Joas Antonio

Computer Forensic – Overview PT.1

Details

- This PDF talks a little about Computational Forensics Analysis, just a basic overview
- https://www.linkedin.com/in/joas-antonio-dos-santos

INTRODUCTION

Computer Forensic Introduction

- A computer is a device that solves problems, manipulates information, processes data, performs calculations, and stores and retrieves data. Computers are classified by size and power. Some categories of the computer are the personal computer, workstation, minicomputer, mainframe, and a supercomputer. It uses different programs to perform different tasks.

- Forensics can be termed as the process of using different processes to gather evidence and also some scientific methods to help in solving crimes.

- Computer forensics is the branch of forensic science in which evidence is found in a computer or digital device. The aim of computer forensics is to examine digital devices in a constructive way with the goal of identifying, preserving, recovering, analyzing, and presenting the evidence in a court of law.

Computer Forensic Introduction

- Computer forensics uses a number of methods for investigation as per the guidelines of the law. Some of its methods are
  - Cross Drive Analysis
  - Live Analysis
  - Deleted Files
  - Stochastic Forensics
  - Steganography
- Computer forensics also uses some tools to perform investigations. Some of them are Digital Forensics
  - Open Computer Forensics Architecture
  - Caine
  - X-Ways Forensics
  - EnCase
  - Registry Recon
  - Volatility and many more…

Processes in Computer Forensic

- **Evaluation**
- In this process of evaluation, computer forensics experts are given instructions, clarification of those instructions if not clear, guidelines for performing activities, and allocation of roles and resources. Such a process includes proper instructions on how to prepare systems for collecting evidence and where to store evidence. Instruction on documentation is also given to help ensure the authenticity of the data.
- The process of computer forensics needs proper steps to determine the details of a case. It includes the proper reading of case briefs, understanding every fact, and obtaining permissions to continue the case.
- **Collection**
- This process involves the labeling and bagging of evidence from the crime scene. Secure and safe transportation of material is also important. Data is transferred to the expert’s system.
- In this process, cyber forensics experts visit the crime scene and collect evidence that is helpful for the investigation of the crime. Documents are needed during and after this process and include detailed information on the evidence. In this process, copies of evidence are made so that no information is lost during the investigation process.

Processes in Computer Forensic

- **Presentation**
- This process involves the proper documentation of evidence and the examination process of evidence. It includes all the methods used in the process, the techniques used, and coping. The securing and transferring of evidence is also included.
- These tasks help experts present the details of an investigation whenever asked when, how, and where the crime happened. It helps experts determine the validity of the evidence. It also helps experts in solving crimes and supporting claims with evidence in a court of law.

Processes in Computer Forensic

- **Advantages**
- Computer forensics has been very helpful in solving crimes like the following:
- **Financial Crimes**
- Financial crimes include bank fraud, credit card fraud, and net banking and phone banking fraud. Financial crimes affect individuals, companies, organizations, and even nations. They can have a negative impact on entire economic and social systems.
- **Intellectual Property Crimes**
- Intellectual property theft is defined as the theft of patents, trademarks, trade secrets, and copyrights. A patent grants property rights. A trademark identifies the source of a business. A trade secret is information for business advantage. A copyright is the legal right of an author, publisher, composer, or another person.
- **Cyber Forgery**
- Cyber forgery includes the modification of a document, false documents, illegal activity with legal contracts and certificates, and making false documents.
- **Cyber Stalking**
- Cyber stalking is the following of a user’s activity over the Internet and includes harassing or threatening the user or frightening someone by sending him threatening emails.
- **Web Defacement**
- Web defacement is an attack in which hackers compromise a website and change the content of that website, leaving social or political messages.

https://www.cybrary.it/blog/0p3n/introduction-to-computer-forensics/

Processes in Computer Forensic

1. **Identification** – the first stage identifies potential sources of relevant evidence/information (devices) as well as key custodians and location of data.

2. **Preservation** – the process of preserving relevant electronically stored information (ESI) by protecting the crime or incident scene, capturing visual images of the scene and documenting all relevant information about the evidence and how it was acquired.

3. **Collection** – collecting digital information that may be relevant to the investigation. Collection may involve removing the electronic device(s) from the crime or incident scene and then imaging, copying or printing out its (their) content.

4. **Analysis** – an in-depth systematic search of evidence relating to the incident being investigated. The outputs of examination are data objects found in the collected information; they may include system- and user-generated files. Analysis aims to draw conclusions based on the evidence found.

5. **Reporting** – firstly, reports are based on proven techniques and methodology and secondly, other competent forensic examiners should be able to duplicate and reproduce the same results.

- A crucial activity that accompanies the first four steps is **contemporaneous note-taking**. This is the documentation of what you have done immediately after you have done it in sufficient detail for another person to reproduce what you have done from the notes alone.

Types Computer Forensic

- **Disk Forensics:**
- It deals with extracting data from storage media by searching active, modified, or deleted files.
- **Network Forensics:**
- It is a sub-branch of digital forensics. It is related to monitoring and analysis of computer network traffic to collect important information and legal evidence.
- **Wireless Forensics:**
- It is a division of network forensics. The main aim of wireless forensics is to offers the tools need to collect and analyze the data from wireless network traffic.
- **Database Forensics:**
- It is a branch of digital forensics relating to the study and examination of databases and their related metadata.
- **Malware Forensics:**
- This branch deals with the identification of malicious code, to study their payload, viruses, worms, etc.

Types Computer Forensic

- **Email Forensics**
- Deals with recovery and analysis of emails, including deleted emails, calendars, and contacts.
- **Memory Forensics:**
- It deals with collecting data from system memory (system registers, cache, RAM) in raw form and then carving the data from Raw dump.
- **Mobile Phone Forensics:**
- It mainly deals with the examination and analysis of mobile devices. It helps to retrieve phone and SIM contacts, call logs, incoming, and outgoing SMS/MMS, Audio, videos, etc.

Advantages Computer Forensic

- To ensure the integrity of the computer system.
- To produce evidence in the court, which can lead to the punishment of the culprit.
- It helps the companies to capture important information if their computer systems or networks are compromised.
- Efficiently tracks down cybercriminals from anywhere in the world.
- Helps to protect the organization's money and valuable time.
- Allows to extract, process, and interpret the factual evidence, so it proves the cybercriminal action's in the court.

Advantages Computer Forensic

- To ensure the integrity of the computer system.
- To produce evidence in the court, which can lead to the punishment of the culprit.
- It helps the companies to capture important information if their computer systems or networks are compromised.
- Efficiently tracks down cybercriminals from anywhere in the world.
- Helps to protect the organization's money and valuable time.
- Allows to extract, process, and interpret the factual evidence, so it proves the cybercriminal action's in the court.

https://www.guru99.com/digital-forensics.html

Evidences Computer Forensic

- Computer documents, emails, text and instant messages, transactions, images and Internet histories are examples of information that can be gathered from electronic devices and used very effectively as evidence. For example, mobile devices use online-based based backup systems, also known as the “cloud”, that provide forensic investigators with access to text messages and pictures taken from a particular phone. These systems keep an average of 1,000–1,500 or more of the last text messages sent to and received from that phone.
- In addition, many mobile devices store information about the locations where the device traveled and when it was there. To gain this knowledge, investigators can access an average of the last 200 cell locations accessed by a mobile device. Satellite navigation systems and satellite radios in cars can provide similar information. Even photos posted to social media such as Facebook may contain location information. Photos taken with a Global Positioning System (GPS)-enabled device contain file data that shows when and exactly where a photo was taken. By gaining a subpoena for a particular mobile device account, investigators can collect a great deal of history related to a device and the person using it.

Evidences Computer Forensic

- On the scene: As anyone who has dropped a cell phone in a lake or had their computer damaged in a move or a thunderstorm knows, digitally stored information is very sensitive and easily lost. There are general best practices, developed by organizations like SWGDE and NIJ, to properly seize devices and computers. Once the scene has been secured and legal authority to seize the evidence has been confirmed, devices can be collected. Any passwords, codes or PINs should be gathered from the individuals involved, if possible, and associated chargers, cables, peripherals, and manuals should be collected. Thumb drives, cell phones, hard drives and the like are examined using different tools and techniques, and this is most often done in a specialized laboratory.
- First responders need to take special care with digital devices in addition to normal evidence collection procedures to prevent exposure to things like extreme temperatures, static electricity and moisture.

Seizing Computer Forensic

- Devices should be turned off immediately and batteries removed, if possible. Turning off the phone preserves cell tower location information and call logs, and prevents the phone from being used, which could change the data on the phone. In addition, if the device remains on, remote destruction commands could be used without the investigator’s knowledge. Some phones have an automatic timer to turn on the phone for updates, which could compromise data, so battery removal is optimal.

- If the device cannot be turned off, then it must be isolated from its cell tower by placing it in a Faraday bag or other blocking material, set to airplane mode, or the Wi-Fi, Bluetooth or other communications system must be disabled. Digital devices should be placed in antistatic packaging such as paper bags or envelopes and cardboard boxes. Plastic should be avoided as it can convey static electricity or allow a buildup of condensation or humidity. In emergency or life-threatening situations, information from the phone can be removed and saved at the scene, but great care must be taken in the documentation of the action and the preservation of the data.

- When sending digital devices to the laboratory, the investigator must indicate the type of information being sought, for instance phone numbers and call histories from a cell phone, emails, documents and messages from a computer, or images on a tablet.

Seizing Computer Forensic

- **Seizing Stand Alone Computers and Equipment:** To prevent the alteration of digital evidence during collection, first responders should first document any activity on the computer, components, or devices by taking a photograph and recording any information on the screen. Responders may move a mouse (without pressing buttons or moving the wheel) to determine if something is on the screen. If the computer is on, calling on a computer forensic expert is highly recommended as connections to criminal activity may be lost by turning off the computer. If a computer is on but is running destructive software (formatting, deleting, removing or wiping information), power to the computer should be disconnected immediately to preserve whatever is left on the machine.

- Office environments provide a challenging collection situation due to networking, potential loss of evidence and liabilities to the agency outside of the criminal investigation. For instance, if a server is turned off during seizure that is providing a service to outside customers, the loss of service to the customer may be very damaging. In addition, office equipment that could contain evidence such as copiers, scanners, security cameras, facsimile machines, pagers and caller ID units should be collected.

- Computers that are off may be collected into evidence as per usual agency digital evidence procedures.

Analysis is Performed - Computer Forensic

- **Exploiting data in the laboratory: Once the digital evidence has been sent to the laboratory, a qualified analyst will take the following steps to retrieve and analyze data:**

- **1. Prevent contamination: It is easy to understand cross contamination in a DNA laboratory or at the crime scene, but digital evidence has similar issues which must be prevented by the collection officer. Prior to analyzing digital evidence, an image or work copy of the original storage device is created. When collecting data from a suspect device, the copy must be stored on another form of media to keep the original pristine. Analysts must use “clean” storage media to prevent contamination or the introduction of data from another source. For example, if the analyst was to put a copy of the suspect device on a CD that already contained information, that information might be analyzed as though it had been on the suspect device. Although digital storage media such as thumb drives and data cards are reusable, simply erasing the data and replacing it with new evidence is not sufficient. The destination storage unit must be new or, if reused, it must be forensically “wiped” prior to use. This removes all content, known and unknown, from the media.**

- **2. Isolate Wireless Devices: Cell phones and other wireless devices should be initially examined in an isolation chamber, if available. This prevents connection to any networks and keeps evidence as pristine as possible. The Faraday bag can be opened inside the chamber and the device can be exploited, including phone information, Federal Communications Commission (FCC) information, SIM cards, etc. The device can be connected to analysis software from within the chamber. If an agency does not have an isolation chamber, investigators will typically place the device in a Faraday bag and switch the phone to airplane mode to prevent reception.**

Analysis is Performed - Computer Forensic

- 3. **Install write-blocking software:** To prevent any change to the data on the device or media, the analyst will install a block on the working copy so that data may be viewed but nothing can be changed or added.
- 4. **Select extraction methods:** Once the working copy is created, the analyst will determine the make and model of the device and select extraction software designed to most completely "parse the data," or view its contents.
- 5. **Submit device or original media for traditional evidence examination:** When the data has been removed, the device is sent back into evidence. There may be DNA, trace, fingerprint, or other evidence that may be obtained from it and the digital analyst can now work without it. Learn more about **DNA**, **trace evidence**, or **fingerprints**
- 6. **Proceed with investigation:** At this point, the analyst will use the selected software to view data. The analyst will be able to see all the files on the drive, can see if areas are hidden and may even be able to restore organization of files allowing hidden areas to be viewed. Deleted files are also visible, as long as they haven't been over-written by new data. Partially deleted files can be of value as well.
- Files on a computer or other device are not the only evidence that can be gathered. The analyst may have to work beyond the hardware to find evidence that resides on the Internet including chat rooms, instant messaging, websites and other networks of participants or information. By using the system of Internet addresses, email header information, time stamps on messaging and other encrypted data, the analyst can piece together strings of interactions that provide a picture of activity.
- http://www.forensicsciencesimplified.org/digital/how.html

First Responder - Computer Forensic

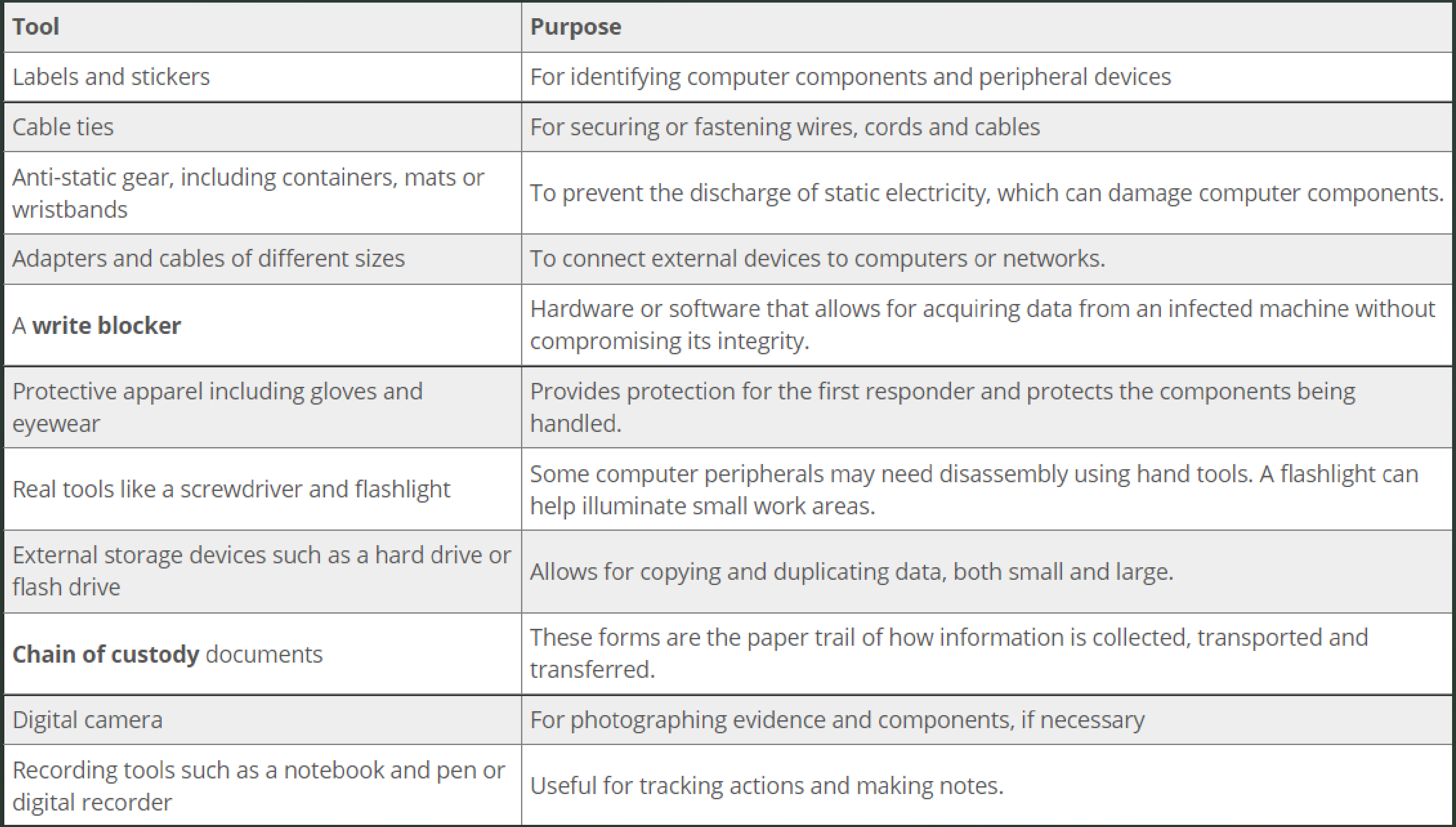
- A first responder in a computer forensic scenario is the individual who is first to find out about the situation and start to address it. In an organization, sometimes, this will be an employee who notices a problem with their company-issued desktop or laptop. In other situations, it may be a member of an IT department or a network administrator.

- A first responder to a computer event will follow a few steps to get a better understanding of the situation and how to proceed. For example, James is a network administrator for the fictional company, Exeter Bank. On a typical day, he works to keep the bank's computer network up and running so that employees can effectively perform work tasks. Today, though, it appears that a security breach has infiltrated the bank's system. So, what happens next?

- In a typical scenario, James will get to work immediately to determine how serious the breach is. To do so, he will gather as many details about the breach as he can, and document everything he discovers. The goal is to use the information collected to figure out the root cause.

- To aid a first responder like James, having a toolkit is essential.

First Responder Toolkit - Computer Forensic



Tool	Purpose
Labels and stickers	For identifying computer components and peripheral devices
Cable ties	For securing or fastening wires, cords and cables
Anti-static gear, including containers, mats or wristbands	To prevent the discharge of static electricity, which can damage computer components.
Adapters and cables of different sizes	To connect external devices to computers or networks.
A **write blocker**	Hardware or software that allows for acquiring data from an infected machine without compromising its integrity.
Protective apparel including gloves and eyewear	Provides protection for the first responder and protects the components being handled.
Real tools like a screwdriver and flashlight	Some computer peripherals may need disassembly using hand tools. A flashlight can help illuminate small work areas.
External storage devices such as a hard drive or flash drive	Allows for copying and duplicating data, both small and large.
Chain of custody documents	These forms are the paper trail of how information is collected, transported and transferred.
Digital camera	For photographing evidence and components, if necessary
Recording tools such as a notebook and pen or digital recorder	Useful for tracking actions and making notes.

First Responder Responsabilities - Computer Forensic

- Identifying the crime scene: After arriving at the crime scene, the first responder identifies the scope of the crime scene and establishes a perimeter. Establishing a perimeter includes a particular area, room, several rooms, or a building depending on the networked computers, After that, the first responder starts listing the computer systems that are involved in the incident from which he or she can collect the evidence.

- Protecting the crime scene: In a cybercrime case, a search warrant is required for searching and seizing digital/electronic evidence. Therefore, a first responder protects all the computers and electronic devices and waits for the case officer in-charge.

- Preserving temporary and fragile evidence; In the case of temporary and fragile evidence that could change or disappear, such as monitor/screen information or a running program, the first responder does not wait for the case officer in-charge. He or she takes photographs of all the evidence.

- Collecting complete information about the incident: For collecting the complete information about the incident, the first responder conducts preliminary interviews of all persons present at the crime scene and asks questions about the incident.

- Documenting all findings: The first responder starts documenting all information about the collected evidence in the chain of custody document sheet, The chain of custody document sheet contains information such as case number, name of the person who reported the case, address and telephone number, location of the evidence, date/time of collecting the evidence, and a complete description of the item.

- Packaging and transporting the electronic evidence: After collecting the evidence, the first responder labels all the evidence and places it in evidence storage bags, which protect the evidence from sunlight and high temperature. These bags also block wireless signals so that wireless devices cannot acquire data from the evidence. Then, the first responder transports these packed bags to the forensics laboratory.

- Gather preliminary information at the scene: At the time of an incident, secure the crime scene and the surrounding area to avoid any tampering of the evidence. Preliminary information at the crime scene provides the basis for the forensics investigation, and helps in finding the evidence easily, if there is no third-party interference at the incident scene.

Fundamentals

File System

- https://www.techopedia.com/definition/5510/file-system#:~:text=A%20file%20system%20is%20a,abstract%20to%20a%20human%20user.
- https://en.wikipedia.org/wiki/File_system
- https://www.freecodecamp.org/news/file-systems-architecture-explained/
- https://www.howtogeek.com/196051/htg-explains-what-is-a-file-system-and-why-are-there-so-many-of-them/
- https://www.javatpoint.com/file-system

Hard Disk

- https://www.britannica.com/technology/hard-disk
- https://en.wikipedia.org/wiki/Hard_disk_drive
- https://www.javatpoint.com/hard-disk-definition-and-function
- https://www.pcmag.com/encyclopedia/term/hard-disk
- https://www.webopedia.com/definitions/hard-disk/

Memory Management

- https://en.wikipedia.org/wiki/Memory_management#:~:text=Memory%20management%20is%20a%20form,reuse%20when%20no%20longer%20needed.
- https://www.tutorialspoint.com/operating_system/os_memory_management.htm
- https://en.wikipedia.org/wiki/Memory_management_(operating_systems)
- https://whatis.techtarget.com/definition/memory-management

Ram Memory

- https://en.wikipedia.org/wiki/Random-access_memory
- https://www.bentley.com/en/products/product-line/structural-analysis-software/ram-concept
- https://searchstorage.techtarget.com/definition/RAM-random-access-memory

Forensic Analysis

Windows Forensic

- https://www.geeksforgeeks.org/windows-forensic-analysis/
- https://nasbench.medium.com/windows-forensics-analysis-windows-artifacts-part-i-c7ad81ada16c
- https://www.sciencedirect.com/book/9780124171572/windows-forensic-analysis-toolkit
- http://index-of.es/Hack/Windows%20Forensic%20Analysis.pdf
- https://www.ijrar.org/papers/IJRAR19K8276.pdf
- https://www.saintleo.edu/hubfs/Resource%20PDFs%20and%20DOCs/Academics/Center%20for%20Cybersecurity/Student%20Projects/2018/Windows_Forensics.pdf
- https://www.irjet.net/archives/V3/i4/IRJET-V3I4118.pdf
- https://www.ijrte.org/wp-content/uploads/papers/v7i6/F2623037619.pdf
- https://github.com/travisfoley/dfirtriage
- https://github.com/cugu/awesome-forensics

Email Forensic

- https://www.stellarinfo.com/blog/email-forensics-investigation-guide-for-security-experts/
- https://www.researchgate.net/publication/344906935_E-MAIL_FORENSICS_TECHNIQUES_AND_TOOLS_FOR_FORENSIC_INVESTIGATION
- https://cybersecop.com/email-forensics-and-investigations-services
- https://www.researchgate.net/publication/227859112_Techniques_and_Tools_for_Forensic_Investigation_of_E-mail
- https://www.forensicfocus.com/articles/email-forensics-investigation-techniques/
- https://www.capterra.com.br/software/172333/forensic-email-collector
- https://www.atlanticdf.com/practice-area/cybersecurity-data-privacy/email-forensics-email-recovery/
- https://github.com/manojtld/email-forensics
- https://github.com/topics/email-header-forensics
- https://github.com/stigster/FMG
- https://github.com/cyberdefenders/email-header-analyzer
- https://github.com/libratom/email-processing-resources

Memory Forensic

- https://digitalguardian.com/blog/what-are-memory-forensics-definition-memory-forensics#:~:text=Memory%20forensics%20(sometimes%20referred%20to,tracks%20on%20hard%20drive%20data
- https://en.wikipedia.org/wiki/Memory_forensics
- https://www.youtube.com/watch?v=BMFCdAGxVN4
- https://www.youtube.com/watch?v=Ha-TXEvSAIM
- https://www.youtube.com/watch?v=1PAGcPJFwbE
- https://stuxnet999.github.io/volatility/2020/08/18/Basics-of-Memory-Forensics.html
- https://www.volatilityfoundation.org/
- https://lifars.com/knowledge-center/windows-memory-forensics-technical-guide-2/
- https://www.memoryanalysis.net/memory-forensics-training
- https://www.sciencedirect.com/topics/computer-science/memory-forensics
- https://resources.infosecinstitute.com/topic/computer-forensics-memory-forensics/

Wireless Forensic

- https://lecto-player.lecto.org/recordings/fer/predmeti/racfor/2016/seminari/hmarosevic/seminar.pdf
- https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=8afe2de6-eefc-42fb-9711-5a2bf1025c70&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
- https://miguelbigueur.com/2017/04/24/wireless-forensics/
- https://www.grin.com/document/512779
- https://www.researchgate.net/publication/224686973_Wireless_Forensic_Analysis_Tools_for_Use_in_the_Electronic_Evidence_Collection_Process
- https://resources.infosecinstitute.com/topic/wireless-networking-fundamentals-for-forensics/
- https://www.dataforensics.org/wifi-forensics/
- https://www.kjbcomputerforensics.com/wirelessforensics.html
- https://www.nist.gov/ctl/wireless-spectrum-forensics

Network Forensic

- https://subscription.packtpub.com/book/networking-and-servers/9781782174905/1/ch01lvl1sec12/differentiating-between-computer-forensics-and-network-forensics
- https://www.nystec.com/insights/network-forensics-101/
- https://www.sciencedirect.com/topics/computer-science/network-forensics
- https://www.itpro.co.uk/cyber-attacks/31660/what-is-network-forensics
- https://searchsecurity.techtarget.com/definition/computer-forensics
- https://lifars.com/2020/06/the-basics-of-network-forensics/
- https://resources.infosecinstitute.com/topic/network-forensics-overview/

Awesome Forensic

- https://github.com/mesquidar/ForensicsTools
- https://github.com/meirwah/awesome-incident-response
- https://github.com/asiamina/A-Course-on-Digital-Forensics

Mobile Forensic

- https://en.wikipedia.org/wiki/Mobile_device_forensics
- https://www.adfsolutions.com/mobile-device-investigator
- https://www.diva-portal.org/smash/get/diva2:1498990/FULLTEXT01.pdf
- https://cybericus.com/best-mobile-forensic-tools/
- https://cyfor.co.uk/digital-forensics/mobile-phone-forensics/
- https://digitalintelligence.com/solutions/mobile_investigations
- https://security.opentext.com/encase-mobile-investigator
- https://www.incibe-cert.es/en/blog/mobile-forensic-analyses-tools
- https://www.iacpcybercenter.org/officers/mobile-forensics/
- https://www.mheducation.com/highered/product/mobile-forensic-investigations-guide-evidence-collection-analysis-presentation-second-edition-reiber/9781260135091.html

Password Cracking

- https://alpinesecurity.com/blog/offline-password-cracking-the-attack-and-the-best-defense-against-it/#:~:text=Offline%20Password%20Cracking%20is%20an,recovered%20from%20a%20target%20system.&text=Using%20Online%20Password%20Cracking%2C%20an,previous%20access%20to%20the%20system.
- https://www.triaxiomsecurity.com/whats-the-difference-between-offline-and-online-password-attacks/
- https://www.youtube.com/watch?v=h9R7AlpNhSM
- https://www.youtube.com/watch?v=23DWqp0EELE
- https://www.youtube.com/watch?v=Gy0bhFhl6R8
- https://davidebove.com/blog/2019/03/18/using-an-offline-password-cracker/
- https://www.hindawi.com/journals/scn/2021/5563884/
- https://www.itpro.co.uk/security/34616/the-top-password-cracking-techniques-used-by-hackers
- https://www.securityweek.com/brute-force-attacks-crossing-online-offline-password-chasm
- https://doubleoctopus.com/security-wiki/threats-and-tools/brute-force-attack/
- https://www.peritoanderson.com.br/offline/

Password Cracking

- https://alpinesecurity.com/blog/offline-password-cracking-the-attack-and-the-best-defense-against-it/#:~:text=Offline%20Password%20Cracking%20is%20an,recovered%20from%20a%20target%20system.&text=Using%20Online%20Password%20Cracking%2C%20an,previous%20access%20to%20the%20system.
- https://www.triaxiomsecurity.com/whats-the-difference-between-offline-and-online-password-attacks/
- https://www.youtube.com/watch?v=h9R7AlpNhSM
- https://www.youtube.com/watch?v=23DWqp0EELE
- https://www.youtube.com/watch?v=Gy0bhFhl6R8
- https://davidebove.com/blog/2019/03/18/using-an-offline-password-cracker/
- https://www.hindawi.com/journals/scn/2021/5563884/
- https://www.itpro.co.uk/security/34616/the-top-password-cracking-techniques-used-by-hackers
- https://www.securityweek.com/brute-force-attacks-crossing-online-offline-password-chasm
- https://doubleoctopus.com/security-wiki/threats-and-tools/brute-force-attack/

Forense Tools

- https://www.peritoanderson.com.br/offline/
- https://github.com/sepinf-inc/IPED
- https://github.com/cugu/awesome-forensics
- https://github.com/mesquidar/ForensicsTools
- https://github.com/danilopcarlotti/scdf
- https://en.wikipedia.org/wiki/List_of_digital_forensics_tools
- https://www.caine-live.net/
- https://accessdata.com/product-download/ftk-imager-version-4-2-1
- https://www.gta.ufrj.br/grad/07_1/forense/encase.html
- https://techbiz.com.br/?products=encase%C2%AE-forensic-v7
- https://www.100security.com.br/encase

Log Analysis

- https://www.sumologic.com/glossary/log-analysis/
- https://sematext.com/blog/log-analysis-tools/
- https://www.solarwinds.com/pt/log-analyzer/use-cases/log-analysis
- https://pestleanalysis.com/log-analysis/
- https://opensource.com/article/19/4/log-analysis-tools
- https://www.tek-tools.com/apm/best-free-log-analysis-tools
- https://github.com/logpai/awesome-log-analysis
- https://github.com/automationlogic/log-analysis
- https://github.com/logpai/loglizer

Forense Courses

- https://www.udemy.com/course/computacao-forense-e-investigacao-digital/
- https://www.edx.org/course/computer-forensics
- https://www.edx.org/learn/computer-forensics
- https://www.infosecinstitute.com/courses/computer-forensics-boot-camp/
- https://digitaldefynd.com/best-computer-forensics-courses/
- https://www.udemy.com/topic/computer-hacking-forensic-investigator/
- https://www.infosectrain.com/courses/chfi-v9-certification-training/
- https://www.cybrary.it/course/computer-hacking-forensics-analyst/
- https://www.hackerschool.in/courses/computer-hacking-forensic-investigator-chfi/
- https://www.globalknowledge.com/us-en/training/certification-prep/topics/cybersecurity/section/ec-council/chfi-computer-hacking-forensics-investigator/
- https://www.eccouncil.org/programs/computer-hacking-forensic-investigator-chfi/
- https://elearnsecurity.com/product/ecdfp-certification/