors
        - Portions of disk unusable due to flaws
        - Configuration issues
        - Physical disturbance to disk

    - Master Boot Record (MBR)
        - Starts at sector 0
        - Organization of logical partitions
        - 512 bytes
        - 0xAA55

    - Clusters
        - Smallest accessible logical storage units of HDD
        - Formed by combing sectors

Lesson 3.2: Hard Disks and File Systems Part 2

Skills Learned From This Lesson: Bit, Byte, Nibble

- Bit, Byte, Nibble
    - Bit = binary digit (0,1)
    - Byte = 8 bits
    - Nibble = 4 bits

- Bios Parameter Block ()
    - Describes physical layout of storage volume
    - Volume boot record
    - FAT16, FAT32, NTFS

- GUID
    - Globally Unique Identifier
    - 128 bits
    - Identify Information

- GPT
    - GUID Partition Table
    - Layout of partition table of HDD/SSD
    - Header at LBA 1 (Logical Block Address)
- UEFI
    - Unified Extensible Firmware Interface
    - Defines software interface between OS and firmware
    - Replaces BIOS
    - Supports remote diagnostics/repair
- UEFI Boot Process Phase
    - Security Phase (SEC)
        - Handles platform restart events
        - Creates temporary memory store
        - Serves as root of trust
        - Passes required handoff information to the PEI
    - Pre-EFI Initialization (PEI)
        - Initialize permanent memory complement
        - Describing that memory in Hand-Off Blocks
        - Describing the firmware volume locations
        - Passing control to the Driver Execution Environment (DXE)
    - Driver Execution Environment (DXE)
        - DXE Dispatcher- discover/execute DXE drivers in correct order
        - Drivers-initialize processor, chipset, and platform components
        - Terminated at successful OS boot
    - Boot Device Selections (BDS)
        - Platform boot policy
        - Initializes consoles
        - Loads the device drivers
        - Loads and executes the boot selections
    - RunTime (RT)
        - Enables the OS to read/write the environment variables
        - Supports updates of firmware
        - Clears UEFI from the memory

Lesson 3.3: Hard Disks and File Systems Part 3

Skills Learned From This Lesson: Boot Processes, Windows, Linux, Mac

- Windows
  - Traditional BIOS-MBR = XP, VISTA, Windows 7
  - UEFI-GPT or BIOS-MBR = Windows 8 and later can use either
- Windows Boot Process
  - System switched on, CPU sends signal to motherboard, check for BIOS firmware
  - BIOS starts a POST (Power-on-self-test) and firmware settings from not-volatile memory loaded
  - POST successful/Add-on adapters perform self-test
  - Valid boot system disk detected
  - Firmware scans boot disk and loads MBR
  - MBR triggers Bootmgr.exe that locates the Windows Loader
  - OS kernel (ntoskrnl.exe) is loaded
  - HAL.dll and System Registry Hive loaded into memory
  - Session manager: Winlogon.exe, Service control manager, user session is created
- Mac Boot Process
  - BootROM activated: initializes system hardware
  - POST for interfaces
  - Remaining hardware interface initialized. EFI for intel-based and Open Firmware for PowerPC-based.
  - OS selected
  - Control passed to BootX or boot.efi boot loaders
  - Kernel loaded
  - Launched runs startup items and prepares systems
- Linux Boot Process – BIOS Stage
  - System hardware initialized
  - BIOS retrieves information stored in CMOS and POST test done
  - BIOS Searches for OS
- Linux Boot Process – Bootloader stage
  - Loads the Linux Kernel (bootloaders: LILO and GRUB)
  - Virtual file system named (initial RAMdisk)
  - Actual root file system prepared for deployment
  - Detection of device that contains the filesystem
  - Kernel loaded into memory

- Linux Boot Process - Kernel stage
  - Virtual root filesystem (VFS) executes Linux program
  - Kernel searches for new hardware and loads drivers
  - Root filesystem mounted.
  - Rest of system loaded and users log in.

Lesson 3.4: Hard Disks and File Systems Part 4
Skills Learned From This Lesson: NTFS, FAT16/32

- Windows File System
  - FAT16
    - FAT = File Allocation Table
    - Designed for small disks and simple folder structures
    - Portable device: such as digital cameras, flash drives
    - Files stored at start of volume
  - FAT32
    - 10-15% more effective space utilization
    - Smaller clusters
    - No restriction on entries in root folder
  - NTFS
    - New technology file system
    - $Bitmap file keeps track of used/unused clusters
    - Compression, Auditing, file-level security, metadata
    - Supports RAID
    - Uses MTF for file attributes
    - Journaling
- Linux File Systems
  - EXT
    - First File system for Linux (1992)
    - Extended File System
    - Metadata structured similar to UFS (Unix File System)
  - EXT2
    - Seen in many distros of Linux
    - Superblock stores info about size/shape of Ext2
    - Data stored in blocks of same length

- EXT3
  - Journaling
  - Max single file size: 2TB
- EXT4
  - Max single file size: 16 TB
  - Scale/Reliability
  - Increased performance and reduces fragmentation over Ext2/Ext3

Lesson 3.5: Hard Disks and File Systems Part 5

Skills Learned From This Lesson: Raid Levels, HFS, HFS+

- RAID 0
  - Raid = Redundant Array of Independent/Inexpensive Disks
  - Disk Striping
  - No redundancy
  - Requires two drives
- RAID 1
  - Mirroring
  - Redundancy, if a disk fails the other disk has the information still.
  - Requires 2 drives minimum
- RAID 2
  - Does not use parity, mirroring or striping
  - Splits data at bit level and distributing to multiple disks
- RAID 3
  - Byte- level striping, with dedicated parity disk
  - Disk stores checksums
  - Supports processor for parity code calculation
  - Unable to cater to multiple data requests at the same time
- RAID 5
  - Byte-level data striping
  - Distributes parity information
  - Requires 3 drives minimum
- RAID 1+0 (10)
  - Combines RAID 0 (striping) and RAID 1 (Mirroring)
  - Requires 4 drives minimum

        - Fault tolerance similar to RAID 1
        - If 2 disks in the same mirrored pair fails, data is not available

Lesson 3.6: Hard Disks and File Systems Part 6

Skills Learned From This Lesson: File Carving, Image Files, Sleuth Kit

- File Carving
    - Reconstructing file fragments from deleted files
    - Tools: OSForensics, DataLifter, Simple Carver Suite

- Image Files
    - JPEG/JPG
        - JPEG= Joint photographic experts group
        - Lossy Compression
        - 90% compression
        - Hex value starts with: FF D8 FF
    - BMP
        - Bitmap
        - Windows
        - Hex Value: 42 4D
        - RGBQUAD Array: color table that comprises the array of elements equal to the colors in the bitmap
    - GIF
        - Graphics interchange format
        - 8 bits per pixel
        - 256 colors per frame
        - Supports lossless data compression
        - Hex value: 47 49 46
    - PNG
        - Portable network graphic
        - Lossless image format
        - Intended to replace GIF and TIF (Tagged image file format)
        - Hex Value: 89 50 4E

- Lossy Vs. Lossless
    - Lossless (GIF/PNG): reduces file size without removing data
    - Lossy (JPG): Permanently discards bits of information
    - Tools for Lossless: WinZip, PKZip, Stuffit, FreeZip (not inclusive list)

- The sleuth kit (TSK)Commands

Fsstat	Displays general details about file system
Istat	Displays details of metadata structure
Fls	List file/directory name on disk image
Img_stat	Display details of an image file

Lesson 3.7- 3.9: Recovering Graphics File Lab part 1-3

Skills Learned From This Lesson: Hands on Lab for Recovering Graphics Lab

- Follow the steps in the provided lab documentation and videos to complete the exercise for recovering graphics.

Module 4: Data Acquisition

Lesson 4.1: Data Acquisition Part 1

Skills Learned From This Lesson: Data Acquisition, Live Acquisition, Static Acquisition

- Data Acquisition
    - Extract information and create a copy
    - Present it to a Court of law
    - Types: live and static
- Live Acquisition
    - Collect Volatile data (RAM, Processes, command history, driver information)
        - Plan
        - Establish trusted command shell
        - Transmission/storage method
        - Ensure integrity (hashing)
        - Record data, time, command history
        - Document
        - Report
    - Powered on (locked/sleep mode)
    - Encrypted drive when decrypted (passphrase/password)
- Static Acquisition
    - Non-volatile data (swap files, slack space, USB)
    - Data will still be present if powered off
    - Police seizure
- Media Sanitization

  - NIST SP800-88
  - Forensics investigator wants to Clear/Purge/Destroy

- Data Acquisition Formats
  - RAW
    - Creates simple, sequential, flat files of suspect drive/data set
    - Fast data transfers
    - Ignore minor data read errors on source drive
    - Universal acquisition format for most tools
    - Requires same space as original disk/data set
    - Free tolls may not collect marginal sectors
  - Proprietary
    - Option to compress image files of suspect drive
    - Split image into smaller segments for archive
    - Data integrity checks for each segment
    - Integrate metadata into the image file (date/time/hash)
    - Inability to share images between tools
    - File size limitations
  - AFF
    - Advanced forensics format
    - Produces compressed/uncompressed image files
    - No size limit disk-to-image
    - Metadata
    - Open source

Lesson 4.2: Data Acquisition Part 2

Skills Learned From This Lesson: Data Collection, Disk to image, Disk to Disk

- Data Collection
  - Disk-to-image file
    - Bit-to-bit replication
    - Most common
    - ProDiscover, EnCase, Sleuth Skit, X-Way Forensics
  - Disk-to-disk copy
    - Used for older software/hardware
    - Encase, X-Ways Forensics
  - Logical acquisition

        - Specific files or filetypes
        - Email: collecting only .pst and .ost files
        - RAID: only specific records
        - E-discovery
    - Sparse acquisition
        - Collects fragments of unallocated data

- DD
    - Linux command
    - Dd stands for Data dump
    - Drive doesn't have to be mounted
    - Raw format
    - Target drive needs to be larger than suspect
    - Less user-friendly
    - Data management
- Dcfldd
    - Specify hexadecimal patterns/text for clearing disk space
    - Logs errors
    - Hashing ability: MD5, SHA-1, SHA-256, SHA-512
    - Split data acquisition into segmented volumes with numeric extension
    - Verify acquired data with original disk
- Common Tools
    - DriveSpy
    - ProDiscover Forensics
    - AccessData Ftk Imager
    - SafeBack
    - F-Response
    - DeepSpar

Lesson 4.3-4.4 : Forensics Lab Part 1-2

Skills Learned From This Lesson: Image Analysis

- Follow the steps in the provided lab documentation and vide to perform an image analysis.

Module 5: Anti-Forensics Techniques

Lesson 5.1: Anti-Forensics Techniques Part 1

Skills Learned From This Lesson: Donating Files in Windows, Anti Forensics Goal

- Goal of Anti-Forensics

    - Volume – Put so much data that the investigation take a long time
    - Integrity – corrupt the data so it cannot be used
    - Difficulty - make it hard for investigator to analyze the data
    - Existence - deleting logs and files to hide what they have done

- Windows File Deletion – FAT
    - OS replaces first letter of deleted filename with E5
    - Marked as unused cluster
    - File can be recovered

- Windows File Deletion – NTFS
    - Index field in MFT marked with special code
    - Cluster marked unused

- Windows 98 and earlier
    - File path C:\ Recycled
    - Deleted file named Dxy.ext
    - X = drive
    - Y = sequence number (0-7)
    - Ext = extension
    - First documented deleted on C = Dc0.doc

- Windows 2000,XP
    - File Path C:\ Recycler
    - File details stored in INFO2 file

- Windows 7,8,10
    - File path C:\$Recycle.Bin
    - $Ry.ext
    - Y = sequence number (0-?)
    - Ext = original extension
    - $RO.doc

- INFO 2
    - Hidden file
    - Original file name
    - Data and time of deletion
    - Original file size
    - Drive number

Lesson 5.2: Anti-Forensics Techniques Part 2

Skills Learned From This Lesson: Brute Force, Dictionary, Rule-Based attacks

- Password Cracking
  - Brute Force
    - Every possible combination of words and numbers used
    - Takes longer to accomplish
  - Dictionary
    - Dictionary file loaded in password cracking application
    - Doesn’t work against passphrases
  - Rule – Based
    - Attacker has information about the requirements to crack the password
    - Rule in cracking application
  - Hybrid
    - Dictionary and Brute force combinations
    - Password1,password1
  - Rainbow
    - Table of password hashes
    - Created in advance
    - Rtgen and Winrtgen
    - Salting your password helps keep it from being cracked
- BIOS password reset
  - Manufacture backdoor
  - CmosPwd
  - DaveGrohl (mac OS)
  - Reset CMOS or remove CHMOS battery located on the mother board
- Reset Administrator Password
  - Active@ Password Changer
  - Windows Recovery Bootdisk
  - Windows Password Recovery Lastic
- PDF Password Recovery tools
  - PDF Password Recovery
  - PDF Password Genius
  - SmartKey
  - Tenorshare
- Steganography/Steganalyis
  - Steganography: Storing and hiding a message in a photo or mp3
  - Steganalyis: The processes of discovering the hidden information

- Encrypting File System (EFS)
  - File system level encryption
  - User account password needs to be strong
- Anti-Forensic Countermeasures
  - Keep tools updated
  - Keyloggers
  - Prevent data from becoming overwritten

Module 6: Operating System Forensics

Lesson 6.1: Operating Systems Forensics Part 1

Skills Learned From This Lesson: Collecting Volatile Data, Information, System Time

- Collecting Volatile Information
  - System Time
  - RAM
  - Logged-on-Users
  - Open Files
  - Print Spool Files
- System Time
  - Proprietary software: go to website to collect or google to see how to collect
  - 64-bit FILETIME (Windows OS): 100 nanoseconds intervals since 01/01/1601 at midnight (UTC)
  - System Time format: year, month, day, hour, minute, second, millisecond (UTC)
  - 32-bit UNIX (Windows): seconds since 01/01/1970 at midnight
  - String format: 12/17/2018 6:40 PM
- System Time Commands
  - GetSystemTime
  - GetSystemTimeAdjustment
  - GetTimeFormat
  - NtQuerySystemTIme
  - SetSystemTime
  - SystemRImeToFileTime
  - FileTimeToLocalFileTime
  - GetLocalTime
  - SetLocalTime
- Ram
  - DumpIT – common tool to dump Ram
  - Volatility Framework

- Logged-on Users
    - PsLoggedOn
    - Net sessions
    - LogonSessions
- Open Files
    - Net file: open shared files/files locks
    - PsFile Utility: files opened remotely
    - Openfiles: see open files
- Print Spool Files
    - Spool file (.spl)
    - Graphics file (.emf)
    - File Carving is needed to grab these files

<u>Lesson 6.2</u>: Operating Systems Forensics Part 2

Skills Learned From This Lesson: Non-Volatile Data Collection, SSID, ESE

- Collecting non-Volatile Information
    - Registry
    - Extensible Storage Engine (ESE)
- Windows Registry
    - HKEY_CLASSES_ROOT
        - Ensures correct program opens when executed
        - Drag and drop rules
        - Shortcuts
        - User interface
    - HKEY_CURRENT_USER
        - Configuration info for current logged in user
    - HKEY_LOCAL_MACHINE
        - Hardware specific information
        - Shows Mounted drives
    - HKEY_USERS
        - Configurations of all users
    - HKEY_CURRENT_CONFIG
        - Shows the system configuration
- Other areas of Registry
    - Share Names
        - HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares
    - Time Zones
        - HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation

  - Prefetching
    - HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\MemoryManagement\PrefetchParameters
    - Try to remember the last half of the file directory because they change due to what the user is looking for
- Wireless Service Set Identifier (SSID)
  - Wireless network identified by SSID
  - HKLM\SOFTWARE\Microsoft\WZCSVC\Parameters\Interface
- Common Registry Tools
  - RegRipper
  - ProDiscover
  - RegEdit
  - RegScanner
- Extensible Storage Engine (ESE)
  - Related to Email
  - Files have .edb extension
  - Server: files, messages, texts

Lesson 6.3: Operating Systems Forensics Part 3
Skills Learned From This Lesson: Browser Path, Microsoft Edge, Firefox, Chrome

- Microsoft Edge (understand the path structure)
  - Cached Files
    - \User\user_name\AppData\Local\Packages\Microsoft.MicrosoftEdge_xxxx\AC\#!001\MicrosoftEdge\Cache\
  - Last Active Browsing Session
    - \Users\user_name\AppData\Local\Packages\Microsoft.MicrosoftEdge_xxxx\AC\MicrosoftEdge\user\Default\Recovery\Active\
- Firefox
  - Cache
    - C:\Users\<Username>\AppData\Local\Mozilla\Firefox\Profiles\xxxxxxx.default/cache2
  - History
    - C:\Users\<Username>\AppData\Local\Mozilla\Firefox\Profiles\xxxxxxx.default/places.sqlite
- Chrome Cache
    - C:\Users\{user}\AppData\Local\Google\Chrome\UserData\Default\cache

- Windows Restore Points
  - Rp.log files
  - HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\SystemRestore
  - Retained for 90 days
  - Snapshots
- ELF_LOGFILE_HEADER
  - Used at start of event log to define information about the log
  - Hader size 0X30 – never changes
  - Signature: 0x654c664c (eLfL in ASCII) – never changes
  - Major and minor version numbers:1
- Linux Shell Commands

Command	Meaning
Dmesg	Displays message/driver message
Fsck	File System Consistency Check
Stat	Displays file/file system status
History	Lists Bash shell commands used
Mount	Mounts file system/device to directory

- Common Linux Log Files
  - Authentication: /var/log/auth.log
  - Kernel: /var/log/.kern.log
  - Apache: /var/log/httpd
  - System boot: /var/log/boot.log
- Mac Log Files
  - System Log Folder: /var/log
  - System Application Log: /Library/Logs
  - System Log: /var/log/system.log

Module 7: Network Forensics

Lesson 7.1: Network Forensics

Skills Learned From This Lesson: Postmortem, Real Time, Log Files

- Network Forensics
  - Monitoring/analysis of network traffic to discover the source of attacks or other problems
  - volatile data
- Postmortem Vs. Real-Time

    - Real – time
        - Event is still happening
    - Postmortem
        - After event is done
- Log files as evidence
    - Hearsay Rule (FRE 802)
    - Regular business activity records
    - Trustworthiness is provided by having untampered log files
    - Prove the logs are being collected Before, during, and after
- Event Correlation
    - Codebook based
        - Stores sets of events in codes
    - Rule based
        - Rules are used to correlate different events
    - Automated field correlation
        - Compares some or all of the fields in the data and determines any correlation across the fields
    - Bayesian
        - Uses statistics and probability to predict the next possible steps
    - Time/role based
        - Monitors the user and computer behavior for abnormal activity
- Network Time protocol (NTP)
    - Clock synchronization across all network devices
    - UTC stands for Coordinated universal time
- What devices have logs?
    - Router
    - Firewall
    - IDS
    - Honeypot
    - DHCP
    - ODBC (open database connectivity)
- Log Management Challenges
    - Variety of logs
    - Sources of data are distributed
    - Data sources change constantly

  - Sensitivity of data
  - Format of log data
  - Log fatigue
  - Retention of logs
  - Centralized logging

- Syslog
  - Separation of log generation, log storage, and log analysis
  - Central repository (printers, routers)

Module 8: Web Attack Investigation

Lesson 8.1: Web Attack Investigation Part 1

Skills Learned From This Lesson: Web Application Architecture, Forensics, Challenges

- Web Application Architecture
  - Client
  - Web server
  - Business layer
  - Database layer
- Web Application Forensics
  - Network Traffic (NIDS)
  - OS (HIDS)
  - Browser (Cookies)
  - Server

- Challenges
  - Possibly no logs
  - No IDS/IPS set up
  - Training/ possibly deleting logs or losing them
- Web Attack Indications
  - Incoming Requests (DDOS) More request then normal
  - HTTP request headers (sqlmap, NetSparker)
  - Fingerprints
  - Geography

Lesson 8.2: Web Attack Investigation Part 2

Skills Learned From This Lesson: OWASP TOP 10

- A1:2017 –Injection
  - Can result in data loss or corruption

        - Prevention
            - Use a safe API (avoids interpreter)
            - Whitelist server side input validation
            - Use SQL controls within queries to prevent mass disclosure of records in SQL injection attacks
- A2:2017- Broken Authentication
    - Can result in identity theft and fraud
        - Prevention
            - Multifactor authentication
            - No default credentials
            - Check for weak passwords
            - Follow NIST 800-63 section 5.1.1 for password guidelines
            - Harden against enumeration of accounts
            - Limit failed login attempts
- A3:2017- Sensitive Data Exposure
    - Can lead to identity theft
        - Prevention
            - Classify data being process, stored, and transmitted
            - Apply appropriate controls
            - Encrypt all data at rest and in transit
- A4:2017- XML External Entities (XXE)
    - Weaknesses in XML processors
    - Can lead to data extraction, DoS, internal system scan
        - Prevention
            - Use less complex data formats like JSON
            - Patch/upgrade all XML processors and libraries
            - Disable XML external entity processing in XML documents and headers
- A5:2017- Broken Access Control
    - Can cause administrator privilege for attacker and users accessing/deleting records
        - Prevention
            - Deny by default
            - Disable web server directory listing
            - Log access control failures
- A6:2017- Security Misconfiguration

- Can lead to remote code execution on victim's browser, stealing of credentials, and delivery of malware to the victim
  - Prevention
    - Separating untrusted data from active browser content
    - Escaping untrusted HTTP request data
    - Enabling content security policy (CSP)

Lesson 8.3: Web Attack Investigation Part 3

Skills Learned From This Lesson: OWASP Top 10 Continued, Risks

- A8:2017- Insecure Deserialization
  - Can lead to remote code execution
    - Prevention
      - Implement integrity checks, like digital signatures
      - Code isolation – do not run as root or Admin
      - Logging deserialization exceptions and failures
- A9:2017- Using Components with known Vulnerabilities
  - Can lead to massive data breaches
    - Prevention
      - Patching
      - Only obtain from official sources
      - Continuous inventory of client and server-side frameworks and libraries
- A10:2017- Insufficient Logging & Monitoring
  - Can lead to successful exploits attacks
    - Prevention
      - Ensure all login and access control failures are logged with sufficient context
      - Ensure all logs are generated in a easily consumed format/ Log any failures
      - Establish effective monitoring and alerts
- Other Risks
  - Information leakage
  - Directory traversal
  - Form/Log tampering
  - CSRF = Cross site request forgery

- After an Attack
  - Grab Date/time
  - Gather IP Address's if possible
  - HTTP method used (GET, POST)
  - HTTP Header and body
  - Event logs
- Commands that can be used
  - Net view 192.168.xx.xx
  - Net session
  - Net use
  - Nbtstat –S
  - Netstat –ano
  - Schtasks.exe
  - Net start
- Deep Log Analyzer Tool
  - Web analytic tool
  - Used for Small/medium websites/businesses

- Error Logs Path
  - Red Hat / Fedora: /var/log/httpd/error_log
  - Ubuntu/ Debian: /var/log/apache2/error.log
  - FreeBSD: /var/log/httpd-error.log

Module 9: Database Forensics

Lesson 9.1: Database Forensics

Skills Learned From This Lesson: SQL Server, Forensics, Location of Evidence

- Microsoft SQL Server (MS SQL)
  - Relation DBMS
  - Transact SQL (T-SQL)
  - SQL Server Native Client (SNAC)
  - SQL Common Language Runtime (CLR)
- MS SQL Forensics
  - Data and logs are stored in 3 different files
    - Primary data file
      - Starting point of the database
      - Points to other files in database
      - .MDF extension

      - Stores all data in database objects (tables, indexes)
    - Secondary data file
      - Optional
      - Database can contain multiple
      - .NDF extension
    - Transaction log data file
      - Holds entire log information associated with database
      - .LDF
- Collect of Database (.mdf) and Log files (.ldf) file path
  - C:\Program Files\Microsoft SQL Server\ MSSQL11.MSSQLSERVER\MSSQL\DATA
- Location of Files for Restoration of Evidence
  - Database and log files: \MSSQL\DATA
  - Trace files: \MSSQL\LOG
  - SQL Server error logs: MSSQL\LOG\ERRORLOG
- Commands
  - Sqlcmd = system procedures
  - Mysqldump = backup of database
  - Mysqldbexport = exports metadata
  - Myisamlog =version info, recovery operations
  - Myisamchk= status of MyISAM table
- SQL Server Plan Cache
  - Stores details on all of the SQL statements that have been executed even if deleted
- SQL Server Trace File Collection
  - Events that occurred on SQL server and the host database
    - C:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\LOG

Module 10: Database Forensics

Lesson 10.1: Forensics with the Cloud Part 1

Skills Learned From This Lesson: Cloud Computing, PaaS, SaaS

- The Cloud
  - Elasticity – able to scale up or down for the size of storage
  - Reliability
  - Cost effective
  - NIST SP800-145

  - Security
  - Compliance
- Types of Cloud Computing
  - Infrastructure as a Service (IaaS)
    - Data storage
    - Virtualization
    - Network
    - Computing Power
    - Scalability
  - Platform as a Service (PaaS)
    - Development
    - Provider provides: OS, storage, middleware
    - scalability
  - Software as a Service (Saas)
    - On-demand application such a Netflix
    - Google Docs
    - Patching – Do not have to manage
    - Version control
    - Compatibility
- Cloud Models
  - Public
    - The service is provided for public use
    - Examples are Gmail, Yahoo mail
  - Private
    - Single tenant environment
    - Usernames/Passwords are needed
    - Security/compliance- allows to control the security needed for use
  - Community
    - Shared by organizations with similar interest
    - Compliance
    - policy
  - Hybrid
    - Combination of public, private, and community clouds
- Cloud Computing Threats
  - Data breach/loss

    - Use of cloud to perpetrate attacks
    - Insecure API’s and interfaces
    - Shared technology issues
    - Insider threats
    - Privilege escalation
- Possible Cloud Attacks
    - Session hijacking
    - Session riding (CSRF)
    - SQL injection
    - DNS attacks
    - Wrapping (SOAP)
    - Side channel
    - DDoS

<u>Lesson 10.2</u>: Forensics with the Cloud Part 2

Skills Learned From This Lesson: Cloud Crimes, Tools, Forensic Challenges

- Cloud crimes
    - Cloud as a Subject
        - Attackers try to compromise security of the cloud environment
            - Steal data
            - Inject malware
            - Delete data
    - Cloud as an Object
        - Attackers use the cloud to commit a crime against the cloud service provider
            - DdoS
    - Cloud as a Tool
        - Attacker uses compromised account to attack other accounts
    - Cloud Forensic Challenges
        - Unable to collect all the logs
        - Large scales data processing
        - IoT (mobile devices, CCT Cameras)
        - Legal –Jurisdiction problems, country Laws
    - Service Level Agreements (SLAs)
        - Restriction on customer by CSP
        - Availability
        - Support

        - Security measures
    - Dropbox Paths
        - Filecache.dbx = stores info on shared directories and file transfers
        - Dropbox prefetch
            - C:\Windows\Prefetch\DROPBOX.EXE
            - C:\Users\username\Dropbox
            - C:\Users\username\AppData\Roaming\Dropbox
    - Google Drive Paths
        - Registry Keys
            - SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folder
            - SOFTWARE\GoogleDrive
            - NTUSER\Software\Microsoft\Windows\CurrentVersion\Run\GoogleDr
            - NTUSER\Software\classes
            - C:\Users\username\AppData\Local\Google\Drive=sync_config.db
            - C:\Users\username\AppData\Local\Google\Drive=snapshot database
            - Snapshot.db=each file accessed, URL path, created/modified, MD5
            - Sync_log.log=user's cloud transaction

Module 11: Malware

Lesson 11.1: Malware Part 1

Skills Learned From This Lesson: Malware Types, Viruses, Worms

- Types of Malware
    - Viruses
        - They Self-replicate
        - Needs a host to work
        - Usually works with User interaction
        - Corrupt/Modify files
    - Worms
        - Self-replicating
        - Self-propagating – continues sending information on the network
        - Consumer bandwidth
    - Trojans
        - Appears to be benign

        - No propagation – needs user interaction
    - Keylogger
        - Records Keystrokes
    - Rootkit
        - Works by maintain access
        - Works on the kernel level
        - Firmware rootkit, to get rid of it you need to replace hardware
    - Ransomeware
        - Works by encrypting files
        - Requires ransom payment to decrypt, but attackers wont after payment
        - A form of Trojan
        - WannaCry Worm
- How does malware enter?
    - Spam/Phishing emails
    - USB
    - Third-party software
    - File sharing
    - Wireless/Bluetooth
    - Compromised websites (malvertising, water-hole)

Lesson 11.2: Malware Part 2

Skills Learned From This Lesson: Malware Components, Exploit, Injector

- Components of malware
    - Crypter
        - Used to conceal existence of malware through encryption, manipulation, and obfuscation
    - Downloader
        - Trojan
        - Internet connection
        - Downloads additional malware
    - Dropper
        - Installs malware on target system
        - Installs it covertly
    - Exploit
        - Code that takes advantage of a vulnerability

    - Injector
        - Injects malicious code into running processes
        - Obfuscates
    - Obfuscator
        - Conceals malicious code
    - Packer
        - Compresses malware files
        - Unreadable format until the file is unpacked
    - Payload
        - Performs desired activity

Lesson 11.3: Malware Part 3

Skills Learned From This Lesson: Static, Dynamic Malware Analysis

- Basic Static Malware Analysis
    - Code not executed, just looking at
    - Scan with tools (Malwarebytes, Sophos, TrendMicro)
    - Collect Hash for fingerprint to see if it’s been used before
    - Search strings (connect to URL, copies file to specific location)
    - Few strings can indicate malicious (packed)
- Malware Analysis string examples
    - C:>strings bp6.ex_
    - VP3
    - VW3
    - T$@
    - D$4
    - 192.168.0.1
    - GetLayout
    - GDI32.DLL
    - SetLayout
    - Mail system DLL is invalid. ISEND Mail failed to send message
- Portable Executable (PE) File Format
    - Header
        - Code information
        - Application type
        - Library function that will be used
        - Space requirements

- File Formats
  - .text = contains instruction that CPU executes
  - .rdata = contains import/export information
  - .data = contains global data
  - .rsrc = contains resources used (images, icons, menus)

- Linking Libraries
  - Runtime linking = only when function needed
  - Static linking = all library code copied into executable
  - Dynamic linking = when program is loaded, most common method
  - Dependency walker tool lists dynamically linked functions

- Basic Static Malware Analysis
  - Software\Microsoft\Windows\CurrentVersion\Run
  - Controls which programs are ran at startup
  - Registry string commonly used by malware
- Basic Dynamic Malware Analysis
  - Execute malware
  - Virtual machine
  - May not execute
  - Process Monitor used for PDF
  - Dependency walker
  - Regshot
  - Netcat
  - Wireshark

Module 12: Email Investigation

Lesson 12.1: Email Investigation Part 1

Skills Learned From This Lesson: Crimes, CAN-Spam Act, Electronic Record Management

- Email Crimes
  - Spamming
    - Unsolicited
    - Much of email traffic is made up of this
    - CAN-SPAM Act – covers commercial email
  - Phishing
    - Social engineering
    - Try's to collect Sensitive information

- Mail Bomb
  - Large volume of emails
  - Overflow
  - Overwhelm
- Spoofing
  - Forging email header
  - Phishing/Spam
- Identify Fraud
  - Someone else's identity used
  - Crime
  - Defraud
  - Without identity theft
- Chain Letter
  - Hoaxes, try to defraud
  - Urban legends: meant to waste time

- Electronic Records Management
  - Legal mandates on protection
  - Prevent Unauthorized accesses
  - Data manipulation
  - Reduces retrieval costs
  - Reduces paper records burden
  - Data on demand

Lesson 12.2: Email Investigation Part 2

Skills Learned From This Lesson: Laws, Email Investigation, Microsoft Exchange Logs

- Other Laws
  - Electronic communications Privacy Act (ECPA)
  - Stored Communication Act (SCA)
  - State
- Email investigation
  - Search Warrant needed to view email
  - Copy (bit by bit)
  - Print
  - View/Analyze email header
  - Trace
  - Investigate types of encoding

  - Acquire email archives
- Web-based Email
  - Search browser cache
  - Tools
- Microsoft Exchange Email Server Logs
  - Extensible Storage Engine (ESE)
  - PRIV.EDB
  - PUB.EDB
  - PRIV.STM
  - Tracking.log
- Exchange Database File
  - PRIV.EDB = RTF that contains message headers, message text, standard attachments
  - PUB.EDB = public folder hierarchies and contents
  - PRIV.STM = s streaming internet content file (MIME, video, audio)

- Email Recovery Tool
  - ProDiscover Basic
  - OSForensics
  - DataNumen (Outlook, Express)
  - Paraben E-Mail Examiner
  - AccessData FTK
  - Fookes Aid4Mail (Outlook, Thunderbird, Eudora)

Module 13: Mobile

Lesson 13.1: Mobile Part 1

Skills Learned From This Lesson: Mobile Investigation, Investigation Team, Workstation

- Mobile Forensics
  - Extraction, Recovery, Analysis
  - Internal Memory
  - SD card
  - SIM card
  - NIST SP800-101
  - Internal phone memory = RAM, ROM, flash memory
  - SIM card = address book, messages, service-related information
  - External memory = SD card, mini SD card, Micro SD, audio/video/image
- Steps Before a Mobile Forensic Investigation

    - Build forensic workstation
    - Build investigation team
    - Review policies/laws
    - Notify decision makers/acquire authorization
    - Risk assessment
    - Build mobile forensics toolkit
- Build Forensics Workstation
    - Laptop
    - Desktop
    - USB connector
    - FireWire
    - Mobile forensics toolkit
    - Cables
    - Sim card reader
    - Micro –SD memory card reader
- Build Investigation Team
    - Expert witness
    - Evidence manager
    - Evidence documenter
    - Investigator
    - Attorney
    - Photographer
    - Incident responder
    - Decision maker
    - Incident analyzer
- Review Policies/Laws
    - Federal
    - State
    - Local
    - Policies
- Notify Decision Makers
    - Decision makers implement policies and procedures
    - No policy
- Risk Assessment
    - Mobile data

  - Priorities
- Build Mobile Forensics Toolkit
  - Depends on mobile device
  - Hardware/Software tools

Lesson 13.2: Mobile Part 2

Skills Learned From This Lesson: Legal, API's, Mobile Threats

- Legal
  - Riley Vs. California
  - Search warrant required before anything is done on a mobile device
  - Redacted from public record any sensitive data found on mobile device
- Mobile Device Threats
  - Malware (Spayware)
  - Social Engineering (Smishing)
  - Data loss
  - Web or network attacks
- APIs
  - Communication
    - Simplifies the process of interacting with web services, email, SMS
  - GUI
    - Creates menus and submenus in designing applications
    - Interface for developer to build other plugins
  - Phone
    - Application Layer
    - Making calls
    - Receiving calls
    - SMS
- Subscriber Identity Module (SIM)
  - Contacts
  - Messages
  - Time stamps
  - ICCID (Integrated Circuit Card ID)
  - Last dialed numbers
  - IMSI (International Mobile Subscriber Identity)
  - Service provider name
- Other Cellular Components

    - Mobile switching center (MSC) – Processes calls and messages through landlines
    - Base transceiver station (BTS) – Allows Wireless connection between the phone and network
    - Base station controller (BSC) – Manages the transceiver equipment
    - Base station subsystem (BSS) – Controls the BSC, Handles traffic
    - Home location Register (HLR) – Database for subscriber data
    - Visitor location register (VLR) – Database for roaming mobile phone out of network

Lesson 13.3: Mobile Part 3

Skills Learned From This Lesson: ESN, IMEI, ICCID

- IMEI
    - International Mobile Equipment Identifier
    - 15 digit unique number
    - Obtained with *#06#
        - AA BBBBBB CCCCC D
        - AA = reporting body ID that allocated TAC (Type Allocation Code)
        - BBBBB = remainder of the TAC
        - CCCCCC = serial sequence of the model
        - D = Luhn algorithm check digit of entire modle
- ESN
    - Electronic Serial Number
    - 32 bit unique number
    - Attached on a chip inside CDMA by the manufacture
    - 8 bits manufacturer code and 24 bits serial number
    - 14 bits manufacture code and 18 bits serial
- ICCID
    - Integrated Circuit Card Identifier
    - Identifies SIM internationally
        - 89 44 245252 001451548
        - 89 = industry identifier
        - 44 = country
        - 245252 = issuer ID
        - 001451548 = individual account ID
- IMSI

- International mobile subscriber identity
- 15 digit ID
- Describes country and mobile network subscriber belongs to

- MSIN
    - Mobile subscriber identification number
    - 10 digit number
    - Identifies mobile phone service provider within a network

Lesson 13.4: Mobile Part 4

Skills Learned From This Lesson: Android Libraries, Boot Process, Root

- Android Libraries
    - Media framework = record/playback
    - SQLite = stores data
    - OpenGL/E5 and SGL = used to render 2D (SGL) and 3D (OpenGL/ES) graphics
    - FreeType = renders bitmap and vector fonts
    - Webkit = displays web pages
    - Libc = C system library
    - Core Java = provides Java functionalities
- Android Boot Process
    - Boot ROM activated and Boot Load is loaded into RAM
    - Boot loader initializes and stars the kernel
    - Kernel initializes interrupt controllers, caches, memory, protection, and scheduling
    - Init process launches
    - Zygote spins up new VMs for each app stated
    - System servers
- Breaking Android
    - Android Debug Bridge (ADB) = used to bypass Android phone lock
        - Root the device
            - OnceClickRoot
            - Kingo Android Root
            - Towelroot
            - RescuRoot

Lesson 13.5: Mobile Part 5

Skills Learned From This Lesson: IOS Boot Process, Rooting, Passcode Bypass

- IOS Architecture
    - Core OS layer
    - Core service layer
    - Media layer
    - Cocoa Touch
- IOS Boot Process
    - Normal Boot Sequence
        - BootROM
        - LLB
        - iBoot
        - Kernel & NAND Flash
    - DFU Mode
        - Device Firmware Upgrade
        - Allows device to be restored from any state
            - BootROM
            - iBSS
            - iBEC
            - Kernel & RamDisk
- Disk Image of iPhone with SSH
    - Jailbroken
    - Image Whole disk (dd)
- Bypass iPhone Passcode
    - Use IExploer
- IOS Rooting tools
    - Pangu Jail Break
    - Redsn0W
    - Sn0wbreeze
    - GeekSn0W
- SIM Cloning
    - MOBILEDIT = logical acquisition
    - Oxygen Forensic Suite = physical acquisition and file system acquisition
- Cellular Network Components
    - Code Division Multiple Access (CDMA)
    - Enhanced Data Rates for GSM Evolution (EDGE)
    - Integrated Digital Enhanced Network (iDEN)

    - General Packet Radio Service (GPRS)
    - Global System for Mobile Communication (GSM)
    - Time Division Multiple Access (TDMA)

Module 14: Forensic Reporting

Lesson 14.1: Forensic Reporting

Skills Learned From This Lesson: Report Types, Witnesses, Standards

- Forensic Reports
    - Communicate results of investigation
    - “First testimony”
    - Verbal (Informal)
    - Written (Formal)
- Verbal Report
    - Informal (Preliminary)
    - Attorney Office
    - Formal: board, jury, managers
        - Addresses investigation areas not yet complete
            - Test being run
            - Deposition
            - Document Production (Subpoenas)
- Written Report
    - Formal
    - Affidavit/declaration (under oath)
    - Informal: discovery, destruction of evidence (spoliation is the legal term)
- Report Structure
    - Summary (Abstract)
    - Table of contents
    - Body of the report
    - Conclusion
    - Reference
    - Glossary
    - Acknowledgments
    - Appendixes
- Expert Witness (opined based)
    - Education
    - Knowledge

    - Skills/experience
    - CV
    - Opinions
- Technical Witness
    - Facts found during investigation
    - No conclusion/options
- Daubert Standard
    - Expert witness testimony admissibility
    - Relevant
    - Reliable
    - Dauber Vs. Merrell Dow Pharmaceuticals, Inc
    - Sufficient facts/data
    - Reliable principles/methods
    - Expert witness has applied these
- Frye Standard
    - Admissibility of scientific examination/experiments
    - Well-recognized scientific principle/discovery
    - Gained acceptance in the field
- Direct Vs. Cross-Examination
    - Direct vs Cross-Examination
    - Cross = opposing side
- Deposition
    - Both attorneys are present
    - Jury/Judge not normally present
    - Opposing counsel asks questions

Module 15: Course Summary

Lesson 15.1: Course Summary

Skills Learned From This Lesson: Overview of Course Summary

- Course Modules
    - Module 1: Computer Forensics Today
    - Module 2: Forensic Process
    - Module 3: Hard Disks and File Systems
    - Module 4: Data Acquisition
    - Module 5: Anti Forensics
    - Module 6: Operating System Forensics

- ○ Module 7: Network Forensics
- ○ Module 8: Web Attack Investigation
- ○ Module 9: Database Forensics
- ○ Module 10: Cloud Forensics
- ○ Module 11: Malware
- ○ Module 12: Email Investigations
- ○ Module 13: Mobile Forensics
- ○ Module 14: Forensics Reporting