Computer Hacking and Forensics Glossary

Created by Paul Marlow Teaching Assistant

1. **Computer/Digital Forensics -** a set of procedures and techniques that help an investigator identify, gather, preserve, extract, interpret, document and preserve evidence from computers in a way that is legally admissible.
2. **Locard's exchange principle** - holds that the perpetrator of a crime will bring something into the crime scene and leave with something from it, and that both can be used as forensic evidence.
3. **Computer Fraud and Abuse Act -** law passed in 1986 which prohibits intentionally accessing a **computer** without authorization or in excess of authorization, but fails to define what "without authorization" means.
4. **Phishing -** the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.
5. **Malware/Ransomware -** software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.
6. **Identity Theft -** the fraudulent practice of using another person's name and personal information in order to obtain credit, loans, etc.
7. **Financial Fraud -**an intentional act of deception involving financial transactions for the purpose of personal gain. Fraud is a crime, and is also a civil law violation.
8. **Cyberterrorism -** the politically motivated use of computers and information technology to cause severe disruption or widespread fear in society.
9. **Cyberextortion -** is a form of online crime which occurs when a person uses the Internet to demand money or other goods or behavior (such as sex), from

another person by threatening to inflict harm to his person, his reputation, or his property.

10. **Cyberwarfare** -the use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes
11. **Cyberbullying -**the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature.
12. **Drug trafficking -** is a global illicit trade involving the cultivation, manufacture, distribution and sale of substances which are subject to drug prohibition laws.
13. **Challenges for Investigators**
14. **Encryption -**the process of converting information or data into a code, especially to prevent unauthorized access.
15. **Steganography** - hiding something inside of another thing
16. **Data Wiping/Anti-forensics -** deleting data to hide or obscure an illegal act
17. **Legal Challenges -** a formal questioning of the legality of a person, act or thing.
18. **Investigative Process**
    - **Assess -** what evidence do we need?
    - **Acquire -** Make a copy of any evidence
    - **Analyse -** Carry out a full analysis of the evidence
    - **Report-** generate a report for legal proceedings
19. **Criminal Investigations -** occur after a law has been violated
    - Generally carry either a fine and/or jail time
    - Standard Forensic Process
    - Formal Investigation Report Required
    - Standard of Proof is high
    - Burden of proof is on prosecution

20. Civil Investigations - occurs after a dispute between two parties

Monetary damages

Preponderance (>50%) of truth

21. Administrative Investigations

Internal Investigations - usually occurs after a policy is violated

May turn into a criminal investigation

22. Chain of custody - who touched the evidence and the reasons why

23. ETI - Enterprise Theory of Investigation

It's a holistic approach to criminal or civil investigations
Dismantles gangs or organised crime

24. Volatile Evidence - evidence we want to collect before we shut a machine down:

System time
Process Information
Open files
Network Information
Process Memory
Clipboard
Service/Driver information
Command History

25. Non-volatile evidence - evidence which will hang around for a short time after the machine is shut down:

Slack space
Hidden files
Swap files
Unallocated clusters
Unused Partitions
Registry Settings
Event Logs

26. Federal rules of evidence:

Rule 101: governs proceedings in courts of the US
Rule 103: rulings on evidence
Rule 105: limited admissibility
Rule 502 Attorney Client Privilege
Rules 801-804: Hearsay
Rule 1002: requirement of original evidence
Rule 1003: admissibility of duplicate evidence
Rule 1004: admissibility of other evidence of content

27. Best Evidence Rule -

Prevents alteration of digital evidence

Duplicate admissible if:
Original evidence is destroyed in a fire/flood
Original evidence is destroyed in the normal course of business
Original evidence in possession of a third party

28. Forensic Readiness - Optimal use of digital evidence in limited time with limited investigation costs
29. Incident Response - using forensic to examine malware data breaches etc.
30. Forensic Investigator
- Evaluates
- Damage
- Extract evidence in sound manner
- Proper handling
- Creates reports
- Testifies
- Stays current

31. Ethics
- Fairness
- Integrity
- Conflicts of interest

32.Hash Calc - tool for analysing photos
33. Hexadecimal editor - useful for decoding image files
34. Visual differences - visual analysis
35. File size - physical analysis
36. Hashes - is generating a value or values from a string of text using a mathematical function.
37. ISO/IEC 17025 - Physical floor to ceiling walls logs secure containers
38, Warrants -
Electronic storage device - hardware and software
Service provider - browsing history etc.
39. Search Warrant - written by a judge that directs law enforcement to search for a particular piece of evidence at a particular location.
40. Warrantless seizure
- Destruction of evidence is imminent and the belief is the item being seized is evidence of criminal activity
- Person with authority consents

41. Post Investigation phase
- Social media behaviour
- Collecting social media evidence
- Tools: Facebook Forensic software, netlytic, social discovery, navigator etc.

42. Chain of custody

Legal document
Demonstrates progression of evidence
Should list all people involved in evidence collection/preservation and their actions and contains a timestamp

43. Exhibit numbering

aaa/ddmmyy/nnnn/zz
aaa= name of investigator seizing
Ddmmyy = date of seizure
nnnn=sequential number of exhibits starting with 0001
Zz = sequence number for parts of the same exhibit

44. Data Recovery Tools

Recuva
Advanced Disk Recovery
Undelete Plus
The Sleuth Klt (TSK & Autopsy)
EnCase
FTK

45. SSD - Solid State Drive

Higher data transfer rate
Area storage density
Reliability
NAND-based flash memory (non-volatile)
Higher cost

46. Hard Disk Interfaces

SATA - Serial AT attachment
PATA - Parallel AT attachment
SCSI - small computer system interface

47. HDD - Hard Disk Drive

Uses magnetic storage to store/retrieve data
Non-volatile storage

48. Platters - circulator metal disks mounted into a drive enclosure - 2 heads per platter = stores information on both sides - hard drives have several platters

49. Tracks - Concentric ring on platter - stores data - numbering 0-1023, contains sectors (disk blocks)

50. Sectors - smallest physical storage on hard disk platter- 512 bytes long for HDD- newer HDDs =4096 byte AF (Advanced Format)
51. Bad sectors - portions of disk unusable due to flaws, configuration issues or physical disturbances to disk
52. MBR - Master Boot Record - Starts at sector 0, Organisation of logical partitions, 512 bytes, 0xAA55 - signature
53. Clusters - smallest accessible logical storage units on HDD - formed by combining sectors
54. Slack space - wasted area of disk cluster - between end of file and end of cluster - small files
55. Bit - binary digits (0,1)
56. Byte = 8 bits
57. Nibble = 4 bits
58. BIOS Parameter Block (BPB)- Describes the physical layout of storage volume
    Volume boot record
    FAT16, FAT 32, NTFS
59. GUID - Globally Unique Identifier - 128 bits - identifies information
60. GPT - GUID Partition Table
Layout of partition table
HDD, SSD
Header at LBA 1 (Logical Block Address)
61. UEFI = Unified Extensible Firmware Interface
    Defines software interface between Operating System and firmware
    Replaces BIOS
    Supports remote diagnostics /repair
62. UEFI Boot Process Phases
63. SEC - security phase - handles platform restart events - creates temporary memory store -serves a root of trust - passes required handoff information to the PEI
64. PEI - Pre-EFI Initialization Phase - initializes permanent memory complement - describes the memory in hand-off blocks - described the firmware volume locations - [asses control to the driver execution environment
65. DXE - Driver Execution Environment - DXE dispatcher - discover/execute DXE drivers in correct order - drivers initialize processors chipset and platform components - terminated at successful OS boot
66. BDS - Boot Device Selection - platform boot policy - initialises consoles - loads device drivers - load/execute boot selections

67. RT - Run Time - Enables OS to read/write environment variables - supports updates of firmware - clears UEFI from memory

68. Windows Boot Process -

System switched on - CPU sends signal to motherboard, checks for BIOS firmware
BIOS starts a POST (Power On Self Test) and firmware settings from non-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 Windows loader
Operating System Kernel (ntoskrnl.exe) loaded
HAL.dll and system registry HIve loaded into memory
Session Manager Winlogon.exe Service control manager, users session created

69. Mac Boot Process

BootROM activated initializes system hardware
POST for interfaces
Remaining hardware interfaces initialized. EFI for intel-based and Open Firmware for PowerOC based.
OS selected
Control passed to BootX or boot.efi boot loaders
Kernel loaded
Launched runs startup items and prepares system

70. Linux Boot Process - BIOS Stage

System hardware initialized
BIOS retrieves information stored in CMOS and POST test done,
BIOS searches for the OS
Linux Boot Process - Bootloader Stage
Loads the Linux Kernel (bootloader LILO and GRUB)
Virtual file system named initrd (initial RAMdisk)
Actual root filesystem prepared for deployment
Detection of device that contains the filesystem
Kernel loaded into memory

71. Linux Boot Process - Kernel Stage

Virtual root filesystem (VFS) executes Linuxrc program
Kernel searches for new hardware and loads drivers

Root filesystem mounted
Rest of system loaded and user logs in

72. Windows file systems

FAT16 - File allocation table - designed for small disks and simple folder structures
Portable devices digital cameras, flash drives etc,
Files stored at the start of volume
FAT32-10-15% more effective space utilization
Smaller clusters
No restriction on entries in the root folder
NTFS - New Technology File System -
$Bitmap file keeps track of used/unused clusters
Compression, auditing, file-level security,, metadata
Supports RAID
Uses MFT for file attributes

73. RAID - redundant array of independent/Inexpensive Disks

RAID 0 - Disk Striping - No redundancy- requires 2 drives
RAID 1 - Offers Mirroring, redundancy and requires 2 drives minimum
RAID 2 - does not use parity, mirroring or striping- splits data at the bit level and distributes to multiple disks
RAID 3 - Uses byte - level striping with dedicated parity disks - 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 10 - or RAID 1+0 - 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 fail data not available.

74. Linux file systems

Ext - Extended File System
Ext2 - seen in may distros of Linux - superblock stores info about suze/shape of Ext2- Data stored in blocks of the same length
Ext3 - Offers Journaling - max single file size: 4TB
Ext4 - Max single file size = 16TB, Scale/Reliability, Increased performance and reduced fragmentation over Ext2 /Ext3

Metadata is similar to UFS - Unix File System

75. HFS vs HFS+ (Mac OS)

HFS - Hierarchical File System

HFS- 16- bit allocation blocks

HFS+ - uses B-tree

File Carving - reconstruction file fragments from deleted files - tools include OSForensics, DataLifter and Simple Carver Suite

76. Image files

JPEG / JPG - 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 an array of elements equal to the colours in the bitmap

GIF - Graphics Interchange Format - 8bits per pixel - 256 colours per frame - 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

77. 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

78. Data Acquisition - Extract information and create a copy - court of law - types live and static

79. Live Acquisition -

Volatile data (RAM etc.) - Powered on (locked/sleep mode) encrypted drive (passphrase/password)

80. Static Acquisition - Non volatile data (swap file, slack space USB etc.)

Powered off

Police seizure

81. Media Sanitization - NIST SP800-88

Clear/Purge/Destroy

82. Data Acquisition Formats -

RAW -

Creates simple sequential flat files of suspect drive/data sets

Fast data transfers

Ignore minor data read error on source drives

Universal acquisition format for most tools
Requires the same space as the original disk/data set
Free tools may not collect marginal sectors

Proprietary -

Option to compress image files of suspect drive
Splits the image into smaller segments for archive
Data Integrity checks for each segment
Integrates metadata into the image file (date/time.hash)
Inability to share image between tools
File size limitations

AFF -

Advanced Forensic Format
Produces compressed/uncompressed image files
No size limit disk to image
Metadata incorporated
Open source

83. Data Collection

Disk to image file - but to but replication Most common - ProDiscover EnCase Sleuth Kitm X-Way Forensics

Disk to disk copies - older software/hardware encase x-ways forensics

Logical acquisition - specific files or file types

Email collecting only .pst and .ost files
RAID only specific record

84. Sparse Acquisition - collects fragments of unallocated data

85. Anti-Forensics -

Goal of anti-forensics - Volume Integrity Difficulty Existence

86. Windows File Deletion - FAT

OS replaces first letter of deleted filename with E5
Marked as unused clusters
File can be recovered until the cluster is overwritten

87. Windows File Deletion - NTFS

Index field in MFT marked with special code
Clusters marked unused

88. Windows 98 and earlier

File Path for deleted files C:\ Recycled
Deleted files named Dxy.ext
Where x = drive, y = sequence number (0-?) ext = extension

89. Windows 2000 & XP

File Path for deleted files C:\ Recycler
File details stored in INFO2 file

90. Windows 7,8 & 10

File Path for deleted files C:\$Recycle.Bin
$Ry.ext
Y = sequence number (0-?)
Ext = original extension

91. INFO2- Hidden file contains Original file name - date and time of deletion, the original file size and drive number

92. Password Cracking

93. Brute Force - Every possible combination - takes longer

94. Dictionary - Dictionary file loaded into a password cracking application - doesn't work against passphrases

95. Rule -Based - Attacker has information about the requirements - reduced the amount of time required to crack a password

96. Hybrid - combination of two of the above eg. dictionary and brute force

97. Rainbow -Table of password hashes - created in advance rtgen and winrtgen and salting

98. BIOS password reset

Manufacturer backdoor
CmosPwd
DaveGrohl technique(Mac OS)
Reset CMOS or remove CMOS battery (on motherboard)

99. Reset Administrator Password

Active@PasswordChanger
Windows Recovery Bootdisk
Windows Password Recovery Lastic

100. Steganography: Hiding a message

101. Steganalysis Process of discovering the hidden information

102. Encrypting File System (EFS) - File level encryption - user account password needs to be strong

103. Anti-Forensics Countermeasures

Keep tools updated
Keyloggers
Prevent data from being overwritten

104. Network Forensics - Monitoring/analysis of network traffic to discover the source of attacks or other problems - Volatile
105.Real Time event - is still happening
106. Postmortem - after the event
107. Log files as evidence
Hearsay Rule (FRE 803)
Regular business activity records
Trustworthiness
Before during and after
108.Codebook based - stores sets of events in codes
109. Rule based - rules are used to correlate events
110. Automated Field Correlation - comparison of some or all of the fields in the data and determines any correlation across the fields
111. Bayesian - uses statistics and probability to predict next steps
112. Time/role based - monitors the user and computer behaviour for abnormal activity
113. NTP = Network Time Protocol
114. UTC - CoOrdinated Universal Time
115. 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 - centralized logging -
116. Syslog - central repository for the logs
117. Buffer Overflow attack - an attack that writes malicious code to adjacent memory locations which an attacker exploits.
118. Web Application Architecture
119. Client - a terminal computer with a web browser - sends requests to the web server
120. Web Server - handles incoming requests from clients
121. Business Layer - C++ or .Net, Java and legacy applications
122. Database Layer -cloud services and database
Web Application Forensics
123. Network Traffic (NIDS) - Network Intrusion Detection System
124. OS (HIDS) - Host Intrusion Detection System

125. Browsers (cookies) - small datasets that are stored on client computers that track where the computer's browsers have been.

126. Web Forensics Challenges

No Logs
No Intrusion Detection systme or Intrusion Protection system
Training

127. Web Attack Indications

Incoming Events - change in amount
HTTP request headers (sqlmap or NetSparker)
Fingerprints - similar attacks from other places
Geography - change in location of incoming requests

128. OWASP -Open Web Application Security Project

129. Injection - can result in data loss or corruption - tricks the sql database into giving up sensitive information by forcing the server to carry out a command input

130. Broken Authentication -Can result in identity theft and fraud - password and session tokens can be accessed or brute forced by attacker.

131. Sensitive Data Exposure -Can lead to identity theft - man in the middle attacks or packet sniffing attacks

132. XML External Entities - weaknesses in XML processors - can lead to data extractions, DoS, Internal system scans.

133. Broken Access Control -Can cause admin privilege escalation and accessing and deleting records

134. Security Misconfiguration -Can lead to unauthorized access to complete system compromise

135. Cross Site Scripting (XSS)-attacker forces a text box to execute a script command

136. DoS-denial of service

137. CHFI - Computer Hacking Forensic Investigator

138. CEH - Certified Ethical Hacker

139. 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.

140. SWGDE - Security Working Group on Digital Evidence

141. HIPAA - Health Insurance Portability and Accountability Act
Safeguarding private medical information - patient data, medical records etc.

142. FISMA - Federal Information Security Management Act

Requires annual reviews of information security programs

143. GLBA - Gramm-Leach-Bliley Act

Requires financial institutions to protect customer information against security threats

144. SOX - Sarbanes - Oxley Act

Protects investors against fraudulent accounting practices in corporations

145. PCI-DSS - standard - used for payment card industry - sets certain standards to secure credit card information

146. MS SQL- is a relational database management system (RDBMS) that supports a wide variety of transaction processing, business intelligence and analytics applications in corporate IT environments.

147. Cloud - is the delivery of different services through the Internet. These resources include tools and applications like data storage, servers, databases, networking, and software.

148. Canned Spam act - is a law that establishes the rules for commercial email and commercial messages, gives recipients the right to have a business stop emailing them, and outlines the penalties incurred for those who violate the law.

149. SIM - a smart card inside a mobile phone, carrying an identification number unique to the owner, storing personal data, and preventing operation if removed.

150. IMEI - International Mobile Equipment Identity is a 15- or 17-digit code that uniquely identifies a mobile phone set. The IMEI code can enable a GSM (Global System for Mobile communication) or UMTS (Universal Mobile Telecommunications Service) network to prevent a misplaced or stolen phone from initiating calls.

151. ICCID- Integrated Circuit Card ID)- A unique number assigned to a SIM card in a GSM cellphone. Using a formula, the ICCID can be converted into the subscriber's IMSI (International Mobile Subscriber Identity) number

152. Vulnerability - An information security "vulnerability" is a weakness or mistake in software or system that can be exploited by an attacker or a hacker to gain access to a system or network.

153. Attack Surface - The areas of a system or software that can be exploited by unauthorized users or attackers.