



Naif Arab University for Security Sciences
Journal of Information Security and Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
<https://journals.nauss.edu.sa/index.php/JISCR>

JISCR

Cybersecurity and Forensic Analysis of IP-Cameras Used in Saudi Arabia

Istabraq M. Alshenaifi, Lujain A. Alharbi, Sandaresan Ramachandran, Kyounggon Kim*

Center of Excellence in Cybercrimes and Digital Forensics (CoECDF), Naif Arab University for Security Sciences, Riyadh, Saudi Arabia.



Received 28 Mar. 2024; Accepted 05 Jun. 2024; Available Online 18 Jun. 2024

Abstract

In smart city infrastructure, IP cameras play a pivotal role in crime prevention and detection. However, not much research has been conducted on IP cameras from a cybersecurity and forensics perspective. In this study, we investigate vulnerability assessment and forensic artifacts for Hanwha and Mobotix IP cameras, which are widely used in Saudi Arabia. Saudi Arabia is using IP cameras which are essential for its smart cities. In this paper, we examine IP cameras in two directions. The first is to assess the vulnerability of IP cameras through various attack scenarios such as denial of service (DoS), brute force, and unauthorized access, and we suggest countermeasures. The second shows how analysis for IP cameras can be used to investigate logs for cyberattacks. Through this study, we expect to contribute to research on cyber-attack and forensic perspectives on IP cameras to be used in smart cities.

I. INTRODUCTION

From 2023 to 2030, the global IP camera market is projected to expand at a compound yearly growth rate of 13.9%, reaching USD 32.63 billion [1]. The deployment of IoT devices has become a crucial component of the country's smart city architecture, with IP cameras playing a vital role in this regard [2], [3]. Studies have shown that the use of surveillance cameras can reduce crime rates in certain environments. As IoT devices develop, traditional surveillance cameras are gradually changing to IP cameras with smart functions.

Despite Saudi Arabia has approved installing security surveillance cameras in critical locations by Royal Decree No. (M/34), not much research

has been done on cybersecurity assessment. Additionally, not much research has been conducted on IP camera devices from a forensic perspective. These challenges make it difficult for cybercrime investigators to obtain reliable and acceptable digital forensic evidence from IP cameras.

To address this existing research gap, this study conducts an analysis of IP cameras from Hanwha and Mobotix products installed in public institutions in Saudi Arabia. The main research direction is to evaluate potential cybersecurity vulnerabilities associated with IP cameras and identify key forensic artifacts. During this analysis, security tools are used to conduct a detailed examination of the log artifacts contained in the IP cameras.

Keywords: Cybersecurity, Digital Forensics, IoT Devices, IP Cameras, Logs, Smart City.



Production and hosting by NAUSS



* Corresponding Author: Kyounggon Kim

Email: kkim@nauss.edu.sa

doi: [10.26735/LLFQ4473](https://doi.org/10.26735/LLFQ4473)

Collecting evidence from IP cameras requires retrieving evidence from cloud-based storage, SD cards, and server repositories. In this study, we focus on examining the logs that can be extracted from IP cameras. Additionally, most IP cameras require a Wi-Fi connection to operate. Users can view live video from any device connected to the Internet. We examined the admin pages of IP cameras in this study. First forensic responders must understand that evidence from IP cameras can reside in cloud storage, local storage, or just live data streaming without storage. As shown in Fig. 1, this study accesses the administrator page of an IP camera connected via Wi-Fi to extract and analyze log information.

In this study, our contribution is conducting a detailed analysis of the most common attacks targeting IP cameras. By examining these attack methods, our goal is to offer a comprehensive understanding of the vulnerabilities inherent in these devices. This valuable insight is represented in cybersecurity report. Additionally, we undertake a forensic examination of IP camera data, extract evidence and provide guidelines and procedures to aid in the digital forensic analysis process.

The remainder of this paper is organized as follows: Section II, discusses the related work from cybersecurity and digital forensics aspects. Section III, presents our methodology to analyze IP cameras logs. Section IV discusses the analysis results from cybersecurity and digital forensics perspective. Section V, conclusion, and future work. Lastly, the research findings are presented as a cybersecurity report and digital forensics guidelines are indicated as an appendix report.

II. RELATED WORKS

In this section, we provide a comprehensive review of the existing literature in the fields of cybersecurity and digital forensics regarding IP cameras. We divide our review into two sections to explore important developments in each area.

A. Cybersecurity of IP-cameras

This section reviews relevant studies and

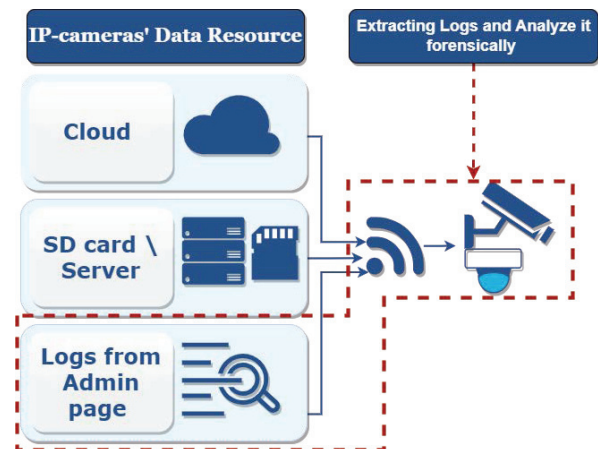


Fig. 1. Data resources for extracting evidence from IP cameras.

discusses the state of research on IP cameras, focusing on security and privacy implications.

Comparative analyses in Table I summarize key findings and methodologies across studies. Alshalawi and Alghamdi [4] presented a new tool for network forensic investigation to address the threats posed by un-authorized access to wireless surveillance cameras. However, like many forensic tools, there is a possibility of false positives (incorrectly identifying normal behavior as an attack) and false negatives (failing to detect actual attacks), which could impact the tool's reliability and effectiveness of the logs of IP-cameras. Tho and Yeung [5] explore the use of IP cameras for remote scientific experiments, highlighting the potential for these cameras to expand educational opportunities beyond traditional laboratory settings. However, the authors did not consider that enhancing security measures, such as encryption and access controls, may impact the usability and accessibility of the IP camera system for educational purposes.

Abdalla and Varol [6] investigate IP-camera vulnerabilities and their impact on security and privacy through testing with Kali Linux tools, emphasizing the need for enhanced security measures to prevent unauthorized access. Alexandrie [7] shows that surveillance cameras can reduce crime, indicating the potential for video surveillance to decrease crime in certain settings, although questions about privacy and the impact on civil liberties need



to be addressed. Castro [8] presents a smart home security system that integrates CCTV cameras and deep learning algorithms to reduce home break-ins, emergencies, and fraud. However, this system doesn't include the statistical models, which might leave the system vulnerable to potential attackers who could manipulate traffic patterns. Manske [9] assesses the vulnerability of an IP camera to malicious attacks and explores 8 of the 13 security goals for IoT devices, emphasizing the importance of addressing vulnerabilities to ensure user privacy and safety. The author has not been able to access online firmware images, and encrypted communication hindering network traffic monitoring. Also, there are challenges in capturing LAN and cloud traffic due to device configurations and potential difficulties in analyzing encrypted packets for comprehensive vulnerability assessment. Dzwigala et al. [10] propose a methodology to evaluate the security of IP cameras commonly used in households, identifying security vulnerabilities and providing recommendations for improving security. The study does not provide an in-depth analysis of the vulnerabilities found in the tested devices, as some results were inconclusive due to a lack of clear information.

Stroeven and So"derman [11] evaluate the security of an internet-connected camera through comprehensive analysis, identifying vulnerabilities, and conducting penetration tests. The authors mentioned that due to the unavailability or restricted access to the source code of the Android application associated with the IP camera being evaluated. This limitation can have several implications on the depth and thoroughness of the analysis conducted.

Vennam et al. [12] provide a review of threats in video surveillance systems and ways to prevent security attacks, emphasizing the need to raise awareness of security risks and promote research in the field. The disadvantages of the research include the challenges in applying existing security methods such as firewalls, access control, and IDSs/IPS to video surveillance systems and smartphones, as these methods may not be fully suitable for these environments.

Dragonas et al. [13] have decoded an overlooked HIKVISION CCTV logs, revealing crucial investigative details. It introduced the Hikvision Log Analyzer, streamlining analysis and bolstering IP-camera cybersecurity. The constraints of the research include the fact that not all types of log records were created during the study due to the equipment used. Additionally, the interpretation of log types was based on how the system's GUI/WebUI translated them, which could potentially lead to inaccurate results.

Almazrouei et al. [14] investigated the security of IoT devices, specifically focusing on IP cameras. By conducting real-world tests with a VAVA Outdoor Wireless IP Security Cam, the research revealed vulnerabilities, highlighting potential risks to user safety. This finding is crucial in the context of related works, emphasizing the need for enhanced security measures in IoT devices like IP cameras. There are several flaws and weaknesses in the VAVA Outdoor Wireless IP Security Cam, such as unencrypted logging tokens and vulnerable credentials stored in vava.db. These vulnerabilities can compromise user privacy and potentially lead to the compromise of cloud servers.

Bella et al. [15] addressed IoT device security, focusing on IP cameras. Using PETIoT, the research identified and fixed three vulnerabilities in the TAPO C200 camera. This practical application led to a vendor-issued firmware update, showcasing PETIoT's real-world impact on IoT security.

We conclude that common vulnerabilities in IP cameras include unauthorized access and challenges in securing communication channels. These vulnerabilities highlight the importance of robust security measures, such as encryption, access controls, and regular firmware updates, to mitigate privacy and security risks associated with IP cameras. Additionally, limitations in analyzing encrypted network traffic and accessing firmware images further complicate comprehensive security assessments. Addressing these vulnerabilities is essential to ensure the reliability and effectiveness of IP camera systems.



TABLE I
COMPARING STUDIES OF CYBERSECURITY IP-CAMERAS

Research study	Proposed solutions	Tools/Method Used	Logs extraction	Limitation
Alshalawi and Alghamdi [4]	Introduce a new monitoring scheme to detect and prevent unauthorized access attacks of IP cameras	Wireshark, algorithms to detect security threats and confusion matrix to evaluate detection performance	Camera transactions are captured and exported as CSV files using Wireshark	Possibility of incorrect attack detection affects reliability.
Tho and Yeung [5]	leveraging IP cameras to enable remotely monitored learning in science education.	Implement remotely monitored learning in science education	There are no logs extracted.	Usability impacted by privacy concerns.
Abdalla and Varol [6]	Identification of security lacks and weaknesses in IP cameras.	Penetration testing tools.	There are no logs extracted.	Limited discussion on detailed logs and audit trails in IP cameras' security testing.
Alexandrie [7]	Review experiments on surveillance cameras' impact on crime.	There are no tools or methods used.	There are no logs extracted.	Enhancing cybersecurity in surveillance cameras raises privacy concerns and potential stakeholder conflicts.
Castro [8]	Exploring IP camera vulnerabilities and analyze data for enhanced security and intrusion detection.	Wireshark, machine learning, network analysis tools.	Wireshark anomalies movement files and to detect predict	Protect the system integrity from potential attackers, leave the system susceptible to infiltration and manipulation of traffic patterns.
Manske [9]	Identifying potential security weaknesses and suggesting countermeasures to enhance its security posture.	Hashcat, Ghidra Expect and	Network traffic, user communication with web servers, interactions with external servers during firmware upgrades.	Challenges in accessing firmware and monitoring encrypted traffic.
Dzwigala et al. [10]	Providing a methodology for evaluating the security IP cameras	Wireshark, Nmap, Hydra, Whois, Nessus, Dirbuster, Curl, and Nikto	Information on default settings, software vulnerabilities, network connections, web application security.	There is lack of detailed analysis on the extraction and interpretation of logs from the tested IoT devices.
Stroeven [11] and So"derman	Highlighting security risks and providing recommendations for improving the overall security posture of the camera system.	Android 86x, CyberChef, Decompiler.com, Ghidra, Hydra, NMAP, Oracle VM VirtualBox, OWASP Threat Dragon, PlayCap, and Wireshark.	Network traffic, system interactions, and security incidents or vulnerabilities.	Challenges in accessing source code impacting the depth of analysis.
Vennam et al. [12]	Provide measures frameworks threats. and to preventive security mitigate	Information assessing launching clean up. gathering, vulnerability, attacks, and	There are no logs extracted.	The authors did not extract events from video surveillance systems or analyze camera logs.
Dragonas et al. [13]	Developing Hikvision Log Analyzer application to automate the extraction, parsing, interpretation, and evaluation log records.	FTK Imager, HxD, OSFClone, DVR Examiner, HX-Recovery, HIKVISION CCTV system GUI/WebUI, HIKVISION LocalPlayback, and Hikvision Log Analyzer	System configurations and access logs.	Incomplete log types due to equipment constraints and potential inaccuracies with system changes.
Almazrouei et al. [14]	Uncovering security weaknesses in IP camera to assist experts in predicting attacker behavior and securing systems.	Penetration techniques. testing	There are no logs extracted.	Unencrypted okens, vulnerable credentials in vava.db, risking privacy and cloud servers.
Bella et al. [15]	Introducing a new cyber Kill Chain called PETIoT to conduct Vulnerability Assessment and Penetration Testing (VAPT) sessions specifically tailored for IoT devices.	Ettercap, Nessus, map, SSL, IPTables, and Wire-shark.	There are no logs extracted.	Various IoT devices differ in architecture, communication protocols, and security measures, potentially impacting the PETIoT approach adaptability across them.



B. Digital forensics of IP-cameras

In the context of digital forensics, thorough examinations have been undertaken regarding the reliability and admissibility of evidence extracted from IoT devices, particularly IP cameras. A meticulous comparative analysis is presented in Table II to illuminate the intricacies of this domain, thereby enhancing comprehension of both challenges and advancements in the field.

Porter [16] presented a theoretical model for evaluating the relationship between photographic evidence and physical evidence, recommending an update to the Daubert principle for photographic evidence to improve its reliability. The research

methods face limitations like unclear photointerpretation methodologies, potential misrepresentation, and gaps in understanding the reliability of CCTV evidence. Sukamto et al. [17] suggested a method to analyze extracted videos from CCTV cameras based on the NIST method to ensure reliability in court proceedings. However, CCTV recordings are volatile and easily altered, posing significant challenges to their reliability and integrity. The complexity of interpreting and legally presenting this digital evidence further complicates forensic analysis. In addition to CCTV cameras, Meffert et al. [18] examined the possibility of taking a big photo of an event that occurred on an IoT device and retrieved forensically relevant state data from it. The research

TABLE II
COMPARING STUDIES OF DIGITAL FORENSICS IP-CAMERAS

Research study	Proposed solutions	Tools/Method Used	Logs extraction	Limitation
Porter [16]	Developing reliable methods for deducing and preparing scientific evidence from CCTV images for police and forensic experts.	Qualitative assessment of visual information, content analysis or reconstruction of images, and a holistic interpretation incorporating information from various sources.	There are no logs extracted.	Risks misrepresenting photographic evidence.
Sukamto et al. [17]	Analyzing CCTV video recordings and extracting valuable digital evidence.	NIST process, Hashing techniques, MedialInfo and Exif tools.	Metadata information from CCTV video recordings.	There are reliability and integrity challenges to CCTV video recordings.
Meffert et al. [18]	Developing Forensic State Acquisition from Internet of Things (FSAIoT) framework	Data acquisition by using three methods: controller to IoT device, controller to cloud, and controller to controller.	Logs capturing the state changes of IoT devices.	There are challenges in accessing historical data, needing physical access to IoT devices, and supporting various wireless protocols.
Lim et al. [19]	Proposing a EVM (Efficient evidential Video Management methodology) for video- evidence management.	EVM	IP camera system information, video record history, file system metadata of stored video, cryptographic hash value of stored video file for integrity check, and more.	security breaches, evidence integrity, chain of custody, storage.
Azhar and Bate [20]	Overview of the artefacts produced during the daily usage of IoT devices, focusing on network-native, cloud-native, and device-native artefacts.	Wireshark, Amazon Echo, and Kali Linux's tools.	User data stored in the cloud through Amazon Echo APIs and Network-native artefacts captured during the devices' usage.	short-lived artefacts, IP camera detection algorithm inaccuracies, and security vulnerabilities in IoT devices.
Kunev et al. [21]	Proposing a triage method to identify the most forensically valuable IoT devices in a crime scene. Developing a system to automate the extraction data from IoT devices, as well as statistical analysis and visualization tools.	Autopsy, bulkextractor, and proposal model.	SQLite databases.	The diversity of IoT devices complicates data extraction and analysis.
Dorai et al. [22]	Developing a framework for forensic data acquisition and analysis from IoT devices.	DEFA system	Data relate to smartphone and wearable devices.	There are admissibility and privacy concern.
Chi et al. [23]	Developing a framework for forensic data acquisition and analysis from IoT devices.	Android Studio and proposal framework.	IoT artifacts stored on user smart devices, Data from IoT sensors.	IoT forensics faces challenges with dispersed data, diverse devices, extraction difficulties, varying formats, limited security, and short data lifespans.



faces several limitations and challenges, including accessing historical and deleted data, a significant issue in both IoT forensics and the FSAC prototype. Additionally, the need for physical access to IoT devices remains a common challenge in digital forensics and security. Furthermore, connecting to various IoT devices with different wireless connection methods requires specific hardware support.

Lim et al. [19] proposed a methodology for evidence video management (EVM) that implemented a chain of custody mechanism and backup archiving mechanism to prevent erasure. The research constraints security breaches affecting the integrity of the evidence and the lack of an established chain of custody for digital evidence. Additionally, constraints on storage capacity for video records.

Other studies aimed to improve the investigation process itself. Azhar and Bate [20] explored an artifact-focused approach to examine and document artifacts in IoT smart environments, presenting a comprehensive investigation process. The research faces limitations with short-lived artefacts like Amazon Echo “cards”, high false positives and negatives from IP camera detection algorithms.

Kunev et al. [21] addressed the challenges of investigating IoT devices in forensics due to the absence of standardization and the use of real-time operating systems, proposing the use of open-source tools and prioritizing valuable devices for effective evidence identification. The challenging cause is when the heterogeneous nature of IoT devices, utilizing various formats, operating systems, network protocols, and hardware, poses challenges in data extraction and analysis. Dorai et al. [22] presented an approach to data analysis in forensic investigations involving wearable devices and IoT devices, using techniques to identify correlations and anomalies and enhance the accuracy and efficiency of the investigation process. The research acknowledges the evolving legal expectations regarding the admissibility of data extracted from wearables and IoT devices, as well as privacy concerns due to the large volumes of data stored.

Chi et al. [23] proposed a process for acquiring and analyzing data from IoT devices and related systems for forensic examination, highlighting the importance of using reliable and standardized

methods for such investigations. The research highlights the challenges in IoT forensics including extracting data from various platforms and hardware and standardizing different data formats for analysis. Additionally, limited security risks evidence tampering, and short data lifespans lead to potential loss due to storage limits.

III. METHODOLOGY





The first step in the research methodology involved setting up a test scenario for the IP cameras Hanhwa and Mobotix primarily used in Saudi Arabia as shown in Table III.

We provide a comprehensive explanation of the methodology used to analyze IP cameras, considering both the perspectives of cybersecurity and digital forensics. The methodology encompasses various steps, as illustrated in Fig. 2

A. Phase 1: Cybersecurity Analysis

The cybersecurity phase contains three sub-phases. They are as follows: Identifying Vulnerabilities, Evaluating vulnerabilities, and Exploiting

TABLE III
IP-CAMERAS INFORMATION.

Camera brand	Hanhwa	Mobotix
Manufacturer	Korea	Germany
Logo	 Hanwha Vision	
Model	PND-A9081RV	MX-VD1A-4-IR
IP Camera picture		

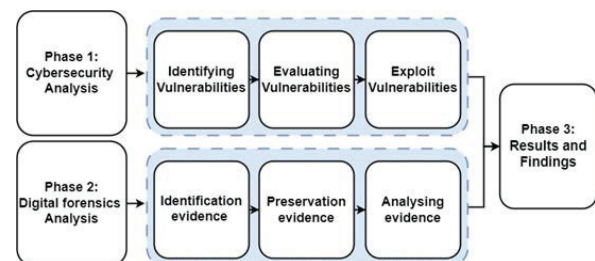


Fig. 2. Our methodology of IP-cameras analysis



vulnerabilities. However, before we delve into this analysis, it is crucial to present the IP addresses associated with Attacker, Hanwha camera, and Mobotix camera. Table IV presents these IP addresses, alongside unauthorized IP addresses attempting access. Once we have this foundational information, we can proceed with the following sub-phases:

TABLE IV
IP ADDRESS INFORMATION

Attacker IP	Hanwha camera	Mobotix camera
192.168.8.121	192.168.8.119	192.168.8.104

1) Identifying Vulnerabilities

This step involves deploying vulnerability assessment scanning tools such as Nikto, Nmap, and OpenVAS to scan for potential vulnerabilities in the devices. The results of these scans are detailed in the following tables:

- Table V presents findings from the Nikto scan, which will help for comprehensive assessment of web servers and identification of common vulnerabilities of IP cameras. The scan revealed several issues: Mobotix’s camera has a missing X-Content-Type-Options header, posing a risk of MIME type rendering vulnerabilities, requires authentication for the root directory, indicating potential access control issues, and only allows limited HTTP methods. Hanwha camera also has a missing X-Content-Type-Options header in the /cgi-bin/ directory, potentially leading to MIME type rendering issues, an improperly configured /clientaccesspolicy.xml file with wildcard entries requiring review, and the presence of a wp-config.php file, raising concerns about the exposure of sensitive credentials.
- Table VI displays results from the Nmap scan, offering additional insights into the cameras’ security posture through robust network scanning capabilities. For the Mobotix camera, the scan identified open ports at 80/HTTP and 443/HTTPS, which is vulnerable to authentication bypass through HTTP verb tamper-

ing, while ports 554/RTSP and 5555/FreeCiv showed no known vulnerabilities. In contrast, the Hanwha camera exhibited vulnerabilities at port 80/HTTP due to cross-domain and client access policy issues, and at port 443/HTTPS, which is susceptible to a Slowloris DOS attack (identified as CVE-2007-6750). These findings highlight critical areas for security improvement and provide a basis for further analysis in the comprehensive assessment of IP camera vulnerabilities.

TABLE V
RESULTS OF NIKTO SCANNING FOR BOTH CAMERAS.

Mobotix’s Camera	
Security Issue	Description
Missing X-Content-Type-Options Header	The site is missing the X-Content-Type-Options header, which can lead to content rendering vulnerabilities based on MIME types.
Authentication Required for Root Directory	The root directory requires authentication, which suggests potential access control issues.
Limited HTTP Methods	The allowed HTTP methods are OPTIONS, GET, HEAD, and POST. It’s important to review if any unneeded methods are enabled.
Hanwha’s Camera	
Security Issue	Description
Missing X-Content-Type-Options Header in /cgi-bin/ Directory	This could potentially allow the user agent to render content differently based on MIME type.
Improper Configuration in /clientaccesspolicy.xml	The file contains a full wildcard entry and 13 lines that require manual review for improper domains or wildcards.
Potential Sensitive Credentials in wp-config.php File	hp Fil The presence of this file raises concerns about the exposure of sensitive credentials.

- Table VII outlines outcomes from the OpenVAS scan, providing a comprehensive view of potential vulnerabilities within the systems. OpenVAS, with its extensive vulnerability scanning features, was instrumental in facilitating thorough assessments of the security posture of the IP-cameras and aiding in the identification and mitigation of potential vul-



nerabilities. For the Mobotix camera, the scan initially found 31 vulnerabilities and 1 CVE, which, after upgrading the firmware, were reduced to 27 vulnerabilities with the CVE issue resolved. Similarly, the Hanwha camera initially had 4 vulnerabilities and no CVEs, and after the firmware upgrade, the vulnerabilities were reduced to 3, with no CVEs identified in either case. These results demonstrate the effectiveness of firmware upgrades in enhancing the security of IP cameras.

TABLE VI
RESULT OF THE NMAP SCAN

IP-Cams	Open Ports/Service	Vulnerability	Exploit?
Mobotix	80/HTTP	Authentication bypass by HTTP verb tampering	Yes
	443/HTTPS		
	554/RTSP 5555/FreeCiv	No known vulnerabilities found	-
Hanwha	80/HTTP	cross-domain and client access policy	Yes
	443/HTTPS	Slowloris DOS attack IDs:CVE-2007-6750	Yes

TABLE VII
RESULT OF THE OPENVAS SCAN

IP-Camera	Result before upgrading firmware		Result after upgrading firmware	
	Number of vulnerabilities found	Number of CVE found	Number of vulnerabilities found	Number of CVE found
Mobotix	31	1	27	solved
Hanwha	4	0	3	0

2) Evaluating vulnerabilities

This step involves assessing the severity of identified vulnerabilities as shown in Table V, Table VI, and Table VII and determining their potential security issues. Due to these vulnerabilities, the IP camera management interface was successfully exploited to gain access, which is discussed in the following section. By utilizing various attack techniques, we aim to gain a better understanding of the potential risks and vulnerabilities of the system, we select several attacks that will enable us to evaluate and address the vulnerabilities of the camer-

as which are: DoS, Brute-force, and Unauthorized access.

3) Exploiting vulnerabilities

This step involves attempting to exploit identified vulnerabilities to gain unauthorized access to the devices. The results of these attempts, including performing brute-force attacks and achieving unauthorized access, are presented in Table VIII. The table shows that for the Mobotix camera, all attack types—Denial of Service (DoS), brute-force, and unauthorized access—were successful.

In contrast, for the Hanwha camera, brute-force and unauthorized access attacks were successful, while the DoS attack failed. These findings provide critical insights into the security weaknesses of each IP camera.

TABLE VIII
RESULT OF PERFORMING ATTACKS ON IP-CAMERAS

IP-Camera	Attack type		
	DoS	Brute-force	Unauthorized access
Mobotix	O	O	O
Hanwha	X	O	O

O: Attack Success. X: Attack Failed.

B. Phase 2: Digital Forensic Analysis

This phase involves identifying, preserving, and analyzing evidence from Hanwha and Mobotix IP cameras' log artifacts. The following sub-phases are typically involved:

1) Identification of evidence

This step involves identifying relevant log artifacts that may contain evidence related to a specific incident or investigation. Upon utilizing the digital forensic tool DFIRKuiper to acquire images from both IP cameras, we encountered issues with the DFIRKuiper tool, which was unable to parse evidence as detailed in Fig. 3. This failure could stem from several factors, including potential incompatibility between DFIRKuiper and the camera firmware, corrupted or incomplete log files, encryption or proprietary formatting of data, or limitations within DFIRKuiper itself. The case panel displaying



the parsing artifacts from the access log file of the Hanwha IP camera has not shown any results, as presented in Fig. 4. In the case of Mobotix, the results of the artifact parsing from the log file are depicted in Fig. 5.

We encountered a challenge when the acquired evidence could not be processed automatically. By carefully examining log files that could hold valuable information, we identified crucial log artifacts that potentially contain valuable evidence pertinent to the attack incident. The identified logs artifacts are as follows:

Hanwha IP Camera:

- System logs present in Fig. 6.
- Event logs present in Fig. 7.
- Access logs present in Fig. 8.

Mobotix IP Camera:

- One log file exists in Fig. 9.

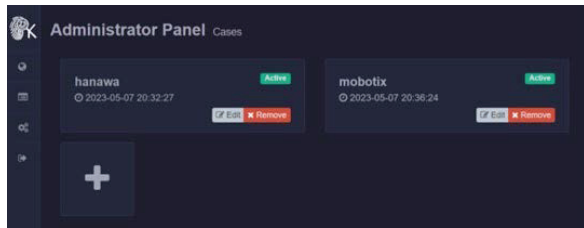


Fig. 3. DFIRKuiper Administrator Panel cases for both IP-Cameras.

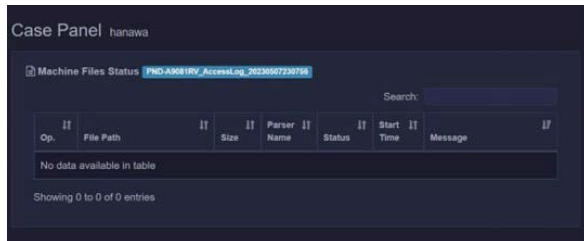


Fig. 4. Case Panel of Hanwha's access log.

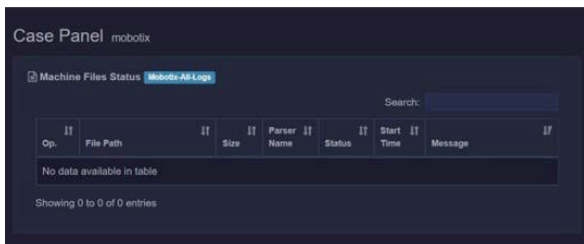


Fig. 5. Case Panel of Mobotix's access log.

No.	Date & Time	Description	Information
1	2023-05-18 09:43:17	Network	System get an IPv4 address: 192.168.8.179
2	2023-05-18 09:39:45	Network	Physical network connection is connected
3	2023-05-18 09:39:27	Network	System get an IPv4 address: 192.168.8.109
4	2023-05-18 09:39:16	HWSelfTest	HW Self test: NAND flash inspection result is success
5	2023-05-18 09:39:15	HWSelfTest	HW Self test: DDR memory inspection result is success
6	2023-05-18 09:39:15	HWSelfTest	HW Self test: CPU inspection result is success
7	2023-05-18 09:39:13	ConfigChange	Alarm Out created at Physical Port 2
8	2023-05-18 09:39:13	ConfigChange	Alarm In created at Physical Port 1
9	2023-05-18 09:39:13	SWSelfTest	SW Self test: NetworkServiceManager initialization is success
10	2023-05-18 09:39:13	SWSelfTest	SW Self test: UserEventManager() initialization is success
11	2023-05-18 09:39:13	SWSelfTest	SW Self test: UserEventManager() initialization is success
12	2023-05-18 09:39:13	PowerOn	Network camera power on.
13	2023-05-07 20:04:34	Network	System get an IPv4 address: 192.168.8.179
14	2023-05-07 20:04:34	Network	System get an IPv4 address: 192.168.8.109
15	2023-05-07 20:04:29	Network	Physical network connection is connected

Fig. 6. System Logs of Hanwha Camera.

No.	Date & Time	Description	Information
1	2023-05-18 09:44:11	GuestLogin	[RTSP] Channel 1 : anonymous login (192.168.8.109)
2	2023-05-18 09:43:50	GuestLogin	[RTSP] Channel 1 : anonymous login (192.168.8.109)
3	2023-05-18 09:43:27	AdminLogin	[HTTP] admin login failed (192.168.8.109)
4	2023-05-18 09:43:51	AdminLogin	[HTTP] admin login failed (192.168.8.109)
5	2023-05-18 09:43:42	AdminLogin	[HTTP] admin login failed (192.168.8.109)
6	2023-05-07 20:07:35	GuestLogin	[RTSP] Channel 1 : anonymous login (192.168.8.109)
7	2023-05-07 20:07:31	GuestLogin	[RTSP] Channel 1 : anonymous login (192.168.8.109)
8	2023-05-07 20:07:18	AdminLogin	[HTTP] admin login failed (192.168.8.109)
9	2023-04-07 10:51:56	GuestLogin	[RTSP] Channel 1 : anonymous login (192.168.8.121)
10	2023-04-07 10:51:50	GuestLogin	[RTSP] Channel 1 : anonymous login (192.168.8.121)
11	2023-04-07 10:50:25	AdminLogin	[HTTP] admin login failed (192.168.8.109)
12	2023-04-07 10:49:51	GuestLogin	[RTSP] Channel 1 : anonymous login (192.168.8.109)
13	2023-04-07 10:49:48	GuestLogin	[RTSP] Channel 1 : anonymous login (192.168.8.109)
14	2023-04-07 10:31:19	GuestLogin	[RTSP] Channel 1 : anonymous login (192.168.8.109)
15	2023-04-07 10:31:08	GuestLogin	[RTSP] Channel 1 : anonymous login (192.168.8.109)

Fig. 7. Event Logs of Hanwha's Camera.

No.	Date & Time	Description	Information
1	2023-05-18 09:44:33	SocialDistancingInitiation	[Channel 1] SocialDistancingDetection Detected End
2	2023-05-18 09:44:33	SocialDistancingInitiation	[Channel 1] SocialDistancingDetection Detected Start
3	2023-05-18 09:44:32	SocialDistancingInitiation	[Channel 1] SocialDistancingDetection Detected End
4	2023-05-18 09:44:32	SocialDistancingInitiation	[Channel 1] SocialDistancingDetection Detected End
5	2023-05-18 09:44:11	SocialDistancingInitiation	[Channel 1] SocialDistancingDetection Detected End
6	2023-05-18 09:44:11	SocialDistancingInitiation	[Channel 1] SocialDistancingDetection Detected Start
7	2023-05-18 09:44:08	ObjectDetection	[Channel 1] Object Detection Start
8	2023-05-18 09:44:04	ShockDetection	Shock Event Detected
9	2023-05-18 09:44:03	ShockDetection	Shock Event Detected
10	2023-05-18 09:44:03	MotionDetection	[Channel 1] Motion Detection Start
11	2023-05-18 09:44:03	ShockDetection	Shock Event Detected
12	2023-05-18 09:44:02	ObjectDetection	[Channel 1] Object Detection End
13	2023-05-18 09:44:02	ShockDetection	Shock Event Detected

Fig. 8. Access Logs of Hanwha's Camera.

System	Date	Time	Message
System	Mon Apr 10 23:35:25 2023	-D-Link@	### 192.168.8.109 GET / HTTP/1.1
Network	Mon Apr 10 23:35:25 2023	sdh@cam001	### 192.168.8.109 GET / HTTP/1.1
UDPS	Mon Apr 10 23:35:25 2023	-MGR@	### 192.168.8.109 GET / HTTP/1.1
Mail	Mon Apr 10 23:35:25 2023	-admin@	### 192.168.8.109 GET / HTTP/1.1
FTP	Mon Apr 10 23:35:25 2023	-admin@	### 192.168.8.109 GET / HTTP/1.1
HTTP	Mon Apr 10 23:35:25 2023	-customer@	### 192.168.8.109 GET / HTTP/1.1
Events	Mon Apr 10 23:35:25 2023	-MGR@	### 192.168.8.109 GET / HTTP/1.1
Storage Management	Mon Apr 10 23:35:25 2023	-sbsd-client@	### 192.168.8.109 GET / HTTP/1.1
Recording	Mon Apr 10 23:35:25 2023	-admin@	### 192.168.8.109 GET / HTTP/1.1
Schedule	Mon Apr 10 23:35:25 2023	-M10@	### 192.168.8.109 GET / HTTP/1.1
File Location	Mon Apr 10 23:35:25 2023	-admin@	### 192.168.8.109 GET / HTTP/1.1
View Information	Mon Apr 10 23:35:25 2023	-admin@	### 192.168.8.109 GET / HTTP/1.1
Log File	Mon Apr 10 23:35:25 2023	-ANAL@	### 192.168.8.109 GET / HTTP/1.1
User Information	Mon Apr 10 23:35:25 2023	-manager@	### 192.168.8.109 GET / HTTP/1.1
Camera Information	Mon Apr 10 23:35:25 2023	-MGR@	### 192.168.8.109 GET / HTTP/1.1
Factory Default	Mon Apr 10 23:35:25 2023	-operator@	### 192.168.8.109 GET / HTTP/1.1

Fig. 9. Log File of the Mobotix's Camera.



2) Preservation of evidence

We generate the hashing of the logs file as presented in Table IX, which involves ensuring that the identified log artifacts are preserved in a forensically sound manner to maintain their integrity and admissibility as evidence.

TABLE IX
HASH VALUE FOR EACH LOG FILE.

Logs filename	MD5 hash value
PND-A9081RV_AccessLog.txt	d701a81ecd-fac405e4f4530df7fdc4b3
PND-A9081RV_EventLog.txt	5251116f518cf3b57c-72d9724a6d7bf4
PND-A9081RV_SystemLog.txt	0125aad1d05dfd-6b549a491967f68186
MOVE-VD1A-4-IR-0003C5C034FB_log.txt	5706aa8d3ad69b6f-e3cd820429df75d1

3) Analysis of evidence

This critical sub-phase involved an in-depth analysis of the preserved log artifacts, employing advanced forensic tools and techniques to extract relevant information. Specifically focusing on the Hanwha camera system, a comprehensive examination of its Access logs, Event logs, and System logs was conducted. Despite the thorough scrutiny, locating definitive traces of the attacks posed a challenge. The logs only revealed instances of unauthorized access, indicated by an IP address distinct from the camera owner, as depicted in Fig. 10.

However, the absence of explicit attack indicators highlighted the sophisticated nature of the intrusion, prompting the need for more advanced detection methods to uncover subtler digital evidence and enhance the depth of our analysis. Moreover, concerning the event logs and system logs, they did not display the attacker's IP address. This absence of crucial information was evident from the disparity between the logged data and the representation in Fig. 11 and Fig. 12.

In the examination of the Mobotix system, which generates a single log file named MOVE-VD1A-4-IR-0003C5C034FB_log.txt, the findings from this log file are meticulously detailed in Table X. This table showcases the reflection of various attacks within

the Mobotix's log data. Specifically, it outlines the results of attacks of Denial of Service (DoS), brute-force attempts, and unauthorized access, indicating whether each attack was successfully reflected in the log file. The table provides reflection of attacks as either successful or failed in the log file.

```
[2023-04-06 21:15:45] [AdminLogout] [[RTSP] Channel 1 : admin logout (192.168.8.121)]
[2023-04-06 21:15:41] [AdminLogin] [[RTSP] Channel 1 : admin login (192.168.8.121)]
[2023-04-06 21:15:41] [AdminLogout] [[RTSP] Channel 1 : admin logout (192.168.8.121)]
[2023-04-06 21:15:40] [AdminLogin] [[RTSP] Channel 1 : admin login (192.168.8.121)]
[2023-04-06 19:34:55] [AdminLogout] [[RTSP] Channel 1 : admin logout (192.168.8.121)]
[2023-04-06 19:34:53] [AdminLogin] [[RTSP] Channel 1 : admin login (192.168.8.121)]
```

Fig. 10. Access logs showing an attempt to login by the attacker.

```
PND-A9081RV_EventLog_20230507230902.txt - Notepad
File Edit Format View Help
[2023-04-07 13:31:02] [DefocusDetection] [[Channel:1] Defocus Event Start]
[2023-04-07 13:30:42] [MotionDetection] [[Channel:1] Motion Detection Start]
[2023-04-07 13:30:36] [MotionDetection] [[Channel:1] Motion Detection End]
[2023-04-07 13:30:32] [MotionDetection] [[Channel:1] Motion Detection Start]
[2023-04-07 13:30:05] [DefocusDetection] [[Channel:1] Defocus Event End]
[2023-04-07 13:29:57] [DefocusDetection] [[Channel:1] Defocus Event Start]
[2023-04-07 13:29:22] [MotionDetection] [[Channel:1] Motion Detection End]
[2023-04-07 13:29:16] [MotionDetection] [[Channel:1] Motion Detection Start]
[2023-04-07 13:29:00] [DefocusDetection] [[Channel:1] Defocus Event End]
[2023-04-07 13:28:52] [DefocusDetection] [[Channel:1] Defocus Event Start]
[2023-04-07 13:27:54] [DefocusDetection] [[Channel:1] Defocus Event End]
[2023-04-07 13:27:47] [DefocusDetection] [[Channel:1] Defocus Event Start]
[2023-04-07 13:27:18] [MotionDetection] [[Channel:1] Motion Detection End]
[2023-04-07 13:27:13] [MotionDetection] [[Channel:1] Motion Detection Start]
[2023-04-07 13:26:49] [MotionDetection] [[Channel:1] Motion Detection End]
[2023-04-07 13:26:49] [DefocusDetection] [[Channel:1] Defocus Event End]
```

Fig. 11. Event logs from Hanwha camera.

```
PND-A9081RV_SystemLog_20230507230902.txt - Notepad
File Edit Format View Help
[2023-04-07 10:00:04] [ConfigChange] [[admin@192.168.8.109] User 1 Authority (Audio-out): Off -> On]
[2023-04-07 10:00:04] [ConfigChange] [[admin@192.168.8.109] User 1 Authority (Audio-in): Off -> On]
[2023-04-07 10:00:04] [ConfigChange] [[admin@192.168.8.109] User 1 Authority (Profile): Off -> On]
[2023-04-07 10:00:04] [ConfigChange] [[admin@192.168.8.109] User 1 Password: **** -> ****]
[2023-04-07 10:00:04] [ConfigChange] [[admin@192.168.8.109] User 1 Enable: Off -> On]
[2023-04-07 10:00:04] [ConfigChange] [[admin@192.168.8.109] Guest Authority (Profile): Off -> On]
[2023-04-07 10:00:04] [ConfigChange] [[admin@192.168.8.109] Guest Access: Off -> On]
[2023-04-07 09:59:06] [ConfigChange] [[Channel:1] Tampering Detection Enable: Off -> On]
[2023-04-07 09:59:06] [ConfigChange] [[Channel:1] IVA : Off -> On]
[2023-04-07 09:59:05] [ConfigChange] [[Channel:1] Motion Detection Record : Off -> On]
[2023-04-07 09:59:05] [ConfigChange] [[Channel:1] Motion Detection Alarm Out : None -> Always]
[2023-04-07 09:59:05] [ConfigChange] [[Channel:1] Motion Detection : Off -> On]
```

Fig. 12. Event logs from Hanwha camera.

```
File Edit Format View Help
[Mon Apr 10 22:37:14 2023] --admin@:ffff:192.168.8.109 GET /cgi-bin/loadcamerastate.cgi HTTP/1.1
[Mon Apr 10 22:38:49 2023] --admin@:ffff:192.168.8.109 GET /cgi-bin/getlog.cgi HTTP/1.1
[Mon Apr 10 23:35:21 2023] --root@:ffff:192.168.8.121 GET / HTTP/1.1
[Mon Apr 10 23:35:21 2023] --root@:ffff:192.168.8.121 GET / HTTP/1.1
[Mon Apr 10 23:35:22 2023] --MGR@:ffff:192.168.8.121 GET / HTTP/1.1
[Mon Apr 10 23:35:22 2023] --MAIL@:ffff:192.168.8.121 GET / HTTP/1.1
[Mon Apr 10 23:35:22 2023] --storwatch@:ffff:192.168.8.121 GET / HTTP/1.1
[Mon Apr 10 23:35:22 2023] --admin@:ffff:192.168.8.121 GET / HTTP/1.1
[Mon Apr 10 23:35:22 2023] --user@:ffff:192.168.8.121 GET / HTTP/1.1
[Mon Apr 10 23:35:22 2023] --MGR@:ffff:192.168.8.121 GET / HTTP/1.1
[Mon Apr 10 23:35:22 2023] --at440@:ffff:192.168.8.121 GET / HTTP/1.1
[Mon Apr 10 23:35:22 2023] --FIELD@:ffff:192.168.8.121 GET / HTTP/1.1
[Mon Apr 10 23:35:22 2023] --root@:ffff:192.168.8.121 GET / HTTP/1.1
[Mon Apr 10 23:35:22 2023] --HELL@:ffff:192.168.8.121 GET / HTTP/1.1
[Mon Apr 10 23:35:22 2023] --mtch@:ffff:192.168.8.121 GET / HTTP/1.1
[Mon Apr 10 23:35:22 2023] --User@:ffff:192.168.8.121 GET / HTTP/1.1
[Mon Apr 10 23:35:22 2023] --devic@:ffff:192.168.8.121 GET / HTTP/1.1
[Mon Apr 10 23:35:22 2023] --cisco@:ffff:192.168.8.121 GET / HTTP/1.1
[Mon Apr 10 23:35:23 2023] --Administrator@:ffff:192.168.8.121 GET / HTTP/1.1
[Mon Apr 10 23:35:23 2023] --MANAGER@:ffff:192.168.8.121 GET / HTTP/1.1
[Mon Apr 10 23:35:23 2023] --MAIL@:ffff:192.168.8.121 GET / HTTP/1.1
```

Fig. 13. Brute-force attack reflected on access log.

```
[Tue Apr 11 04:09:05 2023] --admin@:ffff:192.168.8.121 GET /cgi-bin/showdate.cgi HTTP/1.1
[Tue Apr 11 04:09:09 2023] --admin@:ffff:192.168.8.121 GET /cgi-bin/getlog.cgi HTTP/1.1
[Tue Apr 11 04:09:46 2023] --admin@:ffff:192.168.8.121 GET /cgi-bin/server_openvpn.cgi HTTP/1.1
[Tue Apr 11 04:09:48 2023] --admin@:ffff:192.168.8.121 GET /cgi-bin/getopenvpnlog.cgi HTTP/1.1
[Tue Apr 11 04:09:53 2023] --admin@:ffff:192.168.8.121 GET /cgi-bin/server_https.cgi HTTP/1.1
[Tue Apr 11 04:10:06 2023] --admin@:ffff:192.168.8.121 GET /cgi-bin/server_dot1x.cgi HTTP/1.1
```

Fig. 14. Attacker changed IP camera configuration in system log.



TABLE X
RESULT OF ATTACK REFLECTED ON MOBOTIX'S LOG FILE.

Attack	Reflect on log
DoS	X
Brute-force	O
Unauthorized access	O

O: Attack Successfully reflected in log. X: Attack Failed to reflect in log.

C. Phase 3: Results and Findings

This phase involves presenting the results of the cybersecurity and digital forensic analysis conducted on Hanwha and Mobotix IP cameras. All the results, findings, and recommendations will be documented and presented in Appendix A and Appendix B, which will be provided to the relevant stakeholders. This research includes a detailed description of the vulnerabilities found, the exploitation techniques used, and the recommended mitigation measures to prevent similar attacks in the future. Based on phase 1 and phase 2, we prepare a following documents:

- A. Cybersecurity Report.
- B. Digital Forensic Guidelines.

IV. ANALYSIS

Based on the implementation, the analysis would involve identifying the vulnerabilities of the Hanwha and Mobotix IP cameras to cyberattacks. The analysis would also include exploring and proposing the use of different attack techniques, and evaluating how effective they are in compromising the security of the IP camera administration web page. The study conducted a comprehensive analysis of vulnerabilities in Hanwha and Mobotix IP cameras, with a specific focus on potential cyberattacks and security breaches. By employing various scanning tools such as Nikto, Nmap, and OpenVAS, we successfully identified and addressed critical security issues in both camera systems.

In the case of Mobotix, vulnerabilities related to content rendering inconsistencies and potential

access control problems were discovered. The absence of certain headers and limited HTTP methods exposed potential attack vectors. Through rigorous scanning and subsequent system upgrades, these vulnerabilities were effectively mitigated, emphasizing the importance of prompt software updates in maintaining robust security protocols.

Similarly, the Hanwha camera system exhibited vulnerabilities, including content rendering risks and improper configuration in specific files. Addressing these concerns proved pivotal in ensuring the overall security of the IP camera network. The study's approach also extended to simulating real-world cyber threats, including Distributed Denial-of-Service (DDoS) attacks. By employing tools like Metasploit and Hydra, we were able to assess vulnerabilities related to DoS and unauthorized access, showcasing the significance of robust password policies in preventing unauthorized entry into camera systems. Furthermore, we emphasized the critical role of log analysis in detecting and preventing potential security breaches. By preserving logs securely, we ensured the availability of crucial data for future analysis, thereby enhancing the reliability and admissibility of digital forensic evidence. This meticulous approach not only safeguards against accidental modifications or losses but also ensures the integrity and authenticity of the preserved logs, crucial for any subsequent investigations. Additionally, the study highlighted the challenges in obtaining digital forensic evidence from IP cameras, particularly in the context of Saudi Arabia. By addressing these challenges and improving the digital forensic processes related to IP cameras, the research contributes significantly to advancing cybersecurity practices in the region.

V. CONCLUSIONS AND FUTURE WORK

In conclusion, this research aimed to assess the security vulnerabilities of two commonly used IP cameras in Saudi Arabia and explore potential attack techniques to evaluate their effectiveness. The research underscores the importance of com-



prehending the security implications associated with IoT devices, particularly IP cameras, considering their widespread use in the country's smart city architecture. We identified several vulnerabilities in the cameras and addressed them by upgrading the systems. Additionally, the cameras were tested for their resistance to various attack techniques, highlighting the importance of implementing best practices such as changing default passwords and preserving logs securely to enhance the security and reliability of IP cameras. Nonetheless, the project highlights gaps in the existing literature related to standardization in data acquisition, analysis, and interpretation of IP-camera evidence, emphasizing the need for further research in this area.

Our research was designed to address critical research question. We conducted vulnerability assessments on the cameras to evaluate their susceptibility to cyberattacks, while also exploring methods of extracting relevant evidence from these devices using cybersecurity tools. We provide valuable insights into the vulnerabilities and risks associated with IP cameras, and we have provided clear guidelines for investigators on how to obtain reliable and admissible digital forensic evidence from these devices.

By shedding light on these important issues, we propose addressing the research question: "Can machine learning improve the prediction and prevention of cyberattacks on IP cameras compared to traditional detection methods?" To explore this, we plan to use simulations and real-world deployments to compare the effectiveness of machine learning models against conventional rule-based systems. Additionally, we aim to develop methodologies that ensure the integrity and reliability of data collected from IP cameras for forensic purposes, involving rigorous testing of forensic capabilities focusing on data integrity, accurate timestamp verification, and effective data recovery methods. These initiatives strive to ensure that forensic data from IP cameras is both reliable and admissible in legal contexts, thus addressing challenges in cybersecurity and digital forensics and enhancing device security through more proactive and efficient methods.

Additionally, by integrating the IP camera system with an SIEM solution, the cybersecurity team will be alerted if there are any potential attacks.

FUNDING

This article did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

CONFLICT OF INTEREST

Authors declare that they have no conflict of interest.

REFERENCES

- [1] Global ip camera market on target for over 32billionby2030, Dec. 2023 [Online].
- [2] K. Kim et al., "Cybersecurity and cyber forensics for smart cities: A comprehensive literature review and survey," *Sensors*, vol. 23, no. 7, p. 3681, 2023.
- [3] F. A. Alfouzan et al., "An efficient framework for securing the smart city communication networks," *Sensors*, vol. 22, no. 8, p. 3053, 2022.
- [4] R. Alshalawi and T. Alghamdi, "Forensic tool for wireless surveillance camera," in 2017 19th international conference on advanced communication technology (ICACT), IEEE, 2017, pp. 536–540.
- [5] S. W. Tho and Y. Y. Yeung, "Innovative ip camera applications for scientific investigation," *School Science Review*, vol. 96, no. 356, pp. 58–62, 2015.
- [6] P. A. Abdalla and C. Varol, "Testing iot security: The case study of an ip camera," in 2020 8th International Symposium on Digital Forensics and Security (ISDFS), IEEE, 2020, pp. 1–5.
- [7] G. Alexandrie, "Surveillance cameras and crime: A review of randomized and natural experiments," *Journal of Scandinavian Studies in Criminology and Crime Prevention*, vol. 18, no. 2, pp. 210–222, 2017.
- [8] L. R. Castro, "The privacy leakage of ip camera systems," 2022.
- [9] A. Manske, *Conducting a vulnerability assessment of an ip camera*, 2019.
- [10] G. Dzwigala et al., "A testing methodology for the internet of things affordable ip cameras," in *Communication and Intelligent Systems: Proceedings of ICCIS 2021*, Springer,



- 2022, pp. 463–479.
- [11] T. Stroeven and F. So’derman, Cybersecurity evaluation of an ip camera, 2022.
- [12] P. Vennam et al., “Attacks and preventive measures on video surveillance systems: A review,” *Applied Sciences*, vol. 11, no. 12, p. 5571, 2021.
- [13] E. Dragonas et al., “Iot forensics: Exploiting unexplored log records from the hikvision file system,” *Journal of Forensic Sciences*,
- [14] O. Almazrouei et al., “Penetration testing for iot security: The case study of a wireless ip security cam,” in *2023 IEEE 2nd International Conference on AI in Cybersecurity (ICAIC)*, IEEE, 2023, pp. 1–5.
- [15] G. Bella et al., “Petiot: Penetration testing the internet of things,” *Internet of Things*, vol. 22, p. 100 707, 2023.
- [16] G. Porter, “The reliability of cctv images as forensic evidence,” Ph.D. dissertation, University of Western Sydney (Australia), 2011.
- [17] P. Sukanto et al., “Forensic digital analysis for cctv video recording,” *International Journal of Science, Technology & Management*, vol. 3, no. 1, pp. 284–291, 2022.
- [18] C. Meffert et al., “Forensic state acquisition from internet of things (fsaiot) a general framework and practical approach for iot forensics through iot device state acquisition,” in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, 2017, pp. 1–11.
- [19] K.-S. Lim et al., “Evm: A new methodology for evidential video management in digital cctv systems,” in *Future Information Technology, Application, and Service: FutureTech 2012 Volume 2*, Springer, 2012, pp. 225–230.
- [20] M. Azhar and S. B. L. Bate, “Recovery of forensic artefacts from a smart home iot ecosystem,” in *CYBER 2019: The Fourth International Conference on Cyber- Technologies and Cyber-Systems*, 2019.
- [21] D. Kunev et al., “The investigative significance of digital artefacts discovered in forensic images of household iot devices using open-source software,” *International Journal of Intelligent Computing Research*, vol. 12, no. 1, pp. 1096–1104, 2021.
- [22] G. Dorai et al., “Data extraction and forensic analysis for smartphone paired wearables and iot devices.,” in *HICSS*, 2020, pp. 1–10.
- [23] H. Chi et al., “A framework for iot data acquisition and forensics analysis,” in *2018 IEEE International Conference on Big Data (Big Data)*, IEEE, 2018, pp. 5142–5146.

APPENDIXES

APPENDIX A

CYBERSECURITY REPORT

EXECUTIVE SUMMARY

This document presents the initial security assessment report conducted by a penetration tester on IP cameras manufactured by Mobotix and Hanwha. The objective of the assessment was to identify and report on the security status of these IP cameras, considering the increasing risk posed by cyber threats in the context of internet-connected devices and IoTs. The scope of the assessment covered the following areas:

- 1) *Identification of security vulnerabilities:* The assessment aimed to identify any potential vulnerabilities present in the IP cameras, which could potentially expose them to unauthorized access, data breaches, or other security risks.
- 2) *Access control:* The assessment focused on ensuring that only authorized users had access to the IP cameras and their associated data. This included evaluating the effectiveness of authentication mechanisms and access controls implemented by the camera systems.
- 3) *Vulnerability scanning and penetration testing:* The assessment involved conducting vulnerability scans and penetration tests to identify any weaknesses or gaps in the IP camera system’s security defenses. These tests were aimed at simulating real-world attack scenarios and assessing the system’s resilience against various exploitation attempts.

PENETRATION TESTING PHASES

The penetration testing was conducted in multiple phases, including reconnaissance, scanning, vulnerability assessment, and exploitation. Each phase aimed to systematically evaluate the security posture of the IP cameras, identify potential vulnerabilities, and provide recommendations for remediation.

- 1.1. *Reconnaissance: The reconnaissance phase proved to be an indispensable aspect of the*



penetration test, providing valuable insights and knowledge that informed subsequent phases of the assessment. We identified key information during this phase, such as the camera models, firmware versions, and software in use as shown in Table I.

TABLE I
KEY INFORMATION ON BOTH IP-CAMERAS.

IP-camera	Firmware Ver.	Software
Mobotix	16	mb20221116RP
Hanhwa	10	PNO-A980iR_2.11.10_20220519_R614

1.2. Scanning: During the scanning phase, we utilized scanning tools such as Nmap and OpenVAS to conduct in-depth scans of the IP cameras and their associated networks. Nmap was used to identify open ports and services running on the cameras, while OpenVAS was used to perform vulnerability scans on these services. These tools helped us to identify potential security weaknesses and assess the overall security posture of the IP cameras and their networks.

Mobotix Camera: The Nikto scan result on port 80, as shown in Fig. 1, indicates that the server did not provide a banner, and there is a missing X-Content-Type-Options header, which could allow the user agent to render the content of the site in a different fashion to the MIME type. Additionally, the root directory requires authentication for the realm MegapixelIPCamera. No CGI directories were found, and the allowed HTTP methods are OPTIONS, GET, HEAD, and POST. The scan reported 8254 requests with no errors, and the total scan duration was 175 seconds.

The Nmap scan result shows that there are a few potential vulnerabilities on the target machine. The http-method-tamper script has identified a vulnerability where the web server is vulnerable to authentication bypass via HTTP verb tampering as shown in Fig. 2

```

root@kali:~# nmap -h 192.168.8.104
Nikto v2.5.0

+ Target IP: 192.168.8.104
+ Target Hostname: 192.168.8.104
+ Target Port: 80
+ Start Time: 2023-04-01 14:06:52 (GMT3)

+ Server: No banner retrieved
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ / - Requires Authentication for realm 'MegapixelIPCamera'
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 16 error(s) and 1 item(s) reported on remote host
+ End Time: 2023-04-01 14:13:36 (GMT3) (404 seconds)

+ 1 host(s) tested
    
```

Fig. 1. Result of the Nikto scanning for Mobotix Camera.

The OpenVas result scanning had different results before and after upgrading the Mobotix’s software as shown in Fig. 3, and the main difference is there was CVE vulnerability and it is solved after the upgrading as shown in Fig. 4 and Fig. 5.

```

Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-08 18:49 +03
Nmap scan report for 192.168.8.104
Host is up (0.78s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
|_HTTP-CVEFF: Couldn't find any CSRF vulnerabilities.
|_http-method-tamper:
|_VULNERABLE:
|_ Authentication bypass via HTTP verb tampering
|_ State: VULNERABLE (Exploitable)
|_ This web server contains password protected resources vulnerable to authentication bypass vulnerabilities via HTTP verb tampering. This is often found in web servers that only limit access to the common HTTP methods and in misconfigured .htaccess files.
|_ Extra information:
|_ URIs suspected to be vulnerable to HTTP verb tampering:
|_ / [HEAD]
|_ References:
|_ https://www.owasp.org/index.php/Testing_for_HTTP_Methods_and_XST_S280WASP-CM-008529
|_ http://www.imperva.com/resources/glossary/http_verb_tampering.html
|_ http://cve.mitre.org/data/definitions/274.html
|_ http://www.kit.com.ar/labs/htexploit/
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ 43/tcp open https
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-method-tamper:
|_ VULNERABLE:
|_ Authentication bypass via HTTP verb tampering
|_ State: VULNERABLE (Exploitable)
|_ This web server contains password protected resources vulnerable to authentication bypass vulnerabilities via HTTP verb tampering. This is often found in web servers that only limit access to the common HTTP methods and in misconfigured .htaccess files.
|_ Extra information:
|_ URIs suspected to be vulnerable to HTTP verb tampering:
|_ / [HEAD]
|_ References:
|_ https://www.owasp.org/index.php/Testing_for_HTTP_Methods_and_XST_S280WASP-CM-008529
|_ http://www.imperva.com/resources/glossary/http_verb_tampering.html
|_ http://cve.mitre.org/data/definitions/274.html
|_ http://www.kit.com.ar/labs/htexploit/
    
```

Fig. 2. Result of the Nmap scanning for Mobotix Camera.

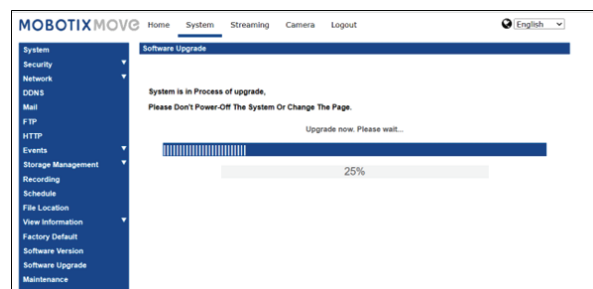


Fig. 3. Upgrading Mobotix’s software.



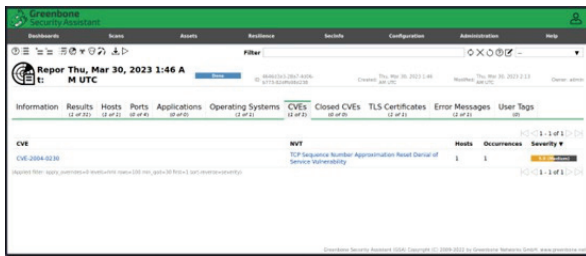


Fig. 4. CVE vulnerability before upgrading Mobotix's software.

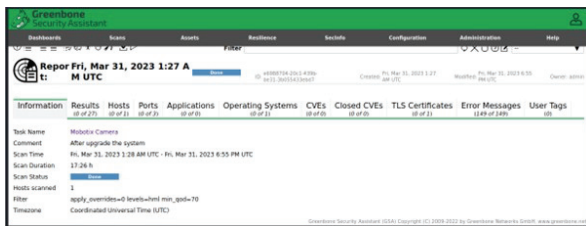


Fig. 5. Result of OpenVAS after upgrading Mobotix's software.

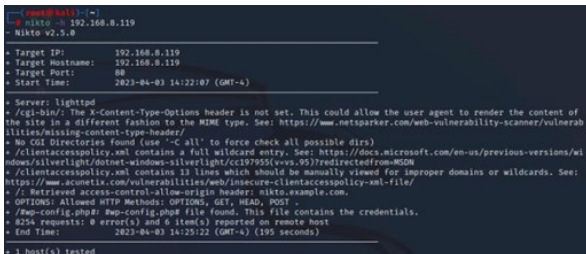


Fig. 6. Result of the Nikto scanning for Hanwha's Camera.

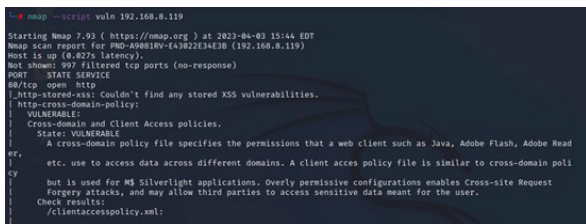


Fig. 7. Nmap scan result of port 80 for the Hanwha camera.

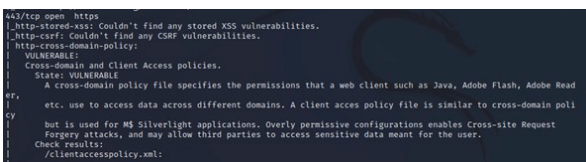


Fig. 8. Nmap scan result of port 443 for the Hanwha camera.

Hanwha Camera: Nikto identified several potential security issues with the web server configuration as shown in Fig. 6, the /cgi-bin/ directory does not set the X-Content-Type-Options header, which could allow the user agent to render the content of the site in a different fashion to the MIME type. The scan also found that the /clientaccesspolicy.xml file contains a full wildcard entry and 13 lines that should be manually viewed for improper domains or wildcards. Additionally, the scan discovered the presence of a wp-config.php file, which could contain sensitive credentials.

Nmap scan identified an open HTTP port and an open HTTPS port. The scan also identified the following vulnerabilities on the HTTP and HTTPS services:

- A vulnerability cross-domain and client access policies was found on both ports. Shown in Fig. 7 and Fig. 8.
- Slowloris DoS attack (CVE-2007-6750) was found on the HTTPS port. Shown in Fig. 9.

The OpenVAS result scanning had slightly dif-

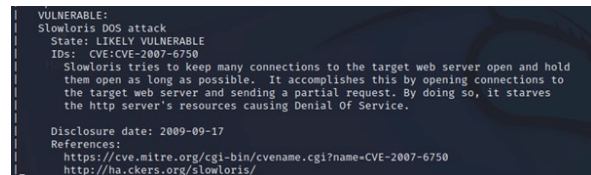


Fig. 9. Slowloris DoS attack in port 443 for the Hanwha Camera.

ferent results. Before and after upgrading the Hanwha's software as shown in Fig. 10 and Fig. 11 which is one vulnerability was solved. Fig. 12 shows Hanwha's software during upgrading.

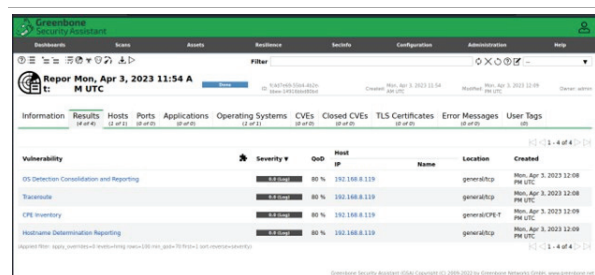


Fig. 10. OpenVAS result before upgrading Hanwha's software.



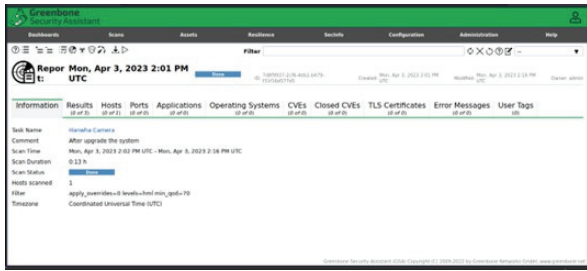


Fig. 11. OpenVAS result after upgrading Hanhwa’s software.

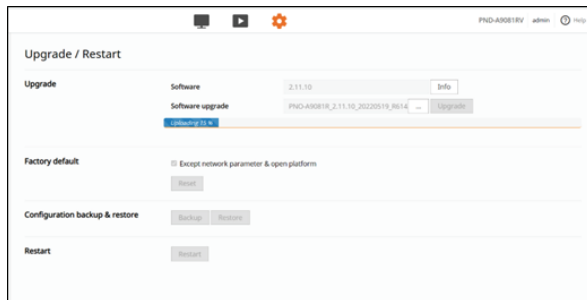


Fig. 12. Screenshot during upgrading Hanhwa’s software.

Hanwha DoS Attack: Exploit of the firmware CVE-2007-6750 by using the Metasploit tool Fig. 15.

1.3. Vulnerability assessment: After completing the reconnaissance and scanning phases, we performed a vulnerability assessment on the IP cameras using OpenVAS. This involved analyzing the information gathered during the previous phases to identify potential vulnerabilities in the cameras’ security architecture. OpenVAS was used to scan for known vulnerabilities in the camera firmware and the software running on them. The results of the vulnerability scan were analyzed to identify critical medium vulnerabilities as shown in Table II.

Motorix	Hanwha	Severity
CVE-2004-0230	CVE-2007-6750	Medium
Authentication bypass by HTTP verb tampering	cross-domain and client-access policy	Medium

1.4. Exploitation: During the exploitation phase, we attempted to exploit the vulnerabilities identified in the previous phase to gain unauthorized access to the IP cameras. We used Metasploit tool to exploit the vulnerabilities. Our goal was to demonstrate the severity of the vulnerabilities and the potential impact of a successful attack as below.

Hydra tool: We attempted brute-force attack as well as unauthorized access through this phase in both cameras as shown in Fig. 13 and Fig. 14. We were able to validate the existence and impact of the identified vulnerabilities.

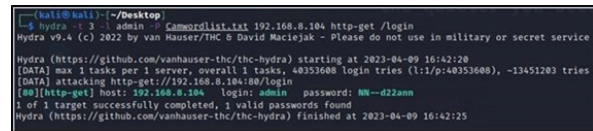


Fig. 13. Brute-force of Motorix’s camera

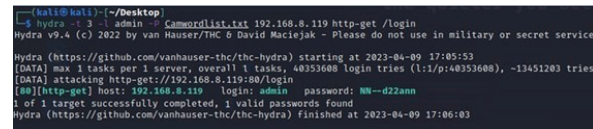


Fig. 14. Brute-force of Hanwha’s camera.

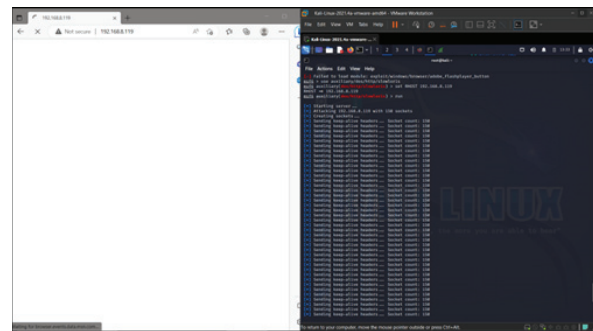


Fig. 15. DoS attack performed on Hanwha.

RISK ASSESSMENT

Based on the vulnerabilities identified, the following are the risk assessments for the IP cameras:

Motorix Camera

The vulnerabilities discovered in the Motorix IP camera present a medium level risk to the or-



ganization. The authentication bypass vulnerability could potentially allow unauthorized access to password-protected resources on the server, while the Slowloris DoS attack vulnerability could render the server unavailable to legitimate users. However, the risks can be mitigated by implementing proper input validation and sanitization to prevent HTTP verb tampering attacks, and by deploying security measures such as web application firewalls to detect and block Slowloris DoS attacks.

Hanwha Camera

The vulnerabilities discovered in the Hanwha IP camera present a medium level risk to the organization. The cross-domain and client access policy vulnerabilities could potentially allow unauthorized access to the camera's data by attackers, while the Slowloris DoS attack vulnerability could render the server unavailable to legitimate users. However, the risks can be mitigated by upgrading the system to eliminate the vulnerabilities, implementing proper access control mechanisms to restrict unauthorized access, and deploying security measures such as web application firewalls to detect and block Slowloris DoS attacks.

APPENDIX B

DIGITAL FORENSIC GUIDELINES FOR EXTRACT AN IP-CAMERA EVIDENCE

Introduction

Digital forensics plays a critical role in investigating and analyzing digital devices for the purpose of uncovering evidence that can be used in legal proceedings. As technology evolves, so do the challenges faced by digital forensics investigators. One such challenge arises when dealing with IP-cameras devices that do not have an SD card or are not connected to a server. They require a specialized approach to ensure the successful identification, preservation, analysis, documentation, and presentation of digital evidence.

Objective

The objective of this guideline is to provide digital

forensics investigators with a structured framework to effectively navigate the investigation process when dealing with devices that lack an SD card or are not connected to a server. By following this guideline, investigators will be equipped with the necessary knowledge and techniques to overcome the unique challenges associated with IP camera.

Scope of Applicability

The scope of applicability for these guidelines is limited to digital forensic investigators who belong to the following segments:

- SME (Small and Medium Enterprises)
- Government or non-government entities

These guidelines provide guidance for conducting a digital forensic investigation utilizing any computing device, whether it is (e.g., personal computer or equipment in a digital forensic lab).

The guidelines are intended to raise awareness of best practices for securely, reliably, and acceptably extracting evidence for presentation in court. It is important to note that these guidelines are flexible and can be modified or expanded upon as needed to ensure their ongoing relevance and effectiveness.

Relationship with other digital forensic best practice

These guidelines are aligned with and build upon existing digital forensic best practices that are recognized globally. They are intended to complement, rather than replace, existing best practice guidelines and standards. Ultimately, the relationship between these guidelines and other digital forensic best practice guidelines is one of mutual reinforcement and support, with the goal of promoting consistency and reliability in digital forensic investigations globally.

Digital Forensic Guidelines for Extracting IP-camera Evidence

These guidelines detailed in this document are organized around four categories. Some guidelines are as follows:



- Identification
- Preservation
- Analysis phase
- Reporting and Documentation

1.1 Identification:

A. Initial Assessment:

- Gather information about the IP camera model, specifications, and its network environment.
- Determine if the IP camera is functioning and accessible within the network.

B. Log Analysis:

- Determine if the IP camera generates logs internally.
- Identify the location and format of the logs, such as stored locally within the camera or remotely in a server.
- Extract and analyze the logs to identify relevant events, timestamps, and potential evidence.

1.2 Preservation:

- Evidence should be preserved in a secure location.
- A hash value should be generated for the evidence to ensure its integrity.
- The device from which the evidence was collected should be isolated from the network after extracting the logs.

1.3 Analysis Phase:

- Look for signs of unauthorized access, suspicious activities, or unusual behaviour in the logs.
- Analyze the relevant logs based on the specifics of the case. This may involve investigating the following types of logs:
 1. System logs
 2. Access logs
 3. Event logs
- Based on the case, the following list are for the

analysis steps for each case scenario:

- Case 1: Look for signs of unauthorized access, suspicious activities, or unusual behaviour in the system logs, camera configuration logs, and settings logs.
- Case 2: Analyze the access logs for evidence of unauthorized access. This includes user account logs, login/logout logs, and timing logs. Some camera brands may show the user based on IP.
- Case 3: Examine event logs for evidence of suspicious activities. This includes analyzing screenshots, recording logs, and implementing the SD card for data storage.

1.4 Reporting and Documentation:

- Record detailed information about the case, including the IP camera model, serial number, and network environment.
- Document the steps taken during the investigation, including evidence collection, imaging, and analysis.
- Maintain a chain of custody log to track the handling and transfer of evidence.
- Document all findings, observations, and conclusions derived from the analysis of the IP camera and associated evidence.
- Include timestamps, metadata, and any other relevant information supporting the investigation in the documentation.

