Computer Forensics

By Jaye Engelhardt

What is Computer Forensics?

- Computer forensics is also referred to as:
  - Computer forensic analysis
  - Digital discovery
  - Data recovery
  - Computer analysis
- Computer forensics is the collection, preservation, analysis, and presentation of computer-related evidence.

Who uses it?

- Computer forensics engineers extract evidence in a legal manner, to ensure it is available for court proceedings.

  - There are 5 important steps for an effective investigation
    - Policy and Procedure Development
    - Evidence Assessment
    - Evidence Acquisition
    - Evidence Examination
    - Documenting and Reporting

Skills Needed

- Knowledge of
  - Programming
  - Operating Systems
  - Malware Types
  - Law and Criminal Investigation
- Code of Ethics
- Critical and analytical thinking
- Communication Skills
- Attention to Details

Recommended Certifications

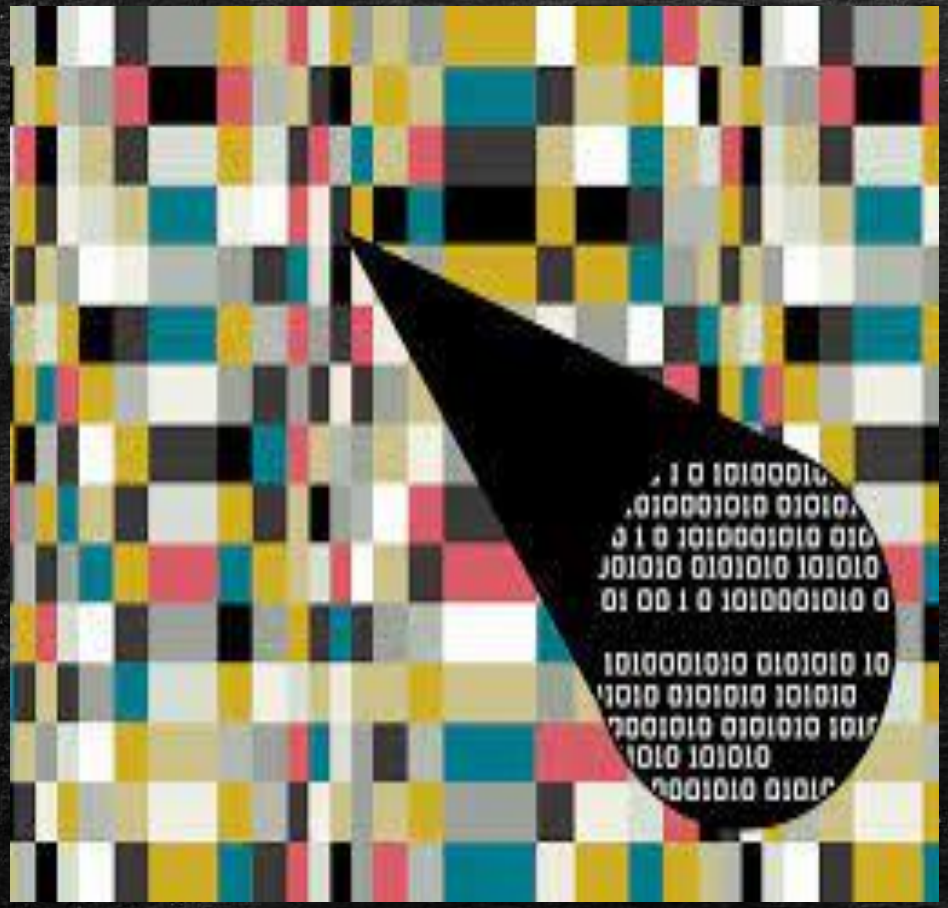
- There are not many institutions that have computer forensics degrees however there are certifications you can obtain.
  - EnCase Certified Examiner
  - Certified Computer Examiner
  - Certified Computer Forensic Examiner
  - GIAC Certified Forensic Examiner
  - Cyber Security Forensic Analyst
- You can pair these certifications with a degree in computer science or cybersecurity and criminal justice and be on the path to becoming a computer forensics engineer.

Types of Computer Forensics

Computer forensics can be broken down into different groups.

- Operating System Forensics
- File System Forensics
- Live Memory Forensics
- Web Forensics
- Email Forensics
- Network Forensics
- Multimedia Forensics
- Others

Stenography



- The technique of concealing data within another message to avoid detection.
  - Derivied from 2 Greek words “steganos” meaning hidden or covered and “graph” meaning to write
- Can be used to hide most types of data including text, video, images, and audio.

Tools Available

- Autopsy and Sleuth Kit
- FTK Imager
- Registry Recon
- Cellebrite UFED
- Wireshark
- Faraday Shielding Bag

Private companies with their own labs

- Mastercard
- Target
- American Express
- Walmart
- Intel

Any Questions?

Resources

Javed, A. R., Ahmed, W., Alazab, M., Jalil, Z., Kifayat, K., & Gadekallu, T. R. (2022). A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions. *IEEE Access*, *10*, 11065–11089. https://doi.org/10.1109/access.2022.3142508

Lavender, L. K. (2020). 17.2. In *Principles of Cybersecurity* (pp. 544–551). essay, The Goodheart-Willcox Company, Inc.

Mitnick. (2020, August 27). *What is Computer Forensics and How Is It Used In Investigations?*. Mitnick Security Consulting. https://www.mitnicksecurity.com/blog/what-is-computer-forensics-and-how-is-it-used-in-investigations

Resources

National University. (2023, May 19). *What is Computer Forensics?*. National University. https://www.nu.edu/blog/what-is-computer-forensics/#:~:text=A%20digital%20forensic%20analyst%20is,and%20other%20digital%20storage%20media.

Poston, H. (2021, January 6). *7 best computer forensics tools [updated 2021]*. Infosec. https://resources.infosecinstitute.com/topics/digital-forensics/7-best-computer-forensics-tools/

Zborg, M. (2020, March 24). *Five Companies With Their Own Digital Forensics Labs*. Forensics Colleges. https://www.forensicscolleges.com/blog/resources/companies-with-internal-forensics-labs