

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

Randi Rizal¹, Imam Riadi² and Yudi Prayudi³

^[1,3] Department of Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia

² Department of Information System, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
randirizal@gmail.com¹, imam.riadi@is.uad.ac.id², prayudi@uii.ac.id³

ABSTRACT

Today is the era of the Internet of Things (IoT), millions of machines or devices such as smart city, smoke detectors, watches, automatic car tracking, smartphone detection, smart lighting, temperature monitoring etc. are being connected to the Internet. In the internet of things, there are various devices which are interconnected to the other devices which share different techniques and the different standards. The rise of new technology in various fields it also makes rise to the new challenges in the area of the forensic investigation. As there will be many new challenges to the forensic investigators. The recent tools and the process flow carried out will not meet the highly distributed and current infrastructure of the IoT. A 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 detection 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 progress of the internet and the innovative evolution of the smart devices leads to the development of the new computing prototype – The Internet of Things (IoT). IoT is considered the future estimation of the internet which works on the Machine-to-Machine (M2M) communication and the Radio Frequency Identification (RFID) [1]. The main goal of the IoT is to allow the secure exchange of the data 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 include 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. Lot of devices are getting connected to the internet to share the local information to the cyberspace. The US National Intelligence Council (NIC) estimates that by 2025 Internet nodes may reside in most of our surrounding things food packages, furniture, paper documents, and many more [3]. According to a report by Gartner, there will be 26 billion IoT devices in next five years [4]. International Data Corporation (IDC) forecasts that the IoT market will reach \$3.04 trillion and there will be 35 billion connected things in 2020 [5]. These things can be varied in different attributes: processing and computation power, communication medium, dimension, etc. [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]. To investigate such attacks we need to apply the aspects of the digital forensics in the IoT parameter which is called as IoT Forensics [1].

As the Digital Forensics in the IoT device is very challenging and diverse, the traditional model of the forensics does not fit with the recent IoT Environment. The large number of the devices will also bring new challenges for the data management. The large number 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 branch of science which encompasses the recovery and investigation of material which is found in

digital devices, often related to computer crime. In the digital forensics we will first be incorporating 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 easily to is lost. Network Forensics has two functions, the first relating to security, including 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, law enforcement-related, in this case, analysis on the capture of network traffic may include sending a file, searching for keywords, and breakdown in communications made as in email and chat.

2.2 Network Forensics Process Model

In the paper “A Generic Framework for Network Forensics” the author proposed a model of the network forensics investigation. This proposed model consists of many different phases of network forensics investigation. The figure 1 shows the model of network forensics which has nine phases illustrated [9].

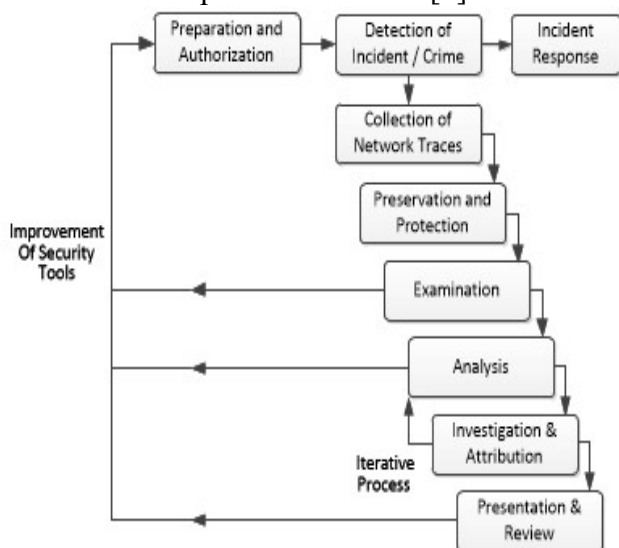


Figure 1. Generic Framework for Network Forensics

- **Preparation Phase** : The main objective is to obtain required authorization and legal warrants.

- **Detection Phase** : Generate a warning or an alert which indicate security violation.
- **Incident Response Phase** : Applicable only when investigation is initiated during the attack.
- **Collection Phase** : The most difficult part because the data flows rapidly and is no possible to generate later traces of the same thing.
- **Preservation Phase** : Original Evidence is kept safe along with computed hashes.
- **Examination Phase** : Examines the previous phase. All hidden or altered data is to be uncovered which is done by the attacker.
- **Analysis Phase** : Collected evidence is analysed to find the source of intrusion.
- **Investigation Phase** : Use information gathered in the analysis phase and focus on finding the attacker.
- **Presentation** : 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 the Figure 2[1].

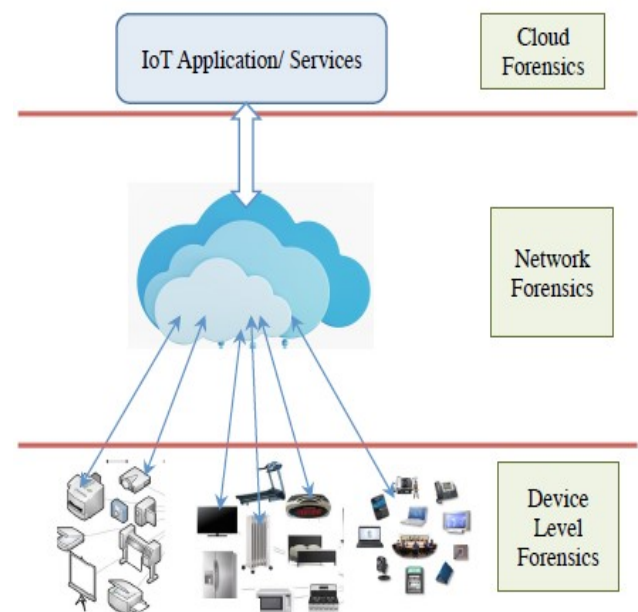


Figure 2. IoT Forensics

- **Device level Forensics** : An investigator may need to collect data from the local memory of the IoT devices. When a crucial piece of evidence needs to be collected from the IoT devices, it involves the device level forensics.
- **Network level Forensics** : The source of different attacks can be identified from network logs. Therefore, network logs can be very crucial to condemn or exonerate a suspect. IoT infrastructures includes different forms of networks, such as Body Area Network (BAN), Personal Area Network (PAN), Home/Hospital Area Networks (HAN), Local Area Networks (LAN) and Wide Area Networks (WAN). Important piece of evidence can be collected from any of these networks.
- **Cloud level Forensics** : One of the most important roles in the IoT forensics domain will be the cloud forensics. Since most of the IoT devices have low storage and computational capability, data generated from the IoT devices and IoT networks are stored and processed in the cloud. This is because cloud solutions offer various benefits including convenience, large capacity, scalability, and on-demand accessibility.

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	RFID, 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 traditional tools and technologies are not designed completely to carry out forensic in the IoT environment as it faces many challenges [11]. In this section we will identify the challenges we are facing for the forensic investigation in 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 wide variety of data generated by the IoT devices makes the collection and analysis phase challenging. The proper logs need to be organized in order to avoid the complication of the data and files.

d. Preservation of Evidence

The final step of the forensic investigation is that the forensic examiner presents the gathered information and the evidence in front of the court of law. As in comparison traditional forensic evidence presentation is easy than the forensic of the IoT Environment as it is challenging task as the jury members don't have enough knowledge as compared to the technical person. They also feel complex to understand.

2.3. Attacks in IoT

The domain of security Attacks on IoT device is increasing day by day. Following figure 2 summarizes the attacks on IoT Systems[12].

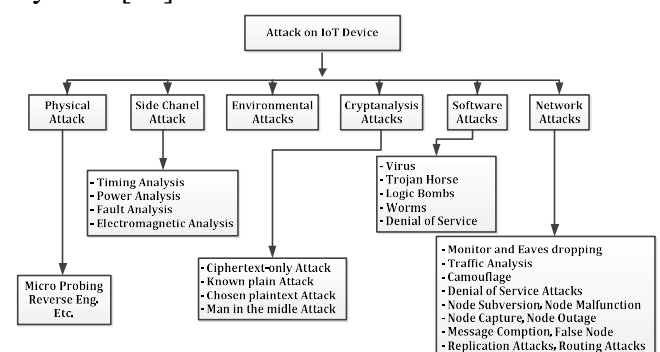


Figure 3. Attacks on IoT Device

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

1) Node Tampering / Node Compromised

An adversary can modify the device and insert a deceiver to the system .Therefore, the device will not function as it is supposed to be work on. This kind of attack usually use to steal information and misuse the software and the hardware of IoT devices.

2) Denial of Service (DoS)

DoS can be performed by misusing the device, manipulating its software and application, or disrupting the communication channel [13]. One of the DoS attack is the jamming attack where the adversary are able to deactivate the sensor communication channel from carrying signals by generating collisions. The collisions will caused the communication message interrupted.

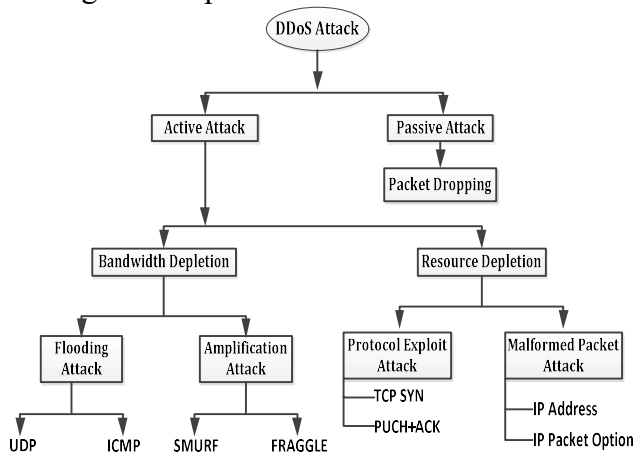


Figure 4. DDoS Attacks

3) Distributed DoS

Take a look at Mirai attack. The Mirai malware is designed to exploit an existing vulnerability within IoT devices for DDoS attacks .There are millions of IoT devices on the market that are misconfigured and set to forward messages via the Transmission Control Protocol (TCP)[17]s.

4) Spoofing

Adversary uses the credential information which belongs to others to get access to the unapproachable service. This credentials can be discovered from the device itself, eavesdropping on the communication channel, or from the reconnaissance activities.

5) The Breach of Privacy

The adversary can gather private data from different sources, for example, meta-information and activity investigation.

6) Buffer Overflow

Using this kind of attack, a buffer overflow lets an adversary to control or crash the processor to alter its core variables. If the program is sufficiently privileged, therefore the adversary can control the host.

7) SQL Injection

A malicious code injection method used to attack the information-driven applications, manipulating a security weakness in an application's software, permit the adversary to spoof identity, modify data which may cause the repudiation issues.

Another case study of attacks is on the glucose monitoring system for diabetic patients. As reported in October 2016, Johnson & Johnson subsidiary 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 major security flaws 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 trivially sniff the remote/pump key and then spoof being the remote or the pump. Another vulnerability is the communication channel where it is taking place between the pump and meter has no timestamps or sequence numbers and because of this, no defence against replay attacks [18].

2.4. Arduino UNO

The Arduino UNO is a little, cheapish device that allows you to easily connect some electronic thing you have made to your computer and to the internet. And it brings all sorts of madcap invention to the Internet Of Things (IoT). Arduino is an open source computer hardware and software company, project, and user community that designs and manufactures single-board microcontrollers and microcontroller kits for building digital devices and interactive objects that can sense and control objects in the physical and digital world.

Arduino board designs use a variety of microprocessors and controllers. The boards are equipped with sets of digital and analog input/output (I/O) pins that may be interfaced to various expansion boards or Breadboards (*shields*) and other circuits. The boards feature serial communications interfaces, including Universal Serial Bus (USB) on some models, which are also used for loading 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.

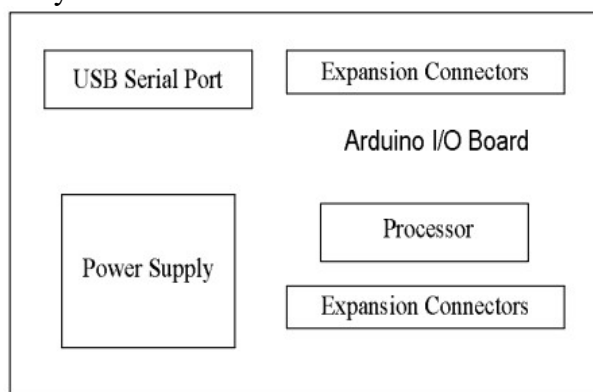


Figure 5. Block Diagram of Arduino Board

2.5 Bluetooth HC05

A typical Internet of Things (IoT) architecture consists of hardware, communication, software system and application layers, with Bluetooth acting as the communication layer. The communication layer is a critical bridge between the layers and consists of a multi-layer stack, including data link, network or transport, and session protocols. Bluetooth or BLE is part of the data link layer, which connects either sensor to sensor or sensor to the gateway. The network layer, on the other hand, is responsible for routing or moving packets across the network, using the most appropriate paths. The session layer protocols enable messaging across 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 [20] :

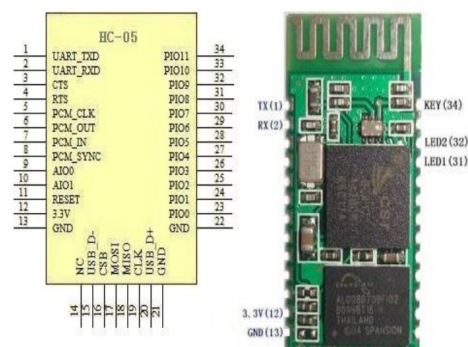


Figure 6. The physical shape of bluetooth HC 05

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 :

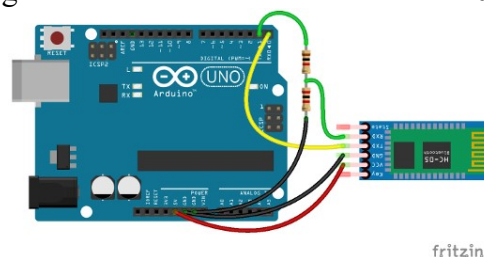


Figure 7. Bluetooth Arduino Configuration Scheme with fritzing

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 Bluetooth 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 conducted to implement network forensics on the Internet of Things (IoT) device. The system simulation aims 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 :

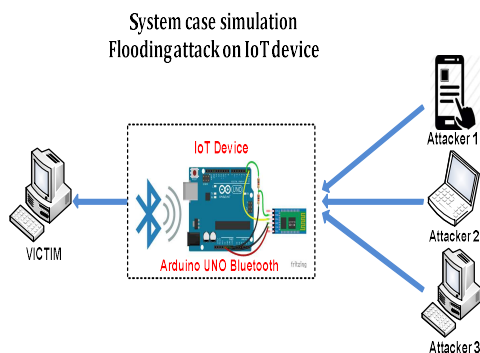


Figure 8. Simulation Flooding Attack

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.

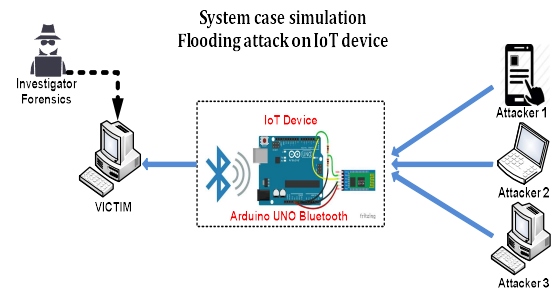


Figure 9. Network Forensic Architecture on IoT Devices

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.

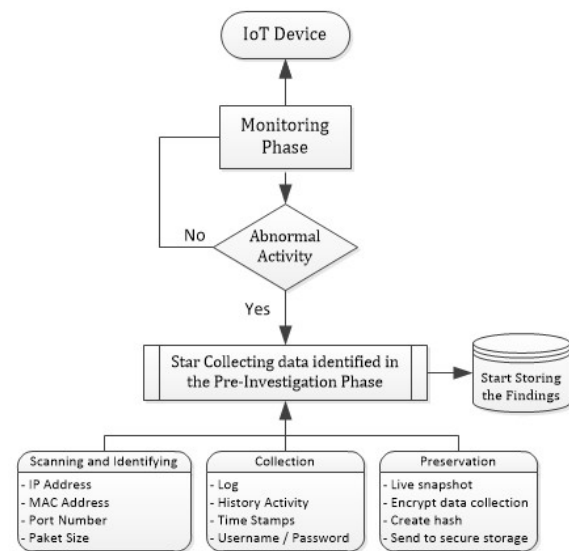


Figure 10. IoT Device Forensics

B. Model Process Forensic

Level Forensic Device on device inspection, network forensics to analyze and record traffic. The number of IoT devices will produce very large data. Here we will do the amount of data network. Because the amount of data evidence will be very large and it will be very difficult to analyze the data and it is difficult to identify evidence that can be used to identify forensics to

find flooding and monitoring attacks so as to identify the source of the attack that the device is infected. The results of this analysis have nine stages Model Process Forensic :

■ Preparation and Authorization

At this stage, network forensics is applicable only to environments where network security tools like packet analyzers, traffic flow measurement software are deployed at various strategic points on the network for detecting flooding attack on IoT device. The staff handling these tools must be trained to ensure 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 obtained and a well defined security policy is in place so that privacy of individuals and the organization is not violated.

■ Detection of Incident / Crime

The alerts generated by various security tools, indicating a security breach or policy violation, are observed. Any unauthorized events and abnormal activity noticed will be analyzed. The confirmation of an incident yields two directions – incident response and collection of data.

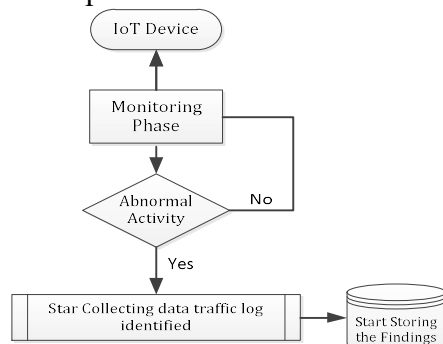


Figure 11. Detection of Findings Log

■ Incident Response

The response to the crime or intrusion detected is initiated based on the information gathered to validate and assess the incident. The response initiated depends on the type of attack identified and is guided by organization policy, legal and business. This phase is applicable only to cases where an investigation is initiated 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.

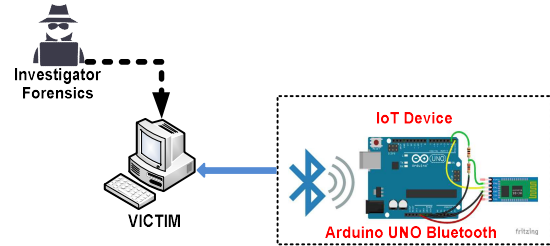


Figure 12. Data Collection Stage

■ Protection and Preservation

The original data obtained in the form of traces and logs is stored on a back up device. A hash of all the trace data is taken and the data is protected. Chain of custody is strictly enforced so that there is no unauthorized use or tampering. Another copy of the data will be used for analysis and the original collected network traffic is preserved. In this stage will use the FTK Imager application for made a hash of data.

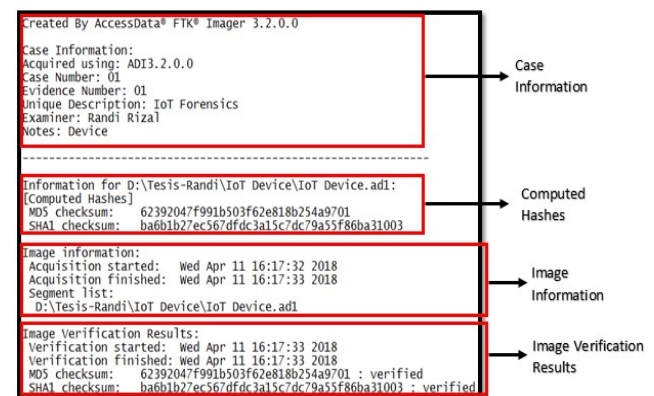


Figure 13. Hash Evidence of Log Traffic

■ 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.

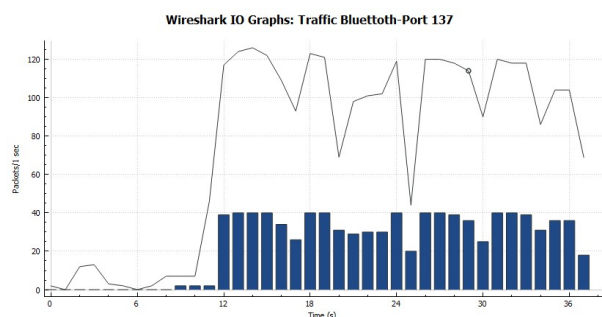


Figure 14 : IO Graph Traffic Log

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.

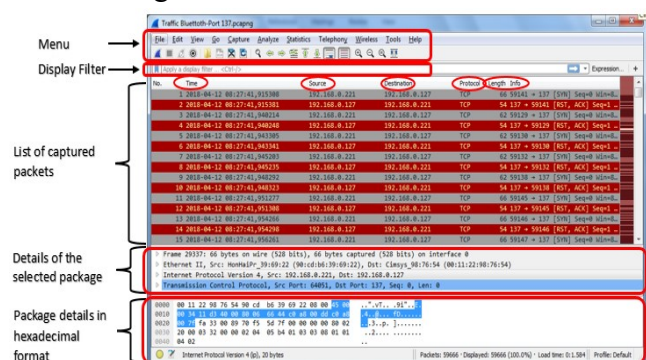


Figure 15 : Traffic Log in Wireshark

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.

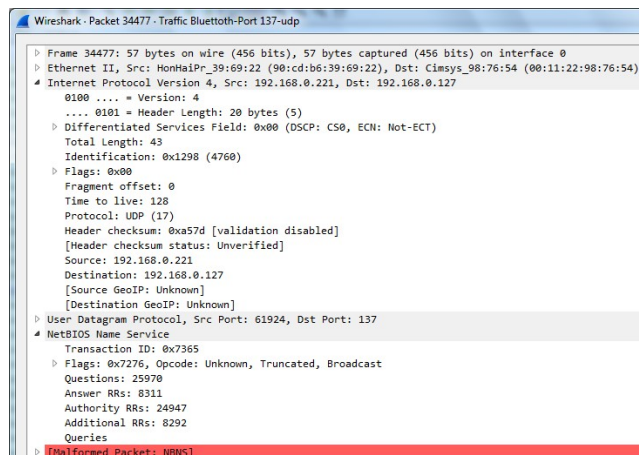


Figure 16 : UDP Follow

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.

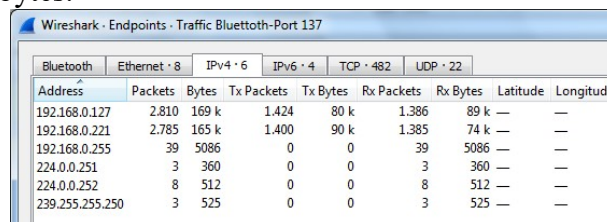


Figure 17 :Statistic Endpoint

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	796f75207761732061747461636b6564206279206d65...
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	552064756e206768666564...

Table 2. File Log Bluetooth Traffic

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, 2013.
- [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?containerId=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: Exhibition & 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] Walsh Ray, 2016. IoT Botnet Launching Massive DDoS Attacks on Websites - BestVPN.com. Available at: <https://www.bestvpn.com/iot-botnet-mirai-ddos/>[Accessed December 14, 2016].
- [18] Charlie Osborne, 2016. Insulin pump vulnerabilities could lead to overdose | ZDNet. Available at : <http://www.zdnet.com/article/insulin-pumpvulnerabilities-could-lead-to-overdose/> [Accessed December 14, 2016].
- [19] 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.
- [20] www.electronicwings.com/sensorsmodules/bluetooth-module-hc-05- [Accessed May 2017].
- [21] Iswardani, A. and Riadi, I. "Denial Of Service Log Analysis Using Density K-Means Method," vol. 83, no. 2, pp. 299–302, 2016.
- [22] 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.
- [23] Bandyopadhyay, Debasis, and Jaydip Sen. "Internet of things: Applications and challenges in technology and standardization." *Wireless Personal Communications* 58.1 (2011): 49-69.
- [24] 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.