FORENSIC TOOLS AND TECHNIQUES FOR IOT DEVICES

Presented By: Sanjay Kumar
Class: M.Sc Cyber Security
Enrol. No. 032200300002036

TABLE OF CONTENT

- IoT Defination & Need of IoT Forensics
- Challenges in IoT Forensics Investigation
- Investigation Process of IoT
- Types of Forensics Tools for IoT
- Frameworks for IoT Forensics
- Techniqes for IoT Forensics
- Reference

WHAT IS IOT

The Internet of Things (IoT) refers to a network of interconnected physical devices embedded with sensors, software, and other technologies that enable them to collect and exchange data over the internet

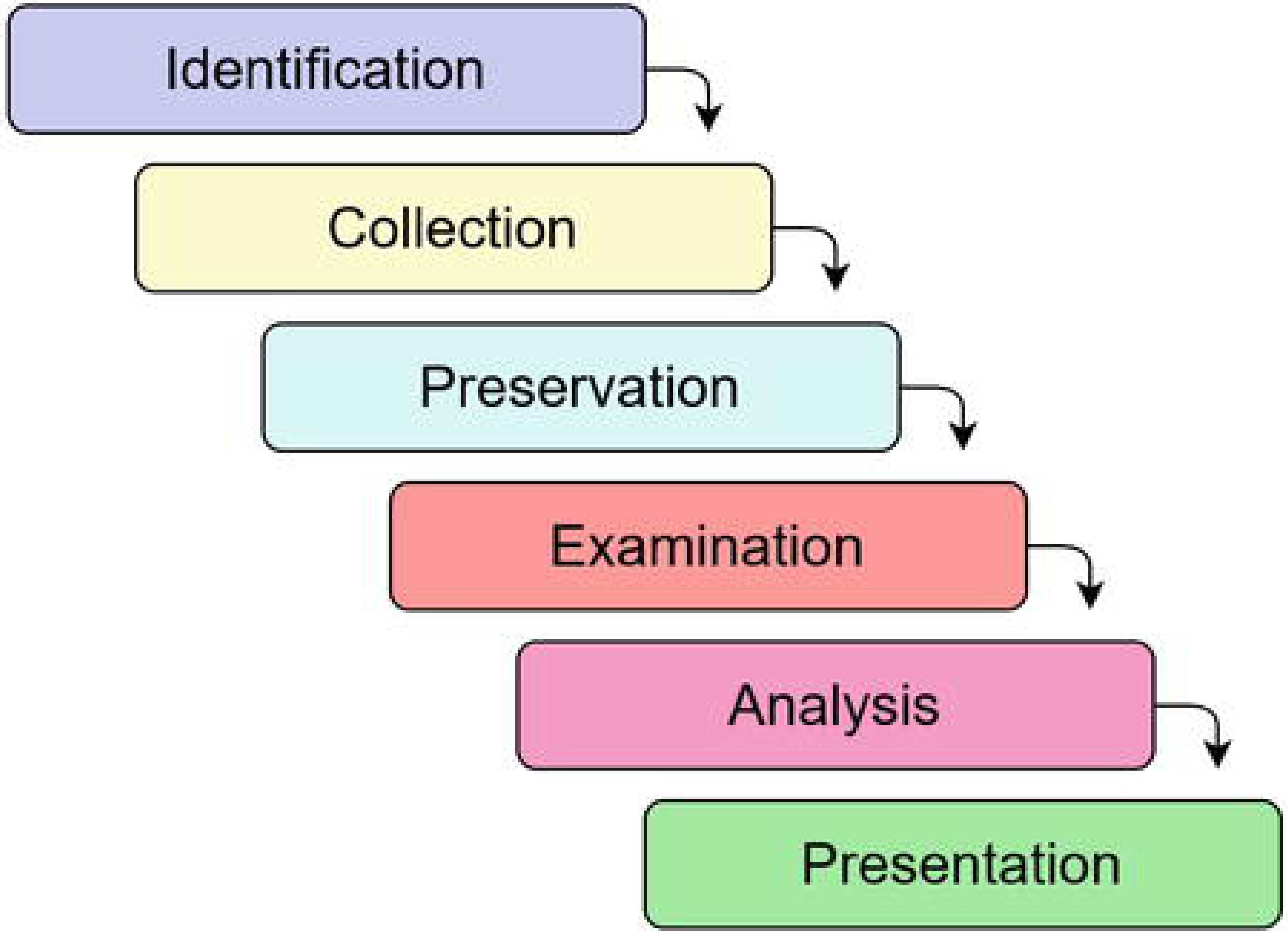
NEED FOR FORENSIC INVESTIGATIONS IN IOT DEVICES

1. Growing Attack Surface
2. Increased Data Collection
3. Emerging Threats and Applications
4. Investigating Cybercrimes
5. Addressing Security Breaches
6. Ensuring Accountability and Legal Compliance

POTENTIAL CHALLENGES IN IOT FORENSIC INVESTIGATIONS

1. Diversity of Devices and Ecosystems
2. Limited Forensic Tools and Expertise
3. Privacy Concerns and Data Collection
4. Rapid Technological Evolution
5. Data Fragmentation
6. Lack of Standardization

Investigative Process for Digital Forensics in IoT



Identification

Collection

Preservation

Examination

Analysis

Presentation

TYPES OF TOOLS

Acquisition Tools:

1. Physical acquisition: Used to directly access the device's memory chips, bypassing the operating system. Examples: Chip-off forensics, JTAG, Serial port analysis.
2. Logical acquisition: Extracts data from the device's storage or filesystem through software interfaces. Examples: Mobile Device Management (MDM) tools, cloud APIs.
3. Network acquisition: Captures network traffic generated by the device, providing insights into its communication activities.

TYPES OF TOOLS

Analysis Tools:

- Memory analysis: Examines the device's volatile memory (RAM) for forensic artifacts, such as malware traces or deleted files. Examples: Volatility, Rekall.
- Filesystem analysis: Investigates the device's storage system for files and artifacts related to the incident. Examples: Autopsy, The Sleuth Kit (TSK).
- Firmware analysis: Analyzes the device's firmware for vulnerabilities or evidence of tampering. Examples: Binary Ninja, IDA Pro.
- Cloud analysis: Analyzes data stored in the cloud associated with the device, such as user logs or sensor readings. Examples: AWS CloudTrail, Microsoft Azure Monitor.
- Threat intelligence: Utilizes information about known threats and vulnerabilities to identify malicious activities on the device. Examples: VirusTotal, MISP.

FRAMEWORKS FOR IOT FORENSICS

Specific IoT Forensic Frameworks:

- Integrated Digital Forensics Investigation Framework (IDFIF): IDFIF is a comprehensive framework developed to streamline and standardize digital forensic investigations across various platforms, including computers, mobile devices, servers, and more. It aims to create a structured methodology for investigators to follow during the investigation process.
- IoT Digital Forensic Investigation Framework (DFIF-IoT): DFIF-IoT is an extension or adaptation of the IDFIF framework that specifically addresses the challenges and complexities associated with conducting forensic investigations on IoT devices.

ADDITIONAL TECHNIQUES

- Sandboxing: Runs suspicious code in a safe environment to analyze its behavior without affecting the live device.
- Emulation: Mimics the behavior of the device's hardware and software for testing and analysis purposes.
- Reverse engineering: Analyzes the device's firmware and software to understand its functionality and identify vulnerabilities.

CASE STUDY

Smart Home Murder Case:: In 2019, a smart home speaker recording was used as crucial evidence in a murder investigation. The recording captured audio of the victim arguing with the suspect, providing strong evidence against the accused.

Forensic Investigation:

- Investigators used specialized tools to extract the audio recording from the smart speaker's internal storage.
- Audio forensics techniques were employed to analyze the recording for authenticity and enhance crucial details.
- This evidence proved instrumental in solving the case and securing a conviction.

Effectiveness of Tools and Techniques:

- Specialized data extraction tools ensured the integrity of the evidence while retrieving the audio recording.

REFERENCE

- **A Metamodeling Approach for IoT Forensic Investigation:** https://www.mdpi.com/2079-9292/12/3/524
- **Investigation process of IoT forensics:** https://www.researchgate.net/publication/335493014_Investigation_Internet_of_Things_IoT_Device_using_Integrated_Digital_Forensics
- **Internet of Things(IoT) digital forensic investigation model: Top-down forensic approach methodology:** https://2totallypsychedhome.files.wordpress.com/2018/11/top-down.pptx
- **A Review on the Internet of Things (IoT) Forensics: Challenges, Techniques, and Evaluation of Digital Forensic Tools:** https://www.intechopen.com/online-first/86010

THANK YOU