Intro to Cyber Forensics

What is Cyber Forensics?

Cyber Forensics is an umbrella term for data monitoring, acquisition, analysis, and interpretation, related to criminal behavior.

The most common type of Cyber crime is stealing data without permission.

“Hacking” is usually synonymous with taking control of an online infrastructure, but actually embodies a lot of different cyber crimes.

Brief History of Cyber Forensics

Brief History

- 1960s - 1980s: Emergence of Digital Computing
  - The history of digital forensics can be traced back to the early days of digital computing.
  - As computers began to be used for various applications, the need to investigate computer-related crimes and incidents arose.
  - Early efforts were often ad hoc and limited by the technology of the time.
- 1970s - 1990s: Computer Crime and Investigations
  - As computer systems became more widespread in business and government, instances of computer-related crimes increased.
  - The term "computer forensics" began to be used in the 1970s to describe the application of investigative techniques to digital evidence.
  - The field was still in its infancy, with investigators primarily focused on hardware-level analysis.

Brief History

- 1990s: The Rise of the Internet
  - The proliferation of the internet during this period led to new challenges for digital forensics.
  - Cybercrimes such as hacking, online fraud, and data breaches became more prevalent, necessitating the development of specialized techniques to investigate these types of incidents.
- Late 1990s - Early 2000s: Formalization of Techniques
  - The field of digital forensics began to formalize during this time, with the introduction of standardized procedures and guidelines for conducting investigations.
  - Organizations such as the International Association of Computer Investigative Specialists (IACIS) and the National Institute of Standards and Technology (NIST) played a role in establishing best practices.

Brief History

- 2000s: Growth and Technological Advancements
  - The 2000s saw a rapid expansion of the digital forensics field due to advancements in technology.
  - The increasing complexity of computer systems, the rise of mobile devices, and the prevalence of digital data storage created new challenges and opportunities for investigators.
  - Techniques for recovering deleted data, analyzing file systems, and extracting information from various devices became more sophisticated.
- 2000s - 2010s: High-Profile Cases
  - High-profile cases, such as computer intrusions, cyberattacks, and corporate scandals, highlighted the importance of digital forensics in legal proceedings.
  - Digital evidence played a crucial role in these cases, emphasizing the need for well-trained professionals and reliable methodologies.

Brief History

- 2010s: Focus on Memory Analysis and Malware
  - With the increase in sophisticated cybercrimes involving memory-resident malware and advanced persistent threats (APTs), the field of digital forensics expanded to include memory analysis and malware analysis.
  - These techniques helped investigators uncover hidden threats and gain insight into attackers' methods.
- 2010s: Cloud Computing and Virtualization
  - The adoption of cloud computing and virtualization presented new challenges for digital forensics.
  - Investigators needed to develop methods to gather evidence from remote servers, virtual machines, and distributed environments while preserving chain of custody.

Brief History

- 2010s: Mobile and IoT Forensics
  - The proliferation of mobile devices and the Internet of Things (IoT) created a need for specialized techniques in mobile and IoT forensics.
  - Extracting data from smartphones, tablets, wearables, and smart home devices became a crucial aspect of digital investigations.

Activity

Research the challenges posed by one of the following technologies to the field of cyber forensics and complete the table on the next slide.

Technologies to Choose from (Choose one to research):

- Artificial Intelligence
- Quantum Computing

Include the following information:

- Why this technology could present a challenge to the field of cyber forensics
- Possible mitigations that can be used to address these challenges

Activity

Technology Chosen	
Challenges Posed (Include at least 3)	**Possible Mitigations (Include at least 3)**

Types of Cyber Forensics

Database Forensics

The examination of information contained in databases, both data and related metadata.

Email Forensics

The recovery and analysis of emails and other information contained in email platforms, such as schedules and contacts.

Malware Forensics

Sifting through code to identify possible malicious programs and analyzing their payload.

Such programs may include:

- Trojan horses
- Ransomware
- Various viruses
- Spyware
- Adware
- Rootkit
- Keylogger
- Worms

Memory Forensics

Collecting information stored in the computer's random access memory (RAM) and cache.

Mobile Forensics

The examination of mobile devices to retrieve and analyze the information they contain, including contacts, incoming and outgoing text messages, pictures and video files.

Network Forensics

Looking for evidence by monitoring network traffic using tools such as a firewall or intrusion detection system.

Sorting Activity

Sort the descriptions at the bottom into the appropriate type of cyber forensic evidence. You should click and drag the description under the appropriate online threat.

Database Forensics	Email Forensics	Malware Forensics	Memory Forensics	Mobile Forensics	Network Forensics

The recovery and analysis of emails and other information contained in email platforms, such as schedules and contacts.

Collecting information stored in the computer's random access memory (RAM) and cache.

The examination of information contained in databases, both data and related metadata.

The examination of mobile devices to retrieve and analyze the information they contain.

Looking for evidence by monitoring network traffic using tools such as a firewall or intrusion detection system.

Sifting through code to identify possible malicious programs and analyzing their payload.

Collage Activity

Create a collage using Google Slides or Google Drawings.

The collage should consist of the following elements:

- 12 different images that represent various types of cyber forensics (i.e. database forensics, email forensics, etc.). You should have two images for each type of forensic category we've discussed.
- Each image should be labeled with a text box that identifies the type of cyber forensics it is displaying
- A title/heading for your collage that describes what it is depicting

I have included an example of a collage so you know what is expected. Note that this example is over the topic of online privacy and not the type of cyber forensics.