Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) Device

By Imam Riadi

WORD COUNT	5164	TIME SUBMITTED	16-NOV-2018 08:09AM
		PAPER ID	42008896

Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) Device

Randi Rizal [1], Imam Riadi [2] and Yudi Prayudi [3]
[1,3] Department of Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia
[2] Department of Information System, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
randirizal@gmail.com[1], imam.riadi@is.uad.ac.id[2], prayudi@uii.ac.id[3]

ABSTRACT

Today is the era of the Internet of Things (IoT), millions of devices such as smart city, smart home, smart retail, automotive, automatic car tracking, smartphone detection, smart lighting, temperature monitoring etc. are being connected to the Internet. There are various devices which are interconnected to the other devices on the internet of things which share different techniques and the different standards. The emergence of new technology in various fields it also brings up challenges in the area of the forensic investigation. As there will be many new challenges to the forensic investigators. The latest tools and the process flow carried out will not fulfill distributed and current IoT infrastructure. The Forensic researcher will have a lot of challenges to face in collecting the piece of evidence from the infected component on the IoT device and also will face complication to analyze those evidence.

In this research, we will do the network forensics investigation for detecting flooding attack on the Internet of Things (IoT) device.

KEYWORDS

Internet of Things, Network Forensics, IoT Device Forensics, Flooding Attack, Digital Investigations.

1. INTRODUCTION

The Internet of Things (IoT) results from internet progress and the innovative evolution of the smart devices leads to the development of the new computing prototype. IoT is calculated the coming estimation of the internet which works on the Machine to Machine (M2M) communication and the Radio Frequency Identification (RFID) [1]. The primary purpose of the IoT is to allow a secure data exchange between the real world devices and applications.

The Internet of Things (IoT) has become quite famous in the recent years. Many of the daily routine devices are getting connected with us that covers many capabilities like sensing, autonomy and contextual awareness [6]. IoT devices include personal computers, laptop, smartphone, tablet, and other home embedded devices [2]. These devices are connected to each other and share a same network for communicating with each other. These all the devices are connected with the sensor to detect the particular surrounding condition and analyze the situation and work accordingly. Devices are also programmed to take the decision automatically or inform according to the user so that the user can make the best decision.

This interconnected network can bring lot of advancement in the technology of application and services that can bring economic benefit to the global business development. Many devices are connected to the internet to share the local information to the cyberspace. The US National Intelligence Council (NIC) suspects that by 2025 Internet nodes will be on of our peripheral things food packages, furniture, paper documents, and many more [3]. In accord with a report by Gartner, in next five years there will be 26 billion IoT devices [4]. International Data Corporation (IDC) estimates that the IoT trade will reach $3.04 trillion and there will be 35 billion connected things in 2020 [5]. Processing and computation power, communication medium, dimension, etc. these things are varied with different attributes[6].

According to the analysis report, since many devices will be connected to the IoT which ultimately turns the attention to the hacker in breaking the security mechanism[2]. IoT Forensics used to investigate attacks such as we need to implement the digital forensics aspects in the IoT parameter [1].

In fact the Digital Forensics in the IoT device is very challenging and varied, the traditional model of the forensics does not match with the current IoT Environment. A large number of the devices will also bring new challenges for the data management. An infinity of IoT devices generating large data also makes it difficult for the investigator to analyze the data.

2. BASIC THEORY

2.1 Digital Forensics

Digital Forensics is a part of science which involve the return to an original state and investigation of stuff which is found in digital devices, related to computer crime. In the digital forensics, we will first be including on the network forensics.

Network forensics is defined in [8] as capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents. In other words, network forensics involves capturing, recording and analyzing of network traffic. Serves to collect of information, evidence gathering and detect attacks. The process of investigation occurred in the network with handling the traffic and activity. Differ from the other method, the network forensics related to dynamic information that is easily lost. Network Forensics has two functions, the first outline to security, belonging traffic monitoring network which aims to get the evidence given is the lack of evidence in the network so that the investigation could not walk. Second, regarding law enforcement that analysis on capturing of network traffic may contain sending a file, searching for keywords, and breakdown in communications made as in email and chat.

2.2 Network Forensics Process Model

In a paper called "A Generic Framework for Network Forensics" the author proposed a model of the network forensics investigation. This proposed model consists of many different stages of network forensics investigation. The figure 1 represents the design of network forensics which has nine stages figured [9].

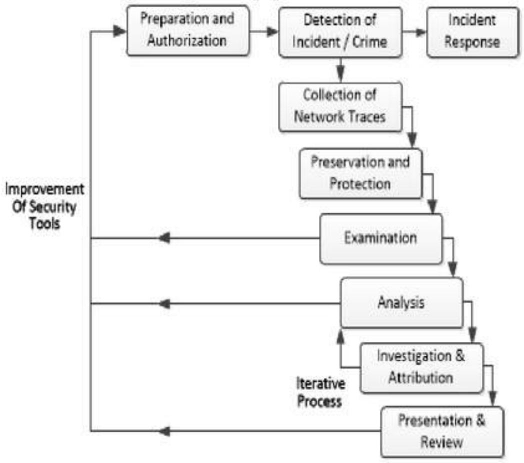

Preparation and Authorization
Detection of Incident / Crime
Incident Response
Collection of Network Traces
Preservation and Protection
Examination
Analysis
Investigation & Attribution
Presentation & Review
Improvement Of Security Tools
Iterative Process

Figure 1. Generic Framework for Network Forensics

- **Preparation Stage :** The main objective is to acquire the fundamental authorization and legitimate guaranteed.
- **Detection Stage :** Generate a warning or an alert which indicate security offense.
- **Incident Response Stage :** Usable only when the investigation is beginning in the course of the attack.
- **Collection Stage :** The most complicated section because the data streams quickly and is no possibility to generate later traces of the same thing.
- **Preservation Stage :** Original Evidence is kept secure through with computed hashes.
- **Examination Stage :** Examines the previous phase. All hidden or altered data is to be uncovered which is done by the attacker.
- **Analysis Stage :** Collected evidence is analyzed to locate the source of the mixing.
- **Investigation Stage :** Use information gathered in the analysis phase and focus on finding the attacker.
- **Presentation Stage :** Final stage for processing the model. Here the documentation is made and the report is generated and is shown to the higher authority.

2.3 Forensic in IoT Environment

The IoT Forensics is also one of the specialized branch in the digital forensics where all the phases discussed deals with the IoT infrastructure to find facts about the crime happened in IoT environment. The IoT Forensics is carried out in the three levels of forensics : Cloud level forensics, network level forensics, device level forensics this can be explained in Figure 2 [1].

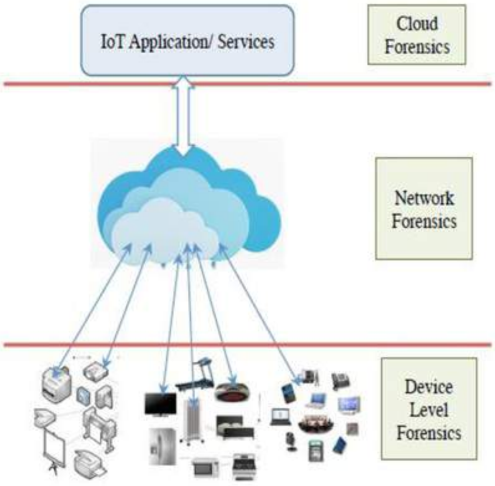
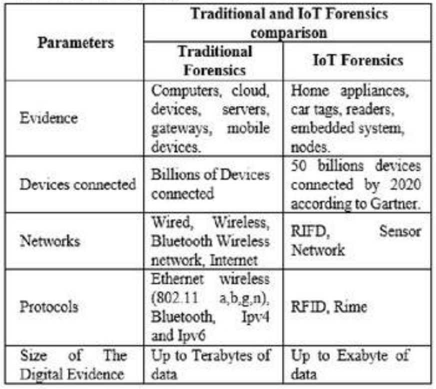


Figure 2. IoT Forensics

- **Device level forensics :** At this level, a forensic investigator needs to collect data first from the local memory contained in the IoT device to be analyzed. It is necessary to use the IoT device that is missed in analyzing data on the forensic level device.
- **Network level forensics :** To detect various sources of attacks can be identified from network traffic logs. Thus, the log traffic network can be very important to determine the guilt or freedom of the suspect. IoT infrastructure includes various forms of networks, such as Body Area Networks (BAN), Personal Area Networks (PAN), Home / Hospital Area Networks (HAN), Local Area Networks (LAN) and Wide Area Networks (WAN). Important evidence obtained is collected from one of these networks so that network forensics.
- **Cloud level forensics :** Cloud forensics is one of the most important part in the IoT forensic domain. Why? Due to the fact that most existing IoT devices have low storage and computing capacity, data generated from IoT devices and IoT networks are stored and processed in the cloud. This is because cloud solvents offer a variety of advantages including convenience, large capacity, scalability, and accessibility on request.

We seen that how the IoT Forensics environment works and the three level of forensics needs to be carried out in the IoT scenario to find out the actual source of the infected device or the network breach[1]. Here in this section we will do the comparison of the different parameters how the how the actual system works and how the proposed solution is to be carried out [10].



Parameters	Traditional and IoT Forensics comparison	
	Traditional Forensics	IoT Forensics
Evidence	Computers, cloud, devices, servers, gateways, mobile devices.	Home appliances, car tags, readers, embedded system, nodes.
Devices connected	Billions of Devices connected	50 billions devices connected by 2020 according to Gartner.
Networks	Wired, Wireless, Bluetooth Wireless network, Internet	RIFD, Sensor Network
Protocols	Ethernet wireless (802.11 a,b,g,n), Bluetooth, Ipv4 and Ipv6	RFID, Rime
Size of The Digital Evidence	Up to Terabytes of data	Up to Exabyte of data

Table 1. Comparison of Traditional and IoT Forensics

The conventional tools and technologies are not deliberated completely to bring out forensic in the IoT environment as it faces many challenges [11]. In this part, we will recognize the challenges we are facing for the forensic investigation in the IoT environment [1].

a. Compromised device identification in IoT.

The criminal. For e.g., there are number of devices in the college and if any of the devices gets compromised and gets breach on the network and extract some of the personal files it will be very hard to find the source of the device which got infected. This challenge is like finding the needle in the haystack.

b. Gathering and analysis of data.

After identification there comes the analysis and gathering which is quite a challenging task to find the piece of evidence. This phase is very crucial phase and depends on the other phase also resulting the error to other phase.

c. Data Organization

The IoT devices produce the wide variety of data makes the collection and analysis stage challenging. The proper logs need to be organized in order to avoid the complication of the data and files.

d. Preservation of Evidence

The last step of the forensic investigation is that the forensic examiner presents information that has been analyzed and use as digital evidence in front of the court of law. As in comparison, giving traditional forensic evidence is easy than IoT Environmental forensics becouse it is a challenging task as the jury members don't have enough knowledge as compared to the technical person.

2.4 Attacks in IoT

Over time, the domain of security Attacks on IoT devices is growing rapidly. The attacks on IoT Systems are summarized in the following figure 2 [12].

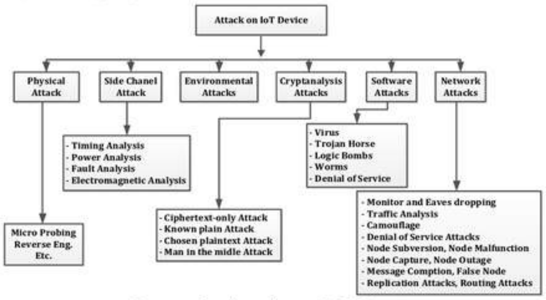


Figure 3. Attacks on IoT Device

Cyber attacks on IoT devices have been classified into a few categories as discussed in [13],[14],[15] and [16] as the following :

a. Node Tampering

An rival can transform the device and place a cheater to the system. Thus, the device will not purpose as it is expected to be work on. This kind of attack generally uses to swipe information and abuse the software and the hardware of IoT devices.

b. Denial of Service (DoS)

DoS attack can be undertaked by mishandle the device, operating its software and application, or upseting the communication channel [13]. One of the DoS attack is the breakdown attack where the enemy is able to disable the sensor communication channel from carrying alerts by generating accidents. The accidents will be caused by the transmission request interrupted.

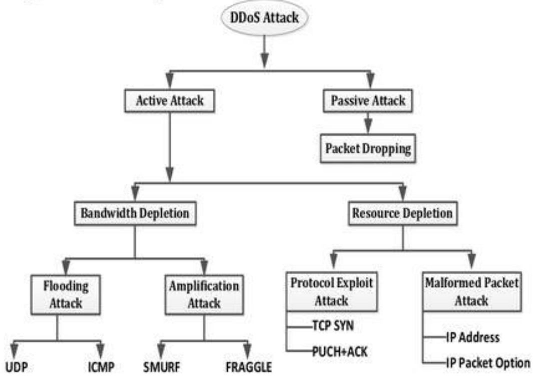


Figure 4. DDoS Attacks

c. Distributed DoS

In the case of Mirai attack. The Mirai malware is outlined to use an existing vulnerability within IoT devices for DDoS attacks .There are millions of IoT devices on the trade that are misconfigured and set to continue request via the Transmission Control Protocol.

d. Spoofing

The credential information become the method used by adversary usually which belongs to others to get access to the unapproachable service. This credentials can be located from the device it self, eavesdropping on the communication line or from the reconnaissance activities.

e. The Violation of Privacy

With this, the adversary can collect private data from diverse sources. For example are meta information and activity investigation which is the main target of the attack.

f. Buffer Overflow

A buffer overflow which using this kind of attack lets an adversary to authority or crash the processor to modify its core element. If the program is enough wealthy, thus the adversary can control the host.

g. SQL Injection

Security attack in this case, a malicious code injection method used to attack the information-driven applications, operating a security weakness in an application's software, license the adversary to cheat identity, modify data which may cause the rejection issues.

The glucose monitoring system for diabetic patients becomes another case study of attacks. The October 2016 report explained that Johnson & Johnson branch Animas produces the device reads user blood glucose levels through a meter before the pump uses these readings by "communicating wirelessly" in the 900 MHz band to deliver insulin. One of the main security faults there is a lack of encryption between these components. This opens the door for eavesdroppers to capture information such as dosage data and blood glucose results. Attackers can easily detect the remote or pump key and then cheat being the remote or the pump. Another vulnerability is the communication line where it is taking place between the pump and meter has no timestamps or sequence numbers and no defence opposed to replay attacks.

2.5 *Arduino UNO*

The Arduino UNO is a small and cheap device that bring through you to easily connect some electronic thing you have made to your computer and to the internet. It brings all kind of rash invention to the Internet Of Things (IoT). Arduino is an open source computer hardware and software enterprise, project and user community that designs and productions single-board microcontrollers and microcontroller kits for frame digital devices and interactive aims that can sense and control aims in the physical and digital globe.

Various microprocessors and controllers are used to design arduino boards. Set digital and analog input / output (I / O) pins to complement the Arduino board which can be connected to various extension boards or Breadboards (shields) and other circuits. Arduino boards display serial communication interfaces, including Universal Serial Bus (USB) on several models, and are also used to create programs from personal computers.

The arduino platform consists of arduino board, shield, arduino programming language, and arduino development environment. Arduino board usually has a basic chip ATmel AVR microcontroller ATmega8 following derivatives. The simplified arduino board diagram is shown in Figure 3. Shield is a board that can be mounted on the arduino board to increase the ability of the arduino board.

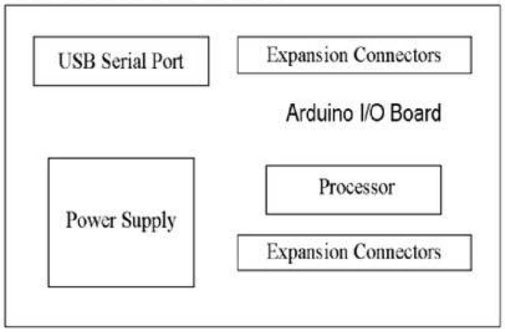


Figure 5. Block Diagram of Arduino Board

2.6 Bluetooth HC05

The Internet of Things (IoT) architecture consists of hardware, communication, software systems and application layers, with Bluetooth being used to act as a communication layer. The communication layer is a serious overpass between the layers and contains of a multi-layer stack, comprising data link, network or transport, and session protocols. Bluetooth is one part of the data link layer, connecting the sensor to the sensor or sensor to the gateway. This network layer, on the other hand, is responsible for routing or moving packets across the network, using the most appropriate path. The session layer protocol allows messaging on various elements of the IoT communication subsystem.

Bluetooth HC05 is a bluetooth that has UART serial communication in the reception and delivery of its data. Bluetooth HC05 allows to communicate directly with the microcontroller through TX and RX lanes contained on the pin out it. Basically, bluetooth HC-05 can only be configured as slave can not be used as master. Here is the physical form of bluetooth HC-05 :

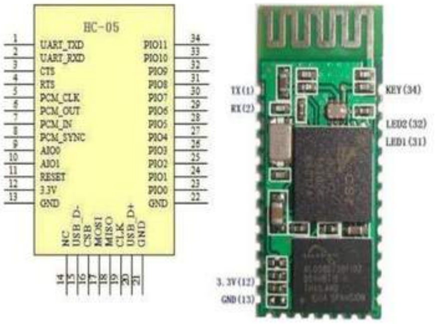


Figure 6. The physical shape of bluetooth HC 05

3. METHODOLOGY

3.1 Bluetooth Arduino Configuration Scheme

Preparing arduino package which is the main package needed in the system, the package used is arduino driver package that can be installed directly. Configuring arduino with Bluetooth Hc-05 is a preliminary configuration for the purpose of detecting and analyzing Traffic log file data contained in arduino. Here is the Arduino configuration scheme with Bluetooth HC-05 :

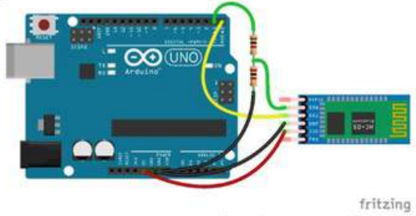


Figure 7. Bluetooth Arduino Configuration Scheme with

Some configurations in Arduino is connect Arduino to a computer, perform serial communication such as sending and receiving sensor data via serial terminal on Arduino IDE via USB Connector. Power Jack : Input voltage to turn on Arduino, IC ATMEGA328p : ATMel microcontroller IC with Arduino booth loader. Digital I / O is used for digital inputs and outputs, at pin 3,5,6,9,10,11 has a sign (~) indicating that the pin in addition to having Digital I / O facility also has PWM (Pulse Width Modulation) with range the output value of 8 bits or equivalent value between 0-255. Next is the Analog Input used for sensor data input, potentiometer and other analog input devices. Then Power is used to take power 5V, 3.3V, GND.

Configuration is also done on bluetooth device HC-05. When doing the bluetooth configuration then bluetooth position in a state not related to arduino device that uses wireless. So it will be absolutely certain that bluetooth is active without a connection. Next is done Default Bluetooth settings are Baudrate : 9600 bps Name : linvor Pairing Code : 1234. Any configuration changes above will be saved even when the power is turned off. All commands sent to Buetooth do not have to be with new line characters. Therefore we recommend to use 'Serial Monitor' on Arduino IDE to configure the Bluetooth module.

Next the procedure to do that bluetooth configuration is connecting Bluetooth to PC, LED should blink, open Arduino IDE software, choose correct COM port that Bluetooth connected.

3.2 Flooding Attack Scenario

Phase flooding attack scenario was established to implement network forensics on the Internet of Things (IoT) device. The system simulation purposes to perform network forensic testing of the IoT Bluetooth Arduino device in detecting flooding attacks. The simulation is done using the LOIC tool used to detect flooding attacks. The exercise starts with the IP packet delivery on the target and the port will be attacked.

Here is a figure of the system simulation case of flooding attack against IoT device :

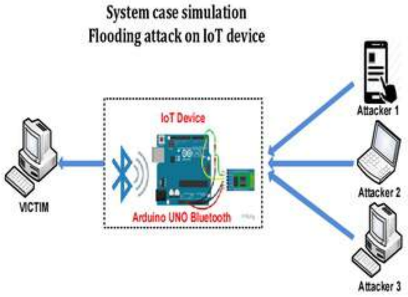


Figure 8. Simulation Flooding Attack

4. IMPLEMENTATION AND RESULT

Phase implementation on network forensic research is in the design of forensic network architecture such as the image shown in Figure 9. Which is the forensic architecture of the network on the IoT device on detecting flooding attacks. The investigator forensic performs an analysis of the IoT device to finding the attack packets.

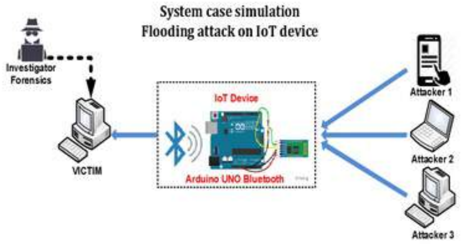


Figure 9. Network Forensic Architecture on IoT Devices

A. Implemetation Model Process Forensics

Implementation of network forensic process model in the design of network forensic architecture to detect attacks on IoT devices with Bluetooth Arduino. Detection of flooding attacks on the case of a process that is trying applied IoT device. Thus the log file will be stored in the data logger file. So researchers will analyze to find evidence by using Wireshark in reconstructing the data log file contained in Bluetooth Arduino UNO.

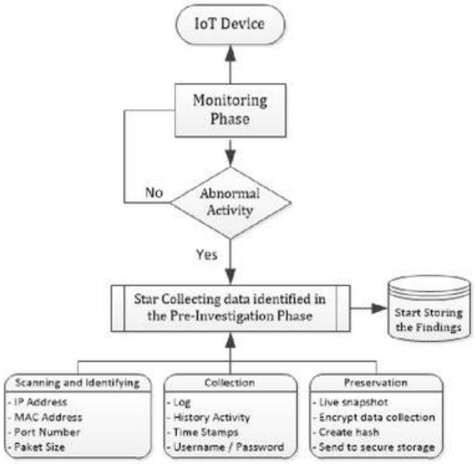


Figure 10. IoT Device Forensics

B. Model Process Forensic

Level Forensic Device on device inspection, network forensics to analyze and record traffic. IoT devices will produce very large data. And do to add up the data network. Because the amount of data evidence will be very large and it will be very difficult to analyze data and it is difficult to identify evidence that can be used to identify digital forensics in finding flood attacks and monitoring so that it can identify the source of the attack that the device is infected with. The results of this analysis have nine stages of the Forensic Process Model:

- **Preparation and Authorization**

At this phase, network forensic investigations apply to environments where network security devices such as packet analyzers, traffic stream evaluation software are located at various planned points on the network to detect flooding attacks on IoT devices. The personnel treatment these devices must be trained to make sure that maximum and quality evidence may be collected in order to facilitate attribution of the crime. The required authorizations to monitor the network traffic are acquired and a well-defined security approach is in a location so that the privacy of individuals and the organization is not breaked.

- **Detection of Incident**

Various security tools generate warnings, indicating a security offense or policy violation are observed. Any unwarranted events and unusual activity noticed will be analyzed. The confirmation of an incident results in two aims that incident response and collection of data.

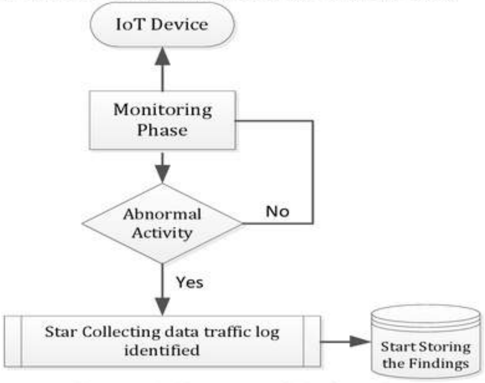

IoT Device
Monitoring Phase
Abnormal Activity
No
Yes
Star Collecting data traffic log identified
Start Storing the Findings

Figure 11. Detection of Findings Log

- **Incident Response**

In this phase, The response to the illegal act or seizure detected is initiated based on the information collected to validate and evaluate the incident. The response starts up turns on the type of attack identified and is guided by organization policy, legal and business. This phase is relevant only to cases where an investigation begins while the attack is underway and not notitia criminis (after notification of crime).

- **Collection of Network Traces**

Collection evidence in this study used recordings of traffic log on IoT device. The process of taking payload as flooding attack file in this study as figure 4.

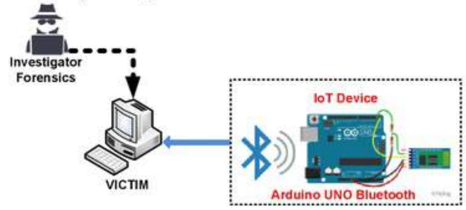
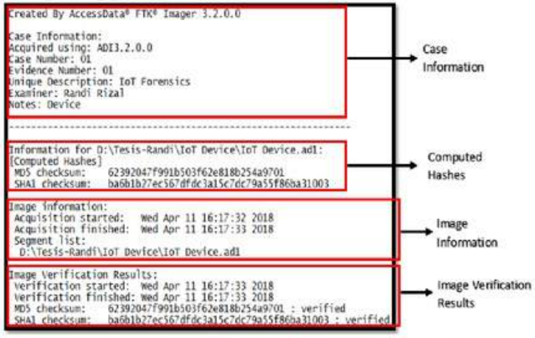


Figure 12. Data Collection Stage

- **Protection and Preservation**

The original data acquired in the form of shreds of evidence and logs are kept on a backup device. A hash of all the clue data is taken and the data is protected. Chain of custody is hardly imposed so that there is no unauthorized use or tampering. Another copy of the data will be used for analysis and the originally collected network traffic is protected. In this stage will use the FTK Imager application for made a hash of data.



```
Created By AccessData® FTK® Imager 3.2.0.0

Case Information:
Acquired using: ADI3.2.0.0
Case Number: 01
Evidence Number: 01
Unique Description: IoT Forensics
Examiner: Randi Rizal
Notes: Device

--------------------------------------------------------------

Information for D:\Tesis-Randi\IoT Device\IoT Device.ad1:
[Computed Hashes]
 MD5 checksum:    62392047f991b503f62e818b254a9701
 SHA1 checksum:   ba6b1b27ec567dfdc3a15c7dc79a55f86ba31003

Image information:
 Acquisition started:   Wed Apr 11 16:17:32 2018
 Acquisition finished:  Wed Apr 11 16:17:33 2018
 Segment list:
  D:\Tesis-Randi\IoT Device\IoT Device.ad1

Image Verification Results:
 Verification started:  Wed Apr 11 16:17:33 2018
 Verification finished: Wed Apr 11 16:17:33 2018
 MD5 checksum:    62392047f991b503f62e818b254a9701 : verified
 SHA1 checksum:   ba6b1b27ec567dfdc3a15c7dc79a55f86ba31003 : verified
```

Figure 13. Hash Evidence of Log Traffic

- **Examination**

Forensic investigators in examining the log file found on the traffic log of bluetooth in the capture (p.cap) by entering parameters to be plugged. The examination process is going capturing traffic with wireshark application.

- **Analysis**

At this stage of the analysis of log files will be checked, the log files that have been recovered will be examination one by one to determine changes in the network and to see a timestamp. Flooding attacks will be visible when the request to the IoT device increased capture traffic that is an anomaly. Then flooding attacks are sent from the attacker so that traffic will increase. In addition to traffic conducted investigator using wireshark to capturing the traffic, also can be in the graphic user requesting increased in figure 14.

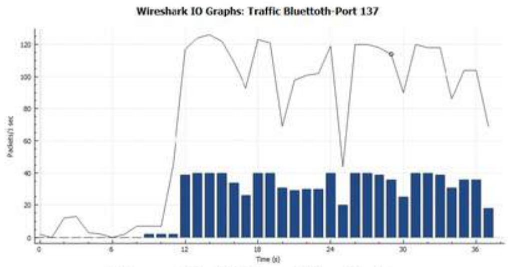


Figure 14 : IO Graph Traffic Log

After the log files are recorded, the log file will be taken and analyzed using Wireshark to have this forensic evidence. In the picture seen demand exceed 15 packets in one second. As shown in figure 15.

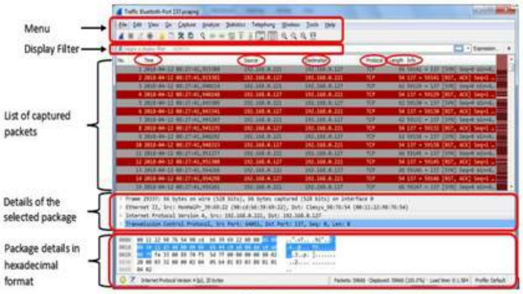
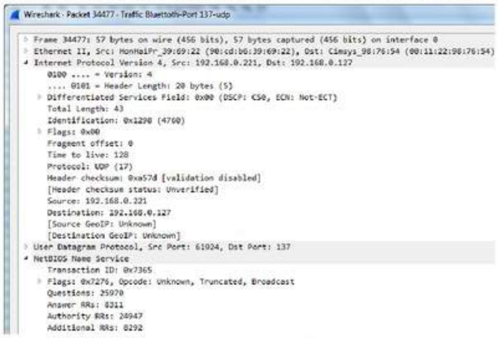

Menu
Display Filter
List of captured packets
Details of the selected package
Package details in hexadecimal format
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No.
Time
Source
Destination
Protocol
Length
Info

Figure 15 : Traffic Log in Wireshark

- **Investigation and Attribution**

The information obtained from the evidence traces is used to identify of the incident. This will help in source traceback, reconstruction of the attack scenario and attribution to a source.

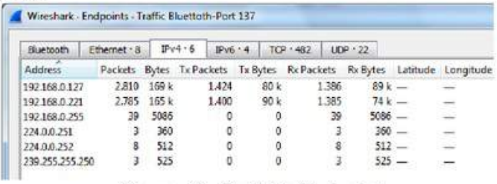


```
▹ Frame 34477: 57 bytes on wire (456 bits), 57 bytes captured (456 bits) on interface 0
▹ Ethernet II, Src: HonHaiPr_39:69:22 (90:cd:b6:39:69:22), Dst: Cimsys_98:76:54 (00:11:22:98:76:54)
◢ Internet Protocol Version 4, Src: 192.168.0.221, Dst: 192.168.0.127
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▹ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 43
    Identification: 0x1290 (4760)
  ▹ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0xa57d [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.221
    Destination: 192.168.0.127
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▹ User Datagram Protocol, Src Port: 61924, Dst Port: 137
◢ NetBIOS Name Service
    Transaction ID: 0x7365
  ▹ Flags: 0x7276, Opcode: Unknown, Truncated, Broadcast
    Questions: 25970
    Answer RRs: 8311
    Authority RRs: 24947
    Additional RRs: 8292
```

Figure 16 : UDP Follow

From the collection of the line can have one line to perform analysis on any part of the frame that represents a frame in an attack packet flooding of IP address 192.168.0.221 has a length (length) range in the 50s Bytes (57 Bytes). On the Internet Protocol Version 4, to read as 192.168.0.221 IP source and destination IP address visible 192.168.0.127 with 20 Bytes header length and the total length of 43. On the part of the user datagram protocol, source port reads as 61924 and destination port read as 137. If the filter is returned to the ip.src == 168.192.0.221 and investigated in another frame, the source port is immutable, but still in a great range (ports 49775-63293). log file analysis results obtained 3 IP address that has acted illegally flooding attacks on IoT device.

In addition, the analysis continued with statistics module endpoint in Wireshark used to collect attack packets contained in log files during the attack simulation. In Figure 9 below explains that the IP address has a different load on each package and at different speeds in each of its bytes.



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Latitude	Longitude
192.168.0.127	2.810	169 k	1.424	80 k	1.386	89 k	—	—
192.168.0.221	2.785	165 k	1.400	90 k	1.385	74 k	—	—
192.168.0.255	39	5086	0	0	39	5086	—	—
224.0.0.251	3	360	0	0	3	360	—	—
224.0.0.252	8	512	0	0	8	512	—	—
239.255.255.250	3	525	0	0	3	525	—	—

Figure 17 :Statistic Endpoint

- **Presentation**

At the presentation stage is the last stage in the forensic process model. This stage was the presentation of all the findings in this study. Based on the analysis that has been done then obtained 3 IP address which becomes the findings in this research scenario, as shown in Table 2.

No.	Timestamp	Source	Dest. IP	Protocol	Source Port	Dest. Port	Payload
1	2018-04-12 08:27	192.168.0.221	192.x.x.127	UDP	59132	137	796f752077617320617474616363 6b6564206279206d65...
2	2018-04-11 14:03	192.168.0.135	192.x.x.127	UDP	49775	137	c2620050b1893e8070022e0c...
3	2018-04-11 14:03	192.168.0.87	192.x.x.127	UDP	63293	137	552064756e20676f666564...

Table 2. File Log Bluetooth Traffic

6. CONCLUSION

In this paper we provide different aspects than those used for IoT and also use IoT devices. The author has presented a network forensic model for detecting attacks and identifying attacks. Here's more about the flooding attack and found the infected IoT Bluetooth Arduino device. Log file data with p.cap extension can be analyzed by network forensic investigation using wireshark application.

Based on the analysis that has been done, it was found that 3 IP addresses committed illegal actions, which led to overload traffic. By applying a forensic process model, it can be used to detect flooding attack on IoT devices.

REFERENCES

[1] Zawoad, Shams, and Ragib Hasan. "FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things." *Services Computing (SCC), 2015 IEEE International Conference on*. IEEE, 2015.

[2] Hossain, Md Mahmud, Maziar Fotouhi, and Ragib Hasan. "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things." *Services (SERVICES), 2015 IEEE World Congress on*. IEEE, 2015.

[3] L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,” Computer networks, vol. 54, no. 15, pp. 2787–2805, 2010.

[4] www.gartner.com, “Gartner Says the Internet of Things Will Transform the Data Center,” http://www.gartner.com/newsroom/id/2684616, 2014.

[5] www.idc.com, “Finding Success in the New IoT Ecosystem: Market to Reach $3.04 Trillion and 30 Billion Connected ”Things” in 2020, IDC Says ,” http://www.idc.com/getdoc.jsp?container =prUS25237214, 2014.

[6] Y. Huang and G. Li, “A semantic analysis for internet of things,” in Intelligent Computation Technology and Automation (ICICTA), 2010 International Conference on, vol. 1. IEEE, 2010, pp. 336–339.

[7] E.S. Pilli, R.C. Joshi, & R. Niyogi. **“**A Generic Framework for Network Forensics”. *International Journal of Computer Applications* (IJCA) (0975 – 8887) *Volume 1 – No. 11*, 2012.

[8] Nguyen, K., Tran, D., Ma., & Shama, D. (2014) An Approach to Detect Network Attacks Applied for Network Forensics, 655-660.

[9] E.S. Pilli, R.C. Joshi, & R. Niyogi. **“**A Generic Framework for Network Forensics”. *International Journal of Computer Applications* (IJCA) (0975 – 8887) *Volume 1 – No. 11*, 2013.

[10] Oriwoh, Edewede, et al. "Internet of Things Forensics: Challenges and approaches." *Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom), 2013 9th International Conference Conference on*. IEEE, 2013.

[11] Buric, J., and D. Delija. "Challenges in Network forensics." *Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2015 38th International Convention on*. IEEE, 2015.

[12] Ramjee Prasad, Antonietta Stango, Neeli Prasad & Sachin Babar.”Proposed Embedded Security Framework for Internet of Things (IoT)**”.** 2011.

[13] Atamli, A.W. & Martin, A., “Threat-Based Security Analysis for the Internet of Things”. *International Workshop on Secure Internet of Things*, pp.35–43. 2014

[14] Hachem, S., Teixeira, T. & Issarny, V., 2012. Ontologies for the internet of things. *Proceedings of the 8th Middleware Doctoral Symposium on - MDS ’11*, pp.1–6.

[15] Huuck, R., 2015. IoT: The Internet of Threats and Static Program Analysis Defense. *EmbeddedWorld 2015: Exibition & Conferences*, p.493.

[16] Borgohain, T., Kumar, U. & Sanyal, S., 2015. Survey of Security and Privacy Issues of Internet of Things. *arXiv preprint arXiv:1501.02211*, p.7. Available at : http://arxiv.org/abs/1501.02211.

[17] Mualfah, D. and Riadi, I. “Network Forensics For Detecting Flooding Attack On Web Server” *(IJCSIS) International Journal of Computer Science and Information Security, Vol.15*, 2017.

[18] Iswardani, A. and Riadi, I. “Denial Of Service Log Analysis Using Density K-Means Method,” vol. 83, no. 2, pp. 299–302, 2016.

[19] Oriwoh, Edewede, and Paul Sant. "The Forensics Edge Management System: A Concept and Design." *Ubiquitous Intelligence and Computing, 2013 IEEE 10th International Conference on and 10th International Conference on Autonomic and Trusted Computing (UIC/ATC)*. IEEE, 2013.

[20] Bandyopadhyay, Debasis, and Jaydip Sen. "Internet of things: Applications and challenges in technology and standardization." *Wireless Personal Communications* 58.1 (2011): 49-69.

[21] T. A. Cahyanto and Y. Prayudi, “Web Server Logs Forensic Investigation to Find Attack’s Digital Evidence Using Hidden Markov Models Method ,” *Snati*, pp. 15–19, 2014.

[22] P.F. Moh, P. Yudi & R. Imam, “Comparison of Attribute Based Access Control (ABAC) Model and Rule Based Access (RBAC) to Digital Evidence Storage (DES)” *International Journal of Cyber-Security and Digital Forensics (IJCSDF) 7(3): 275-282*, 2018.

[23] U. Rusydi, R. Imam & Z.M. Guntur. “Mobile Forensic Tools Evaluation for Digital Crime Investigation” *International Journal on Advanced Science Engineering Information Technology*, Vol.8-no.3, 2018.

[24] K. Ade and R. Imam, “Detection and Analysis Cerber Ransomware Based on Network Forensics Behavior”, *International Journal of Network Security, Vol.20, No.5, PP.836-843*, 2017.

Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) Device

ORIGINALITY REPORT

9%

SIMILARITY INDEX

PRIMARY SOURCES

1	"Bibliography", Elsevier BV, 2016 Crossref	38 words — 1%
2	Ana Nieto, Ruben Rios, Javier Lopez. "Digital Witness and Privacy in IoT: Anonymous Witnessing Approach", 2017 IEEE Trustcom/BigDataSE/ICESS, 2017 Crossref	34 words — 1%
3	pdfs.semanticscholar.org Internet	32 words — 1%
4	orbilu.uni.lu Internet	30 words — 1%
5	Lecture Notes of the Institute for Computer Sciences Social Informatics and Telecommunications Engineering, 2015. Crossref	24 words — < 1%
6	hal.archives-ouvertes.fr Internet	24 words — < 1%
7	Noman Shahid, Sandhya Aneja. "Internet of Things: Vision, application areas and research challenges", 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017 Crossref	23 words — < 1%
8	idcbenelux.com Internet	23 words — < 1%

9	www.tandfonline.com Internet	22 words — < 1%
10	Faheem Zafar, Abid Khan, Saba Suhail, Idrees Ahmed, Khizar Hameed, Hayat Mohammad Khan, Farhana Jabeen, Adeel Anjum. "Trustworthy data: A survey, taxonomy and future trends of secure provenance schemes", Journal of Network and Computer Applications, 2017 Crossref	22 words — < 1%
11	Konstantinos Kotis, Iraklis Athanasakis, George A. Vouros. "Semantically enabling IoT trust to ensure and secure deployment of IoT entities", International Journal of Internet of Things and Cyber-Assurance, 2018 Crossref	21 words — < 1%
12	insightsociety.org Internet	20 words — < 1%
13	www.thieme-connect.com Internet	15 words — < 1%
14	researchprofiles.canberra.edu.au Internet	15 words — < 1%
15	Dimuthu U. Gamage, Lahiru S. Gallege, Rajeev R. Raje. "A QoS and Trust Prediction Framework for Context-Aware Composed Distributed Systems", 2015 IEEE International Conference on Web Services, 2015 Crossref	14 words — < 1%
16	www.erawa.com.au Internet	12 words — < 1%
17	Ahmad W. Atamli, Andrew Martin. "Threat-Based Security Analysis for the Internet of Things", 2014 International Workshop on Secure Internet of Things, 2014 Crossref	11 words — < 1%
18	journal.portalgaruda.org Internet	10 words — < 1%

19	xxx.unizar.es Internet	10 words — < 1%
20	www.ripublication.com Internet	10 words — < 1%
21	www.ukessays.com Internet	10 words — < 1%
22	www.iscturkey.org Internet	8 words — < 1%
23	www.ashfords.co.uk Internet	8 words — < 1%
24	Lecture Notes in Computer Science, 2015. Crossref	7 words — < 1%
25	Quang Do, Ben Martini, Kim-Kwang Raymond Choo. "Cyber-physical systems information gathering: A smart home case study", Computer Networks, 2018 Crossref	7 words — < 1%
26	"Guide to Security Assurance for Cloud Computing", Springer Nature America, Inc, 2015 Crossref	6 words — < 1%
27	Intae Hwang, Young-Gab Kim. "Analysis of Security Standardization for the Internet of Things", 2017 International Conference on Platform Technology and Service (PlatCon), 2017 Crossref	6 words — < 1%

EXCLUDE QUOTES	OFF	EXCLUDE MATCHES	OFF
EXCLUDE BIBLIOGRAPHY	OFF		