IOT FORENSICS

TOOLS & TECHNIQUES

PRESENTED BY NIMITA JOSEPH
ENROLLMENT NO.:032200300003022
MSc DFIS

INTRODUCTION

IoT forensics is the process of collecting, analyzing, and preserving digital evidence from Internet of Things (IoT) devices. With the increasing use of IoT devices in our daily lives, the need for IoT forensics has become more important than ever. IoT forensics helps investigators to retrieve data from IoT devices and analyze it to solve crimes.

CHALLENGES FACED BY FORENSIC INVESTIGATORS

01. **Data acquisition:** The ambiguity of data location, data acquisition, and the diversity of devices are some of the main challenges that forensic investigators have to overcome in any forensics investigation.

02. Data analysis: The huge volume and heterogeneous information and borderless cyber infrastructure pose new challenges in modern digital forensics.

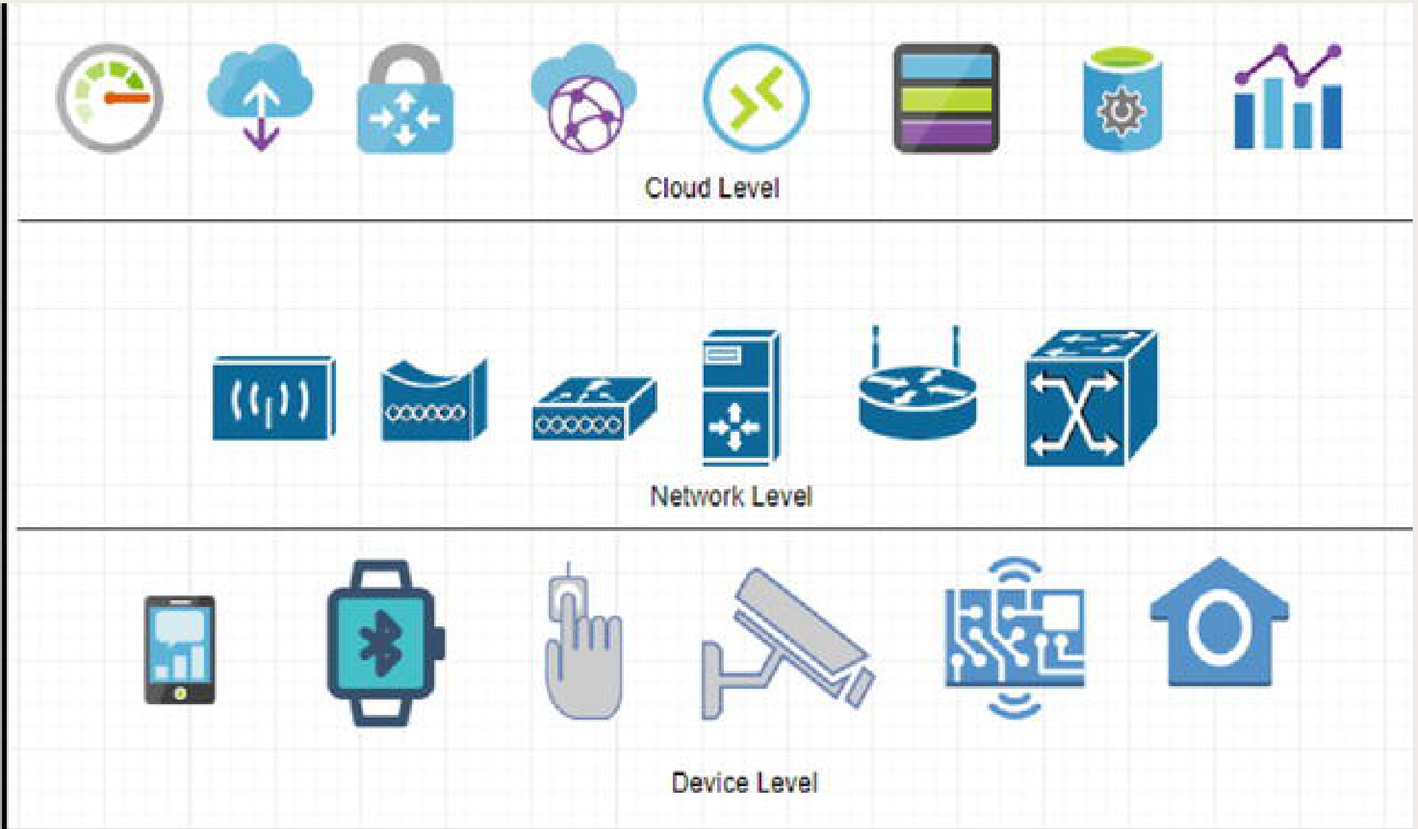
03. Lack of adequate forensics tools: There is a lack of adequate forensics tools for IoT devices, which makes it difficult for forensic investigators to retrieve data from IoT devices.

04. Privacy Concerns:
IoT devices often collect sensitive personal information, raising privacy concerns.Balancing the need for forensic analysis with protecting user privacy is a delicate challenge.

REF: https://link.springer.com/chapter/10.1007/978-3-030-60425-7_10

TECHNIQUES USED IN IOT FORENSICS

Levels of investigation in IoT forensics.



01. Device level: Forensic investigators collect data directly from the local memory of the physical device for analysis. Some common techniques used in this layer include memory analysis and file system analysis

02. Network level: Forensic investigators analyze the network traffic generated by IoT devices. This technique can help investigators identify the source of an attack and the data that was stolen. Network analysis is a technique used to analyze the network traffic generated by IoT devices

03. Cloud level: Forensic investigators collect data from the cloud environment where data is mostly stored and processed on the cloud environment, which makes it difficult to retrieve data from IoT devices. Some common techniques used in this layer include cloud forensics and data recovery

TOOLS USED IN IOT FORENSICS

1. Device level:

FTK Imager

Widely used and trusted tool for creating forensic disk images. It is used in the device level of IoT forensics to collect data directly from the local memory of the physical device for analysis.

Oxygen Forensic Detective

An all-in-one forensic software platform built to extract, decode, and analyze data from multiple digital sources: mobile and IoT devices, device backups, UICC and media cards, drones, and cloud services.

Autopsy

An open-source digital forensics platform that includes features for filesystem analysis, keyword searching, and timeline analysis. Supports the analysis of disk images and filesystems, including file recovery and metadata examination.

2. Network Level:

Wireshark

Widely used network protocol analyzer that allows forensic investigators to capture and analyze network traffic generated by IoT devices.

Tcpdump

Command-line tool that allows forensic investigators to capture and analyze network traffic generated by IoT devices.

NetworkMiner

Network forensic analysis tool that can be used to parse PCAP files and extract files and metadata from network traffic.

3. Cloud Level:

Cellebrite UFED Cloud Analyzer

Allows you to extract and analyze data from cloud services such as iCloud,GoogleDrive,and Microsoft OneDrive. Can potentially extract messages,alerts,orcommunication logs from these cloud services, revealing important information about the IoT devices' activities.

Amazon S3 Inspector

A tool provided by AWS for inspecting and analyzing data stored in Amazon S3 buckets.Can be used to examine objects, metadata, and permissions within S3 storage, potentially uncovering evidence related to IoT devices.

Elastic Stack

Comprises of Elasticsearch, Logstash, and Kibana, is a powerful open-source platform for searching, analyzing, and visualizing log data.Can be used to aggregate and analyze logs from various cloud services, gaining insights into the activities and communications of IoT devices.

CASE STUDIES

1. Domestic violence case: In 2019, a man was arrested in the United States for domestic violence after data from his smart home devices was used as evidence against him. The data showed that the man’s story was inconsistent with the data collected by his smart home devices, which helped investigators establish his guilt .
2. Insurance fraud case: In 2020, a man was convicted of insurance fraud in the United Kingdom after data from his smartwatch was used as evidence against him. The data showed that the man’s story was inconsistent with the data collected by his smartwatch, which helped investigators establish his guilt .

THANK YOU VERY MUCH!