Advanced Digital Forensics

Casey Donaldson

CMP416: Advanced Digital Forensics

2024/25

Note that the Information contained in this document is for educational purposes.

.

Contents

.

.

1 INTRODUCTION

1.1 BACKGROUND

Digital forensics is an ever-growing science and with the increase of IoT devices, the need for improved forensics resilience is mandatory as IoT devices normally introduce additional attack surfaces. This report covers an investigation that was approved by the smart city network which operates lots of IOT services. They approved the investigation after one of their smart homes was compromised. The smart home contains a smart TV, thermostat, smart lighting, and Security cameras. The smart home is further provided with a router and a firewall. The smart home was also connected via the internet using internet links connected to their default gateway(router). The incident was alerted by the homeowner after noticing several symptoms of being hacked, the most notable was the increased temperature of the thermostat.

This report will inform readers on how to investigate a smart network using a 5-step strategy, identification, preservation, analysis, presentation and documentation. The report has identified evidence which should be acquired and from what device, these include routers, firewalls, IoT devices and more. The attack mentioned in this report highlights the challenges and implications of current forensics investigations.

1.2 AIM

This report aims to provide an in-depth analysis of a theoretical investigation covering a compromised smart home. Below are the objectives of this report.

1. Discover vulnerabilities from all devices within the network and plausible causes of the breach taking into consideration 802.11 standards, IoT devices, the infrastructure of the network and more.
2. Create and highlight the strategies for obtaining digital evidence and analysing the evidence.
3. Evaluate challenges which may be faced during the investigation.
4. Critically analyse results, and implications, providing a clear conclusion.

1.3 OVERVIEW

This report is broken down into four main sections.

1. Acquisition and investigation strategy
2. Critical evaluation
3. Reflective component
4. Conclusion

2 ACQUISITION AND INVESTIGATION STRATEGY

2.1 METHODOLOGY.

This investigation will follow 5 steps to secure digital evidence and determine the probable cause of the breach. This strategy starts with **identification**. This stage allows the investigator to identify any device that may hold information that could be useful in the investigation. After the evidence has been identified the next stage is **preservation.** This stage ensures the investigator collects the evidence and does not change or tamper with the evidence upon collecting the data. **Analysis** will start once all the data is collected and stored, ready for the analysis to start. **Documentation** will be done throughout the investigation, taking note of everything that is found to allow the courts to reproduce the result. The final stage is the **Presentation** stage which includes summarizing the findings and concluding what and how the evidence was found in simple terms so the judge and jury can make a decision based on facts. Below is a summary of the stages which this investigation will follow, see Figure 4.

- **Identification** is the stage where the investigators identify any device that may hold information relating to the incident. The information will be further examined to find what format the data is in and whether analysis of the evidence is helpful to the investigator.
- **Preservation** is the stage where the identified evidence is collected safely to ensure the data collected is a bit-by-bit replica of the original data.
- **Analysis** is the stage where the evidence will be examined in a forensically sound environment to determine what happened and in what order to create a factually correct story of the cyber incident.
- **Documentation** is the stage where all the data collected and examined is documented to ensure that the evidence is legitimate and reproducible for the courts.
- **Presentation** is the stage where a summary of the findings is presented in layman's terms, so the outcome of the investigation is satisfactory for all parties.

2.2 IDENTIFICATION AND PRESERVATION

While securing the area several devices that could hold valuable information were identified and shown in Appendix A – Devices and their respective evidence. There is a summary of the devices and their respective data which could contain evidence.

The firewall should be examined and any log files and configurations including rules should be captured and stored. After this, data preservation should be completed by copying an image of the firewall and logs for further traffic analysis. Once the data from the firewall is collected the router should be examined. The router contains log files, network traffic, running configuration, and saved configuration, and the router's firmware and version should be verified.

Several smart devices including smart lighting, smart TVs, and a smart thermostat. These devices should all contain logs which should be captured for further analysis. All firmware and information of these devices should be noted and verified to ensure the firmware is not modified. The smart TV might have accounts linked to itself. These accounts should all be noted and audited to ensure no further attacks are performed against these accounts. The thermostat might contain activity logs that could indicate when the threat actor first increased the temperature. Finally, any traffic relating to IOT traffic should be captured and further analysis should be performed on the traffic.

Security cameras were also on-premises, these systems should contain activity logs and video footage. These should be collected for further analysis. The last object to be examined is the centralized management system for any log files or network traffic used to maintain the network by administrators. Configuration, recent activity, and any databases from the system should be logged and captured for analysis. This platform could be an entry point into the network and thus the whole system should be vetted for any IOC.

2.3 ANALYSIS

Once all the data from the above section has been identified, found, and captured securely without altering the data, an analysis of the data is needed to further the investigation. During this stage, a high-priority aspect is the creation of a timeline, as this can help identify when incidents happened and in what order (Chabot, 2015).

2.3.1 Log Analysis

The firewall, router, IoT devices, and management system should all contain types of logs relating to their activities. Log analysis should follow the OSCAR methodology to correctly identify and gather the required logs, Figure 1. Below is a summary of which logs can contain evidence.

- Network traffic which could give details on IP addresses, session durations, logins, and large data transfers.
- IoT logs with timestamps of commands and changes to the status of the devices. These could be changes to temperature or video playbacks. Additionally, any remote login attempts.
- Firewall and router logs can hold information like SSID changes, and login attempts either into the admin panel or into the network. Additionally, these logs could indicate blocked traffic, and these logs are crucial for identifying the attacker's point of entry.

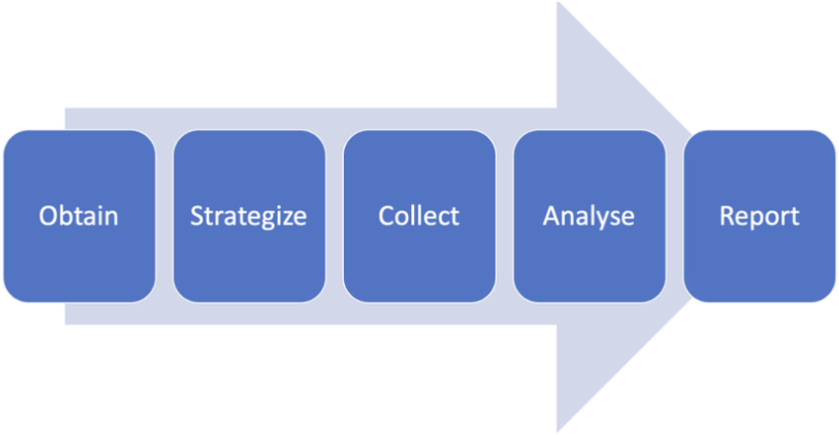


Figure 1 OSCAR methodology was taken from (Researchgate, 2024).

2.3.2 Traffic Analysis

Any traffic which is still present within the network should be analysed by using Wireshark and Snort. This could reveal any files being downloaded, and any IP addresses which are involved. Furthermore, traffic analysis could indicate suspicious domains, ".RU" for example.

2.3.3 Configuration Analysis

Each device has a certain configuration, and an in-depth analysis of these configurations could indicate changes and plausibly any vulnerability introduced due to the changes.

2.4 IDENTIFYING SECURITY WEAKNESSES

This section will cover several plausible vulnerabilities that could be present within the network.

2.4.1 IoT Vulnerabilities

IoT devices are commonly used throughout networks however they are often deployed with minimum security. Below are some common vulnerabilities that should be checked to establish a plausible entry route for the hacker.

- **Firmware** should be checked to see if the devices are up to date. If the devices are not up to date, then hackers can exploit these systems with known vulnerabilities or new attacks.
- **Default credentials**, including IoT devices (thermostats, cameras, and TVs), should be checked throughout the network. This is because IoT devices are sent with factory-set credentials that can be easily found, enabling threat actors to compromise the system.
- **Weak encryption** should be checked as some IoT devices use outdated cypher suites, leaving their data in transit exposed to attackers.

To reduce these vulnerabilities and identify plausible causes of the breach, conducting an audit of all IoT devices documenting firmware versions, current settings, and encryption methods could reveal the above vulnerabilities. Additionally using Wireshark to analyse traffic originating from the IoT devices could alert the investigator on suspicion patterns if the traffic is present.

2.4.2 Wireless Network Vulnerabilities

Most networks utilise wireless traffic however, this introduces a new attack vector. Since the SSID has been changed this indicates that wireless vulnerabilities could have been exploited.

- **Weaknesses in WPA2** could be present. While the protocol used is unknown anything less than WPA3 is considered weak. In WPA2 the KRACK attack could be used to manipulate the handshake and could allow the hacker to perform further malicious activities (Vanhoef, 2017).
- **SSID Tampering** could have been done to mislead the investigator or disrupt legitimate traffic connections.
- **The Evil Twin Attack** could have been employed to fake the SSID and steal credentials to the network. These attacks mimic the actual network's SSID to trick users into using the "fake" access point to send data (Bauer, McCoy and Gonzales, 2015).

Capturing wireless traffic and analysing 802.11 (wireless traffic standard) frames to detect unusual devices. Additionally using Aircrack-ng to test the WP2 configuration and check the encryption strength (Aircrack-ng, 2009).

2.4.3 Firewall and Router Configuration Vulnerabilities

Since the threat actor changed the SSID this also suggests that the router's admin panel has been exploited. The firewall's interface and rules might have been changed or re-configured.

- **Firewall Rules** could have been misconfigured or changed enabling the threat actor to bypass the security device, as per Figure 2.
- **Weak or Default Admin** passwords for the router's login could have been exploited.

Analysing the router's logs for unauthorised login attempts or configuration changes could reveal the initial attack. Furthermore, reviewing the firewall rules and configurations to identify any weaknesses within the devices could find entry points to the network.

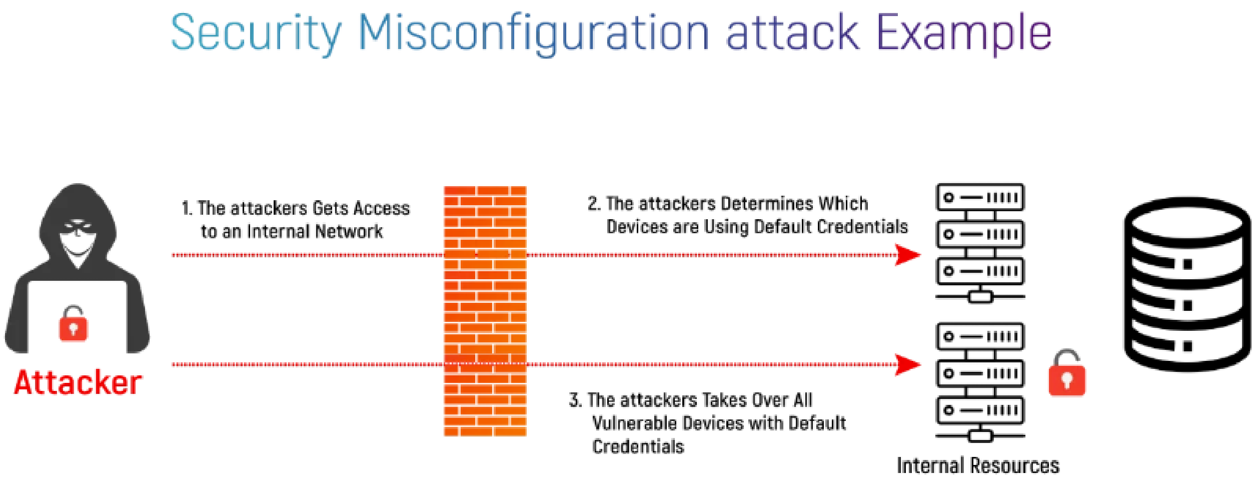

Security Misconfiguration attack Example
Attacker
1. The attackers Gets Access to an Internal Network
2. The attackers Determines Which Devices are Using Default Credentials
3. The attackers Takes Over All Vulnerable Devices with Default Credentials
Internal Resources

Figure 2 Diagram depicting hacker bypassing a firewall, taken from (Natchiar M, 2023).

3 CRITICAL EVALUATION

The first IOC (indicator of compromise) is the thermostat stuck at an uncomfortable temperature. The second IOC is the SSID for the Wi-Fi which has changed. These indicate that the network is compromised. The plan for the investigation has some challenges which should be evaluated.

3.1 EVIDENCE VOLATILITY

A challenge in IoT forensics is evidence volatility. IoT is usually small and efficient but does not perform large amounts of logging due to storage reasons. This limit makes the IoT data volatile which can affect investigations. Below are some challenges with solutions on how to mitigate the risk.

- Short Retention Periods
    - Logs on IoT devices may only retain recent activities creating gaps and causing issues in the timeline reconstruction.
    - IoT devices have small memory and often rewrite their cached data more often causing important data to possibly be lost.

To mitigate this risk the network has been disconnected which should limit how much data is lost on the IoT device. Also, deploying Centralized logging using the centralised management system could prevent loss of log evidence.

- Devices shutting down or rebooting
    - Hackers can wipe IoT device volatile data by simply gaining access and rebooting the device. Login attempts to certain devices might be lost if a hacker reboots the system.

This challenge has to be accepted. Using tools specific to IoT devices could enable the investigator to recover specific data from the device but this is unlikely depending on the storage.

3.2 ENCRYPTED TRAFFIC

Encryption is mandatory for secure communication and to ensure user privacy. However, this also introduces new challenges for investigators see below.

- Limited access to encryption keys and the payload data.
    - Without access to the decryption key then the data is encrypted, this means that only metadata like packet size, timing, and addresses are readable. The payload data is obfuscated which means the payload could be malicious but is difficult to identify.

To combat this challenge analysing clear metadata to find suspicious patterns throughout the traffic could identify IPs which are involved in the compromise. Additionally, deploying statistical flow analysis could identify spikes throughout the traffic. For example, using SiLK to analyse the flow and find anomalies (Carnegie Mellon University, 2024).

3.3 EVASION TECHNIQUES

Established hackers can use techniques to avoid detection. This affects the overall duration of the digital forensics investigation and could also mislead the investigation, below are the evasion challenges which are faced in this investigation.

- Log Tampering
  - If hackers can access the logs, they might be able to alter and delete these logs causing the investigation to be misleading and evidence to be lost.

In the future implementing tamper-proof logging could identify if the log has been tampered with using digital signature detection. Alternatively, employing integrity verification using hashes could also help to identify log tampering.

- Use of VPNs and Proxies
  - It is highly likely that the attacker used a virtual private network(VPN) or proxy to obfuscate their IP address. The diagram below visually shows the differences between a VPN and no VPN, (Anfalovas, 2021).

Using a behavioural analysis approach and focusing on finding patterns that appear to be malicious activity such as login attempts during off hours. This approach can help to narrow down suspects even if the attacker is using proxies and VPNs throughout the attack.

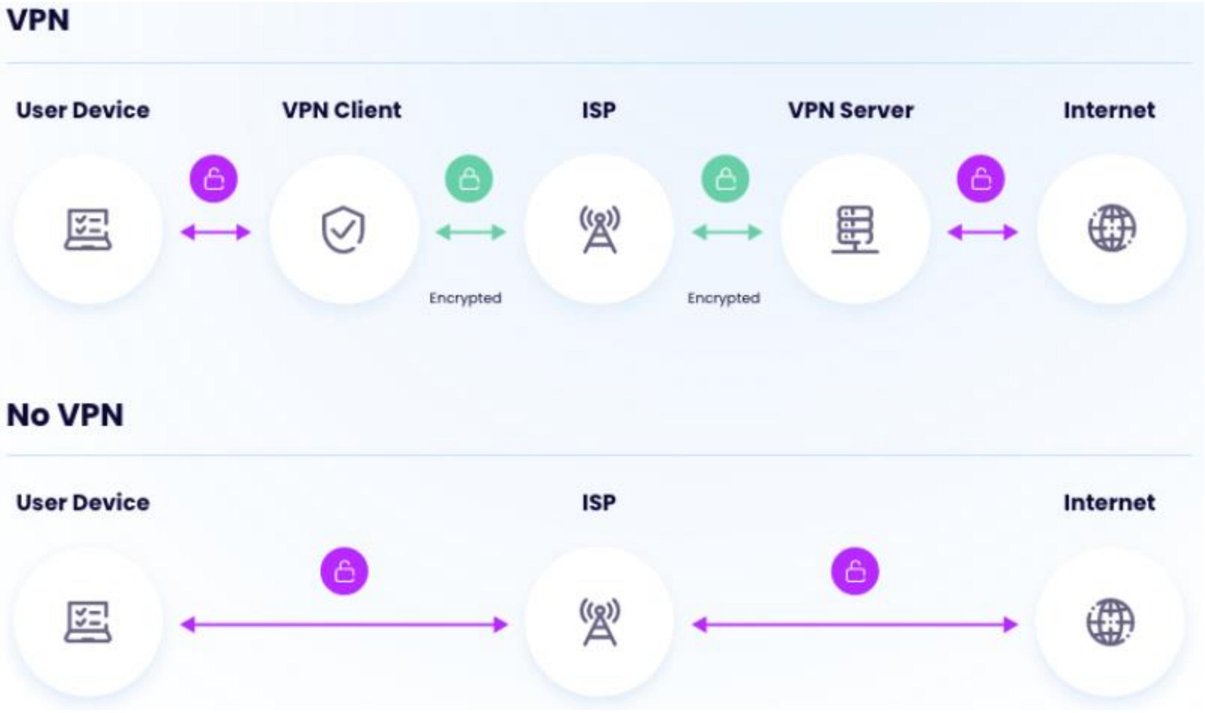


Figure 3 Diagram depicting the change of a network connection with and without a VPN connection, taken from (Anfalovas, 2021).

4 REFLECTIVE COMPONENT

4.1 IMPACT OF ATTACKER BEHAVIOUR

Threat actors use techniques to hinder forensics investigations. Using vulnerabilities within the network to hide their actions and identity. This behaviour affects the data acquisition of evidence and affects the duration of the investigation. Additional anti-forensics techniques can be read at Appendix D – Further Anti-Forensics Techniques.

4.1.1 Wireless 802.11 Exploitation

Wireless access points and networks are ideal entry points for hackers. The SSID was changed causing connectivity issues, this IOC suggests that further attacks were used over the 802.11 standard.

- KRACK attack
  - The key reinstallation attack (KRACK) exploits WPA2 encryption, this attack is utilised could allow the hacker to gain access to password-protected systems by intercepting and decrypting the traffic.
- The Evil Twin Attack
  - This attack is achieved by implementing a fake access point and naming it after the SSID. This could then redirect traffic to the hacker's network. This could allow hackers to intercept data and change and inject data into the network.

These are considered short-term attacks and would require a traffic capture and tools like Wireshark or Tcpdump to investigate, without a proper investigation, vital evidence is likely to be missed.

4.1.2 Log Tampering

Logs hold some of the most vital evidence during an investigation. Unfortunately, hackers target logs to delete or manipulate them to conceal their activity.

- Deletion
  - Hackers may delete log entries; these could be login attempts or configuration changes. This makes data collection severely harder to perform.
- Log Manipulation
  - Altering the logs can mislead the narrative, altering times to hide the actual time of the breach or alternating legitimate entries to make natural traffic look suspicious and divert the investigator away from the actual malicious traffic.

4.1.3 Honeypot Avoiding

Honeypots are often used to help identify and stop cyber-attacks. If the current network contains a honeypot, the hacker may employ techniques to prevent detection.

- Fingerprinting techniques
  - Hackers can use a behaviour analysis approach. Identifying anomalies in response time to identify false systems. This allows the hacker to avoid these traps.

4.2 IMPLICATIONS

4.2.1 Implications from Challenges

The techniques used by the hackers highlight that the compromise might have been done by a proficient hacker. As this network utilises IoT devices then the lack of comprehensive tamper-proof logging makes this investigation vulnerable to data manipulation, additional challenges exist see below.

- Attackers who tamper with the logs and exploit the wireless communication will prolong the investigation which will cause delays for the incident response team.
- Volatile data, missing logs and encrypted traffic can create gaps in the timeline due to the lack of evidence, this issue can make it harder to identify specific incidents and devices involved.
- VPNs and Proxy allow the hackers to obscure their identities, adding more complexity to the investigation.

4.2.2 Improving forensics resilience

When hackers use advanced techniques, the network must employ several strategies to mitigate the overall impact of the compromise.

- Improved logging through the network should be implemented. This included centralized logging to improve retention. Using tamper-proof logging techniques can help reduce the risk of evidence being tampered with or deleted. Moreover, using Spunk could allow users to perform real-time analysis of the logs helping to identify attacks early on.
- Using network intrusion prevention systems and network instruction detection systems could help identify malicious traffic in real-time. This will help prevent malicious activity like SSID changes.
- IoT devices should undergo mandatory updates and annual reviews to reduce vulnerabilities including secure default configuration and improved logging.
- Advance honeypots should be utilised. Advanced honeypots mimic legitimate traffic more closely and are harder to detect. These honeypots can capture traffic which can help digital forensics investigations. Additionally, the use of a honeynet to fake an entire home network should be considered.

5 CONCLUSION

5.1 CONCLUSION

In conclusion, the report has given a comprehensive overview of how an investigation of the smart network would be conducted. The report focuses on data acquisition, security weaknesses and challenges which might be faced in this report. Also, this report discusses the hacker's ability to perform further malicious actions like data manipulation.

During the consideration of the vulnerabilities in the smart network, several were identified. Like default credentials, weak encryption, outdated software, KRACK attacks and many more. The report has also tied CVEs to the identified vulnerabilities. Furthermore, this report has emphasized the importance of data acquisition and analysis. As this network contained several sources of evidence including several IoT devices, it is proven to be difficult, with data volatility for example.

Likewise, technical challenges arise from anti-forensics techniques which have been used. These are log tampering, VPNs, honeypot fingerprinting and many more. These techniques make the investigation longer and more complex. During the report countermeasures to these techniques were mentioned. These include tamper-proof logs, statistical analysis etc. Despite these issues, the investigation strategy has given out recommendations to help mitigate these issues, like centralised logging for retention.

This theoretical report has provided an in-depth review of the vulnerabilities within the smart network. As IoT devices grow in networks so will the attack vectors. This shows why forensics resilience should be considered to safeguard the network's infrastructure. By addressing these challenges, the smart network will become more resilient. Lastly, the procedures and strategy set out should uncover the cause of the compromise and affected systems.

6 REFERENCE LIST

Ahadi, S.A.A., Rakesh, N. and Varshney, S. (2020). Overview On Public Wi-Fi Security Threat Evil Twin Attack Detection. *2020 IEEE International Conference on Advent Trends in Multidisciplinary Research and Innovation (ICATMRI)*. doi:https://doi.org/10.1109/icatmri51801.2020.9398377.

Aircrack-ng (2009). *Aircrack-ng*. [online] Aircrack-ng.org. Available at: https://www.aircrack-ng.org/ [Accessed 5 Dec. 2024].

Anfalovas, I. (2021). *What Is An IP Address? A Comprehensive Guide To Internet Protocol*. [online] IPXO. Available at: https://www.ipxo.com/blog/what-is-an-ip-address/ [Accessed 9 Dec. 2024].

Bauer, K., McCoy, D. and Gonzales, H. (2015). *IEEE Xplore Full-Text PDF:* [online] Ieee.org. Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4745081 [Accessed 5 Dec. 2024].

Carnegie Mellon University (2024). *SiLK*. [online] Cert.org. Available at: https://tools.netsa.cert.org/silk/ [Accessed 5 Dec. 2024].

Chabot, Y. (2015). *Construction, Enrichment and Semantic Analysis of Timelines: Application to Digital Forensics*. [online] *Google Scholar*, p.266. Available at: https://www.researchgate.net/profile/Yoan-Chabot/publication/292152348_Construction_Enrichment_and_Semantic_Analysis_of_Timelines_Application_to_Digital_Forensics/links/56ab530408aed814bde9ac9d/Construction-Enrichment-and-Semantic-Analysis-of-Timelines-Application-to-Digital-Forensics.pdf [Accessed 30 Nov. 2024].

Jackson, M., Jackson, M. and Jackson, M. (2024). *New SSID Confusion Attack Exploits General WiFi Vulnerability*. [online] ISPreview UK. Available at: https://www.ispreview.co.uk/index.php/2024/05/new-ssid-confusion-attack-exploits-general-wifi-vulnerability.html [Accessed 6 Dec. 2024].

Mitre.org (2017). *CVE - CVE-2017-13077*. [online] Mitre.org. Available at: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13077 [Accessed 6 Dec. 2024].

Mitre.org (2018). *CVE - CVE-2018-6402*. [online] Mitre.org. Available at: https://cve.mitre.org/cgi-bin/cvename.cgi?name=2.3.2.CVE-2018-6402 [Accessed 6 Dec. 2024].

Mitre.org (2019). *CVE - CVE-2019-11642*. [online] Mitre.org. Available at: https://cve.mitre.org/cgi-bin/cvename.cgi?name=2.3.2.4.4.4.CVE-2019-11642 [Accessed 6 Dec. 2024].

Natchiar M, R.B. (2023). *What Is Security Misconfiguration?* [online] Prophaze.com. Available at: https://prophaze.com/learning/rajeswari-baby/security-misconfiguration/ [Accessed 9 Dec. 2024].

Noman, H.A., Abu-Sharkh, O.M.F. and Noman, S.A. (2024). *IEEE Xplore Full-Text PDF:* [online] Ieee.org. Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10623179 [Accessed 6 Dec. 2024].

Researchgate (2024). *Researchgate*. [online] ResearchGate. Available at: https://www.researchgate.net [Accessed 5 Dec. 2024].

salvationdata (2024). *What are the key steps in the digital forensics process?* [online] Salvation DATA. Available at: https://www.salvationdata.com/knowledge/digital-forensics-process/ [Accessed 5 Dec. 2024].

Vanhoef, M. (2017). *KRACK Attacks: Breaking WPA2*. [online] Krackattacks.com. Available at: https://www.krackattacks.com/ [Accessed 5 Dec. 2024].

Yaacoub, J.-P.A., Noura, H.N., Salman, O. and Chehab, A. (2021). *Digital Forensics vs. Anti-Digital Forensics: Techniques, Limitations and Recommendations*. [online] arXiv.org. doi:https://doi.org/10.48550/arXiv.2103.17028.

APPENDICES

APPENDIX A – DEVICES AND THEIR RESPECTIVE EVIDENCE

Router

- Volatile evidence
  - Routing table
  - Saved packets for forwarding
  - Packet count and statistics
  - ARP table
  - Running configuration
  - I/O and processor memory.
- Non-volatile evidence
  - OS image
  - Boot loader
  - Stored configuration
  - Access logs
  - DHCP logs

Firewall

- Volatile evidence
  - Routing tables
  - ARP tables
  - Running configuration
- Non-volatile evidence
  - Boot load
  - Stored configuration
  - Access logs
  - DGCP logs
  - Firewall rules
  - Alert logs if present

Smart security cameras

- Non-volatile evidence
  - Saved camera recordings

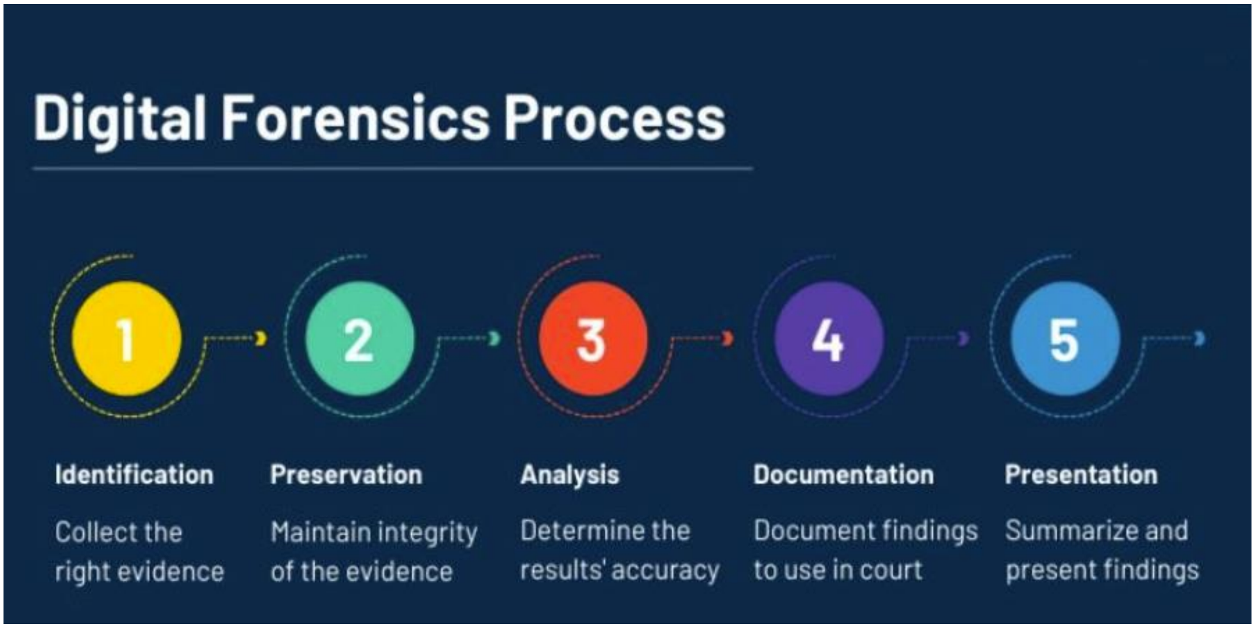
Smart IOT devices

- Thermostat
- Tv
  - The TV and thermostat could contain data surrounding network traffic, device logs, and cloud data.

Centralized administrator security panel.

- Any logs and network traffic from this system could be paramount to ensure no evidence is missed.

APPENDIX B – FORENSICS PROCEDURES


Digital Forensics Process

1 Identification
Collect the right evidence

2 Preservation
Maintain integrity of the evidence

3 Analysis
Determine the results' accuracy

4 Documentation
Document findings to use in court

5 Presentation
Summarize and present findings

Figure 4 Digital forensics process, taken from (salvationdata, 2024).

APPENDIX C – CVES RELATING TO VULNERABILITIES WITHIN THE NETWORK

While examining the plausible vulnerabilities several CVEs relating the current state of the network. These CVEs are not concrete until the investigation has concluded but the investigation should verify that these CVEs are not contained within the network. Below is a summary of these vulnerabilities, see references for sources.

1. CVE-2017-13077
   - This vulnerability is related to the KRACK attack. This attack allows the hacker to reinstall the encryption keys. This attack allows threat actors to decrypt data and also allows them to perform further malicious actions like inserting malicious traffic into the stream.
2. CVE-2018-6402
   - This vulnerability is related to the Evil Twin attack. In this vulnerability, the hacker must create a fake access point which allows them to trick users of the network to use their internet connections. This attack allows the hacker to decrypt the traffic and perform man-in-the-middle (MitM) attacks.
3. CVE-2023-52424
   - This vulnerability is related to the SSID confusion attack. Similar to the above vulnerability but more recent and is known for being highly malicious. For this attack to work the hacker must trick the user into trusting their network. Additionally, there must also be a similar network present with the same authentication credentials. Lastly, the attacker must be in range to perform the MitM attack.

4. CVE-2019-11642
    - This attack allows hackers who have gained authentication to insert malicious payloads into log files.
5. CVE-2017-13078 and CVE-2017-13080
    - These attacks are both related to the KRACK attack suite. They enable the hacker to exploit the reinstallation of the encryption keys in WPA2. Allowing the hacker to decrypt data, inject malicious data or even hijack the session.

APPENDIX D – FURTHER ANTI-FORENSICS TECHNIQUES

Below are further anti-forensics techniques which should be considered throughout the investigation.

- Port Spoofing
    - Port Spoofing is a technique used by hackers to avoid being detected. Using specific tools like hping3, a hacker could spoof (change) the port they are using to bypass firewalls and other security devices. This prolongs investigations and could mislead investigators. An example of this could be sending malicious traffic through port 1234 but altering the port to port 80 to bypass the firewall as website traffic. To counteract this, you can perform traffic monitoring using IDS/IPS to detect anomalies, these can be port 80 traffic which is not acting like port 80 traffic.
- Steganography
    - Steganography is a method used by hackers and other computer enthusiasts to hide data in images and videos. This can be achieved by using advanced tools or manually changing the least significant bit in the picture for each byte until the data is encapsulated. This decreases the chances of hackers being detected by IDS/IPS or by deep packet inspections. Additionally, this method also impedes an investigation.
- Traffic Obfuscation
    - Hackers can obfuscate their traffic by using different tools like I2P or techniques, these can be packet padding where additional padding is added to each packet or by using randomization techniques. Hackers attempt to utilize these techniques to anonymize or hide malicious traffic.
- Packet Manipulation and Injection
    - Hackers might be injecting false data or manipulating the traffic to create false alerts for investigators. The purpose of this is to mislead monitoring systems and analysts by generating false network events and logs.
- MAC Address Spoofing
    - These anti-forensics techniques allow hackers to avoid detection and prevent being tracked by investigators by changing the MAC address of a network interface to a different identity. These risks can be reduced by monitoring the network for unusual patterns or multiple different devices/IPs using the same MAC address.

- DNS Tunnelling
    - Hackers have been able to encode data within DNS queries and responses. The purpose of this is to exploit DNS data which is usually trusted and minimally monitored.
- DDoS Attacks
    - Hackers can overload the network traffic by sending large amounts of data through the network. Which can disrupt legitimate network traffic and also hinder forensics investigations and real-time monitoring. Using properly configured firewalls can prevent DDoS attacks.
- Use of Covert Channels
    - When using wireless access points or other communication protocols which have several channels, some of which are uncommon, then the chance of a hacker using these increases. These channels can be timing channels for example. The reason why hackers use these is to hide their communication and avoid detection. This technique can further impede investigations by avoiding evidence acquisition.