

Article

Forensic Analysis for Cybersecurity of Smart Home Environments with Smart Wallpads

Sungbum Kim ¹, Jewan Bang ² and Taeshik Shon ^{3,*}

¹ Department of Artificial Intelligence Convergence Network, Ajou University, 206, World cup-ro, Suwon-si 16499, Republic of Korea; zx1962@ajou.ac.kr

² Investigation Bureau, National Office of Investigation, Korean National Police Agency, 97, Tongil-ro, Sedaemun-gu, Seoul 03739, Republic of Korea; jwbang@police.go.kr

³ Department of Cybersecurity, Ajou University, 206, World cup-ro, Suwon-si 16499, Republic of Korea

* Correspondence: tsshon@ajou.ac.kr

Abstract: Various smart home companies are adding displays to smart home control devices and are also releasing smart home control functions for devices with displays. Since smart home management devices with displays are multifunctional, they can store more digital evidence than traditional management devices. Therefore, we propose a smart home environment forensic methodology focused on wallpads, which are smart home management devices with displays. And we validate the proposed methodology by building a smart home environment centered around wallpads and conducting tests with three vendors (Samsung, Kocom, and Commax). Following the proposed methodology, we identified the software and hardware specifications of devices within the testbed, particularly the wallpads. Based on this, we were able to extract network packets, disk images, and individual files stored internally using methods such as packet capture, vulnerability exploits, serial ports, and chip-off. Through analysis, we confirmed that significant user-related information and videos are stored in these control devices. The digital evidence obtained through the proposed methodology can be used as critical legal evidence, and this study contributes to efficiently analyzing important security issues and evidential data in various smart home IoT environments.



Citation: Kim, S.; Bang, J.; Shon, T. Forensic Analysis for Cybersecurity of Smart Home Environments with Smart Wallpads. *Electronics* **2024**, *13*, 2827. <https://doi.org/10.3390/electronics13142827>

Academic Editors: Nadia Kanwal, Mohammad Samar Ansari, Yuhang Ye and Brian Lee

Received: 3 June 2024

Revised: 9 July 2024

Accepted: 15 July 2024

Published: 18 July 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: smart home; digital forensic; IoT; smart home forensics

1. Introduction

With developments in information technology (IT), various technologies and devices have been fused leading to the emergence of new Internet of Things (IoT) devices which are being used not only in industries, such as factories and chemicals, but also in healthcare, smart homes, and smart cities. In particular, the demand for smart home services is increasing because users can easily initiate remote automatic control of their homes. IT companies, such as Google and Amazon, are expanding interworking and compatibility between devices by launching their platforms. Smart home systems are used in conjunction with various home IoT devices, the cloud, and smartphones. Among them, the smart home IoT ecosystem controls the house through home management devices, such as smartphones, artificial intelligence (AI) speakers, and smart wallpads. In addition, home management devices serve as a base for communication between IoT devices and the cloud to efficiently provide services, whereby various user information, such as camera images, home monitoring information, and device operation information, are stored in the device.

In the early days, home management devices in smart home systems interacted with users through voice commands. However, with the increasing diversity of IoT devices and complexity of smart home environments, the internal storage capacity of the current home management devices has also increased, leading to improved computing performance. In particular, home management devices with displays are being released for the efficient control of the smart home environment. AI speakers, mainly used as home management

devices, are providing more control through displays, such as Google Nest Hub, and in the case of apartments, the smart home ecosystem is controlled through a smart wallpad, which is a device that combines IoT technology with an intercom system.

Security threats to smart homes are increasing [1,2]. There are also cases where the wallpad installed at home is hacked and secretly recorded through a camera installed inside the home [3,4]. The problem is that these security threats can violate users' personal information. Thus, various forensic studies have been conducted on digital environments [5,6]. However, there is a limitation in that it is difficult to apply existing forensic methods to smart home IoT devices as they are becoming more advanced, and new devices are being continuously released. In particular, no forensic research has been conducted on the smart home environment involving wallpads. Therefore, we propose a smart home environment forensic methodology including a wallpad to cope with the case of cybercrime targeting smart home platforms including a wallpad. The contributions of this study are as follows: (1) a forensic methodology is proposed for the smart home IoT environments focusing on a wallpad, (2) data extraction is performed for the smart home testbeds of three vendors (Samsung, Kocom, and Commax), (3) forensic analysis artifacts on wallpads are acquired, and (4) the applicability of the proposed methodology to the smart home environment is discussed.

The remainder of this paper is organized as follows: Section 2 of this paper describes related studies on smart home forensics; Section 3 proposes a digital forensic methodology applicable to smart homes centered on wallpads; Section 4 applies the methodology to wallpads, acquiring and analyzing data; Section 5 discusses the experiment; and Section 6 concludes the study.

2. Related Research

Many researchers have conducted research to efficiently utilize data generated from IoT devices such as smart speakers, smart plugs, and wearable devices to improve IoT platform services. Due to these efforts, the amount of data generated by smart home systems is increasing [7,8]. Various IoT forensic studies have been conducted since the advent of current IoT devices. Among them, smart home IoT devices interact with smart home environments and generate and store various data related to users and homes [9,10]. Accordingly, many smart home IoT forensic studies have been conducted to use the generated data as digital evidence. Most of the studies have performed data extraction and analysis on smartphones linked to IoT devices. Iqbal et al. conducted a data acquisition study on five smart plugs. They analyzed data from routed smartphones connected to smart plugs. In addition, communication packets using Wireshark were captured and analyzed [11]. Hutchinson et al. conducted data acquisition and analysis studies on August Smart Doorbell Pro and August Smart Lock Pro devices. They extracted user data, user location data, and Doorbell camera photos through smartphone analysis that acquired root privileges. However, it was confirmed that the network traffic was encrypted with TLS v1.2 and could not identify sensitive information [12]. Kim et al. performed data acquisition and analysis on smartphone apps linked to IoT devices. It was linked to a smart home environment for Google Nest, SmartThings, and Kasa Cam. Voice command information, phone information, and smart home device information were identified through data analysis [13]. Bouchaud et al. analyzed a smart home crime environment consisting of AI speakers, hubs, smart bulbs, cameras, and sensors. They reconstructed the timeline of criminal events by extracting and analyzing data within the smart home environment [14]. Grispos et al. explored the iHealth Smart Scale IoT ecosystem, focusing on forensic techniques for data recovery. Their study revealed how forensic artifacts can be extracted, offering insights into the challenges of analyzing IoT devices in digital forensics [15]. Azhar and Bate developed a methodology for identifying forensic artifacts in smart home IoT devices, extracting evidence from ecosystems comprising devices like Amazon Echo and Philips Hue bulbs [16]. Gandhi and Arumugam proposed a unified and secure approach for extracting digital evidence from IoT devices, addressing challenges posed by varied

and heterogeneous IoT environments [17]. Mahmood et al. conducted a comparative analysis of existing IoT forensic frameworks, highlighting their strengths and weaknesses in handling forensic challenges. They emphasized the need for standardized mechanisms to acquire and analyze digital artifacts in IoT devices [18]. Shin et al. developed forensic methodologies for analyzing incidents in smart home IoT environments, emphasizing the need for tailored forensic strategies due to the diversity of IoT devices and their complex data storage characteristics [19]. In addition, forensic analysis was performed on various IoT devices [20–25].

AI speakers, which are the central devices in such smart home environments, generate and store more diverse data than other IoT devices. Accordingly, various studies have been conducted focusing on AI speakers. Oladimeji and Zhou conducted a forensic investigation of the Amazon Alexa Echo Dot 4th generation, focusing on software and cloud levels. They identified methods to extract forensic artifacts from the Alexa application on iPhones and Android smartphones and adapted an open-source tool for cloud data collection [26]. Lorenz et al. developed a novel methodology for locating and identifying IoT device owner information and user activity on Amazon Echo devices, providing practical instructions for law enforcement to handle IoT devices in crime scenes [27]. Li et al. demonstrated the proposed IoT forensic model by conducting forensic analysis on the AI speaker, Amazon Echo [28]. Shin et al. performed cloud and device encrypted traffic collection and analysis on AI speakers and developed a tool to acquire artifacts stored in the cloud through traffic decryption methods through five certificate injection [29]. Youn et al. conducted a forensic study on Echo Show 2nd, an AI speaker with a display. They extracted and analyzed data from Echo Show and proposed a smart display digital forensic framework [30]. In addition, a number of studies have been conducted on AI speakers, which are representative home management devices [31,32]. However, in addition to AI speakers, smart home control functions are currently being included in IoT devices including displays. Accordingly, the smart home control device generates more data, and this study focuses on extracting and analyzing data stored inside the smart home control device including a display.

3. Proposed Forensic Methodology for Smart Wallpads

As mentioned earlier, the smart home IoT environment not only controls devices through home management devices but also provides services by directly communicating with the cloud; therefore, it likely stores a significant amount of user artifacts. Additionally, control devices typically have storage capabilities, making them more likely to store critical information compared to other devices. This is why many forensic studies in the smart home environment have focused on smart speakers, which act as control devices. Therefore, we can infer that wallpads, which can replace the role of smart speakers, will also store a significant amount of important data.

Acquiring and analyzing data from all devices constituting the smart home environment can increase the diversity and accuracy of the evidence. However, such an undertaking complicates the investigation and requires more time. Since most digital forensic investigations have strict deadlines, investigators must efficiently collect evidence within a given timeframe [33]. Therefore, identifying and analyzing control devices that are likely to store data first can reduce investigation time, allowing investigators to conduct their work more efficiently. This section proposes a methodology for acquiring digital evidence within smart home systems, focusing on control devices within smart home IoT environments, as shown in Figure 1. The proposed methodology consists of four steps: forensic readiness, data acquisition, data analysis, and data validation. Forensic readiness identifies devices in the environment and the SW/HW in the device before forensic analysis. After identifying elements in the environment, we derive which methodology to apply according to the software/hardware and extract data through real devices. The extracted data include a dump image, a packet, etc., according to the applied acquisition method, and the data are analyzed from a forensic perspective. The artifacts derived in this way can be used as evidence in actual investigations through verification.

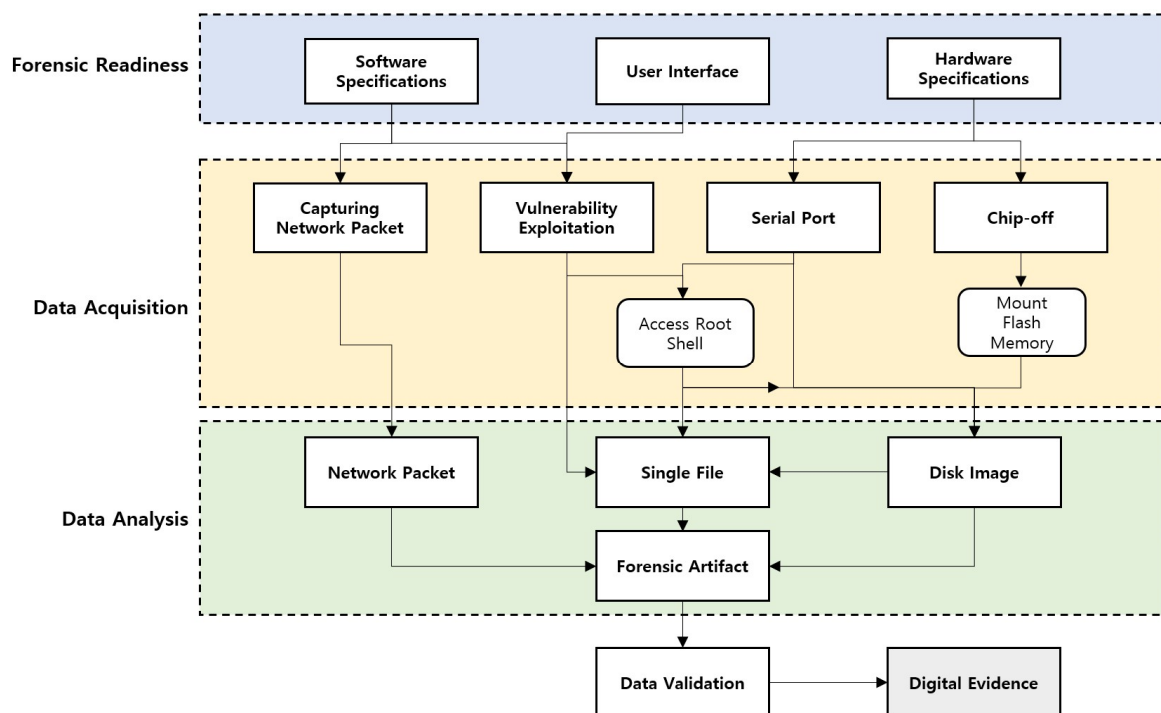


Figure 1. Proposed forensic methodology for wallpads.

3.1. Forensic Readiness

Smart home devices cover a wide range, from simple sensors that operate with low power to home appliances, such as smart refrigerators, and complex devices, such as smart home controllers, smart speakers, and wallpads. Since these devices have different software and hardware depending on the service they provide, the data acquisition method applicable to the device is different. Therefore, to acquire data in smart home systems, it is necessary to understand the characteristics of the devices constituting the smart home environments. Software and hardware analysis is essential, especially for wallpads, as they are very likely to contain data from the smart home systems. Moreover, for devices with user interfaces (UIs), additional data acquisition methods can be applied.

By examining the software specification of the smart home target device, it is possible to identify the device function, installed OS, and software. The software specification thus identified can be the basis for selecting the data acquisition method to apply. For example, forensic acquisition techniques, such as exploiting known vulnerabilities through the operating system (OS) and software versions, can be used. In addition, it is possible to identify whether the control device is connected to other smart home devices through function identification.

When the smart home device has a display, the UI can be additionally examined. Because the control device controls other smart home devices through the display, some internal data can be checked through the UI, and vulnerabilities in using the display can also be explored. If the menu for administrators that is hidden by other manufacturers can be accessed, data can be easily acquired.

Hardware inspection identifies hidden debug ports and flash memory via analysis of the device printed circuit board (PCB) as well as manufacturer-supplied connection interfaces, such as the universal serial bus (USB) on the outside of the device. If a USB or debug port for developers can be identified, the root shell for developers can be accessed through a personal computer (PC) connection. Additionally, by identifying the flash memory, the possibility of chip-off can be determined.

3.2. Data Acquisition

Data from real devices can be acquired using the device information identified by forensic readiness. Based on the previously investigated software and hardware information, the data acquisition method to be applied is selected before acquiring the actual data. In this study, data were acquired by applying four main data acquisition methods to the device, and in certain cases, additional methods were applied depending on the device.

3.2.1. Capturing Network Packets

The wallpad communicates with the cloud server through Wi-Fi and exchanges important data. Therefore, communication packets between the wallpad and cloud can be acquired through the mobile hotspot function of the laptop, as in Figure 2. Since these packets request and send data that can be used as digital evidence, such as device usage information and user information, it is possible to infer the data stored in the cloud server. Accordingly, data stored in the cloud server can be requested and acquired through replay attack. If the packet is encrypted with TLS, there is a way to bypass it by inserting a certificate inside the device and many researcher-conducted variety studies to decrypt TLS packets [29]. But this paper excludes that method because of our technical limitations.

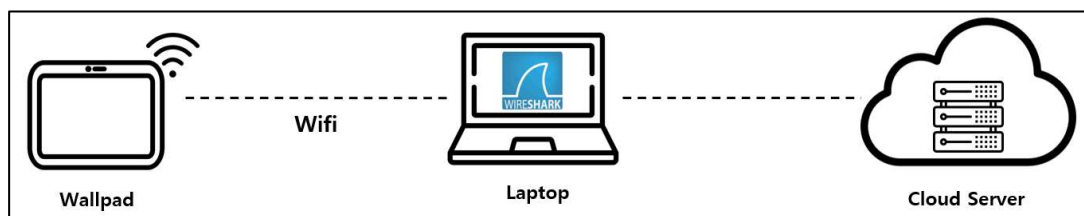


Figure 2. Packet capture between wallpad and cloud server.

3.2.2. Vulnerability Exploitation

This is a method of extracting the data in the wallpad by exploiting the vulnerability of the wallpad. Considering the previously investigated cases, the vulnerability can be derived by performing reverse engineering based on previously analyzed data. IoT devices may have vulnerabilities in the functions implemented to provide specific services. Additionally, some IoT devices are based on an OS version that is lower than the current OS version, and a known vulnerability may apply to one version. In addition, there may be vulnerabilities in using the display interface. Therefore, based on forensic readiness and previously analyzed data, vulnerabilities are detected and applied to extract a disk image or a single file, provided there is access to root privileges.

3.2.3. Serial Ports

This is a method of extracting data using serial ports, such as Universal Asynchronous Receiver/Transmitter (UART) and JTAG. Since these ports are used for debugging the device, the root shell can be accessed through the port connection. To connect to the serial port, initially, it is necessary to identify the UART/JTAG pin in the PCB. This can be identified using a tool, such as a multimeter or JTAGulator, and a PC connection can be made using a tool, such as USB to transistor–transistor logic (TTL). If the connection is successful through the serial port, data extraction is possible, but the possibility of device damage must be considered during port identification and connection.

3.2.4. Chip-off

Chip-off is a method of acquiring data by physically separating a chip. Because the goal of this study is to acquire a disk image, chip-off is performed on the flash memory. After identifying the NAND flash memory in the PCB through hardware specification analysis, the chip is physically separated by applying heat. The detached flash memory can be mounted on a PC through a NAND flash reader. In this method, it is possible to acquire a dump image of the storage device in the wallpad, but destructive methods like chip-off

can cause permanent damage to the device; it is advisable to first use logical methods to acquire data before attempting such techniques.

3.3. Data Analysis

To use the data extracted from the smart home device as evidence, it is necessary to identify important artifacts in the acquired data. Network packets, single files, and disk images can be identified via the previously performed data acquisition.

3.3.1. Network Packets

If the network communication packet between the cloud and smart home system is captured, it is possible to know which data are transmitted and received through packet analysis. User- and device-related artifacts may exist inside these communication packets. In addition, the packet can be used in investigations because it allows inference of the data stored in the cloud.

3.3.2. Single Files

Various files are stored in the smart home system, and forensic artifacts are identified through analysis of each file. The term ‘single file’ mentioned in this paper means every single file that includes forensic artifacts.

Smart home files that can be used as evidence are mainly database (DB) and multimedia files, and there may be other files with logs recorded in various forms.

3.3.3. Disk Image

When a disk dump image is acquired, a single file stored in the image is extracted through file system identification and analysis. Each smart home IoT device can use a variety of OSs, and the file systems used can also partially differ. Therefore, to perform data analysis to enable the use of the data stored in the acquired disk dump image as key evidence in the investigation, the file system must be identified, and the file must be extracted in a manner suitable for each file system. In some cases, deleted files can be recovered through image analysis and forensic tools, such as The Sleuth Kit (TSK), encase, and Forensic Toolkit (FTK) imager.

3.4. Data Validation

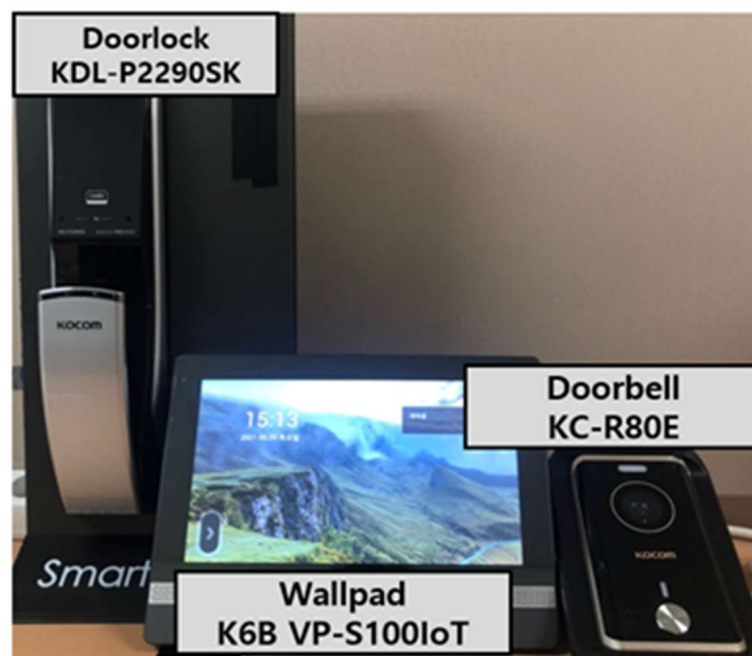
Data verification is required to use the artifacts identified through data acquisition and analysis as evidence in actual courts. Such data verification may be performed in the process of extracting the data, and in general, integrity verification is performed through hash value comparison. However, since data validation may vary depending on the legal requirements of the country, it must follow the method of forensic investigative agencies. This paper focuses on extracting and analyzing data and omits the part of data verification.

4. Case Studies for the Forensics of Smart Home IoT Environments

To verify the forensic methodology presented in this study, digital forensics was performed on three smart home IoT testbeds. We selected three types of wallpads most commonly used in Korea and purchased additional peripherals from the same vendor for compatibility to construct our testbeds. All testbeds were installed in my research lab. The testbeds used in the experiment were products of Samsung, Commax, and Kocom, respectively, as shown in Table 1 and Figures 3–5. Peripheral devices were interlocked around the wallpad and constructed.

Table 1. Smart home tested components.

Manufacturer	Device	Model	Remark
Samsung	Wallpad	SHP-HB700	Equipped with monitor, camera, and microphone
	Doorbell	SHT-CW812	Equipped with camera and microphone
	Doorlock	SHP-DP951	-
	Motion Sensor	SHP-SR100G	-
	Door Sensor	SHP-SB100G	-
Commax	Wallpad	CAV-1021 MGX	Equipped with monitor, camera, and microphone
	Doorbell	DRC-4Y	Equipped with camera and microphone
	Doorlock	CDL-220PB	-
	Kitchen Television	CKV-1020FS	Equipped with monitor
Kocom	Wallpad	K6B VP-S100IoT	Equipped with monitor, camera, and microphone
	Doorbell	KC-R80E	Equipped with camera and microphone
	Doorlock	KDL-P2290SK	-

**Figure 3.** Samsung smart home testbed.**Figure 4.** Commax smart home testbed.

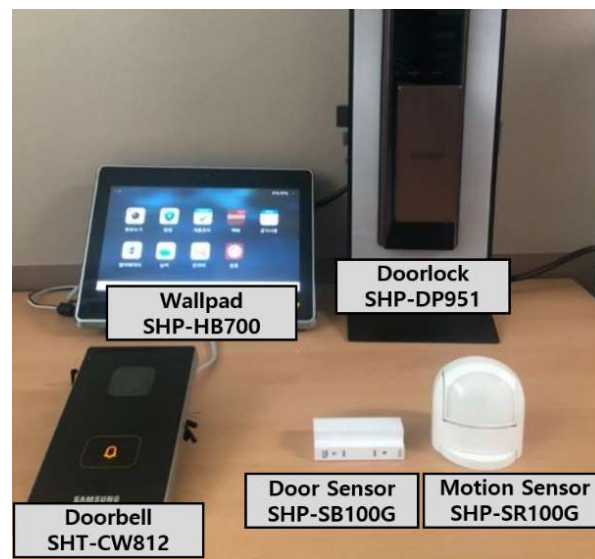


Figure 5. Kocom smart home testbed.

4.1. Forensic Readiness

To acquire and analyze data in the smart home environment, it is necessary to first identify the central device in the testbed and investigate the software and hardware specifications based on this device. In particular, it is important to identify data acquisition techniques applicable to the software and hardware specifications identified in forensic readiness.

For the Samsung testbed, the doorbell, door lock, and sensor are interlocked with the wallpad as the center. Upon investigating the software and hardware specifications of interlocking devices except for the wallpad, no software specifications, connection interfaces, or memory chips were found for data acquisition. However, for the wallpad, it was confirmed that it supports Wi-Fi and uses the Android version 4.2.2 for the OS through network packet sniffing. This Android version is an older version and has the potential to exploit known vulnerabilities to obtain data. By function identification of the UI operation of the wallpad, it was also confirmed that the video and voice memo recorded from the doorbell are stored in the wallpad. In addition, it was confirmed that it is possible to enter the hidden administrator settings by entering ‘#*00’ in the ‘Password’ menu of ‘Settings’, where a password can be set to unlock the security function. The number to enter to gain access to the hidden administrator setting was confirmed by inquiring the device vendor. In the hidden administrator setting, various menus provide the wallpad function, and it was identified that, in some cases, the functions were provided by access through a Uniform Resource Locator (URL). If the user changes this URL, instead of providing the function, the user can access the website of the changed URL. In this process, if you access a website with functions such as a file attachment, such as mail, you can check the Android UI for the file attachment, and there is a possibility that you can extract files by using this. These hidden functions can act as weaknesses of the device.

Through an examination of the hardware, it was determined that the Samsung wallpad consists of two PCBs, and the second PCB was presumed to be a debug port composed of 15 pins, as shown in Figure 6. Pin information used in USB ports, such as USB- and USB+, as well as UART ports, such as C_TX and C_RX, is specified on the back of the PCB. It was confirmed that this PCB is connected to a 15-pin debug port through the power test of the multi-tester, and a 4 GB NAND flash was also identified as shown in Figure 7.

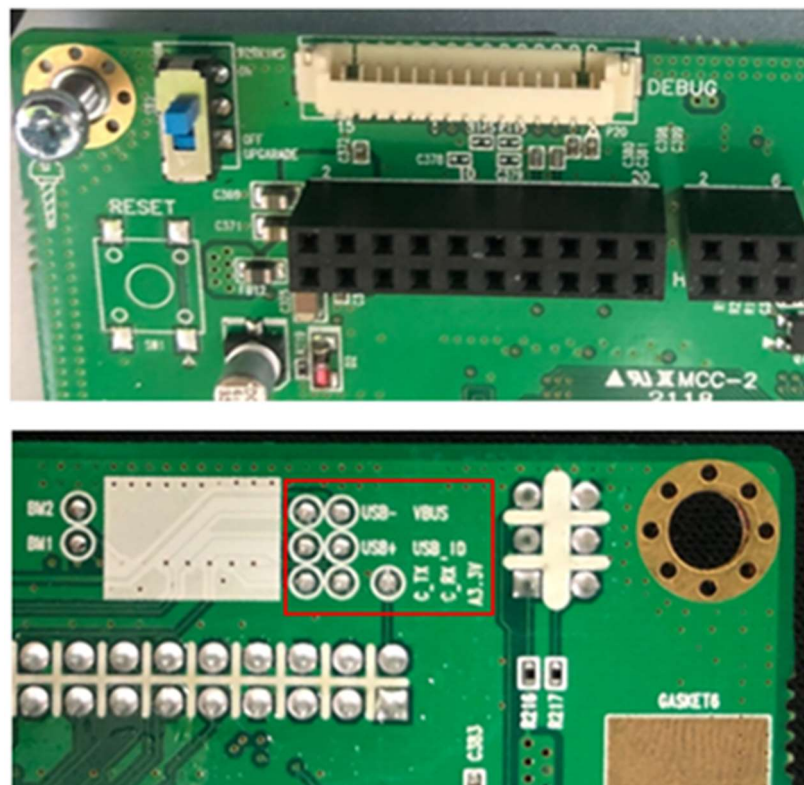


Figure 6. Debug port in the Samsung wallpad PCB.

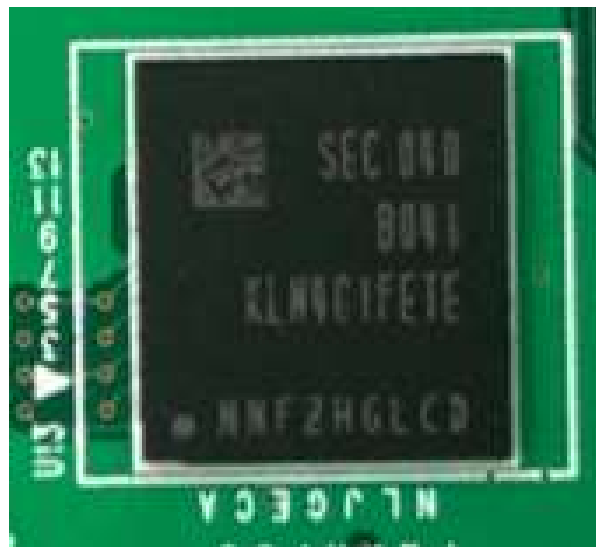


Figure 7. NAND flash memory in the Samsung wallpad PCB.

The COMMAX testbed consists of a wallpad, a doorbell, a door lock, and a kitchen television phone, while the Kocom testbed consists of a wallpad, a doorbell, and a door lock. Both testbeds provide services centered on the wallpad. The Kocom and Commax wallpads support Wi-Fi like Samsung, and the OS was identified as Android version 4.2.2. Also, there is a pin presumed to be a UART port in both wallpads, as well as a 4 GB NAND flash.

4.2. Data Acquisition

Based on the previously performed forensic readiness, data extraction in the wallpad was performed through four acquisition techniques.

4.2.1. Capturing Network Packets

All three wallpads support Wi-Fi, allowing data packets to be captured between the device and the cloud using man-in-the-middle (MITM). MITM performed packet capture using Wireshark after connecting the wallpad and Wi-Fi through the mobile hotspot function of the laptop. Using this technique, it was possible to extract the communication packet capture (PCAP) between the device and cloud server.

4.2.2. Vulnerability Exploitation

In the case of the Samsung wallpad, there is a vulnerability in using the 'URL Settings', which is a function in the hidden administrator settings. Other web pages such as Google can be accessed by changing the URL of the function provided through the URL, as shown in Figure 8. Basically, the wallpad does not have a function to transmit stored data to the outside; however, using a file attachment function such as mail, it is possible to extract the multimedia files stored inside the wallpad to the outside like Figure 9. Other vulnerabilities may exist, but no applicable vulnerabilities were found.

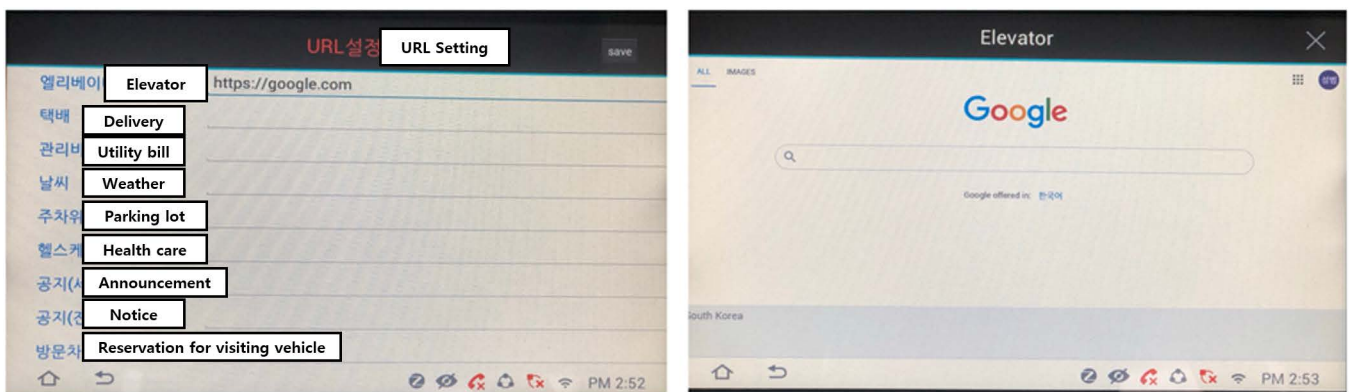


Figure 8. Google access using the Samsung wallpad elevate URL setting.

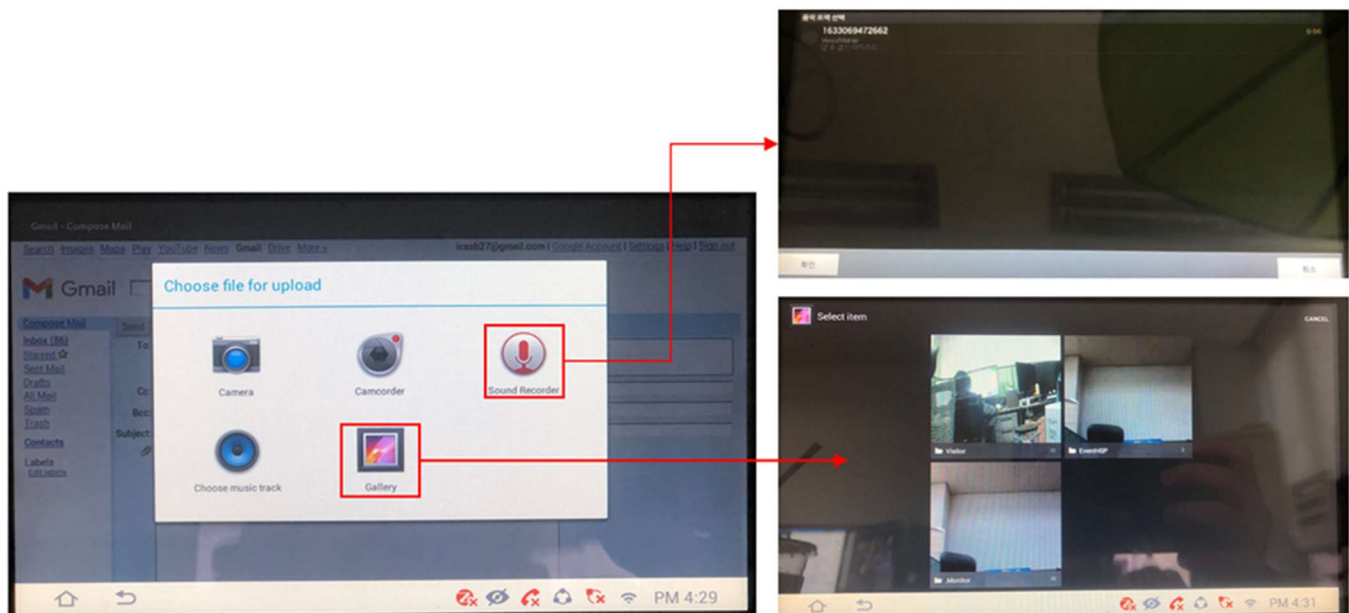


Figure 9. Multimedia file extraction using Samsung wallpad vulnerability.

4.2.3. Serial Ports

If a debug port is present such as UART on the PCB, the inside of the wallpad can be accessed through a connection with the PC. In the case of the Kocom wallpad, a port

presumed to be a UART pin was found, and a PC connection was established through USB to TTL, as shown in Figure 10. With a PC, the root shell of the wallpad can be accessed using PuTTY. The connected shell is assumed to be the Android Debug Bridge (ADB), and the possibility of a memory dump can be explored. For the Samsung wallpad, the UART pin was identified through the energization test among the 15-pin debug ports, but the data input/output could not be confirmed. The COMMAX wallpad identified the UART pin, and PC connection was performed using PuTTY like Figure 11. However, the password had been set, so root shell access was not possible.

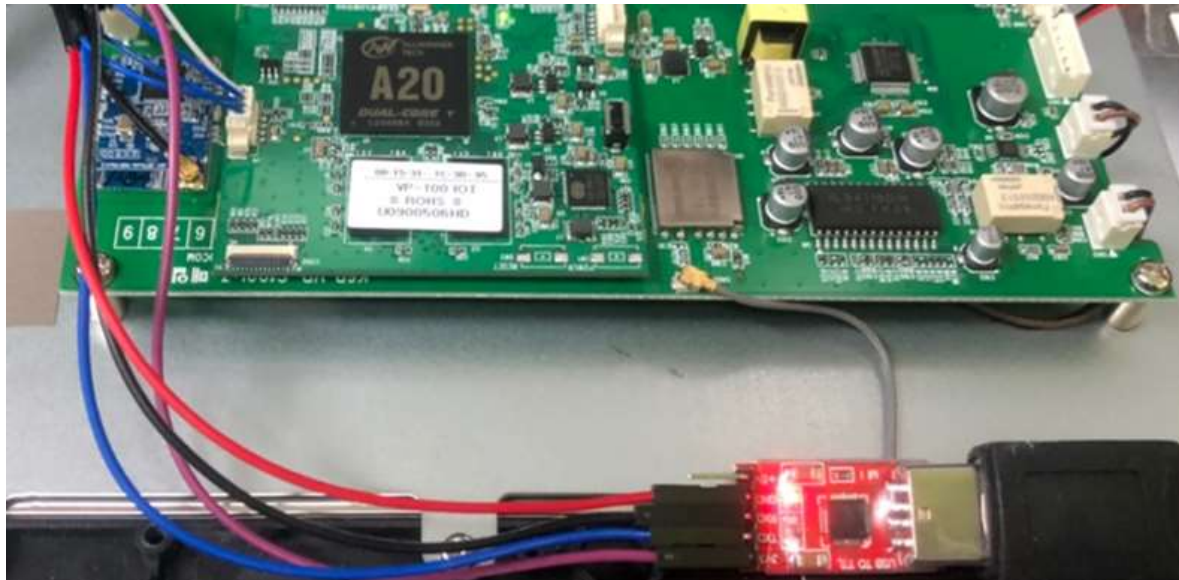


Figure 10. PC connection using the UART port of the Kocom wallpad.

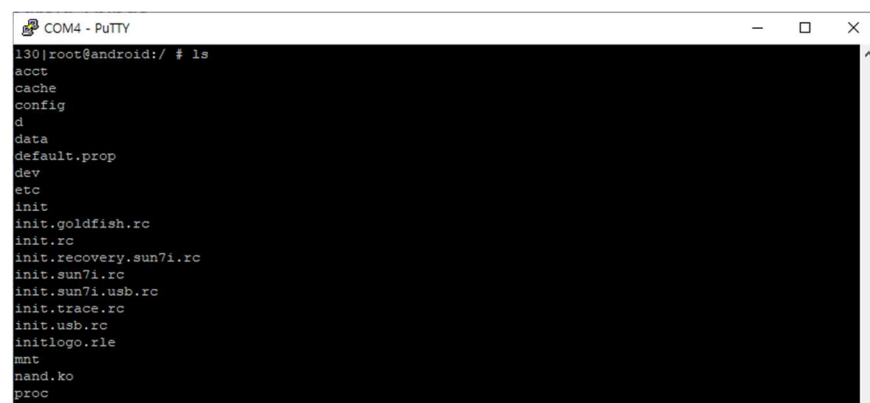


Figure 11. Root shell acquisition through UART.

4.2.4. Chip-off

Chip-off physically removes the memory chip so that a dump image can be acquired through a reader. We were able to identify the same 4 GB NAND flash on all wallpads during our hardware investigation. In particular, all three devices had the same model of NAND flash which was confirmed to be Samsung KLM4G1FETE-B041. The corresponding NAND flash is BGA 153 and is compatible with the ALLSOCKET BGA153 reader as shown in Figure 12. Accordingly, the chips were physically separated from all devices using a hot air rework station and a soldering station, and a dump image was obtained using FTK imager like Figure 13.

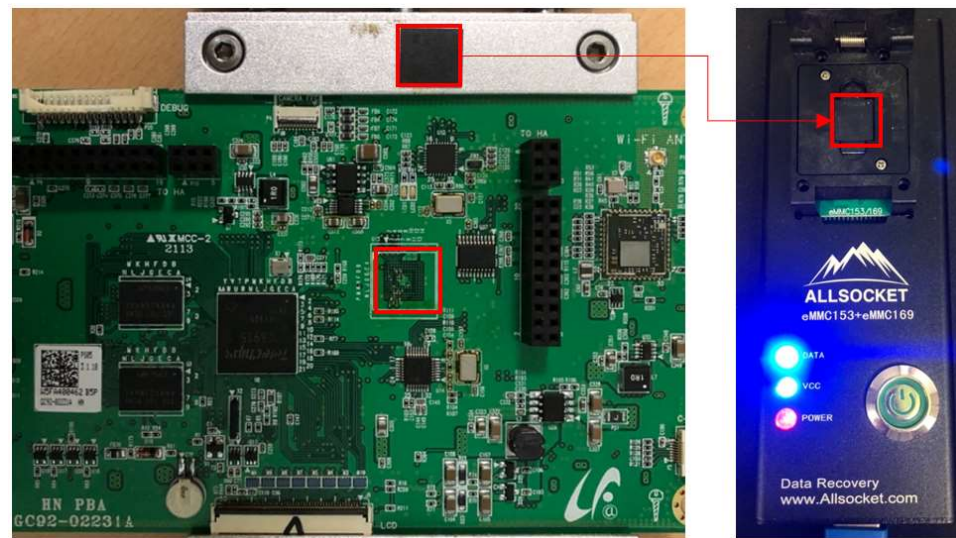


Figure 12. NAND flash memory chip-off (Samsung wallpad).

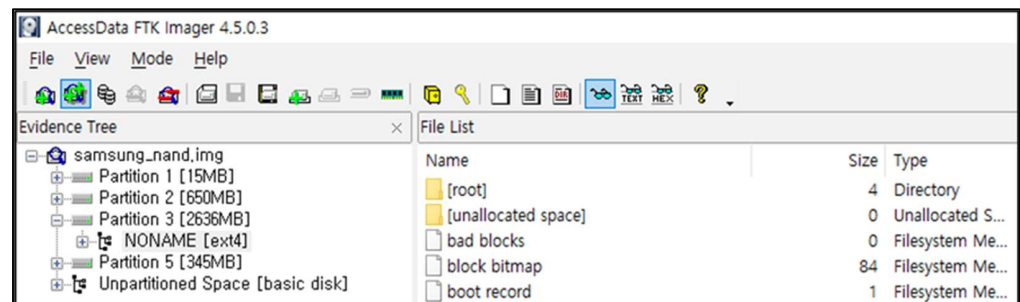


Figure 13. Disk image dump using FTK Imager (Samsung wallpad).

4.3. Data Analysis

Three types of data were acquired from three smart home testbeds: packet files, dump images, and single files. Using data analysis, data that can be used as evidence, such as user information and user behavior, were identified. In addition, an additional data acquisition method was derived using the artifacts identified from data analysis. The artifacts we extracted can be found in Tables A1–A3 in the Appendix A.

4.3.1. Network Packets

User data stored in the cloud server can be inferred through the analysis of the captured packets. This may be helpful in the subsequent review of warrant issuance. In addition, if a replay attack using a session token and a web proxy is possible, user data stored in the cloud can be directly extracted. Additional vulnerabilities can be derived using information such as URLs. In the case of the Samsung wallpad, most of the communication between the cloud and the device is accomplished through Hypertext Transfer Protocol (HTTP). When a crime prevention notification occurs through the sensor, a video is recorded by the camera mounted in the wallpad. When the packet corresponding to this situation is captured, the user ID of the linked smartphone app can be confirmed. In general, the ID of the smartphone app that works with the Samsung wallpad is set to the user's phone number like Figure 14; hence, the association with the user's smartphone can be verified in this case. The name of the recorded crime prevention video can also be checked. In addition, when the doorbell rings, the visitor thumbnail and image are stored by the doorbell camera as shown in Figure 15.



Figure 14. Packet when a security alert occurs (Samsung wallpad).

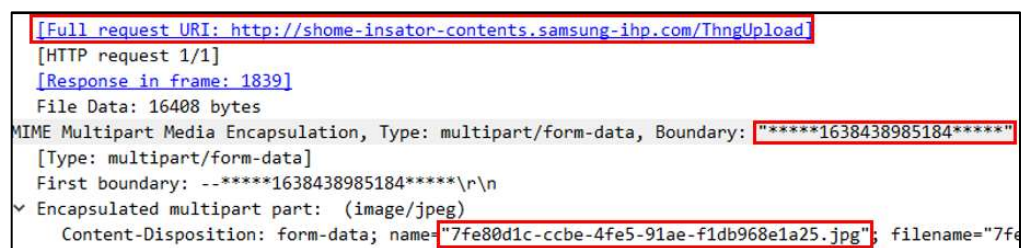


Figure 15. Packet generated when the doorbell rings (Samsung wallpad).

In the packet captured when the doorbell rings, the photo with the estimated visitor thumbnail and the event occurrence time are stored in the cloud server.

The Kocom wallpad communicates with the cloud via HTTP. When entering the ‘Smartphone Registration’ menu of the wallpad, a list of the smartphones linked to the wallpad is received through the captured packet shown as in Figure 16. Thus, it is inferred that the list of smartphone numbers linked to the cloud server is stored. In the case of COMMAX, most packets were encrypted with TLS and could not be verified.

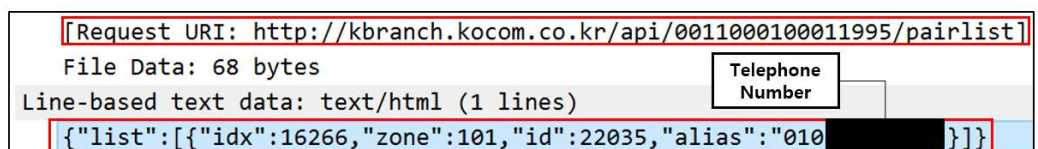


Figure 16. Packet generated when entering ‘smartphone registration’ (Kocom wallpad).

4.3.2. Disk Image

A single file can be extracted by analyzing the internal storage structure through the analysis of the dump image acquired through serial communication or chip-off. As a result of checking the packet extracted from the Samsung wallpad through the ‘fdisk -l’ command of Linux, as shown in Figure 17, a total of 11 partitions were output, where ‘/dev/sdc4’ represents Partitions 5 through 11. The existence of 10 partitions was confirmed. Three of the partitions used the Ext4 file system as shown in Figure 18, and data could be acquired by performing data extraction targeting a partition [34,35].

```

Disk /dev/sdb: 3.7 GiB, 3909091328 bytes, 7634944 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x80a86772

Device      Boot      Start      End  Sectors  Size Id Type
/dev/sdb1               32    30751    30720    15M  0 Empty
/dev/sdb2            30752   1361951   1331200    650M  83 Linux
/dev/sdb3            1361952   6761951   5400000    2.6G  83 Linux
/dev/sdb4            6761952   7634942    872991   426.3M  f W95 Ext'd (LBA)
/dev/sdb5            6761984   7469183    707200   345.3M  83 Linux
/dev/sdb6            7469216   7499935    30720    15M  0 Empty
/dev/sdb7            7499968   7510207    10240     5M  0 Empty
/dev/sdb8            7510240   7518431     8192     4M  0 Empty
/dev/sdb9            7518464   7534847    16384     8M  0 Empty
/dev/sdb10           7534880   7536927     2048     1M  0 Empty
/dev/sdb11           7536960   7634942    97983    47.9M  0 Empty

```

Figure 17. Ext4 file system partition (Samsung wallpad).

```

/dev/sdb5      ext4      342504      200      335232
/dev/sdb3      ext4      2615348    157352    2441612
/dev/sdb2      ext4      644704     336148    295244

```

Figure 18. Dump image partition (Samsung wallpad).

4.3.3. Single File

By analyzing the dump image and the single file extracted through the vulnerability, evidence such as user information and user-behavior-related information can be identified. Data constituting key evidence are mainly stored in the DB and multimedia files.

A number of tables exist in the 'media/0/database/ihome.db' file of the Samsung wallpad, and information such as device link and user ID linked to the server are stored. In particular, the 'tbl_platform_call_log' table stores network camera doorbell call records as shown in Figure 19. When a network camera is triggered, the visitor image is saved, and the device (wallpad/smartphone) processes the notification, including the visitor thumbnail path and visit time, which can be identified through the values stored in the table. The stored location of the visitor thumbnail file can be checked through the table filename and the visit time through starttime and visittime.

The file specified in the file name of the 'tbl_platform_call_log' table is a thumbnail of the video recorded when a visitor rings the doorbell. It is possible to check that the file is saved in the 'media/0/IntelligentHome/Visitor/' directory and the video of the corresponding thumbnail like Figure 20.

In addition, in 'EventHSP' and 'VoiceMemo' in the 'media/0/IntelligentHome' directory, the security video recorded by the wallpad camera and the user's voice memo can be checked, respectively. In the 'media/0/log/' directory, the log recorded when a video-related event occurs is saved as a txt file. Through these logs, it is possible to track the event of a network camera trigger.

tbl_platform_call_log										
id	uuid	type	duration	result	direction	starttime	filename	remoteuserid	upload	call
1	6b6...	2	4	0	1	2021-12-02 18:40:56	/storage/emulated/0/IntelligentHome/...		0	
2	7fe...	2	0	0	1	2021-12-02 18:56:05	/storage/emulated/0/IntelligentHome/...		0	
3	d0f...	2	0	0	1	2021-12-02 18:56:31	/storage/emulated/0/IntelligentHome/...		0	
4	08e...	0	0	3	0	2021-12-02 18:58:06	/storage/emulated/0/IntelligentHome/...	010...	@ihf	0
5	fa6...	2	0	0	1	2021-12-02 18:58:23	/storage/emulated/0/IntelligentHome/...		0	
6	b6a...	0	0	3	0	2021-12-02 18:59:37	/storage/emulated/0/IntelligentHome/...	010...	@ihf	0
7	4b9...	1	11	0	0	2021-12-02 18:59:56	/storage/emulated/0/IntelligentHome/...	010...	@ihf	0
8	b27...	0	0	3	0	2021-12-02 19:01:32	/storage/emulated/0/IntelligentHome/...	010...	@ihf	0
9	a16...	0	4	0	0	2021-12-02 19:03:09	/storage/emulated/0/IntelligentHome/...	010...	@ihf	0
10	279...	0	0	3	0	2021-12-02 19:06:12	/storage/emulated/0/IntelligentHome/...	010...	@ihf	0

filename
Filter
/storage/emulated/0/IntelligentHome/Visitor/6b65cd30-6130-487b-ad0c-adb5f600fc5d.jpg
/storage/emulated/0/IntelligentHome/Visitor/7fe80d1c-ccbe-4fe5-91ae-f1db968e1a25.jpg
/storage/emulated/0/IntelligentHome/Visitor/d0f650f6-079f-42db-9ba9-e784a9b4b8ca.jpg
/storage/emulated/0/IntelligentHome/Visitor/08eaf1b6-22f3-42a8-88d0-e3be8e24b412.jpg
/storage/emulated/0/IntelligentHome/Visitor/fa61fb67-bef7-46a0-81ed-a895dd40c6d0.jpg
/storage/emulated/0/IntelligentHome/Visitor/b6a85011-446e-4c1b-9e21-0b0cffda1f2a.jpg
/storage/emulated/0/IntelligentHome/Visitor/4b96a625-09e9-4e9e-896a-97a5a193ef0c.jpg
/storage/emulated/0/IntelligentHome/Visitor/b2731d46-2f7a-4be6-83a1-cd75243baf17.jpg
/storage/emulated/0/IntelligentHome/Visitor/a165aac2-3602-4fab-ba9f-3e346f08175e.jpg
/storage/emulated/0/IntelligentHome/Visitor/2799a0b6-292a-4d11-a262-d7d9cdec8ea2.jpg

Figure 19. tbl_platform_call_log in ihome.db.

2799a0b6-292a-4d11-a262-d7d9cdec8ea2.mp4
2799a0b6-292a-4d11-a262-d7d9cdec8ea2.jpg
a165aac2-3602-4fab-ba9f-3e346f08175e.mp4
a165aac2-3602-4fab-ba9f-3e346f08175e.jpg
b2731d46-2f7a-4be6-83a1-cd75243baf17.mp4
b2731d46-2f7a-4be6-83a1-cd75243baf17.jpg
4b96a625-09e9-4e9e-896a-97a5a193ef0c.mp4
4b96a625-09e9-4e9e-896a-97a5a193ef0c.jpg
b6a85011-446e-4c1b-9e21-0b0cffda1f2a.mp4
b6a85011-446e-4c1b-9e21-0b0cffda1f2a.jpg
8108659f-0fcd-4c17-b85e-4ec8166175ce.mp4
8108659f-0fcd-4c17-b85e-4ec8166175ce.jpg
7fe80d1c-ccbe-4fe5-91ae-f1db968e1a25.mp4
7fe80d1c-ccbe-4fe5-91ae-f1db968e1a25.jpg
6b65cd30-6130-487b-ad0c-adb5f600fc5d.mp4
6b65cd30-6130-487b-ad0c-adb5f600fc5d.jpg

Figure 20. Multimedia storage path.

4.4. Data Validation

Data verification is required to use the previously extracted and analyzed data as digital evidence. The integrity of the extraction method can be verified by comparing hash values of the same file acquired by applying various extraction methods. For example, since the integrity of the evidence can be verified by comparing the hash value between the video file acquired through the Samsung wallpad UI vulnerability and the file acquired through

chip-off, mutual verification is required by applying various acquisition methods. In this paper, because the experiment was conducted on a testbed, data verification was omitted. However, in actual investigations, the integrity and reliability of the data extraction process and the security and confidentiality of digital evidence obtained during analysis must be ensured through validation.

5. Discussion

As the forensic methodology proposed in this study centered on the wallpad and was applied to the smart home environment, we confirmed that the control devices operating in the smart home environment could be identified and digital evidence could be secured by applying the wallpad. This approach is efficient because we identified devices that are likely to store important data and conducted analysis based on those devices.

In the forensic readiness phase, software and hardware specifications can be investigated to identify and plan acquisition techniques applicable to the device. In addition, in the case of the wallpad, some multimedia files stored in the device were identified using the UI, to confirm that data can be extracted by exploiting the vulnerabilities of the UI.

Based on the device specifications investigated above, data acquisition was performed using applicable methods, which were divided into logical extraction and physical extraction methods. In the case of physical extraction, it is possible to acquire high-level data; however, because there is a risk of device damage, physical extraction is performed after logical extraction. In the case of cloud packet capture, we confirmed that most wallpads from Samsung and Kocom communicate with the cloud via HTTP. However, in the case of the COMMAX wallpad, the packet was encrypted with TLS. Therefore, it was difficult to perform a general check on the contents of the packet. In the case of TLS encryption, the inner packet can be checked by installing a certificate of a web proxy, such as Burp Suite, on the wallpad; however, technical limitations precluded this. If a certificate can be installed inside the device, TLS packet verification and replay attack can be performed. After identifying the vulnerabilities through an analysis of information in the device, the vulnerabilities can be used in the investigation stage to extract data, which may also be accomplished by other acquisition techniques. Although the three wallpads use Android version 4.2.2 and can extract data through a known vulnerability in that version, the data extraction failed. However, IoT devices may use a relatively low version of the OS, so known vulnerabilities may be effective. In the case of the Samsung wallpad, multimedia files can be acquired via UI vulnerabilities, but the integrity of the device may be compromised when operating the device. Therefore, the integrity of the method is verified by comparing the hash value of the multimedia file acquired through the UI vulnerability with the hash value of the same file acquired through other acquisition techniques. Serial communication can be performed using debugging ports, such as JTAG and UART. In this study, the focus was the UART port; however, there are some difficulties in acquiring data through this port. Recent devices hide the debugging port, so it is difficult to identify the port, and there may be device damage in the process of identifying the debugging port. In addition, it was shown that even if a successful connection is established through the UART port, there may be difficulties in data acquisition because a password may have already been set in the shell of the COMMAX wallpad. In particular, identifying and accessing debugging ports for various devices is difficult. To solve this problem, we referred to device documents and conducted several tests with the same device model in preparation for damage to the device. If tools such as an oscilloscope or JTAGulator, which were not utilized in this study, were available, it is anticipated that debugging ports could be identified more easily. In the case of chip-off, it was shown that if the NAND flash can be identified through three wallpads, a dump image can be acquired by physically separating the chip. However, if chip-off is performed, the device is damaged, and there is a limitation in that it is technically difficult to operate the device using a System on a Chip (SOC). In addition to the four acquisition techniques used in this study, data can also be extracted through various other acquisition techniques.

In this study, three types of files (packet, image, and single file) were acquired through data acquisition, and data analysis was performed on these files. As previously mentioned, the packet file can be used in the issuance of a warrant as it can infer the data to be stored in the cloud. We identified the partition through dump image file analysis and extracted a single file. This can be done through tools such as FTK Imager. Using single file analysis, it was confirmed that most user-related information is included in the DB, multimedia, and txt files. Using the information in device usage logs and inferring the user's behavior, the user of the device can be identified, and an alibi can also be provided.

6. Conclusions

With the expansion of smart homes, various products, including refrigerators and televisions with control functions, have been released in addition to AI speakers to manage the smart home. AI speakers are also being equipped with displays, like Google Nest, to simplify device control through touchscreen interaction, expanding their functionality. In the case of control devices featuring displays, it is more likely to store user-related information, and as device performance improves, the potential for applying various data acquisition techniques also increases.

In this study, a forensic methodology was proposed for smart home environments, primarily composed of wallpads and control devices with displays. Furthermore, by applying this forensic methodology to wallpads from three smart home vendors (Samsung, Commax, and Kocom), it was confirmed that various user-related information is stored in the control units. Our research demonstrates that control devices with displays store a significant amount of artifacts. Consequently, prioritizing the analysis of control devices with displays is an efficient approach in forensic investigations of smart home IoT environments. However, as the diversity of IoT devices continues to grow, and considering our selection of smart home platforms and devices is not extensive, there is a need for forensic research in more general environments. We plan to conduct forensic research in typical smart home environments targeting various platforms to improve our proposed methodology. Currently, devices with integrated control functions are being introduced for smart homes, leading to increased diversity in the configurations of smart home environments. In the future, we will conduct digital forensic research that can be universally applied to various smart home environments.

Author Contributions: Conceptualization, S.K., J.B. and T.S.; methodology, S.K.; validation, J.B.; formal analysis, S.K.; investigation, S.K.; writing—original draft preparation, S.K.; writing—review and editing, J.B.; supervision, T.S.; project administration, T.S.; All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MIST) (No.2022-0-01022, Development of Collection and Integrated Analysis Methods of Automotive Inter/Intra System Artifacts through Construction of Event-based Experimental System).

Data Availability Statement: Data is contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A

Table A1. Samsung SmartThings Artifact table.

URL	IP Address	Protocol	Details
http://shome-insator-contents.samsung-ihp.com/ThngUpload	112.107.147.75	HTTP	Visitor video thumbnail File name, Visitor video time

Table A1. Cont.

URL	IP Address	Protocol	Details
http://shome-mvc.samsung-ihp.com/xml3/pb3.do	112.107.147.77	HTTP	Session id/Value
http://shome-cvr.samsung-ihp.com:7200/operators/SC0756/zones/000/users/[Phonenumber]/cameras/CAM1/er	112.107.148.71	HTTP	Security video file name, User phone number
-	112.107.148.67	HTTP	-
-	112.107.148.68	HTTP	-
-	112.107.148.188	HTTP	-
-	112.107.147.63	TLSv1	--

Path	Filename	Details
media/0/database/	ihome.db	Linked device list, Linked device mac address
media/0/database/	ihome.db	User phone number linked to the server, Biz ID
media/0/database/	ihome.db	Call logs, Visitor video info, Voice memo info
media/0/IntelligentHome/EventHSP/	*.jpg	Video thumbnails recorded through the wallpad camera
media/0/IntelligentHome/EventHSP/	*.mp4	Video recorded through the wallpad camera
media/0/IntelligentHome/Visitor/	*.jpg	Video thumbnails recorded through the doorbell
media/0/IntelligentHome/Visitor/	*.mp4	Video recorded through the doorbell
media/0/IntelligentHome/VoiceMemo/	*.mp4	Voice memo
media/0/log/	*.txt	User smartphone number
media/0/log/	*.txt	Video timestamp recorded through the doorbell, Record smartphone calls due to doorbell calls
system/usagestats/	usage-history.xml	Wallpad last use time

Table A2. Commax Artifact table.

URL	IP Address	Protocol	Details
http://swpush1.commax.co.kr/cps/cps.php	52.79.92.196	HTTP	Wallpad information, Security alarm occurrence timestamp
-	13.125.184.86	TLSv1	-
-	15.165.226.116	TLSv1	-
-	52.79.215.165	TLSv1	-
-	121.254.188.30	TLSv1	-

Partition	Path	Filename	Details
Partition 1	CMXdata/	CreateAccount.properties	ID, mac address, Login timestamp, Device info,
	cmx_data/visitor	*.jpg	Photo captured through doorbell
	cmx_data/visitor	*.mp4	Video recorded through doorbell
Partition 8	data/com.android.providers.contacts/data-bases/	contacts2.db	Call history
	system/dropbox	SYSTEM_BOOT@*.txt	SW info
	data/com.android.providers.settings/data-bases/	settings.db	Wi-Fi info, Device setting info
	data/com.android.providers.media/data-bases/	external.db	File creation/modification timestamp, Event log
Partition 12	app/var/db_center/	Tbl_alarm.MYD, .MYI, .frm	Emergency alarm log
	app/var/db_center/	Tbl_call_log.MYD, .MYI, .frm	Call timestamp, Call log

Table A3. Kocom Artifact table.

URL	IP Address	Protocol	Details
http://kbranch.kocom.co.kr/api/0011000100011995/pairlist	222.108.131.111	HTTP	Linked smartphone List
http://222.108.131.112/api/0011000100011995/visitorup/946690749/door/100360902	222.108.131.112	TLSv1	Visitor photo file name

Partition	Path	Filename	Details
Partition 1	VisitorCapture/	*.jpg	Photo captured through doorbell
Partition 7	/	build.prop	Kernel version
Partition 8	/data/com.kocom.iot.ui.s701/data-bases/	Info.db	Wi-Fi info
	/data/com.kocom.iot.ui.s701/data-bases/	KocomUIDB.db	List of photos captured through doorbell
	/data/com.android.providers.media/data-bases/	external.db	File info stored in Partition 1
	/system/netstats	*	Network connection history

References

1. Tinashe, M.; Zhou, Y. Internet of Things (IoT) of Smart Homes: Privacy and Security. *J. Electr. Comput. Eng.* **2024**, *1*, 7716956.
2. Grispos, G.; Studiawan, H.; Alrabaee, S. Internet of things (IoT) forensics and incident response: The good, the bad, and the unaddressed. *Forensic Sci. Int. Digit. Investig.* **2024**, *48*, 301671. [\[CrossRef\]](#)
3. Kim, H. Man Nabbed for Hacking Built-in Home cameras of 400,000 Households. Yonhap News Agency(blog), 20 December 2022. Available online: <https://en.yna.co.kr/view/AEN20221220009100315> (accessed on 3 June 2024).
4. Kelly, S. That Security Camera and Smart Doorbell You're Using May Have Some Major Security Flaws CNN (Blog), 12 March 2024. Available online: <https://edition.cnn.com/2024/03/09/tech/smart-home-cameras-hackers-security/index.html> (accessed on 3 June 2024).
5. Kim, H.; Shin, Y.; Kim, S.; Jo, W.; Kim, M.; Shon, T. Digital forensic analysis to improve user privacy on Android. *Sensors* **2022**, *22*, 3971. [\[CrossRef\]](#)
6. Shin, Y.; Kim, S.; Jo, W.; Shon, T. Digital forensic case studies for in-vehicle infotainment systems using Android Auto and Apple CarPlay. *Sensors* **2022**, *22*, 7196. [\[CrossRef\]](#)
7. Tekler, Z.D.; Low, R.; Yuen, C.; Blessing, L. Plug-Mate: An IoT-based occupancy-driven plug load management system in smart buildings. *Build. Environ.* **2022**, *223*, 109472. [\[CrossRef\]](#)
8. Ansere, J.A.; Han, G.; Wang, H.; Choi, C.; Wu, C. A reliable energy efficient dynamic spectrum sensing for cognitive radio IoT networks. *IEEE Internet Things J.* **2019**, *6*, 6748–6759. [\[CrossRef\]](#)
9. Kim, S.; Jo, W.; Lee, J.; Shon, T. AI-enabled device digital forensics for smart cities. *J. Supercomput.* **2022**, *78*, 3029–3044. [\[CrossRef\]](#)
10. Kim, M.; Shin, Y.; Jo, W.; Shon, T. Digital forensic analysis of intelligent and smart IoT devices. *J. Supercomput.* **2023**, *79*, 973–997. [\[CrossRef\]](#)
11. Iqbal, A.; Olegård, J.; Ghimire, R.; Jamshir, S.; Shalaginov, A. Smart home forensics: An exploratory study on smart plug forensic analysis. In Proceedings of the 2020 IEEE International Conference on Big Data (Big Data), Atlanta, GA, USA, 10–13 December 2020.
12. Hutchinson, S.; Karabiyik, U. Forensic Analysis of the August Smart Device Ecosystem. In Proceedings of the 2020 International Symposium on Networks, Computers and Communications (ISNCC), Montreal, QC, Canada, 20–22 October 2020.
13. Kim, S.; Park, M.; Lee, S.; Kim, J. Smart home forensics—Data analysis of IoT devices. *Electronics* **2020**, *9*, 1215. [\[CrossRef\]](#)
14. Bouchaud, F.; Vantroys, T.; Grimaud, G. Forensic analysis of IoT ecosystem. In Proceedings of the 2021 8th International Conference on Future Internet of Things and Cloud (FiCloud), Rome, Italy, 23–25 August 2021.
15. Grispos, G.; Tursi, F.; Choo KK, R.; Mahoney, W.; Glisson, W.B. A Digital Forensics Investigation of a Smart Scale IoT Ecosystem. In Proceedings of the 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Shenyang, China, 20–22 October 2021.
16. Azhar, M.H.B.; Bate, S.B.L. Recovery of Forensic Artefacts from a Smart Home IoT Ecosystem. In Proceedings of the CYBER 2019: The Fourth International Conference on Cyber-Technologies and Cyber-Systems, Porto, Portugal, 22–26 September 2019; pp. 94–99.
17. Gandhi, K.K.A.; Arumugam, C. Toward a unified and secure approach for extraction of forensic digital evidence from an IoT device. *Int. J. Inf. Secur.* **2023**, *22*, 417–431. [\[CrossRef\]](#)
18. Mahmood, H.; Arshad, M.; Ahmed, I.; Fatima, S.; ur Rehman, H. Comparative study of IoT forensic frameworks. *Forensic Sci. Int. Digit. Investig.* **2024**, *49*, 301748. [\[CrossRef\]](#)
19. Shin, D.H.; Han, S.J.; Kim, Y.B.; Euom, I.C. Research on Digital Forensics Analyzing Heterogeneous Internet of Things Incident Investigations. *Appl. Sci.* **2024**, *14*, 1128. [\[CrossRef\]](#)
20. Li, Z.; Amer, W.; Ruessler, G.; Garcia, M.; Liu, X. A Common but Flexible Method for IoT Device Forensics. In Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 7–11 December 2021.
21. Awasthi, A.; Read, H.O.; Xynos, K.; Sutherland, I. Welcome pwn: Almond smart home hub forensics. *Digit. Investig.* **2018**, *26*, S38–S46. [\[CrossRef\]](#)
22. Koroniotis, N.; Moustafa, N.; Sitnikova, E. A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework. *Future Gener. Comput. Syst.* **2020**, *110*, 91–106. [\[CrossRef\]](#)
23. Sadineni, L.; Pilli, E.S.; Battula, R.B. Ready-IoT: A Novel Forensic Readiness Model for Internet of Things. In Proceedings of the 2021 IEEE 7th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 14 June–31 July 2021.
24. Sharma, P.; Awasthi, L.K. Unveiling the hidden dangers: Security risks and forensic analysis of smart bulbs. *Forensic Sci. Int. Digit. Investig.* **2024**, *50*, 301794. [\[CrossRef\]](#)
25. Wu, T.; Breiting, F.; Niemann, S. IoT network traffic analysis: Opportunities and challenges for forensic investigators? *Forensic Sci. Int. Digit. Investig.* **2021**, *38*, 301123. [\[CrossRef\]](#)
26. Oladimeji, D.; Zhou, B. Forensic analysis of amazon alexa echo dot 4 th generation. In Proceedings of the 2022 IEEE International Conference on Big Data (Big Data), Osaka, Japan, 17–20 December 2022.
27. Lorenz, S.; Stinehour, S.; Chennamaneni, A.; Subhani, A.B.; Torre, D. IoT forensic analysis: A family of experiments with Amazon Echo devices. *Forensic Sci. Int. Digit. Investig.* **2023**, *45*, 301541. [\[CrossRef\]](#)
28. Li, S.; Choo KK, R.; Sun, Q.; Buchanan, W.J.; Cao, J. IoT forensics: Amazon echo as a use case. *IEEE Internet Things J.* **2019**, *6*, 6487–6497. [\[CrossRef\]](#)

29. Shin, Y.; Kim, H.; Kim, S.; Yoo, D.; Jo, W.; Shon, T. Certificate Injection-Based Encrypted Traffic Forensics in AI Speaker Ecosystem. *Forensic Sci. Int. Digit. Investig.* **2020**, *33*, 301010. [[CrossRef](#)]
30. Youn, M.A.; Lim, Y.; Seo, K.; Chung, H.; Lee, S. Forensic analysis for AI speaker with display Echo Show 2nd generation as a case study. *Forensic Sci. Int. Digit. Investig.* **2021**, *38*, 301130. [[CrossRef](#)]
31. Lin, L.; Liu, X.; Fu, X.; Luo, B.; Du, X.; Guizani, M. A non-intrusive method for smart speaker forensics. In Proceedings of the ICC 2021-IEEE International Conference on Communications, Montreal, QC, Canada, 14–23 June 2021.
32. Liu, X.; Li, A.; Fu, X.; Luo, B.; Du, X.; Guizani, M. Understanding digital forensic characteristics of smart speaker ecosystems. In Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 7–11 December 2021.
33. Gupta, J.N.; Kalaimannan, E.; Yoo, S.M. A heuristic for maximizing investigation effectiveness of digital forensic cases involving multiple investigators. *Comput. Oper. Res.* **2016**, *69*, 1–9. [[CrossRef](#)]
34. Kim, H.; Kim, S.; Shin, Y.; Jo, W.; Lee, S.; Shon, T. Ext4 and XFS File System Forensic Framework Based on TSK. *Electronics* **2021**, *10*, 2310. [[CrossRef](#)]
35. Lee, J.; Shon, T. Forensic Analysis of IoT File Systems for Linux-Compatible Platforms. *Electronics* **2022**, *11*, 3219. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.