IoT Botnet Detection Mechanism Based on UDP Protocol

Myint Soe Khaing
Faculty of Computer Science
University of Computer Studies,Yangon
Yangon, Myanmar
myintsoekhaing@ucsy.edu.mm

Yee Mon Thant
Faculty of Computer Science
University of Computer Studies,Yangon
Yangon, Myanmar
yeemonthant@ucsy.edu.mm

Thazin Tun
Faculty of Computer Science
University of Computer Studies,Yangon
Yangon, Myanmar
thazintun@ucsy.edu.mm

Chaw Su Htwe
Faculty of Computer Science
University of Computer Studies,Yangon
Yangon, Myanmar
chawsuhtwe@ucsy.edu.mm

Mie Mie Su Thwin
Cyber Security Lab
University of Computer Studies,Yangon
Yangon, Myanmar
drmiemiesuthwin@ucsy.edu.mm

Abstract

Today is the time of the Internet of Things (IoT), a great many devices, for example, smart homes, smart retail, smart phone identification, smart lighting, and so forth are being associated with the Internet. There are different devices that are interconnected to a different device on the Internet of things that offer various procedures and forms. The Forensic specialist will have many difficulties to look into gathering the bit of proof from the tainted segment on the IoT devices and furthermore will confront complexities to break down those proof. This paper introduces a UDP flood attack begins by sending countless UDP packet from various IP addresses. The graphical proof is likewise displayed for the DDOS attack utilizing UDP packet flooding. We will do the network forensics investigation for flooding attacks on IoT environments Using Wireshark

Keywords: *Internet of Things, IoT Forensics, Botnet, DoS, DDoS*

I. Introduction

The Internet-of-Things (IoT) is developing quickly, making openings and difficulties for investigators of a crime, including cyberattacks and physical ambushes (Kebande, 2017, Akatyev and James, 2017). By definition and configuration, keen homes and other IoT situations are associated, dynamic, and can be changed from anyplace whenever (Minerva, 2015; Loung, 2018; Barnard-Wills, 2014). Numerous IoT gadgets have sensors or actuators that produce information, now and again independently and at times in light of human activities (movement discovery, entryway opening). This constantly dynamic, continually producing makes them astounding computerized observers, catching hints of exercises of potential use in examinations. IoT gadgets can be significant wellsprings of proof gave computerized investigators can deal with the amount of information created, the number and assortment of gadgets, the heterogeneity of conventions utilized, and their dispersed nature [1]. A DDoS Attack is one of the most well-known and significant risks to the Internet in which the objective of the attacker is to devour PC assets of the person in question, generally by utilizing numerous PCs to send a high volume of apparently authentic traffic mentioning a few administrations from the person in question. Accordingly, it makes arrange blockage on the target, along these lines disturbing its typical Internet activity.

The transport layer gives a mechanism to the trading of information between end frameworks. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are two primary transport protocols that give connection-oriented and connectionless administrations individually. TCP guarantees dependable and requested information conveyance while additionally presenting handling overhead and bandwidth constraints because of congestion and flow control mechanisms. The lightweight UDP neither gives solid conveyance nor experiences preparing overhead and bandwidth confinements and subsequently is utilized in time-sensitive applications on the grounds that dropping packets is desirable over hanging tight for postponed packets, which may not be an alternative in a constant framework like Voice over IP (VoIP), IPTV, video on demand and web-based gaming [2]. Specifically, a UDP flood attack happens when an attacker creates various bundles to arbitrary goal ports on the unfortunate victim’s computer. The unfortunate victim system, on receipt of the UDP packet demands, would react with proper ICMP bundles, if the port is shut. An enormous number of packet reactions would hinder the framework or crash.

II. Related Work

Ryba in [3] in detail depicted the state of the art of research suggestion for counteracting, distinguishing, and the following upgrade and dispersed reflected renouncing of organization assaults similarly as investigated boundary frameworks against the source an IP address spoof, which is major for the increase and the DRDoS assaults.

It is also imperative to suggest the paper of Bekeneva in [4], where the tests DRDoS assaults and security frameworks against them are presented.

IoT devices and DRDoS assaults. A couple of investigators have inspected the DRDoS assault, in any case, only two or three they have focused on IoT devices. Generally, the investigators endeavored to portray the condition around Mirai botnet and to set up a specific proposition for the endorsed methodology or for lively security models for IoT contraptions, and wholesalers [5, 6].

Correspondingly, as in the past subject, there is moreover a push to find numerical or amusement models for DRDoS assault reliant on IoT contraptions and their consequences for sorting out security, for instance [7].

III. Internet of Things (IoT)

The Internet of Things (IoT) depicts the arrangement of physical items—"things"— that is introduced with sensors, software, and various advancements to partner and exchanging data with various gadgets and frameworks over the internet. These gadgets go from customary nuclear family articles to complex mechanical contraptions. With more than 7 billion related IoT gadgets today, masters are envisioning that this number ought to create to 10 billion by 2020 and 22 billion by 2025 [8]. In the course of recent years, IoT has gotten one of the most significant advances of the 21st century. Since we can interface ordinary objects—kitchen apparatuses, vehicles, indoor regulators, child screens—to the internet by means of embended devices, consistent correspondence is conceivable between individuals, procedures, and things.

While the possibility of IoT has been in presence for quite a while, an assortment of ongoing advances in various advances has made it down to earth.

- Access to minimal effort, low-control sensor
  innovation.
- Connectivity.
- Cloud figuring stages
- Machine learning and investigation.
- Conversational computerized reasoning.

Industrial IoT (IIoT) alludes to the usage of IoT development in industrial settings, especially for instrumentation and control of sensors and gadgets that interface with cloud advances. Starting late, businesses have used machine-to-machine correspondence (M2M) to achieve remote automation and control. In any case, with the improvement of cloud and joined progressions, (for instance, examination and AI), adventures can achieve another computerization layer and it makes new salaries and strategies. IIoT is now and again called the fourth influx of the industrial unrest, or Industry 4.0. Coming up next are some essential uses for IIoT are Smart, assembling, Preventive and prescient support, Smart power networks, Smart urban networks, Connected and shrewd collaborations and Smart mechanized inventory chains.

A. IoT Lifecycle

An IoT system is involved in associated devices that are much of the time sending information about their status and condition around them.

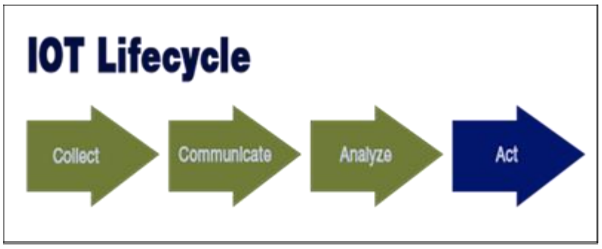


Figure 1. IoT Lifecycle

Collect: The existence cycle of IoT begins with gathering information from various sources conveyed in a specific district. These sources could be any sensors or devices equipped for transmitting information associated with a portal. Information is productively gathered and gone ahead through a correspondence channel for investigation.

Communicate: This stage includes the protected and solid exchange of information. Switches, switches and firewall advancements assume a crucial job in setting up the correspondence between devices. The Information is sent to the cloud or other server farms utilizing the internet which is our significant methods for correspondence in IoT.

Analysis: This stage is a significant piece of the IoT lifecycle. In this stage information gathered from the various sensors, devices are gathered and examined dependent on the utilization case to separate some valuable yield/data.

Action: This is the last phase of the IoT lifecycle. Data got by the investigation of sensor information is followed up on and appropriate moves and measures are made dependent on the examination result [9].

B. IoT Forensics

IoT devices have limitations in battery, calculation, memory, and radio data transfer capacity. Along these lines, applying security arrangements that for the most part requires overwhelming correspondence burden and more calculation assets, are difficult. Validation, get to control and malware recognition of helpless IoT devices should be considered. The IoT including devices, service, and networks are defenseless against various attacks, for example, physical, software, DoS, DDoS, sticking, spoofing, man-in-the-center and protection spillage. Most IoT security dangers originate from uncertain IoT devices, the attacker focus to exhaust the compromised IoT devices asset particularly network traffic. Network forensics includes catching account and breaking down of network traffic. Serves to gather data, proof assembling and identify attacks. The procedure of examination happened in the network with dealing with the traffic and action. Not quite the same as the other technique, the network forensics-identified with dynamic data that effect is lost.

C. Forensic Investigation in IoT Environment

The Internet of Things (IoT) represents various novel and convoluted difficulties in the field of advanced crime scene investigation. Assessments express that the quantity of arranged devices will remain at 50 billion by 2020, and said devices will create a significant measure of information (Botta , 2014). The handling of gigantic measures of IoT information will prompt a proportionate ascent in the remaining tasks at hand borne by server farms; this will, thus, imply that suppliers are left to manage new provokes identified with limit, security, and investigation.

Guaranteeing that said information is dealt with advantageously comprises a significant test, since the application execution, in general, depends intensely on the information the board administrator's properties (MacDermott, 2018). It is felt that IoT criminology comprises of a blend of three advanced legal sciences plans: cloud level forensics, device-level forensics, and system level forensics (Zawoad and Hasan, 2015) as appeared in figure 2.

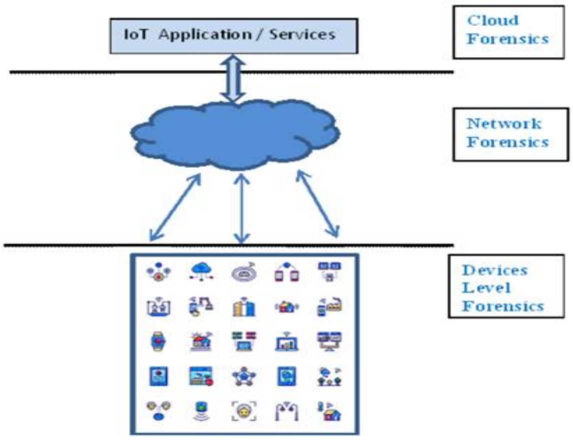


Figure 2. IoT Forensics

Device-level forensics: At this level, a criminological agent needs to gather information first from the nearby memory contained in the IoT device to be dissected. It is important to utilize the IoT device that is missed in breaking down information on the criminological level device.

Network-level forensics: To recognize different sources of attacks can be distinguished from network traffic logs. Hence, the log traffic network can be critical to deciding the blame or opportunity of the suspect. IoT infrastructure incorporates different types of networks, for example, Body Area Networks (BAN), Personal Area Networks (PAN), Home /Hospital Area Networks (HAN), Local Area Networks (LAN) and Wide Area Networks (WAN). Significant proof acquired is gathered from one of these networks with the goal that network forensics.

Cloud level forensics: Cloud forensics is one of the most significant pieces of the IoT scientific space. Why? Because of the way that most existing IoT devices have a low stockpiling and registering limit, information created from IoT devices and IoT networks are put away and handled in the cloud. This is on the grounds that cloud solvents offer an assortment of points of interest including comfort, enormous limit, adaptability, and availability on demand [1].

IV. BOTNET

In this segment, data identified with Botnets, Botnet Environment, architecture, and activities are given.

A. Botnet Environment

Botnets have had a rich history and movement reliably, defiling and upsetting PC and framework structures. From the outset, botnets were made for caring purposes, with their basic limit being to give credible help to Internet Relay Chats (IRC), a kind of correspondence acclaimed during the '90s. The first IRC bot appeared in 1993, was named Eggdrop and offered help to IRC bot appeared in 1993, was named Eggdrop and offered help to IRC channel correspondence. Following Egg drop, the first perilous bots appeared, with GTbot in 1998 being the first of its sort, which had the choice to execute substance when influenced through its Command and Control (C&C) IRC channel. For example, different bots. It was brought down in December 2009. Another obvious achievement for botnets in 2009 was the proximity of the ancestor of preservationist botnets, where botnets use telephones as their bots (zombies), named SymbOS \ Y xes which centered Symbian contraptions and utilized SMS messages to self-duplicate. Following the surfacing of SymbOS, the first botnet concentrating on Android contraptions named Geinimi was seen, during the completion of 2010. Basically found in China, it utilized a brief HTTP-based C&C structure and was set prepared for sending SMS, messages, bring the zone of the undermined contraption and also made conceivable the further spread of malware.

Generally, botnet makers have manhandled the wide confirmation and strong widening of the IoT, and we need to begin at now scene instances of IoT botnets and what they are set up to do. Botnets included IoT contraptions were the going with the formative improvement of botnets. The most outstanding first appeared in September 2016, under was related as Mirai. Mirai played out probably the most overwhelming DDoS attacks in Internet History, explicitly: 620 Gbps against Brian Kreb's site page, 1.1 Tbps against French Cloud authority affiliation OVH and in October 2016 ambushed Dyn ace concentration and separate down bits of the web like Twitter, Netflix and GitHub. After the nearness of Mirai's source code, different assortments showed up Persirai which is dynamic since, After the nearness of Mirai's source code, different assortments showed up Persirai which is dynamic since April 2017, a more refined understanding of Mirai which targets specific devices of select sellers. Other IoT botnets unite Hajime, which appeared in October 2016, and utilized a decentralized C&C framework that appeared to 'shield' contraptions from Mirai ailments. At long last, BrickerBot was found in April 2017, and as the name proposes attempted to 'square' IoT contraptions in what can be viewed as a permeant DoS assault [10].

B. Botnet Architectures and Characteristics

Botnet models join a few sections. Notwithstanding, a bot is a program that, in the wake of landing at a vulnerable host, sullies it and makes it a pinch of the Botnet. Bots change from other malware, in that they join a channel of correspondence with their makers, empowering them to offer commands to their arrangement of bots (i.e., zombies) and thusly making botnets flexible concerning their handiness. A botnet's malware gets given to frail fixations through what is known as a spread instrument. Most usually there exist two sorts of development, saved and dynamic. Torpid growth strategies predict that clients should locate a functional pace, or other exchanged off-sort out portions and through client affiliation download the malware (bot), dirtying it and making it part of the botnet. Dynamic or self-development methodologies use sub-segments of their framework to effectively check the Internet for uncovered devices, endeavoring to mishandle the identified vulnerabilities, changing the undermined hosts into bots themselves.

The trademark that makes botnets fascinating is where that they permit their controller, by and large, suggested as a botmaster to offer orientation to their arrangement of spoiled devices and get a responsibility, as appeared in Figure 3.This is made conceivable through a Command and Control (C&C) structure. There exist different sorts of C&C frameworks subject to their topology and those sorts are: bound together, P2P, dynamic and crossbreed. In a consolidated topology, bots accomplice, get rules and report/pass on their work in the focal establishment, with most essential developments used here being IRC and HTTP shows. The basic weight of the bound together topology is that the C&C is a singular inspiration driving disillusionment.

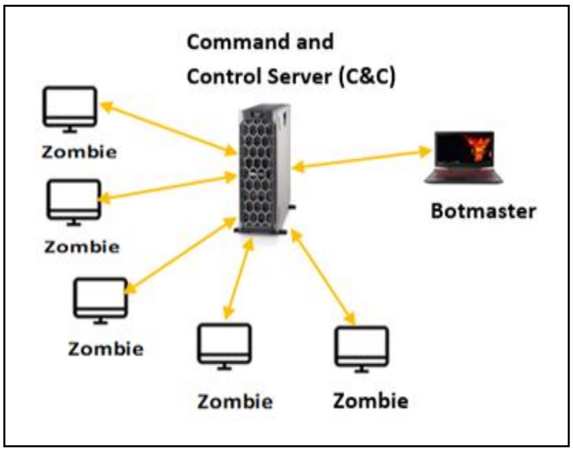


Figure 3. Centralized Botnet and activities

Finally, right now, botmaster fuses center individual bots between their machine and the botnet, with each bot sending commands to the bots that they wrangled, making an other leveled topology and making takedown endeavors difficult, correspondingly as allowing the botmaster to rent bits of their botnet [10].

C. Botnet Activities

Botnets are clearly the most versatile bits of code to explore the Internet. The standard inspiration driving why they get so a great deal of thought isn't an inevitable result of the wonderful ways that botmasters use to scatter their bots from law basic, yet rather the pleasing farthest arrives at that botnets have and the affiliations they oblige the botmasters and their clients. There are varying hacking frameworks used by botnets, including Distributed Denial of Service ambushes (DDoS), Keylogging, Phishing, Spamming, Snap mutilation, Click duplicity and even the enlargement of other Bot malware [10].

V. WHAT IS DDOS ATTACK?

A Denial of Service (DoS) attack is an endeavor by an attacker to make organize assets inert to its real clients by flooding the service's host. Distributed Denial of Service (DDoS) attack is a DoS attack that is begun from various sources. By and large, DoS attack is started from one gadget or virtual machine utilizing Internet association while DDoS attacks are started from a wide range of compromised devices, virtual machines to over-burden the victim frameworks. DDoS is performed by sending an extensive number of solicitations all the while through botnets and compromised IoT devices to exhaust registering assets (Bandwidth and Traffic) of the objective. The compromised devices which are likewise called bot or Zombie works under the supervision of one or huge numbers of the bot-masters and attack controls gatherings of bots (botnet) remotely as in Figure 4. Bots can be either malicious clients whose expectation is an attack or authentic clients who are contaminated.

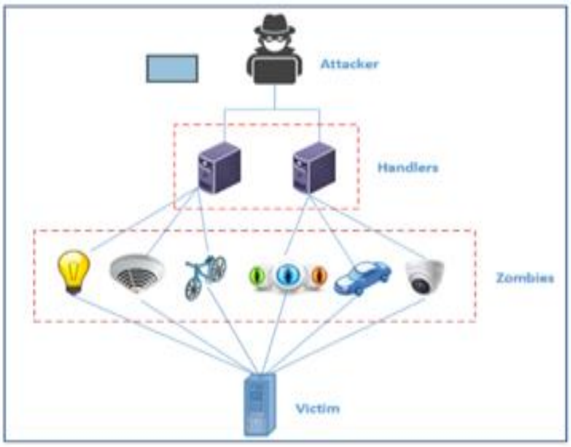


Figure 4. DDoS attack network infrastructure.

A. Direct and Indirect DDoS attack

The DDoS attack can be launched in two different ways either legitimately or with a reflector as in Figure 5. In the immediate system attack, the attackers legitimately send the packets to the objective victim machine. Notwithstanding, an aberrant attack which is likewise called enhancement or reflection attack the attacker utilizes a reflector server and the attacker spoofs the source IP. The attacker sends the IP packet to the reflector server, and afterward, the reflector server sends the reaction to the objective. In the immediate attack, the victim gets the packet with a similar payload as sent by the attacker while in a circuitous attack the reflection server enhances the solicitation it gets from the attacker and sends the reaction to the victim.

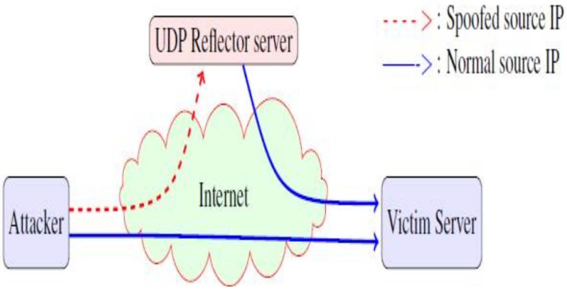


Figure 5. Direct and Indirect Attack

Begin to frame a DDoS attack, at first, attackers recognize vulnerabilities of one or various gatherings of IoT devices to introduce malicious software on them. At the point when malicious software is introduced on the devices, they are called zombies. At that point, the attacker's structure an enormous gathering of zombies geologically distributed which are known as botnet. Each gathering of zombies has a handler which is a software bundle set over the Internet. The handlers are legitimately speaking with attackers and zombies since they have data about the dynamic zombies. While propelling an attack, attackers send the attack to the zombie handlers who will disseminate the attack to all zombies. At that point, zombies will attack the objective framework. DDoS attacks which are created by spoof IP is trying to deal with and channel [11].

B. IP Address spoofing in DDoS attacks

IP address spoofing is utilized for two reasons in DDoS attacks: to Masking botnet devices zones and to arrange a Reflected DDoS.

Masking botnet devices: A botnet is a social event of malware-contaminated gadgets remotely constrained by blameworthy gatherings without the data on their proprietors. They can be encouraged to everything looked at entryways as a given district or server, equipping liable gatherings with the arrangement and frameworks organization preferences for delivering colossal traffic floods. Such floods connect with botnet managers, (a.k.a. shepherds), to help their objective's preferred position limit, accomplishing server singular time and framework immersion. Botnets are generally included either discretionary, topographically dispersed gadgets or PCs having a spot with a similar exchanged off framework (e.g., hacked encouraging stage). By utilizing derided IP passes on to shroud the genuine characters of their botnet gadgets, blameworthy gatherings plan to: Avoid revelation and suggestion by law need and legal automated bosses. Keep bases on lighting up contraption proprietors about an assault in which they are accidentally taking an interest. Avoid security substances, gadgets, and organizations that endeavor to moderate DDoS attacks through the boycotting of assaulting IP addresses.

Reflected DDoS: A reflected DDoS attack uses IP parodying to make fake sales, clearly to support a goal, to move responses from under-verified center individual servers. The's guilty party will presumably improve its traffic yield by enacting huge responses from a ton of more diminutive sales. Fundamental reflected DDoS attack systems include:

- *DNS amplification* – An ANY request beginning from an objective's satirize address is sent to various unbound DNS resolvers. Every 60-bytes deals can incite a 4000-bytes reaction, drawing in assailants to increase traffic yield by as much as 1:70.
- *Smurf attack* – An ICMP Echo request is sent from a goal's satirize address to a widely appealing convey arrange, actuating answers from every device on that system. The degree of amplification relies upon the number of devices to which the sales are imparted. For example, a system with 50 related hosts realizes a 1:50 amplification.
- *NTP amplification* – A get monist request, containing a goal's parodied IP address, is sent to an unbound NTP server. As in DNS amplification, a little sales trigger much greater response, allowing the best amplification extent of 1:200. for how the ridiculed IP is delivered in DDoS attack[11].

VI. WHAT IS A UDP FLOOD ATTACK?

UDP flood is a kind of Denial of Service (DoS) attack in which the assailant overwhelms random ports on the concentrated on the host with IP parcels containing UDP datagrams. The getting host checks for applications identified with these datagrams and—finding none—sends back a "Goal Unreachable" bundle. As progressively more UDP bundles are gotten and answered, the system gets overwhelms and dormant to various clients. Some working framework avoids the UDP flood by constraining the amount of ICMP response [12].

A. UDP Flood DDoS Attack Scenarios

In this scenario uses to perform forensic testing of the IoT device in recognizing flooding attacks using Wireshark. The chose dataset is "IoT_Dataset_UDP_DDoS__00001_20180604180103" in Bot-IoT Dataset was utilized for network forensic in UDP DDoS flooding attack.

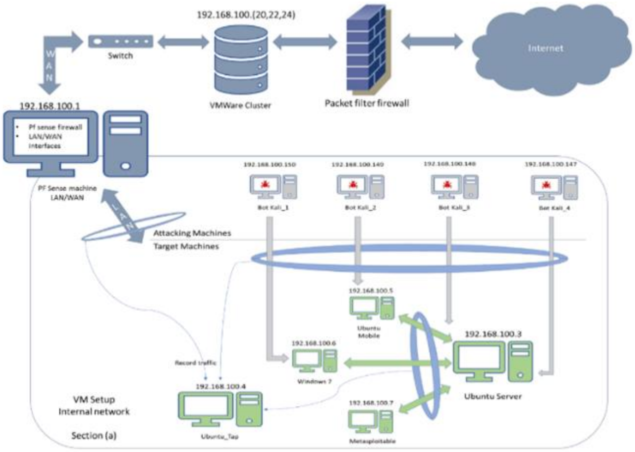


Figure 6. BoT-IoT Dataset

Cyber Range Lab of The focal point of UNSW Canberra Cyber, as appeared in Figure 6. The environment consolidates a mix of typical and botnet traffic. The dataset's source files are given in various formats, including the first pcap files, the produced argus files, and CSV files. The files were isolated, in view of assault classification and subcategory, to all the more likely aid the naming procedure.

The caught pcap files are 69.3 GB in size, with more than 72.000.000 records. The extracted flow traffic, in CSV format, is 16.7 GB in size. To facilitate the handling of the dataset, we extracted 202.7MB of the original dataset is 13.7GB of UDP_DDOS pcap files.

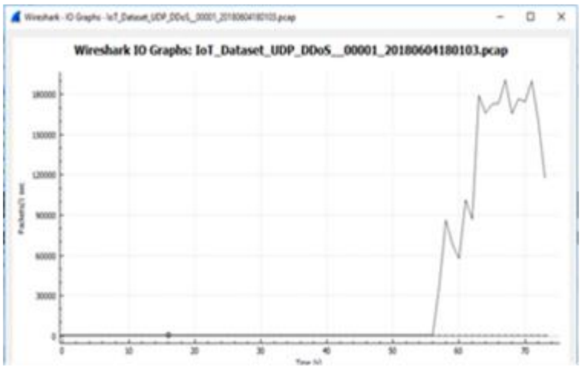


Figure 7. IO Graph for IoT_Dataset_ UDP_DDOS pcap file

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.

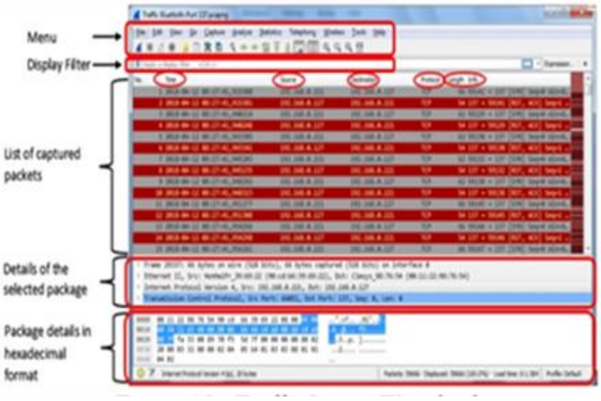
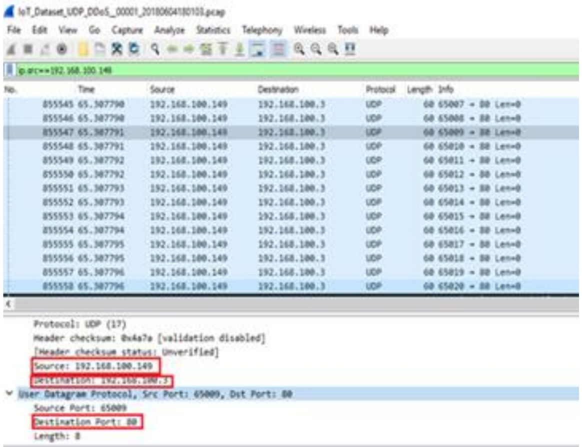

Menu
Display Filter
List of captured packets
Details of the selected package
Package details in hexadecimal format

Figure 8. Traffic Log in Wireshark

After the log files are recorded, the log file will be taken and analyzed using Wireshark to have this forensic evidence.

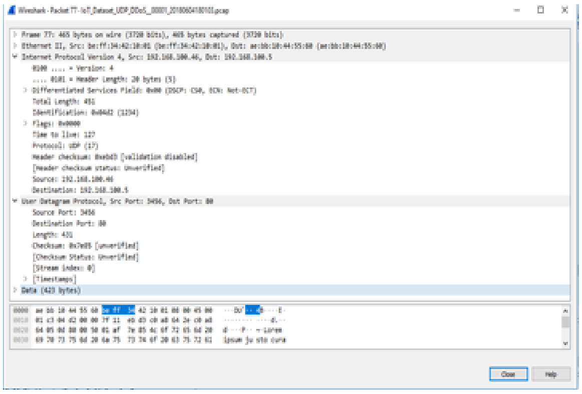

IoT_Dataset_UDP_DDoS_00001_20180604180103.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.src==192.168.100.149

```
No.     Time          Source            Destination      Protocol  Length  Info
855545 65.307790     192.168.100.149   192.168.100.3    UDP       60 65007 → 80 Len=0
855546 65.307790     192.168.100.149   192.168.100.3    UDP       60 65008 → 80 Len=0
855547 65.307791     192.168.100.149   192.168.100.3    UDP       60 65009 → 80 Len=0
855548 65.307791     192.168.100.149   192.168.100.3    UDP       60 65010 → 80 Len=0
855549 65.307792     192.168.100.149   192.168.100.3    UDP       60 65011 → 80 Len=0
855550 65.307792     192.168.100.149   192.168.100.3    UDP       60 65012 → 80 Len=0
855551 65.307793     192.168.100.149   192.168.100.3    UDP       60 65013 → 80 Len=0
855552 65.307793     192.168.100.149   192.168.100.3    UDP       60 65014 → 80 Len=0
855553 65.307794     192.168.100.149   192.168.100.3    UDP       60 65015 → 80 Len=0
855554 65.307794     192.168.100.149   192.168.100.3    UDP       60 65016 → 80 Len=0
855555 65.307795     192.168.100.149   192.168.100.3    UDP       60 65017 → 80 Len=0
855556 65.307795     192.168.100.149   192.168.100.3    UDP       60 65018 → 80 Len=0
855557 65.307796     192.168.100.149   192.168.100.3    UDP       60 65019 → 80 Len=0
855558 65.307796     192.168.100.149   192.168.100.3    UDP       60 65020 → 80 Len=0

    Protocol: UDP (17)
    Header checksum: 0x4a7a [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.100.149
    Destination: 192.168.100.3
v User Datagram Protocol, Src Port: 65009, Dst Port: 80
    Source Port: 65009
    Destination Port: 80
    Length: 8
```

Figure 9. UDP Flood packet being sent to port 80

Above figure, the server IP is 192.168.100.149 and it send UDP packets to 192.168.100.3 with port 80. This is profoundly unusual and as a rule, UDP does not have to send to port 80 genuinely. These are the first signs of a UDP flood attack.

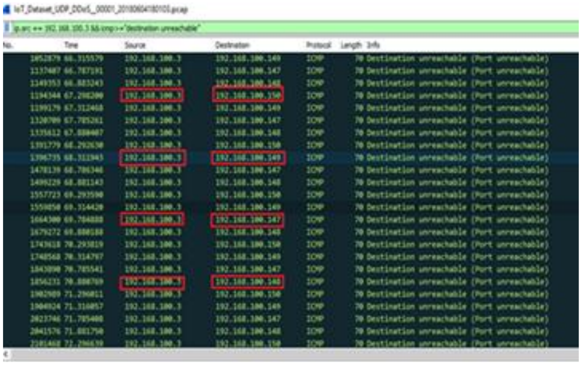

Wireshark · Packet 77 · IoT_Dataset_UDP_DDoS_00001_20180604180103.pcap
Close
Help

```
> Frame 77: 465 bytes on wire (3720 bits), 465 bytes captured (3720 bits)
> Ethernet II, Src: be:ff:34:42:10:01 (be:ff:34:42:10:01), Dst: ae:bb:18:44:55:60 (ae:bb:18:44:55:60)
v Internet Protocol Version 4, Src: 192.168.100.46, Dst: 192.168.100.5
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 451
    Identification: 0x04d2 (1234)
  > Flags: 0x0000
    Time to live: 127
    Protocol: UDP (17)
    Header checksum: 0xebd3 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.100.46
    Destination: 192.168.100.5
v User Datagram Protocol, Src Port: 3456, Dst Port: 80
    Source Port: 3456
    Destination Port: 80
    Length: 431
    Checksum: 0x7e85 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
> Data (423 bytes)

0000  ae bb 18 44 55 60 be ff  34 42 10 01 08 00 45 00   ···DU`·· 4B····E·
0010  01 c3 04 d2 00 00 7f 11  eb d3 c0 a8 64 2e c0 a8   ········ ····d.··
0020  64 05 0d 80 00 50 01 af  7e 85 4c 6f 72 65 6d 20   d····P·· ~·Lorem 
0030  69 70 73 75 6d 20 6a 75  73 74 6f 20 63 75 72 61   ipsum ju sto cura
```

Figure 10. UDP Follow

The data got from the proof follows is utilized to distinguish the episode. This will help in source trace back, reproduction of the assault situation and attribution to a source. 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 192.168.100.46 has a length (length) range in the 465 Bytes). On the Internet Protocol Version 4, to read as 192.168.100.46 IP source and destination IP address visible 192.168.100.5 with 20 Bytes header length and the total length of 451. On the part of the user datagram protocol, source port reads as 3456 and destination port read as 80.



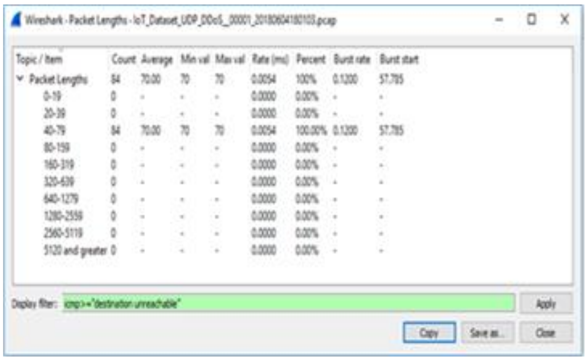
IoT_Dataset_UDP_DDoS_00001_20180604180103.pcap

ip.src == 192.168.100.3 && icmp>="destination unreachable"

```
No.      Time        Source          Destination      Protocol  Length  Info
1052879 66.315579   192.168.100.3   192.168.100.149  ICMP      70 Destination unreachable (Port unreachable)
1137487 66.787191   192.168.100.3   192.168.100.147  ICMP      70 Destination unreachable (Port unreachable)
1149353 66.883243   192.168.100.3   192.168.100.148  ICMP      70 Destination unreachable (Port unreachable)
1194344 67.298290   192.168.100.3   192.168.100.150  ICMP      70 Destination unreachable (Port unreachable)
1199179 67.312468   192.168.100.3   192.168.100.149  ICMP      70 Destination unreachable (Port unreachable)
1320789 67.785261   192.168.100.3   192.168.100.147  ICMP      70 Destination unreachable (Port unreachable)
1335612 67.888487   192.168.100.3   192.168.100.148  ICMP      70 Destination unreachable (Port unreachable)
1391779 68.292630   192.168.100.3   192.168.100.150  ICMP      70 Destination unreachable (Port unreachable)
1396735 68.313945   192.168.100.3   192.168.100.149  ICMP      70 Destination unreachable (Port unreachable)
1478139 68.786346   192.168.100.3   192.168.100.147  ICMP      70 Destination unreachable (Port unreachable)
1499229 68.881143   192.168.100.3   192.168.100.148  ICMP      70 Destination unreachable (Port unreachable)
1557723 69.293598   192.168.100.3   192.168.100.150  ICMP      70 Destination unreachable (Port unreachable)
1559858 69.314420   192.168.100.3   192.168.100.149  ICMP      70 Destination unreachable (Port unreachable)
1664300 69.784888   192.168.100.3   192.168.100.147  ICMP      70 Destination unreachable (Port unreachable)
1679272 69.880188   192.168.100.3   192.168.100.148  ICMP      70 Destination unreachable (Port unreachable)
1743618 70.293819   192.168.100.3   192.168.100.150  ICMP      70 Destination unreachable (Port unreachable)
1748568 70.314797   192.168.100.3   192.168.100.149  ICMP      70 Destination unreachable (Port unreachable)
1843898 70.785541   192.168.100.3   192.168.100.147  ICMP      70 Destination unreachable (Port unreachable)
1856231 70.880769   192.168.100.3   192.168.100.148  ICMP      70 Destination unreachable (Port unreachable)
1982989 71.296811   192.168.100.3   192.168.100.150  ICMP      70 Destination unreachable (Port unreachable)
1984924 71.316857   192.168.100.3   192.168.100.149  ICMP      70 Destination unreachable (Port unreachable)
2023746 71.785408   192.168.100.3   192.168.100.147  ICMP      70 Destination unreachable (Port unreachable)
2041576 71.881750   192.168.100.3   192.168.100.148  ICMP      70 Destination unreachable (Port unreachable)
2181468 72.296639   192.168.100.3   192.168.100.150  ICMP      70 Destination unreachable (Port unreachable)
```

Figure 11. Detecting ICMP host unreachable packet

Server IP is 192.168.100.3. The server is sent to 192.168.100.150, 149,147148 ICMP host unreachable packet. So, this four IP address would be the victim IP.



Wireshark · Packet Lengths · IoT_Dataset_UDP_DDoS_00001_20180604180103.pcap

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Packet Lengths	84	70.00	70	70	0.0054	100%	0.1200	57.785
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	84	70.00	70	70	0.0054	100.00%	0.1200	57.785
80-159	0	-	-	-	0.0000	0.00%	-	-
160-319	0	-	-	-	0.0000	0.00%	-	-
320-639	0	-	-	-	0.0000	0.00%	-	-
640-1279	0	-	-	-	0.0000	0.00%	-	-
1280-2559	0	-	-	-	0.0000	0.00%	-	-
2560-5119	0	-	-	-	0.0000	0.00%	-	-
5120 and greater	0	-	-	-	0.0000	0.00%	-	-

Display filter: icmp>="destination unreachable"

Figure 12. Packet Lengths for Destination Unreachable

ICMP destination unreachable packet number is 84 and Capture traffic increased in 40-79 packet length. We noted the following:

- If no service is listening on that UDP port, the server responds to the client with an "ICMP host unreachable" packet.
- Thus there is a high chance of being this DDoS UDP flood attack.
- Logfile data with p.cap expansion can be broke down by network forensic investigation utilizing the Wireshark application got 4 IP addresses for the attacker.

VII. CONCLUSION

The Internet is one of the fundamental necessities of society, yet it very well may be effectively attacked. Generally speaking, through this venture, we planned to completely appear and portray how hazardous a focused on DoS/DDoS attack can be in the present mechanical world through running the open-source DoS UDP Packet Flood and reenacting a DoS attack. Log file information with p.cap expansion can be examined by network forensic examination utilizing the Wireshark application. We presume that the current IoT systems must fuse the forensic arrangements inside its design to guarantee a sheltered and secure condition. In this paper, we had done the network forensics in IoT forensics investigation for detecting DoS/DDoS flooding attacks on the Internet of Things (IoT) devices.

REFERENCES

[1] Servida, Francesco, and Eoghan Casey. "IoT forensic challenges and opportunities for digital traces." Digital Investigation 28 (2019): S22-S29.

[2] Maheshwari, Sumit, Sudipta Mahapatra, and K. Cheruvu. Measurement and Forecasting of Next Generation Wireless Internet Traffic. No. 525. EasyChair, 2018.

[3] F.J. Ryba, M.Orlinski, M. Wählisch, C. Rossow, T.C. Schmidt, "Amplification and DRDoS Attack Defense -A Survey and New Perspectives",CoRR abs/1505.07892,2015.

[4] Y. Bekeneva, N. Shipilov, A. Shorov,"Investigation of Protection Mechanisms Against DRDoS Attacks Using a Simulation Approach",Internet of Things, Smart Spaces, and Next Generation Networks and Systems. Lect Notes Comput Sc, vol 9870. Springer, 2016.

[5] Kolias, Constantinos, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. "DDoS in the IoT: Mirai and other botnets." Computer 50, no. 7 (2017): 80-84.

[6] I. van der Elzen, and J. van Heugten,"Techniques for detecting compromised IoT devices",Project Report. University of Amsterdam,2017.

[7] https://www.oracle.com

[8] https://www.aapnainfotech.com/iot-beginners-perspective/?

[9] Karim, Ahmad, Rosli Bin Salleh, Muhammad Shiraz, Syed Adeel Ali Shah, Irfan Awan, and Nor Badrul Anuar. "Botnet detection techniques: review, future trends, and issues." Journal of Zhejiang University SCIENCE C 15, no. 11 (2014): 943-983.

[10] Saeedi, Kubra. "Machine Learning for Ddos Detection in Packet Core Network for IoT." (2019)..

[11] https://www.imperva.com

[12] 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.

[13] Nickolaos Koroniotis, Nour Moustafa, Elena Sitnikova, Benjamin Turnbull, "Towards the Development of Realistic Botnet Dataset in the Internet of Things for Network Forensic Analytics: Bot-IoT Dataset", https://arxiv.org/abs/1811.00701, 2018.

[14] Rizal, Randi, Imam Riadi, and Yudi Prayudi. "Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) Device." Int. J. Cyber-Security Digit. Forensics 7, no. 4 (2018): 382-390.

[15] J. D. T. Gonzalez, and W.Kinsner, "Zero-crossing analysis of Lévy walks for real-time feature extraction: Composite signal analysis for strengthening the IoT against DDoS attacks",Proc. ofIEEE 15thInt.Conf.on Cognitive Informatics & Cognitive Computing (ICCI* CC), IEEE, 2016.

[16] Koroniotis, Nickolaos, Nour Moustafa, Elena Sitnikova, and Benjamin Turnbull. "Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset." Future Generation Computer Systems 100 (2019): 779-796..

[17] https://www.cloudflare.com/enau/learning/ddos/?