WEEK-3

Asad Muhammad Channar

DHC-56

Task-4:

Forensic Data Analysis with Autopsy

Required:

- Use Autopsy to analyze a disk image for evidence of malicious activity.
- Identify suspicious files, data, or logs that could indicate a security breach.

Deliverables:

- A 1page forensic report detailing your findings and insights.

Forensic Data Analysis with Autopsy

Introduction to Autopsy

Autopsy is a widely-used open-source digital forensics platform that helps investigators analyze disk images and gather evidence of potential security incidents. It is popular among law enforcement, cybersecurity professionals, and corporate investigators due to its user-friendly interface and versatile capabilities. Autopsy supports various file systems (NTFS, FAT, EXT) and image formats, making it suitable for analyzing different storage devices, such as hard drives, SSDs, and USBs.

A key feature of Autopsy is its ability to recover deleted data, such as files, browser history, and emails, which can be crucial in investigations. Additionally, it analyzes file metadata to provide timestamps and access information, helping investigators reconstruct a timeline of events.

Autopsy's modular architecture allows users to customize the platform by adding plugins tailored to specific investigative needs, such as memory analysis, email extraction, or network traffic analysis.

Uses of Autopsy

Autopsy has several important applications, from investigating malware infections to retrieving critical evidence in criminal cases.

1. Incident Response and Malware Analysis

Autopsy is an essential tool in cybersecurity for investigating malware infections and security breaches. When a system is compromised, Autopsy helps identify the cause of the attack and the extent of the damage. By analyzing disk images, investigators can detect malicious files, track changes to the file system, and identify any data exfiltration.

In a case of a ransomware attack, Autopsy was used to identify the malware's entry point, which was a phishing email. The tool also helped reveal which files were encrypted and enabled the organization to prioritize recovery efforts.

2. Law Enforcement Investigations

Law enforcement agencies use Autopsy to recover digital evidence in criminal cases. This includes deleted files, communication logs, browsing history, and more. For example, in a child exploitation case, Autopsy helped recover incriminating images that had been deleted from the suspect's computer. The software also provided metadata that revealed when and where the images were captured, which was essential for the investigation.

Autopsy's ability to construct timelines based on file modifications and access times allows investigators to track criminal activities and piece together the sequence of events in a case.

3. Corporate Investigations

In corporate investigations, Autopsy helps uncover insider threats, intellectual property theft, and policy violations. Investigators use it to analyze employee devices for signs of data leaks or unauthorized activities, such as copying confidential information to external drives.

In one corporate investigation, an employee was suspected of leaking sensitive information. Autopsy recovered deleted emails that contained proprietary data, which led to the discovery of unauthorized communications with a competitor.

Examples of Autopsy in Action

1. **Ransomware Investigation**: Autopsy was used to trace the source of a ransomware attack, which had spread through a phishing email. Investigators recovered logs showing the timeline of the infection and used the information to prevent future attacks.
2. **Intellectual Property Theft**: In a corporate case, Autopsy helped recover deleted files that contained confidential blueprints. The investigation confirmed that an employee had shared the designs with a competitor, leading to a legal case.
3. **Human Trafficking Case**: Autopsy was used in a human trafficking investigation to recover deleted chat logs and photos, providing crucial evidence. Metadata from recovered images also helped place the suspect at key locations related to the crime.