Digital Forensics Investigation on Xiaomi Smart Router Using SNI ISO/IEC 27037:2014 and NIST SP 800-86 Framework

Dedy Hariyadi[1] Mandahadi Kusuma [2,*] Adkhan Sholeh [1,] Fazlurrahman [1]

[1] *Universitas Jenderal Achmad Yani, Yogyakarta, Indonesia*
[2] *Universitas Islam Negeri Sunan Kalijaga, Yogyakarta, Indonesia*
[*]*Corresponding author. Email: mandahadi.kusuma@uin-suka.ac.id*

ABSTRACT

The factual conditions reinforced by research data show the increasing number of connected smart devices in a house. The interconnection of these smart devices is able to form a smart home ecosystem with capabilities in the form of file sharing services, multimedia services, access to the internet network, to surveillance applications. Today's smart home interconnection is supported by the use of smart routers. The existence of the threat of exploitation of security gaps in the smart home ecosystem requires mitigation steps after cyber attacks on the smart home ecosystem. The research proposes a digital forensic investigation on the Xiaomi Smart Router using NIST SP 800-86 and SNI ISO/IEC 27037:2014 in a smart home ecosystem. Based on the findings in this study, to obtain and secure potential digital evidence from the Xiaomi Smart Router using the live acquisition method through the Xiaomi Smart Router web interface and the Mi Wi-Fi application installed on an Android smartphone. Live acquisition via the Xiaomi Smart Router web interface using web scraping techniques to obtain and secure digital evidence in the form of smart router device logs. Meanwhile, the digital evidence found from the Mi Wi-Fi application is a SQLite database file.

Keywords: *Digital Forensics, Live Acquisition, Smart Home, Smart Router, Xiaomi.*

1. INTRODUCTION

It is predicted that the installed and interconnected smart devices in the home will increase about 20 times by 2023 [1]. Smart devices installed in homes cannot stand alone, these smart devices require a connector or gateway so that they can be connected to each other using either wired or wireless media [2].

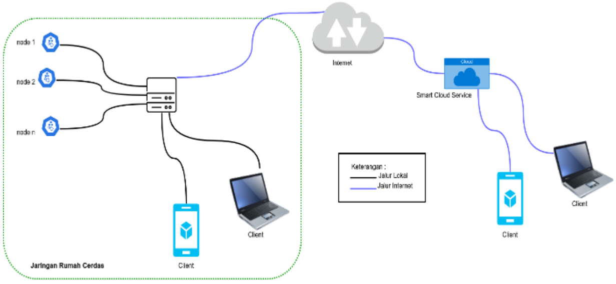


Figure 1 Home Network Topology

In general, the smart devices installed in the smart home have a topology as shown in Figure 1, between the smart device or node and the client connected to the internet through the gateway. Meanwhile, smart home services can also be accessed via public networks or the internet [3].

Internet of Things (IoT) is an object that can communicate, connect with each other, and share information through internet media including its control system [4]. According to the National Institute of Standards and Technology (NIST), smart devices that are a real form of IoT technology have affected on information security. NIST divides into three IoT capabilities that have the potential risk of affecting information security, they are; signaling capabilities, interface capabilities, and service support capabilities, as shown in Figure 2 [5]. This article focuses on the potential risks that affect information security in the IoT interface capability section with a digital forensics approach as a form of mitigation after a cyber attack incident occurs. The standard of digital forensics used in mitigating after a cyber attack incident is SNI ISO/IEC 27037:2014 concerning Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence.

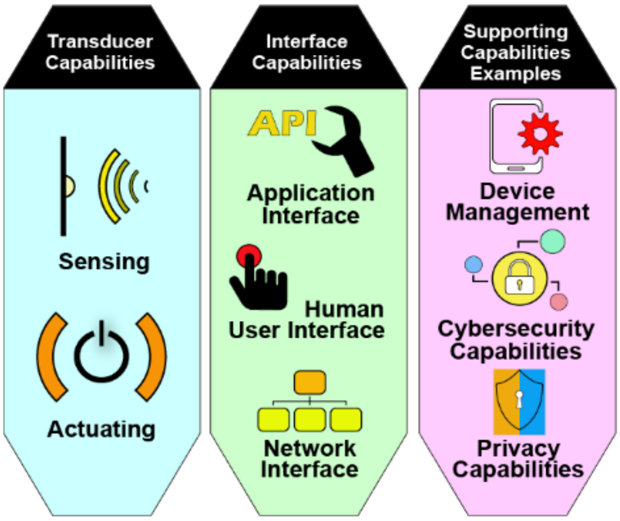


Figure 2 Potential IoT device could increase security risk

Cybercrimes are categorized into two type, they are computer crime and computer-related crime. Computer crime is a crime whose targets are electronic devices and the tools for the crime activity also use electronic devices. Meanwhile computer-related crime is a traditional crime such as stealing, cheating, drug abuse, pornography, and gambling that have used electronic devices in committing crimes [6]. Based on thus definitions it means that when commiting a crime could be happen anywhere using electronic devices, including in the home environment. In the era of the industrial revolution 4.0, we could find many homes have used electronic devices that are interconnected via the internet and using the smart devices [7].

Therefore smart devices that have potential risks to information security in smart homes include smart routers which are gateways of intelligent devices that are connected to each other, communication lines and information sharing via the internet. A smart router or smart wi-fi router is a smart device that has been equipped with additional software compared to other router devices such as file sharing capabilities, local multimedia services, and cloud computing service-based management [8]. In previous research, cyber attack incident mitigation still focused on file sharing service systems and smart router devices [9], [10] . Those previous research, not mentioned any detailed comprehensif accusition process along with digital evidence from smartphone and smart router altogether. Basically smart device could be controlled by using smartphone or web based access. A smart device system has managed centralized system and cound be controlled by using smartphone.[11].

This research proposes a comprehensive digital forensic analysis method for both smart router devices and smartphone control systems

2. MATERIALS AND METHODS

2.1. Material

The smart home ecosystem is the main object of this research. The digital forensics process in the smart home ecosystem involves many devices that need attention. However, in this study focused only on smart router devices. The needs for tools and materials used are as listed in Table 1.

Table 1. Short cut keys for the template

No	Material	Description
1	Access Point HD	Xiaomi AIoT Router CPU IPQ8071A A53 4Core 1GHz ROM 256MB Internal Memory 512MB Wi-Fi IEEE802.11ax, IEEE402.11ax
2	Android Phone	Xiaomi dengan sistem operasi MIUI
3	Computer	CPU dengan 4 Core @ 1.90GHz RAM 8GHz Hard Disk 500GB Sistem Operasi LinuxMint
4	Data Cable	Konektivitas ponsel cerdas dengan komputer
5	Android Debug Bridge (ADB)	SDK dari Android yang menghubungkan komputer dan ponsel cerdas
6	Python3	Potential evidence acquisition support programming language
7	Selenium	Python3 programming language support

2.2. Methods

NIST SP 800-86 has regulated the process of handling electronic and/or digital evidence in general. However, these guides are still relevant for handling after cyberattack incidents that occurred on smart homes. The investigation process according to NIST is collection, examination, analysis, and reporting which can be seen in Figure 3 [12]. The instructions from NIST are broadly combined with SNI ISO/IEC 27037:2014 in handling post-information security incidents in smart homes. The smart devices that are the object on this research are smart routers and smartphones, both of which are inseparable from digital evidence that is non-volatile and dependent on the device. Therefore, the method of acquisition/security of digital evidence follows the path as shown in Figure 4.

Live acquisition on the forensic digital process could be done by copying digital evidence based on SNI ISO/IEC 27037:2014 framework, as can be seen at Figure 4 [13] . The copying process must strictly follow the rules of digital forensics framework. In this paper live acquisition uses the Monca application, which is an application for the acquisition of digital evidence in the form of router log from electronic evidence such as Xiaomi Smart Router.

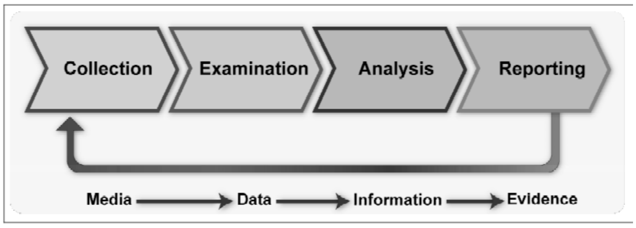


Figure 3 by NIST SP 800-86 Forensic Steps

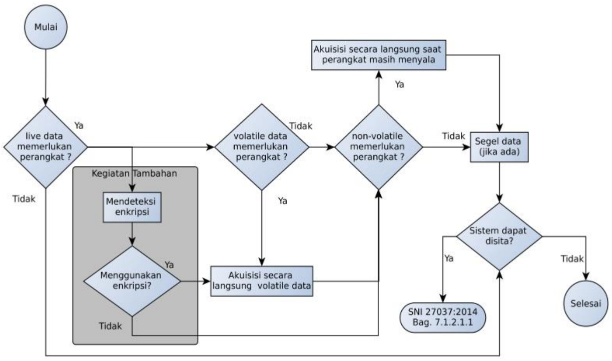

Mulai
live data memerlukan perangkat ?
Ya
Tidak
Kegiatan Tambahan
Mendeteksi enkripsi
Menggunakan enkripsi?
Ya
Tidak
volatile data memerlukan perangkat ?
Tidak
Ya
Akuisisi secara langsung volatile data
non-volatile memerlukan perangkat ?
Ya
Tidak
Akuisisi secara langsung saat perangkat masih menyala
Segel data (jika ada)
Sistem dapat disita?
Ya
Tidak
SNI 27037:2014 Bag. 7.1.2.1.1
Selesai

Figure 4 SNI ISO/IEC Acquisition Process

Accessing the smart router device system can be done by using two methods, which is accessing the Web UI using a web browser and using applications on smartphones such as Android and iOS. Then the collection stage in the digital forensic process is carried out by these two methods. In connection with securing evidence that has the potential to require equipment, according to SNI ISO/IEC 27037:2014, the stages of securing evidence are when the smart router device is on. The nature of the evidence from the smart router is non-volatile, which means that the stored data does not depend on electricity and is still stored on storage media [14]. So the digital forensics process is combined based on NIST SP 800-86 and SNI ISO/IEC 27037:2014 which divides the process review based on data sources or potential evidence from web browsers and applications running on Android and iOS smartphones as shown in Figure 5.

3. RESULTS AND DISCUSSION

In general, Access Point (AP) products from China use the OpenWRT operating system, especially the low-cost Access Point. OpenWRT is an embedded operating system that is installed on a router or AP with a web-based interface making it easier for users to operate it [15]. Likewise, the modified OpenWRT is also installed on the Xiaomi Smart Router so that it has a web-based interface combined with the application on the Android smartphone, Mi Wi-Fi.

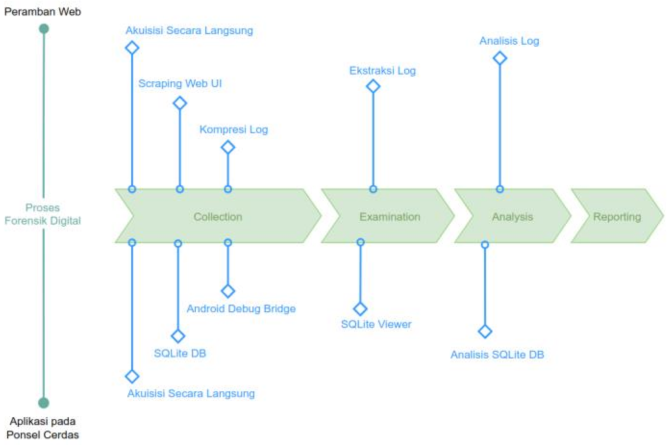


Figure 5 Forensic Process

With a web-based interface, the collection stage in the forensic process can be carried out by direct acquisition on the device. In this research, direct acquisition is done by scraping the web interface. The purpose of direct acquisition using scraping technique is to maintain potential digital evidence according to the rules of evidence, i.e relevance, reliability, and adequacy [16]. The web interface on the Xiaomi Smart Router has a feature to download Access Point Logs.

Direct acquisitions process has been done by downloading logs from Xiaomi Smart Router. In order to meet the rules of evidence, i.e relevance, reliability, and adequacy, the acquisition process directly uses the selenium driver to perform web scraping. The steps for downloading logs on the Xiaomi Smart Router consist of five main steps, they are: (1) entering the smart router password, (2) logging into the smart router, (3) selecting the settings menu, (4) selecting the status sub menu, and (5) downloading the log. The five steps have an XML Path which can be found on the webpage of the Xiaomi Smart Router. XML Path or so-called XPath is a query-based language contained in the data structure of a web page [17]. The XPath of the direct acquisition process can be seen in Table 2. The output of the direct acquisition process using web scraping is a collection of log files from the Xiaomi Smart Router which is compressed in .tar.gz format.

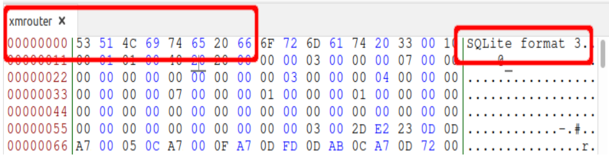
Table 2. XML Direct Path Accusition

No	Steps	XML Path
1	Input password smart router	/html/body/div[1]/div[2]/div[1]/form/div[1]/span/input
2	Login to smart router	/html/body/div[1]/div[2]/div[1]/form/div[2]/a
3	Choosing menu setting	/html/body/div[1]/div[1]/div/div[1]/div[1]/ul/li[2]/a
4	Choosing sub menu status	/html/body/div[1]/div[1]/div/div[2]/ul/li[5]/a
5	Download log	/html/body/div[1]/div[2]/div[2]/div[2]/div/button/span

The output of the acquisition process directly using web scraping is a collection of log files from the Xiaomi Smart Router which is compressed in .tar.gz format. In the examination process, the log file is then extracted using an extraction application that supports .tar.gz file extraction. Furthermore, all logs recorded by the Xiaomi Smart Router are carried out in-depth analysis according to the founded cases.

In addition to the web interface, the Xiaomi Smart Router has another access method, that is through an application on an Android smartphone called Mi Wi-Fi. The Mi Wi-Fi application can be classified as a smart controller based on cloud computing services like other Xiaomi IoT ecosystems [11]. Direct acquisition on Android smartphones utilizes Android Debug Bridge (ADB) to download SQLite files from Mi Wi-Fi applications [18]. In general, SQLite files from applications installed on Android smartphones can be found in the /data/data directory [19]. The potential digital evidence in the Mi Wi-Fi application is located in the /data/data/com.xiaomi.router/databases directory. The files to be secured are transfer_manager.db and xmrouter.

The transfer_manager.db and xmrouter files were transferred to the digital forensic analyst's computer for analysis of the information recorded in the SQLite database. Before analyzing the xmrouter file, first change the name to xmrouter.db. This is because the signature file of xmrouter is SQLite 3.x database with hex signature 53 51 4C 69 74 65 20 66 as shown by the signature file analysis in Figure 6 [20]. The next step is to analyze potential digital evidence in the form of SQLite database files using the SQLite Viewer application.



```
00000000 53 51 4C 69 74 65 20 66 6F 72 6D 61 74 20 33 00 10 SQLite format 3..
00000011 00 01 01 00 40 20 20 00 00 00 03 00 00 00 07 00 00 ....@............
00000022 00 00 00 00 00 00 00 00 00 03 00 00 00 04 00 00 00 .................
00000033 00 00 00 00 07 00 00 00 01 00 00 00 01 00 00 00 00 .................
00000044 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
00000055 00 00 00 00 00 00 00 00 00 00 03 00 2D E2 23 0D 0D ............-.#..
00000066 A7 00 05 0C A7 00 0F A7 0D FD 0D AB 0C A7 0D 72 00 ...............r.
```

Figure 6 Signature file from xmrouter

4. CONCLUSION

Investigations on smart router devices require more in-depth identification both in terms of the process of using the device and the technology used. This is a challenge for digital forensic analysts to investigate IoT devices installed in smart home ecosystems such as smart routers. In this study, the smart router device that is used as the object of electronic evidence is the Xiaomi Smart Router with device management methods using web technology and Android smartphone applications. To obtain potential digital evidence from the Xiaomi Smart Router, acquisitions are carried out directly through the web interface and utilizing ADB. The acquisition process is directly through the web interface using a web scraping technique that utilizes XPath from the Xiaomi Smart Router web interface. Digital evidence obtained from the acquisition process directly on the web interface is a compressed .tar.gz log. Meanwhile, to get digital evidence from the Mi Wi-Fi application installed on an Android smartphone using ADB. The digital evidence obtained from the acquisition process directly on the Android smartphone is the SQLite transfer_manager.db and xmrouter files.

The limitation of this research is that the process of obtaining potential digital evidence in the form of logs from Xiaomi Smart Routers and former SQLite still uses separate applications. Hopefully in the future research can develop more comprehensive and integrated applications in securing the two digital evidences. Of course, the development still need pays attention to the guideline applicable digital forensic rules such as SNI ISO/IEC 27037:2014, NIST or other digital forensic rules

ACKNOWLEDGMENTS

The author would like to express his deepest gratitude to the Ministry of Education, Culture, Research, and Technology of the Republic of Indonesia for funding this research and providing other support. This research is a collaboration between the Ministry of Education, Culture, Research, and Technology of the Republic of Indonesia, Jenderal Achmad Yani University Yogyakarta, and the NgeSec Community as a form of the Merdeka Campus program

REFERENCES

[1] David Cearley et al., “Top 10 strategic technology trends for 2020: A Gartner trend insight report,” 2020.

[2] W. Najib, S. Sulistyo, and W. Widyawan, “Survey on trust calculation methods in internet of things,” Procedia Computer Science, vol. 161, pp. 1300–1307, Jan. 2019, doi: 10.1016/j.procs.2019.11.245.

[3] M. U. H. A. Rasyid, F. A. Saputra, and A. Prasetiyo, “I-on smart controller: Portable smart home solution based on arduino and raspberry pi,” in 2018 international conference on applied science and technology (iCAST), Oct. 2018, pp. 161–164. doi: 10.1109/iCAST1.2018.8751609.

[4] K. K. Patel and S. M. Patel, “Internet of Things-IOT : Definition , Characteristics , Architecture , Enabling Technologies , Application & Future Challenges,” 2016. https://www.semanticscholar.org/paper/Internet-of-Things-IOT-%3A-Definition-%2C-%2C-%2C-Enabling-Patel-Patel/dd89eb44fb82d553432927c8083442edabdebfee (accessed Nov. 02, 2021).

[5] K. Boeckl et al., “Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks,” National Institute of Standards and Technology, Gaithersburg, MD, NIST IR 8228, Jun. 2019. doi: 10.6028/NIST.IR.8228.

[6] M. N. Al-Azhar, Digital Forensic: Panduan Praktis Investigasi Komputer. Jakarta: Salemba Infotek, 2012.

[7] sosiasi Penyelenggara Jasa Internet Indonesia, “Penetrasi dan Perilaku Pengguna Internet Indonesia Tahun 2018,” Jakarta, 2019.

[8] A. R. Supriyono, B. Sugiantoro, and Y. Prayudi, “EKSPLORASI BUKTI DIGITAL PADA SMART ROUTER MENGGUNAKAN METODE LIVE FORENSICS,” Infotekmesin, vol. 10, no. 2, Art. no. 2, Jul. 2019, doi: 10.35970/infotekmesin.v10i2.48.

[9] Dedy Haryadi and Abdul Rohman Supriyono, “Kerangka Investigasi Forensik pada Peladen Pertukaran Berkas Samba Berdasarkan SNI ISO/IEC 27037:2014,” Telematika, vol. 14, no. 1, pp. 62–67, Apr. 2017, doi: 10.31315/telematika.v14i01.1967.

[10] A. R. Supriyono and Y. Prayudi, “LIVE FORENSICS ACQUISITION FILE SHARING SAMBA PADA MIKROTIK ROUTER OS,” Cyber Security dan Forensik Digital, vol. 1, no. 1, Art. no. 1, May 2018, doi: 10.14421/csecurity.2018.1.1.1210.

[11] “Akuisisi Barang Bukti Digital Pada Smart CCTV Menggunakan Standarisasi ACPO DAN SNI ISO/IEC 27037:2014 | Jurnal Informa : Jurnal Penelitian dan Pengabdian Masyarakat.” https://informa.poltekindonusa.ac.id/index.php/informa/article/view/179 (accessed Nov. 03, 2021).

[12] T. Grance, S. Chevalier, K. A. Scarfone, and H. Dang, “Guide to Integrating Forensic Techniques into Incident Response,” Aug. 2006, Accessed: Nov. 03, 2021. [Online]. Available: https://www.nist.gov/publications/guide-integrating-forensic-techniques-incident-response

[13] M. P. Aji, D. Hariyadi, and T. Rochmadi, “Logical Acquisition in the Forensic Investigation Process of Android Smartphones based on Agent using Open Source Software,” IOP Conf. Ser.: Mater. Sci. Eng., vol. 771, no. 1, p. 012024, Mar. 2020, doi: 10.1088/1757-899X/771/1/012024.

[14] C. Lim, Suryadi, K. Ramli, and Y. S. Kotualubun, “Mal-Flux: Rendering hidden code of packed binary executable,” Digital Investigation, vol. 28, pp. 83–95, 2019, doi: https://doi.org/10.1016/j.diin.2019.01.004.

[15] T. A. Cahyanto and I. S. Nurhuda, “Implementasi Smart Router Berbasis OpenWRT Sebagai Media Untuk File Sharing dan Chatting Pada Laboratorium Terpadu Unmuh Jember.” INA-Rxiv, Feb. 04, 2018. doi: 10.31227/osf.io/p6bws.

[16] Badan Standarisasi Nasional, “Teknologi Informasi - Teknik Keamanan-Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital (SNI ISO/IEC 27037:2014).” Badan Standarisasi Nasional, 2014.

[17] “How to start with web scraping in the HICP: Evidence from EU member states. Pavel Belchev, Eurostat | UNECE.” https://unece.org/statistics/documents/2021/05/session-documents/how-start-web-scraping-hicp-evidence-eu-member (accessed Nov. 03, 2021).

[18] D. Hariyadi, A. A. Huda, Kharisma, and A. Priadana, “Laron v2: Pengembangan Aplikasi Forensik Logikal untuk Mengakusisi Percakapan Whatsapp di Android | SMARTICS,” SMARTICS Journal, vol. 7, no. no.1, pp. 7–13, Dec. 2020, doi: https://doi.org/10.21067/smartics.v7i1.5026.

[19] D. Hariyadi and I. Y. Pasa, “IDENTIFIKASI BARANG BUKTI DIGITAL PADA APLIKASI MI VIDEO MENGGUNAKAN METODE LIVE FORENSICS,” Seminar Nasional Informatika (SEMNASIF), vol. 1, no. 1, Art. no. 1, Nov. 2018, Accessed: Nov. 03, 2021. [Online]. Available: http://jurnal.upnyk.ac.id/index.php/semnasif/article/view/2634

[20] X. Lin, “File Signature Searching Forensics,” Introductory Computer Forensics, pp. 235–244, 2018, doi: 10.1007/978-3-030-00581-8_10