Digital Forensics for Health

CSP012

PRESENTATION BY: STYLIANOS KARAGIANNIS (PDMFC, PORTUGAL)

Ghidra and GDB

Where can be used?

Ghidra is a software reverse engineering framework developed by the National Security Agency (NSA) that helps analyze and understand executable files.

Application in Healthcare: Used to analyze medical device firmware and software for vulnerabilities and backdoors.

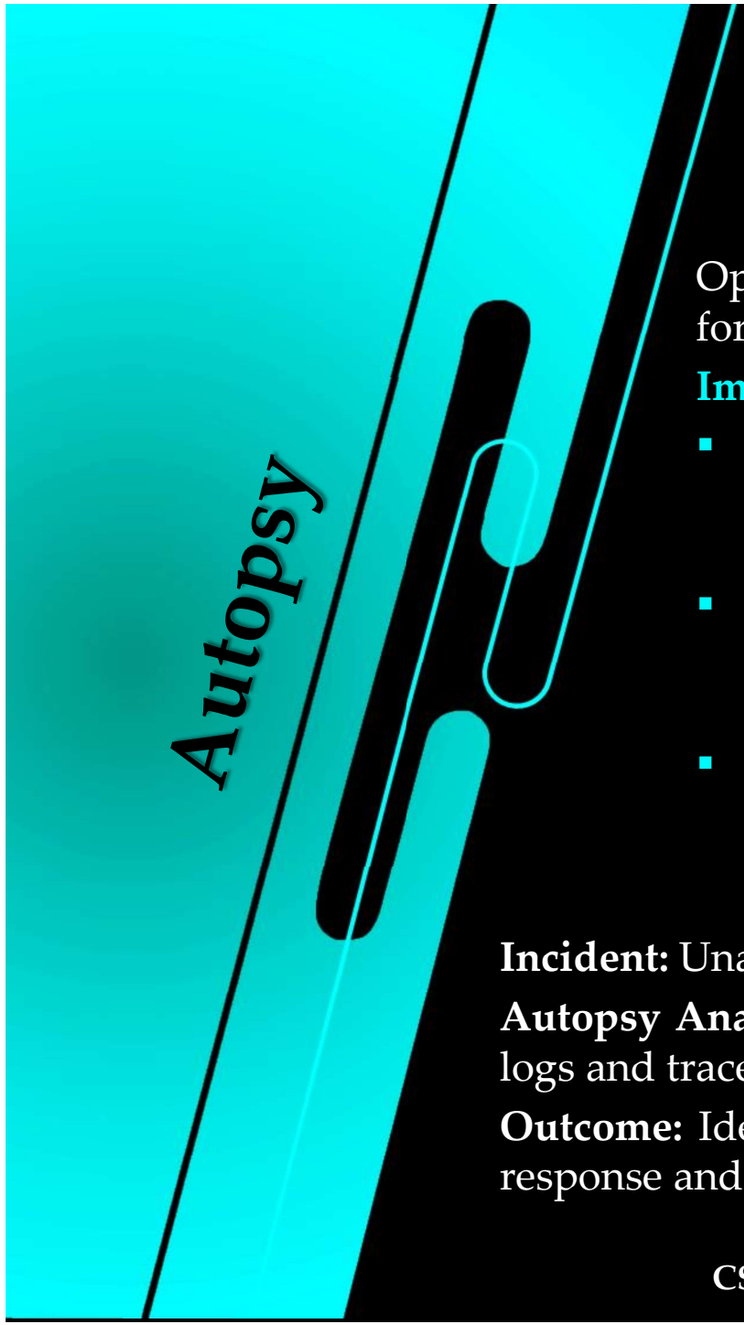
Example: Analyzing the firmware of a medical infusion pump to identify potential vulnerabilities that could lead to unauthorized access or tampering. Provides insights into the inner workings of medical device software, enabling security researchers to identify and address vulnerabilities proactively.

GDB (GNU Debugger)

GDB is a powerful debugger that allows developers to inspect and manipulate the execution of programs during runtime.

Application in Healthcare: Used for debugging and analyzing medical device software to identify and fix software bugs and vulnerabilities.

Example: Debugging a medical device firmware to trace the root cause of a software crash or unexpected behavior. Enables healthcare organizations to ensure the reliability and security of medical device software by identifying and resolving potential issues during development and testing phases.



Autopsy

How can be used?

Open-source digital forensics platform for analyzing disk images and conducting forensic investigations.

Importance in Healthcare Domain

- **Analysis of Medical Imaging Data:** Autopsy can be used to examine disk images from medical imaging devices, such as MRI or CT scanners, to investigate potential security incidents or data breaches.
- **Recovery of Deleted Electronic Health Records (EHRs):** Autopsy's file system analysis capabilities can aid in recovering deleted EHR files, ensuring data integrity and compliance with healthcare regulations.
- **Examination of Medical Device Data:** Autopsy enables forensic analysis of data from medical devices, such as infusion pumps or pacemakers, to identify security vulnerabilities or tampering attempts.

Incident: Unauthorized access to patient medical records.

Autopsy Analysis: Forensic examination of disk images from hospital servers to identify access logs and traces of unauthorized access.

Outcome: Identification of the attacker's actions and potential data breaches, enabling incident response and mitigation measures.

DFIRKuiper (Kuiper)

Digital Forensics, Especially Healthcare Domain

Automated digital forensics and incident response tool developed by Google, leveraging machine learning algorithms.

Importance in Healthcare Domain

- **Rapid Analysis of Healthcare Data:** Kuiper's automation capabilities allow for quick analysis of large volumes of healthcare data, such as electronic health records (EHRs) or medical imaging files.
- **Detection of Anomalous Activities:** Kuiper's machine learning algorithms can identify suspicious patterns or anomalies within healthcare data, helping detect potential security incidents or breaches.
- **Scalability in Incident Response:** Kuiper enables scalability in incident response efforts within the healthcare domain, allowing DFIR teams to efficiently triage and prioritize critical findings.

Incident: Suspicious activity detected in a hospital's EHR system.

Kuiper Analysis: Automated analysis of EHR data to identify anomalous access patterns or unauthorized modifications.

Outcome: Early detection of potential security incidents, enabling timely response and mitigation actions to protect patient data and ensure healthcare system integrity.

CoC and IoC

Chain of Custody

Chain of custody refers to the documented trail that shows the chronological sequence of custody, control, transfer, analysis, and disposition of physical or digital evidence.

- It is crucial in legal proceedings and investigations to ensure the integrity and admissibility of evidence in court.
- Chain of custody records include details such as who collected the evidence, when and where it was collected, who handled it, and any changes in possession or storage conditions.
- Maintaining a proper chain of custody helps establish the authenticity and reliability of evidence, demonstrating that it has not been tampered with or compromised during the investigation process.

Indicators of Compromise (IOCs)

- IOCs are artifacts or evidence observed in an organization's network or systems that indicate potential security incidents or compromises.
- They can include suspicious files, network traffic patterns, system log entries, or behavioral anomalies that suggest malicious activity.
- IOCs are used by cybersecurity professionals and incident responders to detect, investigate, and mitigate security threats in real-time.
- Common types of IOCs include IP addresses, domain names, file hashes, registry keys, and patterns of activity associated with known malware or attack techniques.

Kuiper, CoC and IoC

Kuiper, Chain of Custody and IoC

Chain of custody: Kuiper can document the handling and analysis of digital evidence, providing a detailed record of who accessed the data, when it was accessed, and any actions performed on it. This ensures the integrity and admissibility of evidence in legal proceedings.

- Kuiper provides a centralized platform for digital investigations, allowing teams to document and maintain a clear chain of custody for all collected evidence.
- With Kuiper's centralized server, all evidence is stored in a single location, reducing the need to copy data onto multiple machines during investigations.
- Kuiper ensures evidence integrity and admissibility by tracking access details and actions taken. Consistent parsing using trusted parsers enhances reliability, vital for maintaining a reliable chain of custody. With advanced analytics and data handling, Kuiper efficiently detects IOCs.
- Analysts can set rules for alerting suspicious activities and collaborate, tagging and visualizing records for swift IOC identification and response.

Kuiper, CoC and IoC

Kuiper, Chain of Custody and IoC

Digital Forensics, Especially Healthcare Domain

An organization using Kuiper notices unusual network activity originating from a specific workstation. The activity includes repeated attempts to establish connections with known malicious IP addresses.

- **Detection:** Kuiper's network monitoring capabilities flag the suspicious network activity on the workstation as an IoC.
- **Alert Generation:** Based on predefined rules set within Kuiper, an alert is automatically generated for the suspicious network connections.
- **Investigation:** Analysts access Kuiper's interface to investigate the alert further. They examine the timeline of events associated with the workstation's network activity.
- **Analysis:** Kuiper's advanced analytics tools analyze the network traffic data to identify patterns and anomalies indicative of malicious behavior.
- **Confirmation:** Through Kuiper's visualization features, analysts confirm that the workstation has been attempting to connect to known malicious IP addresses, confirming the presence of an IoC.

Data Breacch and IoC

Kuiper, Chain of Custody and IoC

Healthcare Use Case – Data Breach Pt.1

1. IP Addresses: These are numerical labels assigned to devices connected to a network. In a healthcare data breach scenario, suspicious IP addresses could indicate unauthorized access attempts, command and control servers, or locations of attackers.

- Example: 203.0.113.10 might be an IP address used by an attacker to access a healthcare database.

2. Domain Names: Domain names are human-readable addresses used to access websites or servers on the internet. In the context of a healthcare data breach, malicious domain names could be used for phishing campaigns targeting healthcare employees or patients, or for hosting fake healthcare portals.

- Example: healthcaresystembreach.com might be a domain used in a phishing campaign impersonating a healthcare system.

3. File Hashes: Hash values represent unique digital fingerprints of files. In a data breach, file hashes can identify compromised files containing patient records or sensitive healthcare data. Comparing hashes helps identify known malicious files.

- Example: MD5: 5a4b63e90d2a8129bc070137645c5287 could be the hash of a compromised database file.

Data Breacch and IoC

Kuiper, Chain of Custody and IoC

Healthcare Use Case – Data Breach Pt.2

4. URLs: URLs are web addresses that specify the location of resources on the internet. Malicious URLs in a healthcare data breach context could lead to phishing websites or malware distribution sites.

- Example: http://fakehealthportal.com/login might lead to a phishing website impersonating a healthcare portal.

5. Email Addresses: Email addresses are used for communication purposes. In a healthcare data breach, attackers might use email addresses for phishing campaigns targeting healthcare employees or patients, or for communication related to the breach.

- Example: hr@healthcaresystembreach.com could be an email address used in a phishing email targeting healthcare staff.

6. Registry Keys: Registry keys are entries in the Windows registry that store configuration settings or other information. In the context of a healthcare data breach, suspicious registry keys could indicate unauthorized access or tampering with healthcare system settings.

- Example: HKLM\Software\HealthcareSystemBreach\DataLeakage might be a registry key indicating a breach-related activity.

Data Breacch and IoC

Kuiper, Chain of Custody and IoC

Healthcare Use Case – Data Breach Pt.2

7. Behavioral Patterns: Behavioral patterns refer to abnormal activities observed in system logs or network traffic. In a healthcare data breach, these patterns could include unusual access patterns to patient records or abnormal data transfers.

- Example: Unauthorized access to patient records outside of normal business hours could indicate suspicious behavior.

8. Signatures: Signatures are unique identifiers or patterns associated with known malware variants or attack techniques. In a healthcare data breach, signatures can help identify malicious software or attack methods used by cybercriminals.

- Example: Signature for ransomware used in healthcare data breaches could help detect ransomware activity.

9. File Paths: File paths indicate the location of files within a file system. In a healthcare data breach, file paths can identify the location of compromised patient records or other sensitive data.

- Example: C:\Data\HealthcareSystemBreach\PatientRecords might be the file path to a directory containing compromised patient records.

10. Registry Values: Registry values are data stored within registry keys. In the context of a healthcare data breach, suspicious registry values could indicate unauthorized changes to healthcare system configurations or settings.

- Example: Value "LeakedDataPath" set to a non-standard directory could indicate an attempt to hide compromised data.

Kuiper, CoC and IoC

Kuiper, Chain of Custody and IoC

Digital Forensics, Especially Healthcare Domain

1. IP Addresses: List of known malicious IP addresses involved in cyberattacks or hosting malicious content.

- Example: 192.168.1.100, 10.10.10.10, 172.16.0.1

2. Domain Names: Suspicious domain names associated with phishing campaigns, malware distribution, or command and control servers.

- Example: maliciousdomain.com, phishing-site.org, malware-server.net

3. File Hashes: Hash values of malicious files or executables used in cyberattacks.

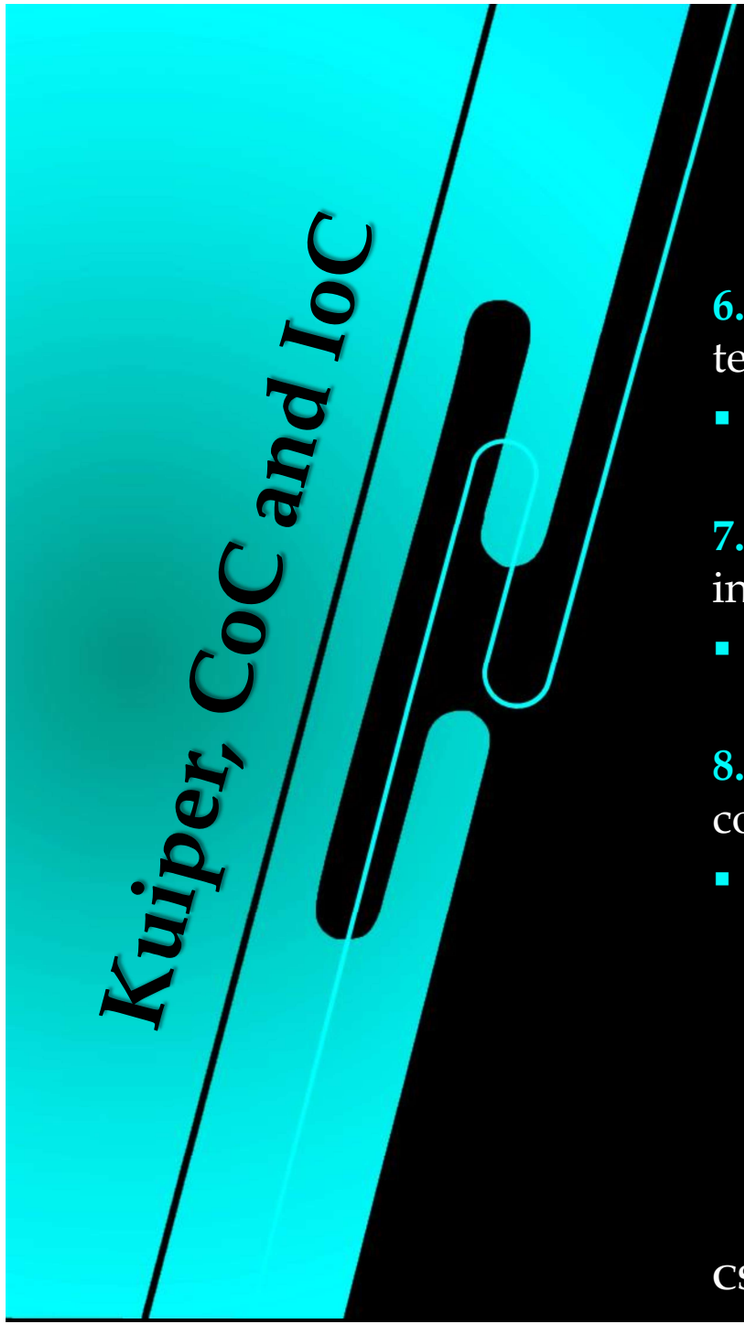
- Example: MD5: d41d8cd98f00b204e9800998ecf8427e, SHA256: 5b73209e4ef5b194c7c52b1fd2c5490aef2f0cd

4. URLs: URLs of malicious websites, exploit kits, or malicious payloads.

- Example: http://maliciouswebsite.com/malware.exe, https://exploit-kit.org/exploit.php?id=123

5. Email Addresses: Known email addresses used for phishing attempts, spam campaigns, or communication with malicious actors.

- Example: phishing@example.com, malware_sender@maliciousdomain.net



Kuiper, Chain of Custody and IoC Pt.2

Digital Forensics, Especially Healthcare Domain

6. **Signatures:** Signatures or patterns of known malware variants, exploit techniques, or attack methods.
   - Example: Signature for a specific ransomware family, pattern for SQL injection attacks.
7. **File Paths:** Paths to files or directories commonly associated with malware infections or unauthorized activity.
   - Example: C:\Windows\System32\malicious.dll, /var/www/html/backdoor.php
8. **Registry Values:** Values within the Windows registry indicating potential compromise or malicious activity.
   - Example: Value "EnableLUA" set to 0 in HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System

RVT2 and Forensics

RVT2 in Forensic Investigations

Digital Forensics, Especially Healthcare Domain

RVT2 automates routine tasks and analysis in forensic investigations, reducing manual effort and increasing efficiency. Tasks include evidence collection, data parsing, artifact analysis, and report generation.

Example Scenario: Suppose a healthcare organization experiences a data breach, leading to the compromise of patient information. Forensic investigators deploy RVT2 to analyze the compromised systems and identify the extent of the breach.

Evidence Collection: RVT2 facilitates the collection of digital evidence from various sources, such as hard drives, memory dumps, and network captures. Investigators use RVT2 to create forensic images of affected servers and workstations for analysis.

Artifact Analysis: RVT2 parses collected artifacts, including file system metadata, registry entries, and network logs, to extract relevant information. Investigators analyze registry hives and event logs to identify suspicious activity patterns and potential entry points for attackers.

Indicators of Compromise (IoC): RVT2 helps identify IoCs, such as unauthorized access attempts, malware signatures, and network anomalies, to understand the attack vector. Investigators use RVT2 to correlate IoCs across multiple systems and pinpoint the initial point of entry for the attacker.

RVT2 and Forensics

RVT2 in Forensic Investigations

USB Data Exfiltration Example

In this scenario, an insider threat within a healthcare organization aims to steal sensitive patient information using USB devices. The attacker, a disgruntled employee with access to patient records, plans to exfiltrate data for personal gain.

Utilizing RVT2 USB Event Parsing Job

- **Input Parameters:** The absolute path to the Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx file containing USB event logs.
- **Execution Flow:** RVT2 parses Windows event files to extract USB-related events, including device insertion and removal timestamps. Relevant USB event data is stored in a JSON format file for analysis and investigation.
- **Analysis:** Forensic analysts leverage the parsed USB event data to identify suspicious USB device insertions and data exfiltration attempts.
- **Investigation:** By correlating USB event timestamps with user activity logs, investigators can attribute unauthorized data access to the insider threat.
- **Response:** The healthcare organization implements stricter USB device usage policies, conducts employee awareness training, and enhances endpoint security measures to prevent future incidents.

Thank you

Presenter: Stylianos Karagiannis (PDMFC, Portugal)

Please send all questions to:
stylianos.karagiannis@pdmfc.com