Computer Forensics

By Jaye Englehart and Robert Squires

What is Computer Forensics?

- Computer forensics is also referred to as computer forensic analysis, electronic discovery, electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis, and computer examination.
- Computer forensics is the process of methodically examining computer media (hard disks, diskettes, tapes, etc.) for evidence. In other words, computer forensics is the collection, preservation, analysis, and presentation of computer-related evidence.

https://mrcet.com/pdf/Lab%20Manuals/IT/R15A0533%20CF.pdf
https://www.mitnicksecurity.com/blog/what-is-computer-forensics-and-how-is-it-used-in-investigations

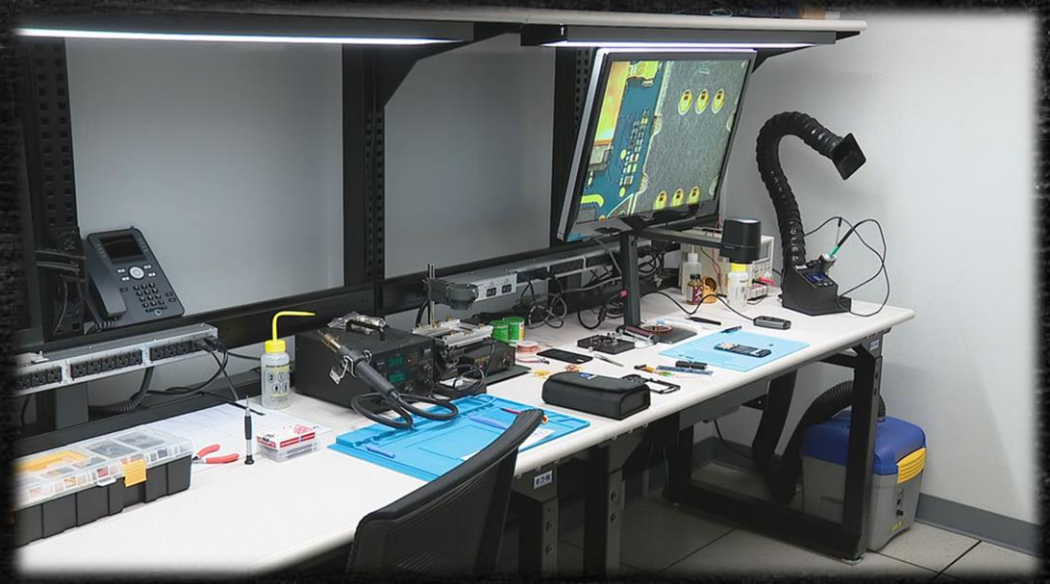
Computer Forensics Collection

- Collection is typically performed by Law Enforcement/Military Personnel
  - Will typically take the physical device for analysis
  - Situationally, personnel may perform a data collection on scene:
    - Dead box collection: The device is powered off and then the data is collected
    - Live box collection: The data is collected from the device before it is powered off

https://drivesaversdatarecovery.com/digital-forensic-process-preservation-collections/

Computer Forensics Preservation

- Imperative that nothing may alter digital evidence
- Isolation and protection of digital evidence exactly as it was found
- Duplicate of the electronically stored information (ESI) is created
  - Preserves the original device for evidence
- Duplicate ESI is analyzed



https://drivesaversdatarecovery.com/digital-forensic-process-preservation-collections/

Computer Forensics Analysis

- The in-depth analysis and examination of ESI.
- Analysts use software such as Autopsy, FTK Imager, Volatility, etc.
- Analysts search for potential evidence in:
  - Documents
  - Photographs
  - User Web/App history
  - Windows Registry
  - Metadata
  - Network Traffic Captures

https://drivesaversdatarecovery.com/digital-forensic-process-preservation-collections/
https://resources.infosecinstitute.com/topic/7-best-computer-forensics-tools/

Forensic Reporting/Presentation

- Contains all pertinent information found on the device
- Is a detailed chain of evidence for a device
- Can be done with software such as Autopsy
- Could include giving testimony for a trial

https://drivesaversdatarecovery.com/digital-forensic-process-preservation-collections/
https://resources.infosecinstitute.com/topic/7-best-computer-forensics-tools/
http://www.msainvestigations.com/com/msainvestigations/www/clients-we-help/private-individuals/computer-forensics/computer-forensics-faq.html

Who uses Computer Forensics?

- Computer forensics is used by:
  - Law Enforcement/Government Agencies/Military
    - National Security Agency (NSA)
    - Federal Bureau of Investigation (FBI)
    - U.S. Immigration and Customs Enforcement (ICE)
    - U.S. Military (DOD)
  - Commercial Corporations
    - Target
    - American Express
    - Walmart
    - Intel
    - Mastercard

https://www.forensicscolleges.com/blog/resources/companies-with-internal-forensics-labs

When is Computer Forensics used?

- Unauthorized disclosure of corporate information
- Employee Internet abuse or other violations of a computer policy
- Damage assessment and analysis (post incident)
- Industrial espionage
- Negligence, sexual harassment, and deception cases
- Evidence collection for future employee termination
- Criminal fraud and white-collar crime

https://www.computerpi.com/resources/using-computer-forensics/
http://www.msainvestigations.com/com/msainvestigations/www/clients-we-help/private-individuals/computer-forensics/computer-forensics-faq.html

Practice with Computer Forensics!

- Now we will use the program Autopsy in NETLAB+ to gain hands-on forensics experience.