Digital Forensic Challenges in Investigating Air-Gapped Infrastructure Attacks

Achyutha Sri Sai Koushik[1], K.V. Ravikumar[2]*

[1]Undergraduate Student, School of Forensic Science, Centurion University of Technology and Management, Andhra Pradesh

[2]Professor, Dean of School of Forensic Science, Centurion University of Technology and Management, Andhra Pradesh

*Corresponding Author:

K.V. Ravikumar[2]

Professor

Dean of School of Forensic Science

Centurion University of Technology and Management,

Andhra Pradesh- 535003

Email: kvravikumar09@gmail.com

How to Cite this Article:

Koushik, A. S. S. (2026). Digital Forensic Challenges in Investigating Air-Gapped Infrastructure Attacks. International Journal of Creative and Open Research in Engineering and Management, 02(6). https://doi.org/10.55041/ijcope.v2i6.213

License:

This article is published under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author(s) and the source are credited.

© The Author(s). Published by International Journal of Creative and Open Research in Engineering and Management.

https://doi.org/ 10.55041/ijcope.v2i6.213

Abstract

The quick digitalisation of the key infrastructure and industry control systems has contributed to a high level of operational efficiency, automation, and connectivity. Nevertheless, it is this technological reliance that has also led to an increase in the cyber threat environment, especially when it comes to systems that handle critical services like power, industrial production, defence, and water cleanup. These environments are the most sensitive of them all; one being the air-gapped systems, which are based on physical isolation in protecting critical missions. Although they believe that their infrastructure is safe, real-life experience has shown that even air-gapped infrastructure can fall prey to advanced cyberattacks. The given paper is a detailed analysis of hacking methodology and the specifics of infrastructure hacking in air-gapped systems. It categorically examines the nature of hacking in terms of intent and legality, such as ethical hacking, malicious hacking, hacktivism, cyber espionage, insider threats and supply chain attacks. The paper also discusses the special attack vectors used against air-gapped systems, including infected removable media, breached maintenance systems, insider activities, and supply chain weaknesses. One of the key contributions of this paper is the fact that it provides an in-depth examination of how the forensic investigation process is conducted in air-gapped infrastructure attacks. It identifies the problems of the limited logging, the constraints of the operation, and the safety-critical environment, and the significance of the multidisciplinary approach to forensics. Digital forensics, malware and memory analysis, industrial control system forensics,

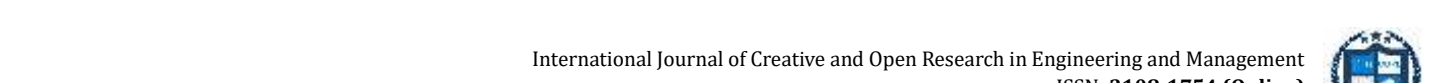
firmware and hardware analysis and correlation of cyber-physical systems are comprehensively discussed. The paper shows limitations of physical isolation and the importance of forensic intelligence in protecting infrastructure by discussing real-world cases like Stuxnet, German steel mills attack and the intrusion of the Ukrainian power grid. The results support the need to prepare forensically, adopt an integrated approach to security, and maintain a continuous risk evaluation to protect air-gapped critical infrastructure against the changing cyber threats.

KEY WORDS:

Air-Gapped Systems, Infrastructure Hacking, Cyber Forensics, Industrial Control Systems (ICS), Critical Infrastructure Security.

Introduction

The high rate of adoption of technology in the critical infrastructure, industrial systems, and operations of the organisation in the modern digital age has provided unparalleled ease of performance, connection, and productivity. Nevertheless, this dependence on digital and cyber-physical systems has also created some enormous weaknesses that can be used by evil agents. Hacking, as the general term for unauthorised access to digital systems, networks and devices, has a variety of different types with different motives, methods and consequences. (Chng et al., 2022) These classes of hacking are also critical in understanding not only by cybersecurity professionals but also forensic investigators, industrial engineers, and policy-makers who have to safeguard critical infrastructure and sensitive data. The intent and legality can be used to broadly classify hacking. White-hat hacking, or ethical hacking, is a process whereby professional hackers are employed to evaluate systems in order to find out what can be exploited to breach their security. These tests, like penetration testing, code review of code, and phishing simulation exercises, assist the organisations to tighten their defences and adhere to the regulatory requirements. Black-hat hacking, or malicious hacking, on the other hand, is motivated by personal, political or financial gain, and it usually leads to either breach of data, loss of money or even physical damage. In between these two extremes lies Grey-hat hacking, which resides somewhere in the grey area of morality, where unauthorised access is made without evident malicious intent, but nevertheless, legal and operational risks. There are also other types like hacktivism, cyber espionage and cyber terrorism that emphasise the variety of reasons - ideological propaganda or national security in jeopardy. Hacking of infrastructure, especially in operation and industrial settings, is one of the most complicated and high-stakes problems. (Alsmadi et al., 2022) This notwithstanding, history lessons also demonstrate that air-gapped systems are not resistant to advanced cyberattacks, as witnessed with Stuxnet (2010), the attack on the German steel mill (2014), and the attack on the Ukrainian power grid (2015). These instances prove that even those systems that seem the most secluded may be compromised by attackers who may use such indirect vectors as removable media, insider activities, supply chain attacks, and sophisticated malware. Such attacks are multidisciplinary and challenging to conduct a forensic investigation. Air-gapped systems are also special by nature as there is little logging, operational complexities, and safety-critical settings, and investigators have limited access to the systems. In such cases, digital forensics, malware analysis, memory forensics, hardware and firmware testing, ICS investigation, and physical evidence correlation are all needed in a forensic investigation. When conducted correctly, forensic studies can be used to recreate the manner in which an attack was carried out, identify the culprits, the effects of the operations, and put in place measures to make organisations more resilient. Owing to the growing interdependence of both the digital and cyber-physical systems, the role of forensic intelligence in cybersecurity activities has become indispensable. Comprehending the types of hacking, hacking methods, and methods of forensics is critical to provide defence to critical infrastructure, continuity of operations, as well as human and national security. The paper examines the continuum of hacking, focusing especially on air-gapped systems and infrastructure hacking, and emphasises the critical role of cyber forensics in pre-emptive security and in investigating an incident. (Khan et al., 2024)



1. Types of Hacking

Hacking is a very general term that includes actions that use the vulnerabilities of digital systems, networks or devices. These activities differ in motives, permission, advancement and moral uprightness. Cybersecurity, forensic investigation, and research are not possible without a clear understanding of various forms of hacking.

Figure 1. Types Of Hacking

1.1 Ethical Hacking (White-Hat)

Ethical hacking does the following in critical infrastructure:

Resource and infrastructural hardiness to possible cyber-attacks. Weaknesses are detected early to reduce the risk. Cybersecurity regulatory standards at the national and international levels. Some of the methods employed by ethical hackers are penetration testing, code review, configuration analysis, and simulated phishing campaigns.(Yaacoub et al., 2023) Indicatively, white-hat teams are frequently contracted by power utilities and oil refineries to check their SCADA systems against vulnerabilities before they can be used maliciously.

1.2 Malicious Hacking (Black-Hat)

Unauthorised intrusion that is malicious is known as malicious hacking. Attackers can seek either financial benefit, espionage, political benefits, sabotage, or revenge.(Winkler & Gomes, 2017)

Common techniques include:

The implementation of malware and ransomware. Fraudulent emails against key staff. Malicious use of a zero-day vulnerability. Identity theft and breach. Malicious hacking has high stakes when targeted at critical infrastructure, such as the disruption of services, loss of finances, and threats to human lives. The Stuxnet attack on the nuclear facilities of Iran (2010) is one of the high-profile attacks that can demonstrate the destructive power of specific cyberattacks on the industrial control system.

1.3 Grey-Hat Hacking

Grey-hat hackers are working in a grey ethical space. They can gain access to systems that are unauthorised, but without any blatant intention of being malicious. Although not all Grey-hat hackers will disclose the vulnerabilities in a responsible manner, their acts are still unlawful and may negatively affect the running of

operations or sensitive information inadvertently. Companies should therefore prepare for expected as well as non-hypocritical threats during security implementation procedures.

1.4 Hacktivism

Hacktivism is politically driven hacking, which is usually geared towards awareness creation or social/political advocacy. Common methods include: Website defacement, Data leaks, DDoS attacks, and spread-out denial-of-service attacks.(Singh & Jain, 2024) Social media manipulation, Hacktivist activities, albeit peaceful, may interfere with the functioning of the population, harm the reputation of organisations, and change the political discussion. The most prominent case is the cyber campaigns organised by Anonymous against governmental websites and corporations based on ideological grounds.

1.5 Cyber Espionage

Cyber espionage is a clandestine action of stealing politically, military or corporate secrets. Intrusion is frequently carried out over a long period of time using advanced persistent threats (APTs) and zero-day exploits.(Salim et al., 2023) Examples of targets can be strategic industrial research, defence planning or intellectual property. Consequences include: Theft of proprietary technology. Geopolitical Disadvantage in Strategy: Weak national security.

1.6 Cyber Terrorism

Cyber terrorism is used to apply fear, panic or disruption to a society by attacking critical infrastructure.(Iftikhar, 2024) The targets are usually common to power grids, transport, and emergency services. Those consequences tend to go as far as: Human casualties, Economic instability, Mistrust towards any government or a private organisation.

1.7 Infrastructure Hacking

Operational systems that are deployed to support critical services are particularly targeted by infrastructure hacking.(Hunorfi & Farkas, 2025) Attackers can exploit ICS logic, install malware that is specific to the SCADA systems, or infect safety controls. In contrast to traditional cybercrime, infrastructure attack may cause physical damage, environmental risks and prolonged service disruptions. Being refined and potentially impactful makes it border on cyber warfare as opposed to regular cybercrime.

1.8 Insider Hacking

Insider attacks come about as a result of people with privileged access. (Day, 2009)These may be: Malicious insiders who are out to sabotage systems knowingly. Careless insiders who lead to accidental disobedience. Hackers who were compromised or pressured by other parties. Insider threats are especially perilous because they will be able to defeat more traditional cybersecurity measures and leave little traces.

1.9 Script Kiddie Attacks

Script kiddies rely on the ready-made tools to capitalise on the vulnerability without having specialised knowledge. These are simpler forms of attack, but they can also impact operations, particularly in cases of attack on poorly secured legacy systems.

1.10 Supply Chain Attacks

Supply chain attacks breach software, hardware, or services to gain access to various downstream systems.(Gokkaya et al., 2026) Jack of All Trades. There can be malicious firmware updates, hardware backdoors, or hacked software libraries. It is hard to detect and mitigate through exhaustive monitoring and audits of vendors, as well as active threat intelligence.

Type of Hacking	Primary Intent	Typical Targets	Potential Impact on Critica Infrastructure
Ethical Hacking (White-Hat)	Security assessment and defence	Organisational IT and OT systems	Early vulnerability detection and risk reduction
Malicious Hacking (Black-Hat)	Financial gain, sabotage, o revenge	IT networks, ICS, SCADA systems	Service disruption, data loss and physical damage
Grey-Hat Hacking	Unauthorised access without explicit malicious intent	Enterprise and industria systems	Operational risk and accidental system compromise
Hacktivism	Ideological or politica motivation	Government and corporate systems	Reputational damage and service interference
Cyber Espionage	Intelligence gathering and surveillance	Defence, energy, and industrial research systems	Long-term stealthy compromise and data exfiltration
Cyber Terrorism	Fear generation and mass disruption	Power grids, transport, and emergency services	Threats to public safety and national security
Infrastructure / ICS Hacking	Manipulation o operational processes	SCADA, PLCs, industria controllers	Physical damage and prolonged operational failure
Insider Hacking	Misuse of legitimate access	Internal IT and OT environments	Stealthy intrusion with minimal forensic traces
Script Kiddie Attacks	Curiosity or reputation seeking	Poorly secured legacy systems	Minor disruption and exposure of weak defences
Supply Chain Attacks	Indirect compromise through trusted vendors	Software, firmware hardware components	Widespread systemic compromise across organisations

Table 1. Classification of Hacking Types Based on Intent and Impact on Critical Infrastructure

2. Forensic Branches in Cybercrime Investigations

The hacking of infrastructure requires a multifaceted forensic investigation. This contrasts with traditional cybercrime, where the primary target is often the computer or servers; infrastructure attacks need to be analysed in many different aspects: digital, network, industrial, memory, hardware, and physical evidence.(Sarkar & Shukla, 2023)

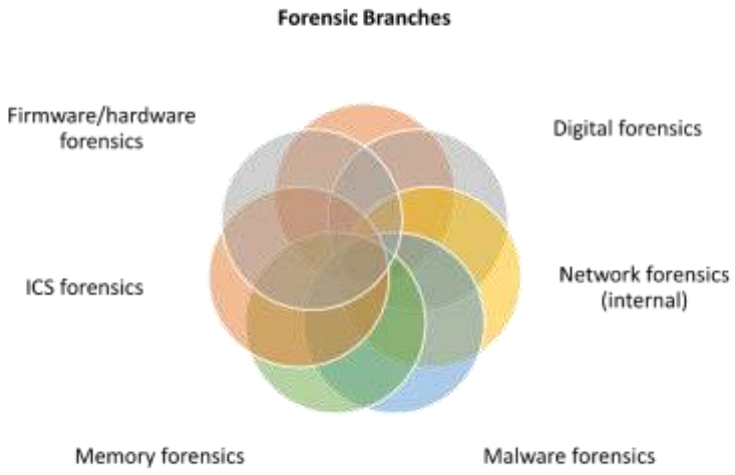


Figure 2. Forensic Branches in Cyber Crime Investigations

2.1 Digital (Cyber) Forensics

Digital forensics emphasises the detection, recovery, storage and examination of electronic evidence.(Klasén et al., 2024) Investigators create timelines of the attacks, identify the extent of system intrusion, and derive evidence of acts to prosecute. There are such tools as forensic imaging applications, log analysis frameworks, and disk recovery tools.

2.2 Network Forensics

Network forensics is used to analyse network traffic to identify any anomalies, track illegal access, and identify data loss. The techniques include packet capture analysis, intrusion detection system (IDS) logs, and an anomaly detection algorithm.(Hunt & Zeadally, 2012)

2.3 Malware Forensics

Malware forensics investigates malicious code in order to determine its conduct, payload, command-and-control facilities and persistence. It is possible with the help of static and dynamic analysis, reverse engineering, and sandbox testing.(Talukder, 2020a)

2.4 Memory Forensics

The area of memory forensics is centred on volatile memory (RAM), finding fileless malware, the execution of in-memory code, and the discovery of temporary evidence that has not been persisted to disk. It plays an important role in identifying sophisticated threats in industrial systems. (Bozkir et al., 2021)

2.5 Mobile Device Forensics

Mobile forensics retrieves the deleted messages, detects phishing, and tracks insider-related attacks with the help of smartphones or tablets. BYOD policies and mobile SCADA interfaces make mobile evidence an even more applicable one.(Khaled Zakarneh, 2024)

2.6 Cloud Forensics

Cloud forensics deals with the threats on distributed platforms, including the analysis of the virtual machines, cloud storage logs, and SaaS applications. The difficulties involve a multi-tenant environment, jurisdiction, and impermanent storage of data.(Shetty et al., 2014)

2.7 Email and Web Forensics

Cases that are explored in this branch are phishing attacks, spoofed emails, rogue websites, and social engineering vectors. Cyber fraud, identity theft and insider attack cases all require proof.(Rekouche, 2011)

2.8 Forensics of Industrial Control Systems (ICS)

ICS forensics includes PLC logic, SCADA settings, and industrial communication protocols. This branch associates digital intrusions with physical effects, and this allows investigators to establish the effects of operation and causality. (Karabiyik et al., 2018)

2.9 Hardware and Software Forensics

The nature of firmware and hardware forensics reveals the low-level activity of some type of tampering, such as compromised embedded systems, backdoors, and rogue malware that remains persistent even when rebooting the system. There is the use of specialised tools, including chip readers and firmware analysers. (Sasi et al., 2024)

2.10. Physical Forensics (Cyber-Physical Correlation)

Physical forensics investigates mechanical, electrical or material failures that occur due to cyberattacks. Whether digital evidence is correlated with physical damage is the difference between unavoidable failures and intentional sabotage, which is a necessity to comply with the law and regulations. (Nemeth, 2012)

3. Air-Gapped Systems

Air-gapped systems are special computer systems of networks that are physically separated by all possible external communication means, including the internet and unsecured internal networks. This seclusion is accomplished by making sure that there are no wired and wireless connections that interconnect the secured system with any other network. The main purpose of air-gapping is to establish a very secure environment where sensitive information, vital operations and mission-critical systems are protected against cyber threats. Air-gapping is regarded as one of the strongest security precautions when it comes to cybersecurity practice since it essentially eliminates the means of direct attack by remote intrusions. Such systems are commonly used in situations where the possible impacts of the compromise are highly devastating. This has been used in examples like nuclear power plants, where the manipulation of operational data can pose a danger to the people; in military command and control systems, which control and direct strategic operations; in weapons and defense facilities, which contain classified designs of weapons and strategic information; in intelligence databases, which hold sensitive information on national security, and in critical industrial installations like chemical processing plants, water treatment facilities, and power generation units. The basic idea that air-gapping assumes is that having a physical distance serves as a protective barrier, and it offers a great chance of limiting cyberattacks. Nevertheless, even when these two are thought to be secure, the concept of complete isolation has lately gotten harder and harder to acquire in the modern working conditions. The industrial, defence, and research systems of modern times frequently demand periodical updates of software, configuration changes, and data exchange between the autonomous system and the rest of the networks. This is usually done on removable media, e.g. USB drive, external hard drive or optical disk. Although these approaches allow maintaining the system and providing the flow of information, they also present the potential vectors of attack that may overcome the protective air gap. Human operators, as the bridges between the remote systems and the outside world, may also unintentionally contribute to the introduction of malicious software or the violation of the integrity of sensitive data.(Swanzy et al., 2024) Techniques of advanced cyberattacks have proved that air-gapped systems are not immune to intrusion. Hackers have used the weaknesses of removable media, breached firmware, and the supply chain to compromise isolated systems. Initially introduced malware is capable of spreading in a lateral way across the network, altering key control activities and even taking a long pause before being activated by certain conditions or commands. One such notable case is the Stuxnet worm that attacked enrichment centrifuges of Iran in 2010.(Shakarian et al., 2013) The malware

was loaded onto air-gapped industrial control systems through infected USB drives, proving that even a system not connected to the internet directly is vulnerable to very advanced attacks.

Besides traditional infection vectors, other studies have also established that air-gapped systems may also end up exposing sensitive information to unorthodox media. Methods based on electromagnetic emissions, sound signals, optical and thermal fluctuations have already been widely investigated in the field of cybersecurity.

4. Infrastructure Hacking in Air-Gapped Systems

Hacking of infrastructure in air-gapped systems is a distinctly problematic threat environment since the critical systems are physically isolated from the network.(Sati & Muthalagu, 2023) Air-gapped systems, unlike traditional IT attacks, are based on indirect vectors of intrusion, including compromised removable media, supply chain weaknesses, insider activities and maintenance equipment. In such settings, attacks are frequently planned out, highly targeted, and designed to the smallest detail about industrial processes and operational control logic. Forensics plays an essential role in this type of attack. Forensic investigations aid in the reconstruction of the occurrence, establishment of the mode of attack, evaluation of effects on the system, assigning blame and implementation of measures to strengthen security.(Casey et al., 2010) The forensic process should be carefully planned, specialised and use a multidisciplinary approach due to operational, technical, and safety limitations of air-gapped environments. In this section, the process of forensic investigation and the forensic branches involved in the cases of air-gapped infrastructure hacking are described.

4.1 Air-gapped Environment Attack Vectors

Attackers of air-gapped systems use indirect approaches, given that there is no traditional network connection:

Infected Removable Media: Software updates and configuration files/data are normally transferred using USB drives, external hard disks and optical media. These media can be used to introduce malware, such as in the case of the Stuxnet attack, where infected USB drives were used as a form of bypassing air-gap defences to attack Iran's nuclear centrifuges.

Weakened Supply Chains: The hardware or software bought by vendors may already be infected or compromised and brought into the working environment as malware. Supply chain attacks build on the trust between companies and vendors. Insider Actions: The malware can be introduced either intentionally or accidentally by the malicious insiders or careless personnel. Social engineering can also be used to convince employees to avoid security measures.

Maintenance Devices: Laptops, Programmable Logic Controller (PLC) interfaces, and other external diagnostic devices engaged in routine maintenance are prone to carrying malicious code unless they are properly vetted or sanitised.

Side-Channel Attacks: Advanced studies have shown that it is possible to obtain information by electromagnetic emission, acoustic, thermal, or optical channels. Although they are very advanced, such methods have the drawback of relying on air-gaps.(Park et al., 2023)

4.2 Characteristics of Attacks

Air-gapped systems are normally attacked by:

Extremely focused: In most cases, attackers use a large amount of reconnaissance to learn about the system architecture, protocols and control logic.

Stealthy: Network monitoring may not exist, and thus malware may lie in a dormant state over a long period of time.

Timed attacks: Sometimes, in critical operations, they may be launched at certain times in order to cause as much effect as possible.

Operationally advanced: To be exploited, one needs a thorough understanding of industrial processes, programming of PLCs and communication protocols of SCADA. Such attacks are more likely to be likened to cyber warfare or cyber espionage sponsored by a state rather than standard cybercrime, since they are complex.

5. Forensic Investigation Process on Air-Gapped Infrastructure Attacks

The process of forensic investigation of an air-gapped environment has a structured approach that can be generalised to include the following steps: incident identification, evidence identification and preservation, analysis and reconstruction, attribution analysis, and documentation/reporting. A different approach is needed in every stage because of the limitations of air-gapped systems.

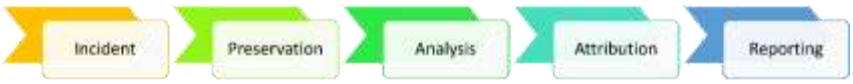


Figure 2. Forensic Investigation Workflow in Air-Gapped Attacks

5.1 Incident Identification

The air-gapped networks do not usually have automated intrusion detection systems, as opposed to conventional IT systems. Security alerts can be very low or non-existent, and odd behaviour of the systems can be the initial indicator of compromise.

Typical indicators include: Abnormal behaviour of equipment or control system outputs: When the equipment or control system does not operate within normal operational parameters, including irregular motor speed, irregular valve position or control signal output, then it may be a sign of malicious intervention.

Sensors with discrepancies: Sensors that give erratic data, with the sensors operating in a way that is not parallel to the baseline operation, could indicate malware tampering and manipulation.

Unaccounted downtime of the equipment or manufacturing processes: The unexpected cessation of any production process or the shutdown of any system without apparent reason can indicate an attack.

Physical damage associated with system commands: Included in the damages to machinery or environmental control systems have been observed to be a result of malicious manipulations of the control logic. The timeliness of detection is of paramount importance since the promptness with which the attack will be detected can also increase the severity of the attack and complicate the process of subsequent forensic reconstruction. With air-gapped environments, operational engineers are usually crucial in identifying anomalies before the automated monitoring can detect their occurrence.

Attack Vector in Air-Gapped Environments	Likely Observable Evidence	Primary Forensic Domains Involved
Infected removable media (USB, external drives)	Malicious binaries, altered file timestamps, artefacts on removable storage	Malware forensics, digital forensics, removable media analysis
Insider-assisted introduction of malware	Irregular access patterns, timing inconsistencies, and operator activity records	Log analysis, digital forensics and physical forensics.
Compromised firmware or software updates	Firmware hash deviations, unauthorised configuration changes	Firmware forensics, hardware forensics
Contaminated maintenance equipment	Residual malware traces on service laptops, abnormal update behaviour	Digital forensics, malware forensics
Internal lateral movement within the OT network	Unexpected controller communications, altered control commands	Internal network forensics, ICS forensics
Fileless or memory-resident malware	Volatile memory artefacts, anomalous runtime processes	Memory forensics, malware forensics
Manipulation of industrial control logic	Modified PLC ladder logic, unsafe control sequences	ICS forensics, operational process analysis
Cyber-physical impact on equipment	Mechanical damage, abnormal sensor readings	Physical forensics, cyber-physical correlation

Table 2. Relationship Between Air-Gapped Attack Vectors, Observable Evidence, and Applicable Forensic Domains

5.2 Preservation of Evidence

After the possible compromise is discovered, all possible evidence sources have to be carefully discovered and kept, but operational continuity must be maintained. The areas of key evidence comprise:

System logs: PLC event logs, DCS system event logs, SCADA server event logs and controller event logs. In the old industrial world, there could be little or fast overwritten logging, which necessitates immediate intervention.

Snapshot memory: Fileless malware, in-memory injected code, or malicious scripts can be captured by capturing volatile memory (RAM) with the least amount of evidence left on disk.

Firmware images: During firmware analysis of an embedded device, one can determine any tampering or malicious modifications, and this can be maintained even after a reboot.

Removable media: USB drives, external hard drives, and optical media to update configuration, patches or maintenance routines are usually used as vectors of infection.

Physical access logs: Badge access records, surveillance videos and records of operator activity can be used to determine who accessed the sensitive systems and at what time. Chain-of-custody integrity, operational safety, and additional system compromise should be prevented in evidence preservation. An example of this is that, analogous to write-protected imaging devices with USB or firmware stripping, analysts can extract evidence by using write-protected imaging devices. (Watson & Jones, 2013)

5.3 Analysis and Reconstruction

Analysis and reconstruction are parts of the reconstruction process that allow the researcher to analyse data and examine the information. Key tasks include:

Behavioural analysis of malware: Static analysis and dynamic analysis of malicious code will be necessary to ascertain the propagation and payload operations, as well as control mechanisms. When in air-gapped environments, malware frequently follows the lateral path through removable media or through internal network paths.(YusirwanS et al., 2015)

Control command analysis: This is an evaluation of PLC or SCADA command logs that the investigator uses to detect manipulated command sequences, sensor data or command performance. This discloses the way malware affects physical processes. (Oyedotun et al., 2025)

Reconstruction of timelines: The sequence of compromise is reconstructed by the analysts through the system logs, actions of the operators, and malware activity, in order to determine the attack windows.

Lateral motion testing: Figuring out whether malware was spread to several devices in the air-gapped system aids in evaluating the extent of compromise fully. Digital forensics usually involves the interaction of digital forensic specialists, ICS experts, operational engineers, and firmware specialists because attacks in such a setting are a blend of cyber, hardware, and process manipulation components. (Farwell & Rohozinski, 2011)

5.4 Attribution Analysis: Investigators determine the extent to which the attack indicates the motive of the crime, i.e. industrial espionage or sabotage due to economic or competitive reasons. Demonstrates the features of state-level advanced threats, such as advanced persistent threats (APTs) and protracted, focused campaigns. Findings of accidental compromise: e.g. careless human operators dropping malware on a USB drive or maintenance equipment. The attentions of attribution are based on malware profiling, operational expertise, forensic data and intelligence environment. Effective attribution is used to guide mitigation measures, policy amendments and judicial actions.(Goel & Nussbaum, 2021)

5.5 Documentation and Reporting:

This document will detail the method of data documentation and reporting (data gathered throughout the program and the subsequent final report). Any results have to be carefully recorded to aid regulatory compliance, legal action and learning by the organisation. Documentation includes Chain-of-custody records and evidence collection logs, which are accountable and legally defensible. Analysis reports with methodology of attack, malware nature, vulnerabilities exploited and impact of attack on the system. Policy revisions, patch schedules, staff training and monitoring improvements are all suggestions on how to enhance the posture of cybersecurity.(Busetti & Scanni, 2025) Properly organised documentation or documents is not only helpful in ongoing research but also serves to increase the forensic preparedness for future events.

6. Forensic Branches Involved in Air-Gapped Infrastructure Investigations

Air-gapped system investigation is a challenging multidisciplinary forensic task as it involves a special combination of cyber, industrial, and operational factors. The most important branches of forensics are:

6.1 Digital (Cyber) Forensics

Air-gapped investigations are based on digital forensics. Analysts discover, gather, preserve and examine computer, controller and storage device digital evidence.

Tasks include: Restoring erased files, logs and configuration records. Checking malware presence and system intrusion. Rebuilding the attack time history and user activities.

6.2 Network Forensic (Internal Networks)

Even air-gapped systems can also internally communicate within the network between controllers, HMIs or SCADA elements.

Network forensics traces: Illegal inter-device lateral movement. Unusual network traffic activities. Internal buses are used to send command-and-control messages. The branch plays a crucial role in comprehending the spread of malware in a system that is not collaborative.

6.3 Malware Forensics

Customised and covert malware against air-gapped environments is common.

Malware forensics includes:

Static analysis: Analysis of structure and built-in functions.

Dynamic analysis: Dynamic values of execution within sandboxed environments.

Reverse engineering: Learn the rationale, triggers, and possible data exfiltration.

6.4 Memory Forensics Detection of fileless malware or in-memory manipulation of control logic would not be possible without memory forensics. Volatile memories are identified by snapshots picked by analysts to determine RAM executable malicious code. Injections of command are temporary. Perishable objects that are not stored in storage media.(Talukder, 2020b)

6.5 Forensics of Industrial Control Systems (ICS)

ICS forensics is an area that deals with operational manipulation.

Key areas include: PLC logic analysis and ladder diagram analysis. Analysis of the configuration of SCADA servers. Anomaly detection and industrial protocol monitoring. ICS forensics fills the divide between online attacks and physical system attacks.

6.6 Firmware and Hardware Forensics

Low-level compromises that are unable to be stopped by software-based defences are detected by firmware and hardware forensics.

Key tasks include: Backdoor or malicious modifications, Firmware image analysis. Checking of device embedded components or modifications. To monitor the buses and signals to check whether control manipulation is hidden.

6.7 Forensics Mobile device and removable media

Human operators tend to add removable media to make an update or a maintenance. This branch focuses on: Checking USB disks and external drives for malware. Restoring files that have been deleted or infected with malicious code. Following the operational metadata to compare the use of media and the compromise of the system.

6.8 Physical Forensic (Cyber-Physical Correlation)

Physical forensics will associate digital evidence with physical impacts, including: Damage to equipment or mechanical failures.(Reedy, 2023) Environmental risks caused by modified control instructions. Cyber manipulation is associated with operational disruption. This branch ensures that forensic inferences are pegged on cyber and actual realities.

6.9 Cloud and Remote Maintenance Forensics

Other air-gapped systems engage with external cloud-based services periodically through regulated maintenance mechanisms. Forensics on the same domain analyses: Maintenance platform/virtual management console logs. Malware infection through provisional connectivity. Remotely configured changes and their effects.

7. Case Studies and Real-life Incidents

Physical isolation of critical infrastructure by external networks makes air-gapped systems generally believed to be the gold standard of safeguarding critical infrastructure against cyber threats. History has proved, though, that even such systems cannot be resistant to advanced attacks. Several high-profile incidents underscore the abilities of attackers to compromise, compromise and physically damage air-gapped or semi-isolated industrial settings. These case studies can be used as warning stories by operational engineers as well as cybersecurity practitioners.

Incident	Initial Entry Method	Primary Target Environment	Nature of the Attack	Observed Operational Consequences
Stuxnet (2010)	Infected removable media introduced by human operators	Air-gapped nuclear industrial control systems	Highly targeted malware manipulating PLC control logic	Physical degradation of centrifuges with delayed detection
German Steel Mill Attack (2014)	Compromise through interconnected IT-OT segments	Industrial production control environment	Disruption of operational control and safety mechanisms	Severe equipment damage and uncontrolled shutdown
Ukrainian Power Grid Attack (2015)	Phishing-based IT intrusion followed by OT pivoting	Electricity distribution and control systems	Coordinated remote manipulation of SCADA components	Widespread power outage affecting the civilian population

Table 3. Comparative Overview of Major Cyber Incidents Involving Industrial and Air-Gapped Infrastructure

7.1 Stuxnet (2010)

Stuxnet is one of the most advanced and documented air-gapped system compromises. Stuxnet, which was a computer worm, was discovered in the year 2010 and was highly targeted, with the main aim being to penetrate the uranium enrichment facilities in Iran. Its initial entry mode was by use of infected USB drives that people manually inserted into air-gapped systems, and this has shown how human factors can compromise physical isolation. When within the network, Stuxnet used various zero-day vulnerabilities in the operating systems of Windows and PLC programming software to spread through interconnected industrial computers. Its final objective was Uranium enrichment centrifuges that were managed by Siemens Step7 PLCs.

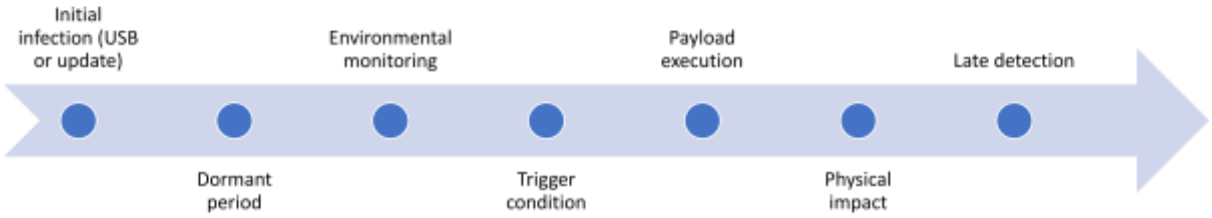


Figure 3. Timeline (Stuxnet / Generic Air-Gap Attack)

Stuxnet hacked centrifuges' rotational speeds in such a way that they could create mechanical stress and ultimately be destroyed without raising any alarm to the operators.(*(PDF) Stuxnet: Cyberwar Revolution in Military Affairs*, n.d.) Stuxnet was sophisticated in that it went without being noticed; it took weeks to be detected using conventional antivirus software and network monitoring systems. It is a marriage between sophisticated malware code and a strong understanding of the industrial operation, and therefore, it showed that even air-gapped systems, although they are not communicating with the internet, can fall prey to targeted assaults with the help of removable media, internal expertise, and even tailored malware.

7.2 German Steel Mill Attack (2014)

A cyberattack on a German steel mill in 2014 resulted in physical damage to industrial equipment, which made the issue of cyberattacks in critical infrastructure a real concern. As the facility was not completely air-gapped, the attack overcame the conventional IT-OT boundaries and used the vulnerabilities in industrial control systems. Hackers used breached network segments and controls of operations, which resulted in uncontrolled process states that harmed a blast furnace. It has been found that it was malware that interfered with emergency shutdown processes and used loopholes in operational procedures. This event is notable in that it has proved that partial network isolation or network segmentation does not completely remove risk. The attackers can take advantage of process control weaknesses, human factors, or internal connectivity to produce operational disruption, and therefore, it is essential to have effective monitoring, anomaly detection and forensic preparedness in industrial settings.

7.3 Ukrainian Power Grid Attack (2015)

Another critical example that reveals how infrastructure systems, including partially isolated ones, are vulnerable to cyber threats is the Ukrainian power grid attack of 2015. Hackers attacked ICS and SCADA systems that operate electricity distribution in the region and managed to shut down power to about 225,000 clients. The attack started with spear-phishing and malware attacks on corporate IT networks. In spite of the fact that operational networks were somewhat separated, attackers exploited internal jump points and access tools to breach control systems. They controlled circuit breakers, hampered communications, and shut down safety monitoring systems, pointing to the fact that network segmentation, as well as partial air-gaping, though decreasing the attack surface, does not completely prevent manipulation of operations. The case with Ukraine can be taken as an example of the cascading process of the influence of cyberattacks on public services and economic stability, as well as on national security. It also highlights the significance of combining digital forensics, ICS forensics, and physical forensic analysis in order to know the attack pattern, vulnerability evaluation, and the creation of mitigation measures.

Conclusion

The growing use of digital and cyber-physical systems by critical infrastructure has not only changed the way things run but also made these systems vulnerable to unprecedented cyber threats. The type of hacking that poses a complex and high-stakes problem, which is infrastructure hacking, especially in air-gapped or semi-isolated systems, has implications of compromise that are much more far-reaching than just monetary loss, and also includes physical destruction, environmental risks, risks to human life, and implications on national security. The case studies like Stuxnet, German steel mill attack and the Ukrainian power grid incident vividly demonstrate that physical isolation does not secure immunity against highly targeted and sophisticated attacks. Air-gapped forensic research is a difficult and essential task. Lack of direct network connectivity, minimal logging, and operational constraints require a multidisciplinary response, which is digital forensics, network, malware analysis, memory and firmware forensics, ICS and hardware analysis, and physical evidence correlation. Proper forensic procedures help the investigators to determine the attack vectors, reconstruct the events, evaluate the effect of operations, assign blame, and design mitigation programs that are evidence-based. Further, forensic preparedness in the form of trained staff, standardisation of response procedures and safe evidence management is essential to reduce the impact of any future occurrences. One of the ways to enhance organisational resilience is the incorporation of forensic knowledge into the security strategies of the infrastructure. The experience of cyber intrusions enhances the policy formulation, system hardening, supplier and system vetting, staff training and anomaly detection measures. Forensic analysis can be utilised to help close the gap between cyber compromise and real-world consequences in order to support the legal and regulatory needs, as well as to promote operational safety and national security preparedness. Finally, to ensure the security of air-gapped critical infrastructure, there is a necessity to combine technological, human, and forensic intelligence to prevent any threats. As much as air-gapping lowers the exposure to external threats, coupled with the ability to defend and investigate network activities, the level of advanced attack is likely to occur and necessitates measures to predict, monitor, and act in response to the occurrence. Cyber forensics, hence, forms one of the axes of the contemporary infrastructure security so that the critical systems keep working safely, securely, and reliably in a world that has become more interconnected and threat-prone.

Conflict Of Interest

The author declares no conflict of interest, financial or otherwise.

Acknowledgement

I would like to express my heartfelt thanks to **K.V. Ravi Kumar (Professor, Dean of School of Forensic Science)**, whose continuous guidance, encouragement, and insightful feedback provided the foundation for this paper. His support throughout the research process was invaluable and deeply appreciated.

References

1. **Alsmadi, I., Dwekat, Z., Cantu, R., & Al-Ahmad, B. (2022). Vulnerability assessment of industrial systems using Shodan. *Cluster Computing*, *25*(3), 1563–1573. https://doi.org/10.1007/s10586-021-03330-3**
2. **Bozkir, A. S., Tahillioglu, E., Aydos, M., & Kara, I. (2021). Catch them alive: A malware detection approach through memory forensics, manifold learning and computer vision. *Computers & Security*, *103*, 102166. https://doi.org/10.1016/j.cose.2020.102166**
3. **Busetti, S., & Scanni, F. M. (2025). Evaluating incident reporting in cybersecurity. From threat detection to policy learning. *Government Information Quarterly*, *42*(1), 102000. https://doi.org/10.1016/j.giq.2024.102000**
4. **Casey, E., Daywalt, C., & Johnston, A. (2010). Intrusion investigation. *Handbook of Digital Forensics and Investigation*, 135–206. https://doi.org/10.1016/B978-0-12-374267-4.00004-5**
5. **Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behaviour Reports*, *5*, 100167. https://doi.org/10.1016/j.chbr.2022.100167**

6. **Day, C. (2009). Intrusion prevention and detection systems. *Computer and Information Security Handbook*, 293–306. https://doi.org/10.1016/B978-0-12-374354-1.00018-2**
7. **Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, *53*(1), 23–40. https://doi.org/10.1080/00396338.2011.555586**
8. **Goel, S., & Nussbaum, B. (2021). Attribution across Cyber Attack Types: Network Intrusions and Information Operations. *IEEE Open Journal of the Communications Society*, *2*, 1082–1093. https://doi.org/10.1109/OJCOMS.2021.3074591**
9. **Gokkaya, B., Aniello, L., & Halak, B. (2026). Software supply chain: A taxonomy of attacks, mitigations and risk assessment strategies. *Journal of Information Security and Applications*, *97*, 104324. https://doi.org/10.1016/j.jisa.2025.104324**
10. **Hunorfi, P., & Farkas, T. (2025). Cybersecurity of Operational Technology in Critical Infrastructures. *Belügyi Szemle*, *73*(1.ksz), 183–197. https://doi.org/10.38146/bsz-ajia.2025.v73.i1si.pp183-197**
11. **Hunt, R., & Zeadally, S. (2012). Network forensics: An analysis of techniques, tools, and trends. *Computer*, *45*(12), 36–43. https://doi.org/10.1109/MC.2012.252**
12. **Iftikhar, S. (2024). Cyberterrorism as a global threat: a review of repercussions and countermeasures. *PeerJ Computer Science*, *10*, e1772. https://doi.org/10.7717/peerj-cs.1772**
13. **Karabiyik, U., Celebi, N., Yildiz, F., Holekamp, J., & Rabieh, K. (2018). Forensic analysis of SCADA/ICS systems with security and vulnerability assessment. *ASEE Annual Conference and Exposition, Conference Proceedings*, *2018-June*. https://doi.org/10.18260/1-2--30530**
14. **Khaled Zakarneh, S. (2024). Mobile Forensic Investigation on iOS & Android Smartphones: Case Study Investigation on WhatsApp. *International Journal of Applied Sciences and Smart Technologies*, *6*(1), 63–98. https://doi.org/10.24071/ijasst.v6i1.6770**
15. **Khan, S. K., Shiwakoti, N., Diro, A., Molla, A., Gondal, I., & Warren, M. (2024). Space cybersecurity challenges, mitigation techniques, anticipated readiness, and future directions. *International Journal of Critical Infrastructure Protection*, *47*(3), 100724. https://doi.org/10.1016/j.ijcip.2024.100724**
16. **Klasén, L., Fock, N., & Forchheimer, R. (2024). The invisible evidence: Digital forensics as key to solving crimes in the digital age. *Forensic Science International*, *362*, 112133. https://doi.org/10.1016/j.forsciint.2024.112133**
17. **Nemeth, C. P. (2012). Civil Liability of Security Personnel. *Private Security and the Law*, 117–190. https://doi.org/10.1016/b978-0-12-386922-7.00005-8**
18. **Oyedotun, S. A., Oise, G. P., & Ozobialu, C. E. (2025). Towards Intelligent Cybersecurity in SCADA and DCS Environments: Anomaly Detection Using Multimodal Deep Learning and Explainable AI. *Journal of Science Research and Reviews*, *2*(3), 20–31. https://doi.org/10.70882/josrar.2025.v2i3.76**
19. **Park, J., Yoo, J., Yu, J., Lee, J., & Song, J. S. (2023). A Survey on Air-Gap Attacks: Fundamentals, Transport Means, Attack Scenarios and Challenges. *Sensors (Basel, Switzerland)*, *23*(6), 3215. https://doi.org/10.3390/s23063215**
20. ***(PDF) Stuxnet: Cyberwar Revolution in Military Affairs*. (n.d.). Retrieved February 3, 2026, from https://www.researchgate.net/publication/230898148_Stuxnet_Cyberwar_Revolution_in_Military_Affairs**
21. **Reedy, P. (2023). Interpol review of digital evidence for 2019–2022. *Forensic Science International: Synergy*, *6*, 100313. https://doi.org/10.1016/j.fsisyn.2022.100313**
22. **Rekouche, K. (2011). *Early Phishing*. http://arxiv.org/abs/1106.4692**
23. **Salim, D. T., Singh, M. M., & Keikhosrokiani, P. (2023). A systematic literature review for APT detection and the Effective Cyber Situational Awareness (ECSA) conceptual model. *Heliyon*, *9*(7), e17156. https://doi.org/10.1016/j.heliyon.2023.e17156**

24. **Sarkar, G., & Shukla, S. K. (2023). Behavioural analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminology*, *2*, 100034. https://doi.org/10.1016/j.jeconc.2023.100034**
25. **Sasi, T., Lashkari, A. H., Lu, R., Xiong, P., & Iqbal, S. (2024). A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges. *Journal of Information and Intelligence*, *2*(6), 455–513. https://doi.org/10.1016/j.jiixd.2023.12.001**
26. **Sati, V., & Muthalagu, R. (2023). Analysis on Hacking the Secured Air-Gapped Computer and Possible Solution. *Cybernetics and Information Technologies*, *23*(2), 124–136. https://doi.org/10.2478/cait-2023-0017**
27. **Shakarian, P., Shakarian, J., & Ruef, A. (2013). Attacking Iranian Nuclear Facilities. *Introduction to Cyber-Warfare*, 223–239. https://doi.org/10.1016/b978-0-12-407814-7.00013-0**
28. **Shetty, J., Anala, M. R., & Shobha, G. (2014). A Study on Cloud Forensics: Challenges, Tools and CSP Features. *Biometrics and Bioinformatics*, *6*(6), 149–153. https://www.researchgate.net/publication/275833813_A_Study_on_Cloud_Forensics_Challenges_Tools_and_CSP_Features**
29. **Singh, C., & Jain, A. K. (2024). A comprehensive survey on DDoS attacks detection & mitigation in SDN-IoT network. *E-Prime - Advances in Electrical Engineering, Electronics and Energy*, *8*(3), 100543. https://doi.org/10.1016/j.prime.2024.100543**
30. **Swanzy, P. N., Abukari, A. M., & Ansong, E. D. (2024). Data Security Framework for Protecting Data in Transit and Data at Rest in the Cloud. *Current Journal of Applied Science and Technology*, *43*(6), 61–77. https://doi.org/10.9734/cjast/2024/v43i64387**
31. **Talukder, S. (2020a). *Tools and Techniques for Malware Detection and Analysis*. http://arxiv.org/abs/2002.06819**
32. **Talukder, S. (2020b). *Tools and Techniques for Malware Detection and Analysis*. http://arxiv.org/abs/2002.06819**
33. **Watson, D., & Jones, A. (2013). Case Processing. *Digital Forensics Processing and Procedures*, 367–420. https://doi.org/10.1016/b978-1-59749-742-8.00009-1**
34. **Winkler, I., & Gomes, A. T. (2017). Threat. *Advanced Persistent Security*, 47–66. https://doi.org/10.1016/B978-0-12-809316-0.00006-3**
35. **Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2023). Ethical hacking for IoT: Security issues, challenges, solutions and recommendations. *Internet of Things and Cyber-Physical Systems*, *3*, 280–308. https://doi.org/10.1016/j.iotcps.2023.04.002**
36. **YusirwanS, S., Prayudi, Y., & Riadi, I. (2015). Implementation of Malware Analysis using Static and Dynamic Analysis Methods. *International Journal of Computer Applications*, *117*(6), 11–15. https://doi.org/10.5120/20557-2943**