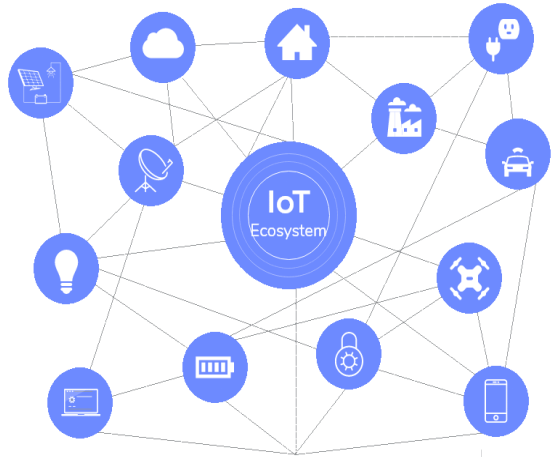
Unit 5:
IoT Forensics



Dr. Ujjaval Patel

Assistant Professor (IOT/SCADA)

ujjaval.patel@nfsu.ac.in

+91 987 987 9746

Unit Outlines:

- Introduction to IoT Forensics
- Forensic Investigation of IoT Devices
- Need of IoT Forensic
- Levels of IoT Forensic
- IoT Forensic Phases
- Forensic Tools & Techniques

IOT Forensics

- The IoT Forensics could be perceived as a subdivision of the Digital Forensics.
- IoT Forensics is a relatively new and unexplored area.
- The purpose of the IoT Forensics is similar to the one of the Digital Forensics, which is to identify and extract digital information in a legal and forensically sound manner.

The need of IOT forensics

- ***Extensive attack surface***

  Despite all the benefits and the wide prospects of IOT, some IOT technologies are particularly vulnerable to cyber-attacks.

  IoT devices with public interfaces are exposed to greater risk levels because they could bring a malware to the private network from a less secure public space [2].

- ***New cyber-physical security threats***

  Using IoT technology, virtual crimes could step across the limit of cyberspace and threaten human life.

  E.g.: US FDA published a warning that certain pacemaker models are vulnerable to hacking .

- ***Contains Digital traces***

  IoT devices which is able prove or disprove certain hypothesis, and could, help the forensics professionals find answers and reconstruct the crime scene [3].

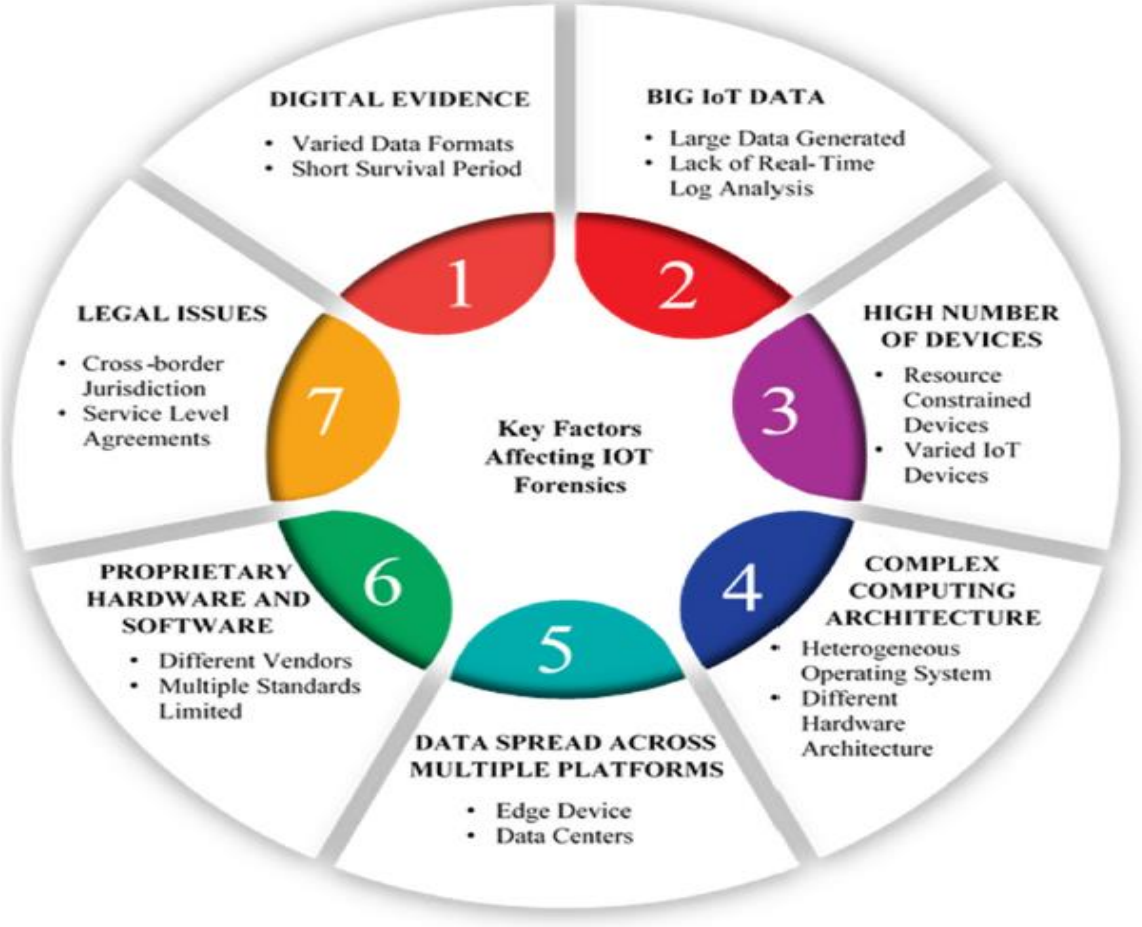
Categories of Evidences With Respect To A Crime Scene

1. **Smart devices and sensors :** It includes sensors, smart devices, automation tools those are powered by IoT Architecture, in other words, **the gadgets those are present in the Crime Scene**.

2. **Hardware and Software : Communication link** between smart devices and the external world which includes IPS, Firewalls, Computers.

3. **External resources : Areas outside networks under investigation**, that includes Cloud, Social Media, ISPs, Network Providers.

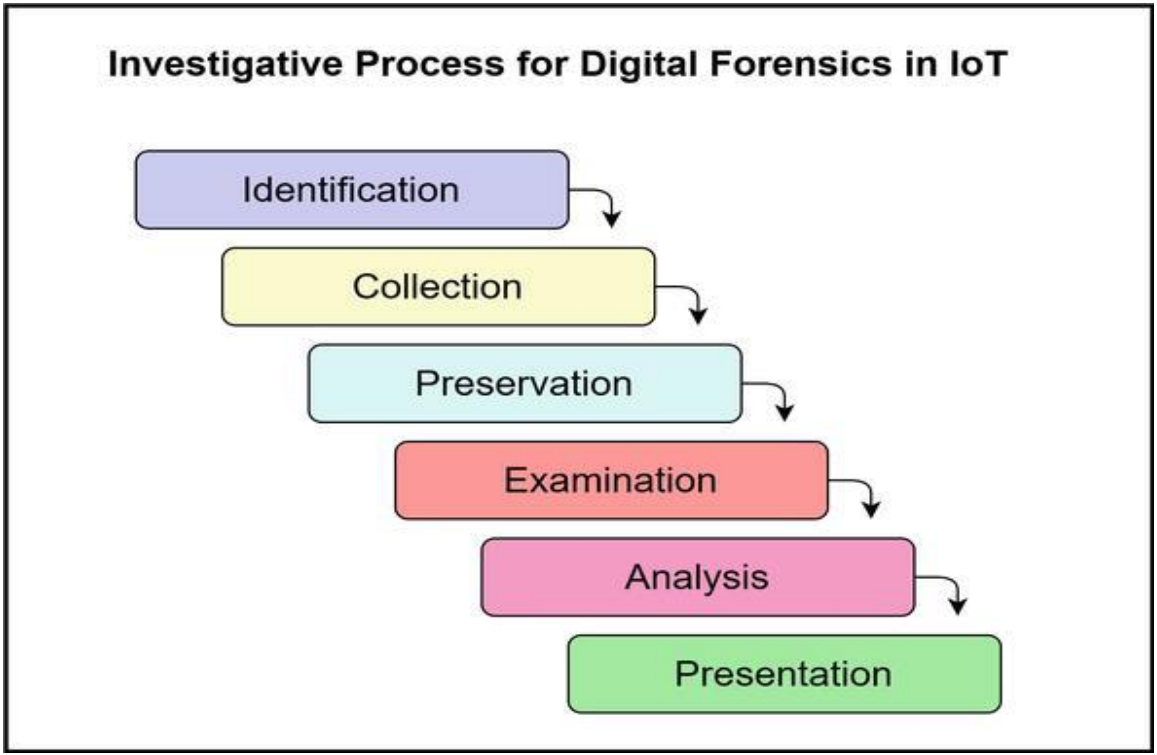
Reference:- https://hub.packtpub.com/iot-forensics-security-connected-world/


DIGITAL EVIDENCE
• Varied Data Formats
• Short Survival Period
1
BIG IoT DATA
• Large Data Generated
• Lack of Real-Time Log Analysis
2
HIGH NUMBER OF DEVICES
• Resource Constrained Devices
• Varied IoT Devices
3
COMPLEX COMPUTING ARCHITECTURE
• Heterogeneous Operating System
• Different Hardware Architecture
4
DATA SPREAD ACROSS MULTIPLE PLATFORMS
• Edge Device
• Data Centers
5
PROPRIETARY HARDWARE AND SOFTWARE
• Different Vendors
• Multiple Standards Limited
6
LEGAL ISSUES
• Cross-border Jurisdiction
• Service Level Agreements
7
Key Factors Affecting IOT Forensics

IoT Forensic:

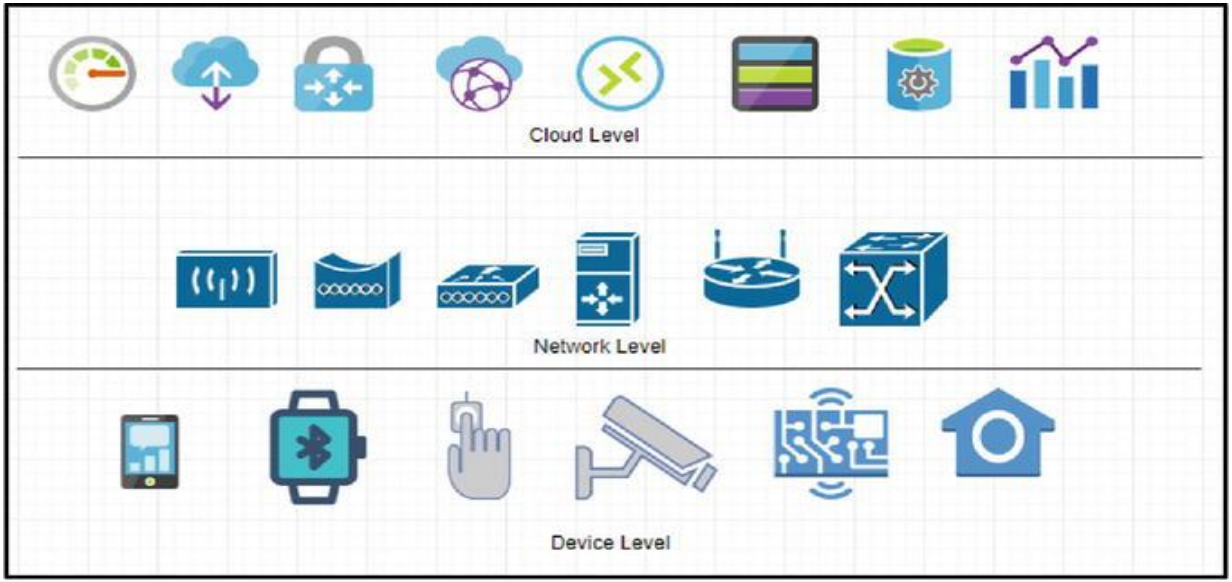
- The extensive connection between IoT devices results in numerous security breaches and violations.
- Due to the increasing prevalence of IoT-related cybercrimes, forensic investigators and researchers face numerous obstacles when attempting to recover evidence from a variety of different types of IoT smart devices.
- The primary challenge in performing forensic analysis on the IoT is the heterogeneity of IoT devices.
- Additionally, the bulk of IoT devices has flash memory or limited memory, which makes generating and converting evidence for presenting forensic data in court is very problematic.

IoT Forensic:



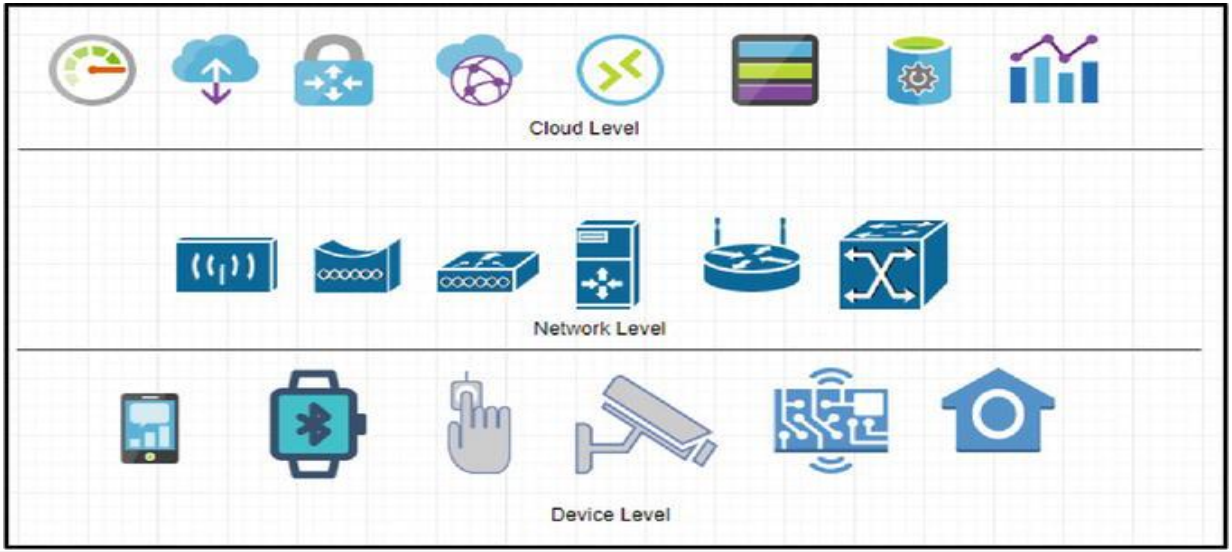
Levels of IoT Forensic:

- IoT forensics consists of three layers:
  - Device Level
  - Network Level
  - Cloud Level



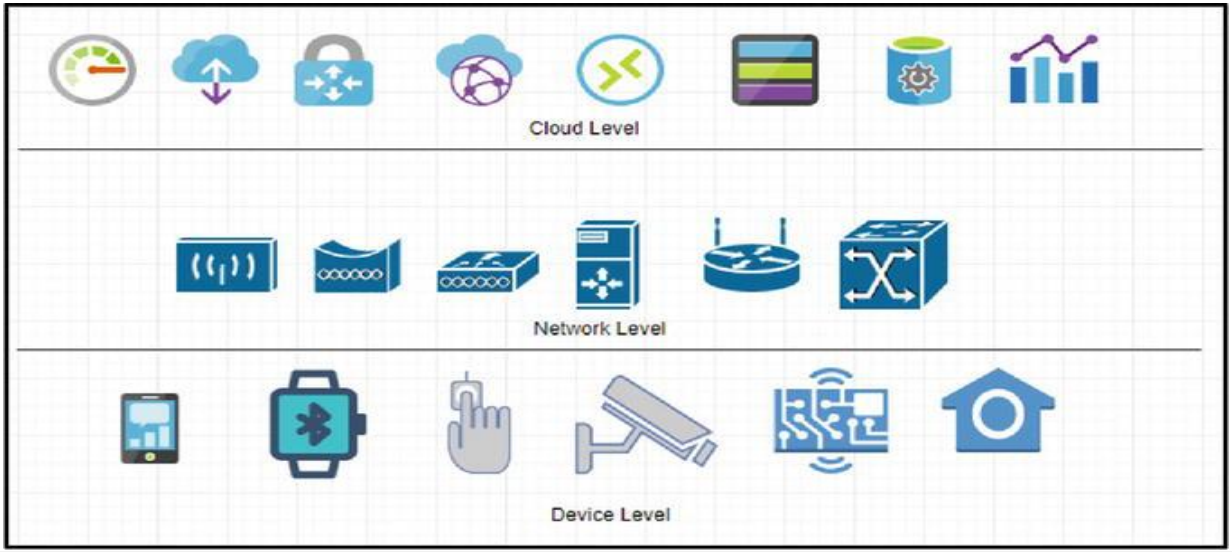
Levels of IoT Forensic: Device Level

- On a device level, forensic investigators collect data directly from the local memory of the physical device for analysis.
- However, due to the low memory capacity and processing power of the majority of IoT devices, collecting historical information can be challenging.



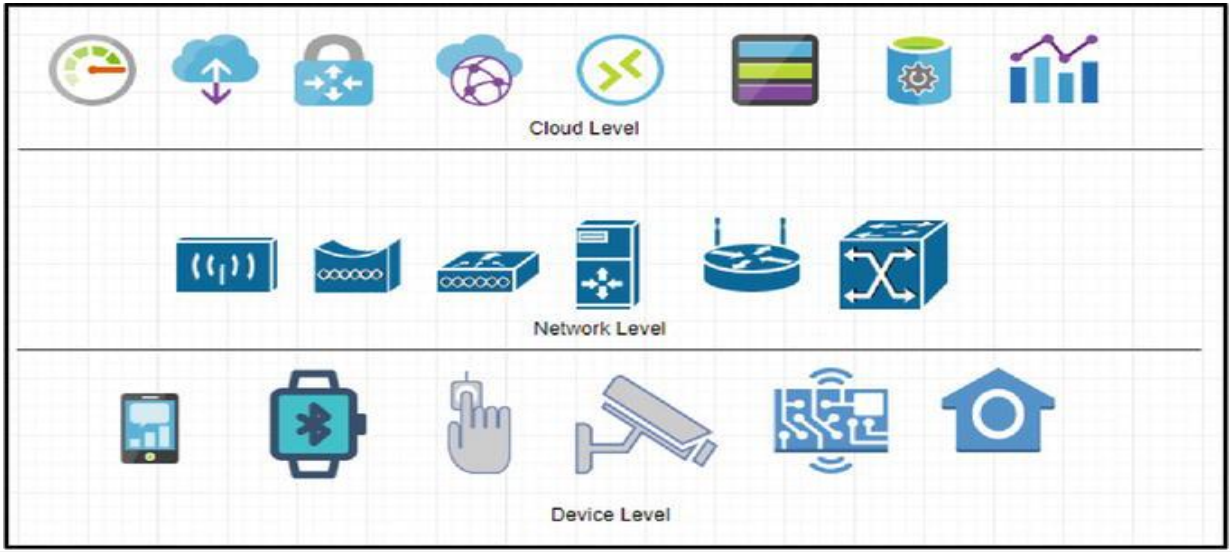
Levels of IoT Forensic: Network Level

- Network-level forensics provides more details, such as traffic logs, which can identify patterns, sources, destinations, or even confirm the identity of a suspect/attacker.



Levels of IoT Forensic: Cloud Level

- Most IoT devices push their data to the cloud servers for storage due to the limited storage and processing capacity of the physical device.
- Data analysis of data stored in cloud, can reveal critical information about the crime scene.



Typical investigation phases

1. Acquisition
2. Recovery
3. Analysis
4. Presentation

Phase 1: Acquisition

- Goal is to recover as much evidence without altering the crime scene
- Investigator should document as much as possible
- Maintain *Chain of Custody*
- *Determine if incident actually happened*
- *What kind of system is to be investigated?*
- *Can it be shut down? Does it have to keep operating?*
- *Are there policies governing the handling of the incident?*
- *Is a warrant needed?*
- *Get most fleeting information first*
  - *Running processes*
  - *Open sockets*
  - *Memory*
  - *Storage media*
- *Create 1:1 copies of evidence (imaging)*
- *If possible, lock up original system in the evidence locker*

Phase 2: Recovery

- Goal is to extract data from the acquired evidence
- Always work on copies, never the original
- Must be able to repeat entire process from scratch
- Data, deleted data, “hidden” data

File systems

- *Get files and directories*
- *Metadata*
  - *User IDs*
  - *Timestamps (MAC times)*
  - *Permissions, …*
- *Some deleted files may be recovered*
- *Slack space*

Phase 2: Recovery

Slack space

- Unallocated blocks: Mark blocks as allocated to fool the file system
- Unused space at end of files if it doesn't end on block boundaries
- Unused space in file system data structures

Steganography

- Data hidden in other data
- Unused or irrelevant locations are used to store information
- Most common in images, but may also be used on executable files, meta data, file system slack space

Encrypted data

- Depending on encryption method, it might be infeasible to get to the information.
- Locating the keys is often a better approach.
- A suspect may be compelled to reveal the keys by law.

Phase 2: Recovery

Encrypted data

- Depending on encryption method, it might be infeasible to get to the information.
- Locating the keys is often a better approach.
- A suspect may be compelled to reveal the keys by law.
- Locating hidden or encrypted data is difficult and might even be impossible.
- Investigator has to look at other clues:
  - Steganography software
  - Crypto software
  - Command histories

File residue

- Even if a file is completely deleted from the disk, it might still have left a trace:
  - Web cache
  - Temporary directories
  - Data blocks resulting from a move
  - Memory

Phase 3: Analysis

- Methodology differs depending on the objectives of the investigation:
  - Locate contraband material
  - Reconstruct events that took place
  - Determine if a system was compromised
  - Authorship analysis

Locating material

- Requires specific knowledge of file system and OS.
- Data may be encrypted, hidden, obfuscated
- Obfuscation:
  - Misleading file suffix
  - Misleading file name
  - Unusual location

Event reconstruction

- Utilize system and external information
  - Log files
  - File timestamps
  - Firewall/IDS information
- Establish time line of events

Phase 3: Analysis

- Methodology differs depending on the objectives of the investigation:
  - Locate contraband material
  - Reconstruct events that took place
  - Determine if a system was compromised
  - Authorship analysis

Locating material

- Requires specific knowledge of file system and OS.
- Data may be encrypted, hidden, obfuscated
- Obfuscation:
  - Misleading file suffix
  - Misleading file name
  - Unusual location

Event reconstruction

- Utilize system and external information
  - Log files
  - File timestamps
  - Firewall/IDS information
- Establish time line of events

Phase 4: Presentation

- An investigator that performed the analysis may have to appear in court as an expert witness.
- For internal investigations, a report or presentation may be required.
- Challenge: present the material in simple terms so that a jury or CEO can understand it.

Investigator Profile

- Understanding of relevant laws
- Knowledge of file systems, Microcontrollers, Protocols and its communication
  - Where are the logs, what is logged?
  - What are possible obfuscation techniques?
  - What programs and libraries are present on the system and how are they used?
- Know what tools exist and how to use them
- Create more meaningful audit data
- Ensure integrity and availability of audit data
- Develop detection techniques
- Develop automation processes

Challenges in IoT Forensics

- The IoT Forensics field is encountering an array of challenges, none of which has a simple solution.

  - General Issues.
  - Evidence Identification, Collection and Preservation issues.
  - Evidence Analysis and Correlation.
  - Presentation

General Issues

- Lack of a methodology and framework for IoT forensics.
- There is a lack of appropriate tools for IoT forensics.

Impact

- Could contaminate or destroy evidence.
- Absence of common forensic model could jeopardize the trust and agreements in cross jurisdictional investigations.

Evidence Identification, Collection and Preservation issues

- Detecting the presence of IoT systems, and identification of IoT devices that can provide evidence in an investigation.
- Lack of training for first responders.
- Wide range of software and/or hardware specifications.
- Lifespan limitations

Evidence Identification, Collection and Preservation issues

Impact

- Data could be easily overwritten.
- The responding officers often neglect or shut down the system directly, without first creating the necessary forensic image.

Evidence Analysis and Correlation

- Overwhelming amount of data that an IoT system might produce.
- Time Lining and Limited Correlation of Evidence.
- Data provenance -Less certainty about data ownership and modification history.
- Metadata – vast majority of IOT devices do not store any metadata.

Evidence Analysis and Correlation

Impact

- The amount can be overwhelming for an investigator and the tools used.
- Creating a time-line can be challenging.

Presentation

- Jury most probably has only basic understanding of cloud computing and forensics.
- It would be a challenging task to explain to them the technicalities behind such a complex architecture in the very limited time of the trial.
- Will the court accept the methodology and tools used since they are not yet standardized.

Presentation

Impact

- if an investigative body chooses unsuitable methods for acquisition it can harm the data integrity and can easily be challenged in Court due to omissions in the way of collection.

IOT FORENSICS METHODS AND TOOLS

- There are very few tools designed specifically for IOT forensics
- There is no unique methodology to investigate in a IOT environment
- None of the approaches has been widely accepted by the forensics community.
- Most of the approaches are still of theoretical nature.

Perform standard data acquisition

- Various proven techniques and procedures for Digital forensics are still applicable to IoT devices.
- if an IoT device can be connected to a computer, the internal storage of the device can be forensically imaged.
- Various Digital forensic tools are available to perform standard data acquisitions

  e.g.:
  - FTK Imager
  - X-ways forensics
  - ENCASE
- More practical and cost effective method [4], [5]

Perform standard data acquisition

Limitations

- In IoT forensics, where traditional investigative techniques & tools have a very low success rate.
- Useless against Proprietary echo systems e.g.: apple, amazon.
- Occasionally, formats of the collected data are invalid or vendor specific.

Interface testing

- Most IoT devices have web interfaces.
- Can get general knowledge of how the system works
- By testing the interface investigators can validate whether the relevant digital evidence is present and its condition.
- Investigators can identify any indicators of compromise.

Limitations

- Can lead to accidental contamination of evidence.

Oxygen Forensic Detective

- Oxygen Forensic Detective is an all-in-one forensic software platform.
- Able to extract, decode, and analyze data from multiple digital sources mobile and IoT devices, device backups, drones, and cloud service.
- Oxygen Forensic offers data extraction from two popular IoT devices based on Amazon & Google.
- Can performs logical acquisition from smart-wearables (apple watch, Fitbit, Samsung Health).

Oxygen Forensic Detective

Limitations

- Its support for range of devices is limited.
- It uses a brute force technique which can take a lot of time to complete the process.
- Oxygen Forensic suite is very expensive.

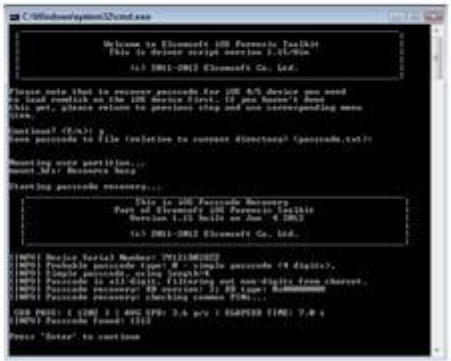
OXYGEN FORENSICS

Elcomsoft iOS Forensic Toolkit

- Perform full file system and logical acquisition for Apple ecosystem devices.
- The toolkit provides jailbreak-free forensic extraction
- Inbuilt write blocker.

Limitations

- Only supports Apple devices



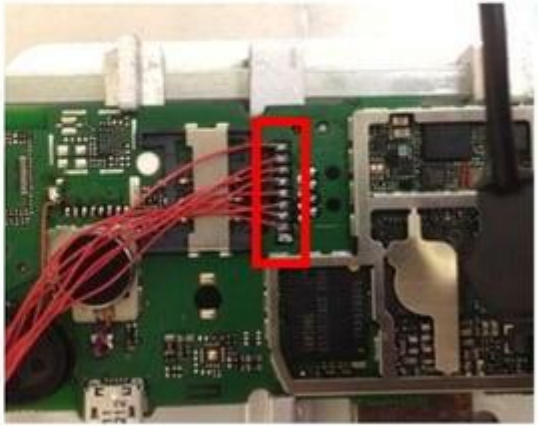
Firmware data extraction by JTAG

- JTAG stands for Joint Test Action Group is a common hardware interface that provides a way to communicate directly with the chips on a board.
- The port was initially designed for testing PCB (Printed Circuit Boards).
- JTAG Forensics involves acquiring firmware data using standard Test Access Ports (TAPs).
- Doesn't require specific data cables for each make/model.
- The data is transferred in a raw format.
- Able to recover data from damaged devices. [5]

Firmware data extraction by JTAG

Limitations

- it's difficult to find out the entire JTAG pin
- Not all Devices have a JTAG enabled chip.
- Forensics image creating process is slow.
- Need expert knowledge in electronics.



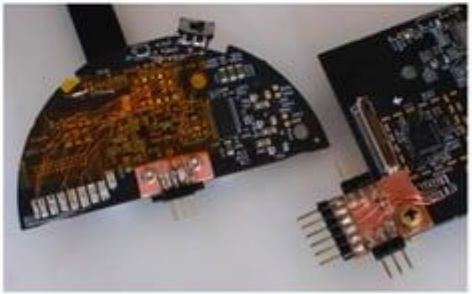
Firmware data extraction by UART

- UART is Universal Asynchronous Receiver/Transmitter.
- UART is a widely used method.
- It is a hardware device which is a part of Integrated circuitry and used for serial communications.
- UART converter translates serial data into readable data via USB.
- Hardware complexity is low. [5]

Firmware data extraction by UART

Limitations

- It can accidently reset the devices to factory settings resulting in loss of data.
- Size of a data frame is limited to 9 bits.



Cloud-based IoT Forensic Toolkit

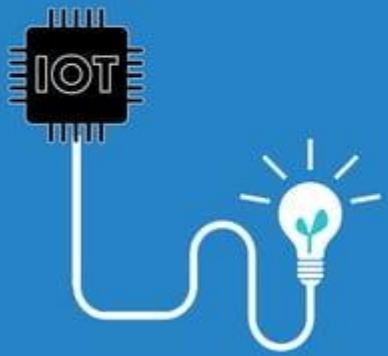
- Alexa is a cloud based assistant, it manages through a mobile application or the web.
- Previously, methods such as disassembling the Amazon Echo device and unofficial Alexa APIs to access cloud data were used.
- Researchers utilized mobile applications and web browsers to retrieve additional artifacts from the client to automate this process of data collection, visualization and evaluation [8]

Cloud-based IoT Forensic Toolkit

Limitations

- New technology.
- Concerns about evidence Integrity.

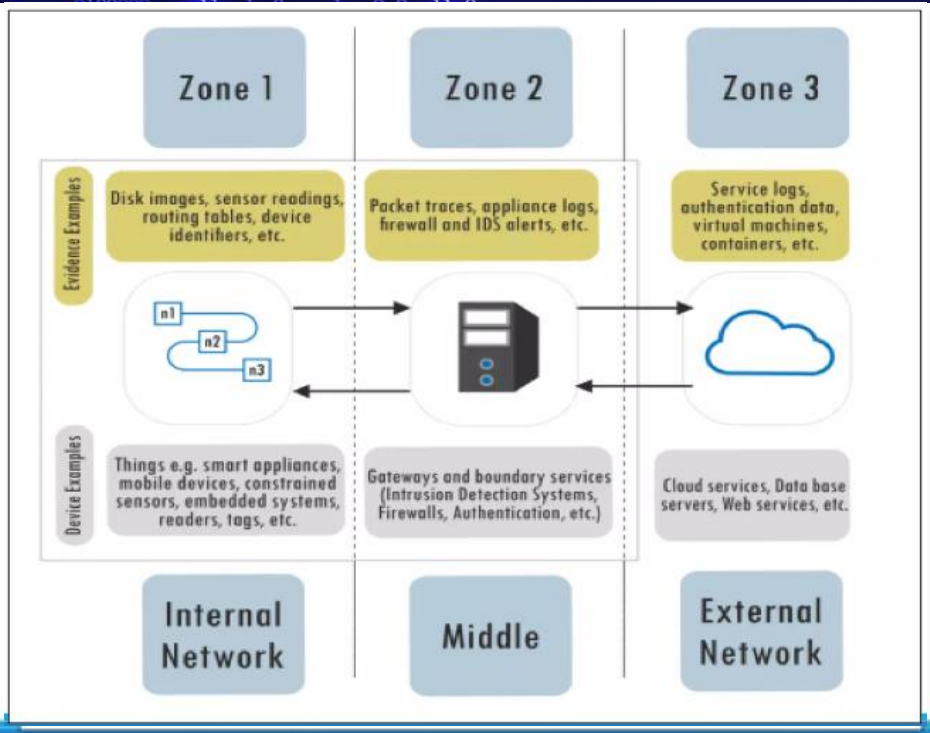
Future Developments



- IoT forensics is a new area open for research. There is already a need for practical solutions to questions that arise during investigations that include IoT.
- Therefore, researchers and forensics professionals work hard to present new tools and methodologies that could mitigate IOT forensic challenges.

The 1-2-3 Zones Approach

- 1-2-3 zones are correspond to three areas of IoT forensics: device, network and cloud.
- This method makes it is easier to plan and systematize an IoT investigation.
- Reduces the complexity and the timing of investigations,
- All zones can be investigate in parallelly or a zone of greatest priority can be investigated first. [6]


Zone 1
Zone 2
Zone 3
Evidence Examples
Disk images, sensor readings, routing tables, device identifiers, etc.
Packet traces, appliance logs, firewall and IDS alerts, etc.
Service logs, authentication data, virtual machines, containers, etc.
n1
n2
n3
Device Examples
Things e.g. smart appliances, mobile devices, constrained sensors, embedded systems, readers, tags, etc.
Gateways and boundary services (Intrusion Detection Systems, Firewalls, Authentication, etc.)
Cloud services, Data base servers, Web services, etc.
Internal Network
Middle
External Network

IOTdots

- IoTDots general architecture divides into two parts:

IoTDots - Modifier (ITM)

- performs source code analysis of smart applications
- Detects relevant forensic information
- The tracing logs are stored in an IoT database

IoTDots - Analyzer (ITA)

- uses the log information stored in the IoT database with data processing and machine learning techniques to perform forensic investigation. [1], [5], [6]

Reference

[1]Avoine, G. and Hernandez-Castro,J., n.d. Security of Ubiquitous Computing Systems.

[2]R. C. Joshi and E. S. Pilli, Computer Communications and Networks Fundamentals of Network Forensics A Research Perspective. 2016.

[3]D. Quick and K. K. R. Choo, 'IoT Device Forensics and Data Reduction', IEEE Access, vol. 6, pp. 47566–47574, 2018.

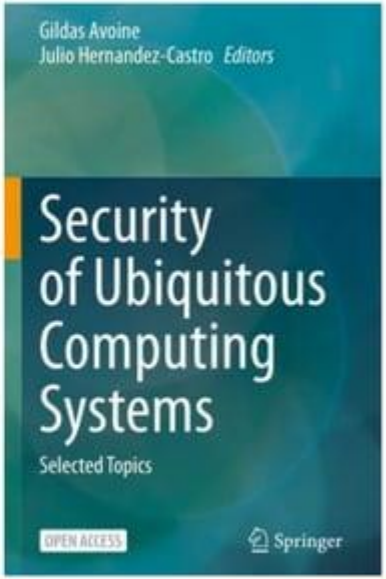
[4]Slideshare.net. 2021. Iot forensics. [online] Available at: <https://www.slideshare.net/AbeisAb/iot-forensics-117926663.

[5]Linkedin.com. 2021. Internet of Things Forensics: Challenges and Approaches. Evaluation of Digital Forensic Tools. [online] Available at: <https://www.linkedin.com/pulse/internet-things-forensics-challenges-approaches-tools-hamal-b-k

[6] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis and E. K. Markakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues," in IEEE Communications Surveys & Tutorials,

[7] S. Zawoad and R. Hasan, 'FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things',

[8] Hyunji Chung, Jungheum Park, and Sangjin Lee. Digital forensic approaches for amazon alexa ecosystem. Digital Investigation, 22:S15–S25, 2017.



THANK YOU !!!