2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS) | 978-1-7281-9537-7/20/$31.00 ©2021 IEEE | DOI: 10.1109/ICAIS50930.2021.9395852

A Survey On Network Packet Inspection And ARP Poisoning Using Wireshark And Ettercap

Majidha Fathima K M
Assistant Professor
Department of Computer Science and Engineering
Sri Krishna College of Engineering and Technology
Coimbatore, India
majidhafathimakm@skcet.ac.in

Dr. N. Santhiyakumari
Professor & Head,
Department of Electronics & Communication Engineering
Knowledge Institute Of Technology
Salem, India
santhiyarajee@rediffmail.com

***Abstract*— A network consists of a collection of nodes such as hubs, bridges, switches, routers, firewalls, brouters, packet shapers. The hubs help in connecting two devices. The bridges and switches function in layer 2 of ISO-OSI (Open Systems Interconnection). Routers perform the role of delivering packets from source to destination. Firewalls protect the networks by filtering the traffic between sender and receiver. The packet shapers help in regulating the traffic by cutting out spikes in a connectivity. The network is being utilized as 24*7 days support. The network is being exposed to various kinds of attacks such as ARP (Address Resolution Protocol), DDOS (Distributed Denial of Service). Hence the performance monitoring plays a vital role in preserving a network. The tools such as wireshark and ettercap are being analyzed in this paper. The network traffic is being interpreted by wireshark. Ettercap analyzes ARP poisoning attack. The preventive actions are taken based on the output of the monitoring tools.**

***Keywords*— ISO-OSI, ARP, DDOS**

I. INTRODUCTION

A customer can access the IVPN (Internet Virtual Private Network) or VPN (Virtual Private Network) or intranet via the network. The devices in his network viz., the workstations are connected in LAN (Local Area Network) via a switch. Then this traffic is forwarded to the WAN (Wide Area Network) through a router. As per figure 1, the network is divided into three layers as Compute, Network and Storage. Compute layer consists of computational hosts such as servers. The network layer is again divided into core network, aggregation network and access network [1].The core network consists of two switches viz., one for southern state (Tamilnadu) and another for northern state (Delhi) of a country. Every switch in a region covers the district under it. The switch in Tamilnadu covers districts as Coimbatore and Chennai. The switch in Delhi offers connectivity in Ghaziabad and Faridabad. As the name suggests, aggregation switches provide the connectivity in the respective districts. The access network consists of switches to provide connectivity locally. i.e. Coimbatore switch connects to Brook Bond road; the traffic from Nungambakkam gets aggregated to Chennai; Raj Nagar in Ghaziabad is connected to switch in Ghaziabad. New industrial town is connected to switch in Faridabad.The storage layer consists of an array of disks organized as RAID (Redundant Array of Independent Disks) or ISS (Intelligent Storage System). Every L3 (Layer 3) switch in core network is connected to every other L3 switch in the access network. Similarly, each switch in aggregation network is connected to other L2/L3 switches in access network to store or retrieve contents from server. The Core and aggregation switches are connected by 10 GE (Gigabit Ethernet) links. 1 GE link connects aggregation and access network. When a user wants to access the server at remote end, the traffic flows as follows:

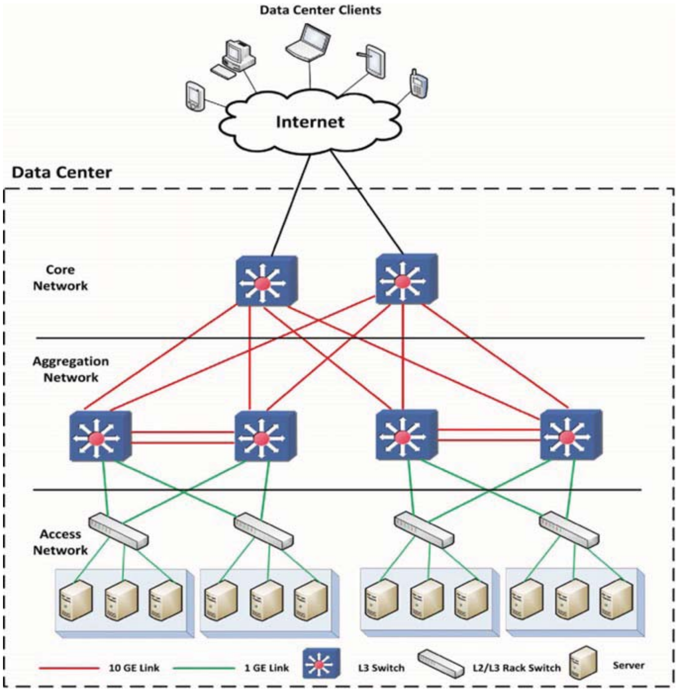


Fig. 1. Traffic Analysis in 3 Tier Layered Network

- Client end to LAN
- LAN to WAN
- WAN to core network (backbone network with redundancy) in the ISP (Internet Service Provider)
- Core to aggregation network
- Aggregation to access network
- Access network to server/storage

II. LITERATURE SURVEY

As per Table 1, twenty one network traffic analysis tools are compared.

SNO	TOOLS	FEATURES
1	ENDACE	Deep Packet Analyzer
2	Wireshark	Network Protocol Analyzer
3	Tcpdump [2]	Network Sniffer
4	Dsniff	Passive sniffs the network
5	Etherpeek	Protocol Analyzer
6	Sniffit [3]	Network Analyzer
7	Etherflood [4]	White hat hacking purpose
8	ETHERCAP	Packet sniffer
9	Insider	Network Scanner
10	Pof [5]	Identify the Operating system
11	NetworkMiner	Forensic Analyzer
12	Ettercap	Sniffs dynamic connections
13	KISMET	Passive sniffer
14	Cain and Abel	Cracking passwords
15	NetStumbler [6]	Active sniffer
16	Ntop	Determines network status
17	Ngrep	Packet sniffer
18	EtherApe [7]	Network traffic monitor
19	KisMAC	Network discovery tool
20	Aircrack-ng	Detection of network packets
21	SUITE	Creates encrypted packets

TABLE I. COMPARISION OF NETWORK TRAFFIC ANALYZERS

In ENDACE, the packets in a network are analyzed deeply and bandwidth utilization on the link is captured. Incase of bursty traffic, the investigation is made for any attack. The input and output (to and fro) traffic utilization of the customer's network is monitored for any high consumption of bandwidth. The source and destination ip generating the traffic is identified. High bandwidth consuming applications are tracked [8]. Wireshark is a network protocol analyzer with monitoring parameters as number, time, source, destination, protocol such as Transmission Control Protocol/Secure Socket Layer (TCP/SSL) , length and information of the type of communication being established. Tcpdump filters traffic based on basic communication, IP, source/destination, network, port, protocol, IPV6, port ranges, packet size, TCP flags, HTTP user agents, cleartext HTTP GETs, HTTP hosts, HTTP cookies, SSH connections, DNS, FTP, cleartext passwords, packets with evil bit and writes to a file. dsniff is a password sniffer which handles FTP, Telnet, SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, PPTP MS-CHAP, NFS, VRRP, YP/NIS, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft SMB, Oracle SQL*Net, Sybase and Microsoft SQL protocols. Etherpeek comprises capture button, send button, filters, node stats, protocol stats, size stats, summary stats, conversation stats, net stats, history stats and name table. It checks for errors, capture and view some packets, identifies protocols, packet sizes, applies filter, history statistics, sets an alarm, locates similar packets based on IP, TCP, HTTP, UDP, DNS, ARP (Req,Rsp), portrays an overview of network communications. The linux command for sniffit is

```
./sniffit –e "port 80".
```

It sniffs on port 80 using device enp0s25 with packet number, source ip, destination ip, source port, destination port. Etherflood encounters a firewall or a packet-filtering router and traces the '*' hops in tracert command. ETHERCAP snifs the packet on the switches. Insider threat detection software scans the network. POF identifies the operating system. NetworkMiner encloses tabs such as hosts, frames, files, images, messages, credentials, sessions, DNS, parameters, keywords, cleartext, anomalies. Files contains information as source port, destination port, source ip, destination ip, protocol as HttpGetNormal, filename, extension (html,txt) and size. Ettercap sniffs dynamic connections. KISMET reveals network details as name, SSID, server, BSSID, carrier, manufacturer, maximum rate, BSS time, maximum speed, access time as first and latest, number of clients, type of infrastructure, information, channel, privacy, encryption, decryption, beacon, packets (data, LLC, crypt, weak, dupe IV), data, signal (power). Cain and Abel looks into dictionary attack, brute-force attack, cryptanalysis attack and tests password. NetStumbler consists of fields like channels, SSIDs and filters [9]. The options are

- New document starts scanning
- Reconfigure card automatically
- Query APs for names

Ntop classifies traffic as WAN: top local talkers, top remote destinations, realtime top application traffic and traffic last day view. Ngrep matches traffic pattern as

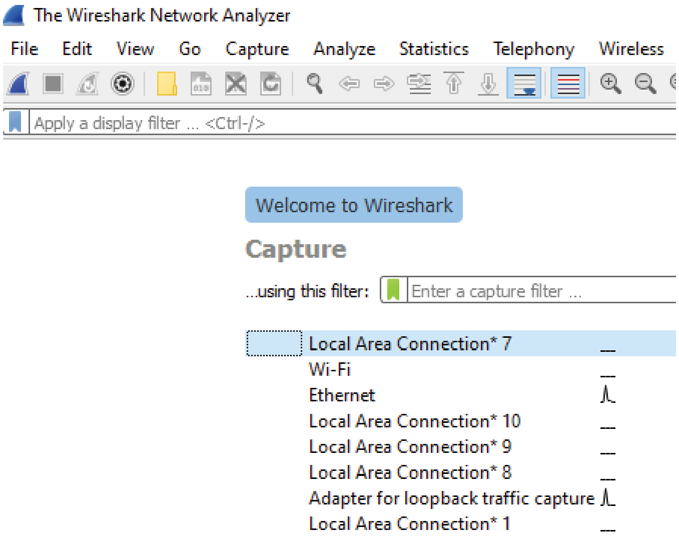
```
"ngrep –W byline port 80"
```

EtherApe comprises protocol stack level, node size variable, size mode, maximum node radius, maximum link width, diagram refresh period, diagram node timeout, font, hide node names, group unknown ports and node anti aliasing. KisMAC displays SSID, vendor, first seen, last seen, Channel, main channel, supported rates, signal, MaxSignal, AvgSignal, type, encryption and packets. Aircrack-ng has options as force attack mode, target selection, no of CPUs to use, enable quiet mode, merge the given APs to a virtual one and write key to file. NetCrunch Suite monitors IP networks, physical segments, custom views, performance views and creates network atlas.

III. EXEMPLIFICATION OF THE TOOLS

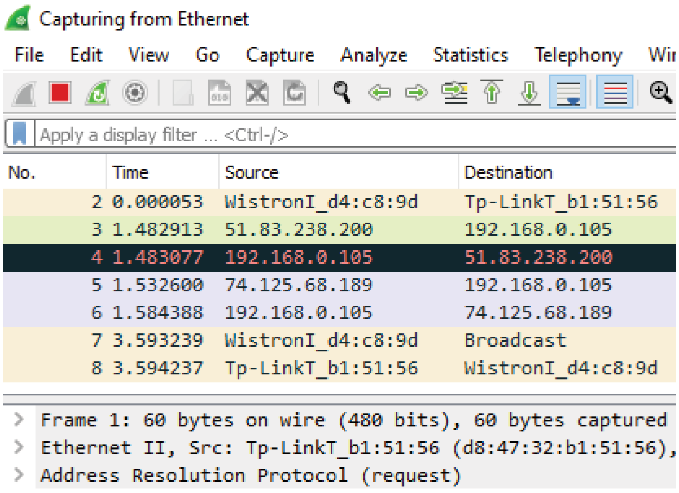
A. Wireshark

After Wireshark installation, the interface on which traffic flows is selected as shown in figure 2.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...

Local Area Connection* 7
Wi-Fi
Ethernet
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Adapter for loopback traffic capture
Local Area Connection* 1

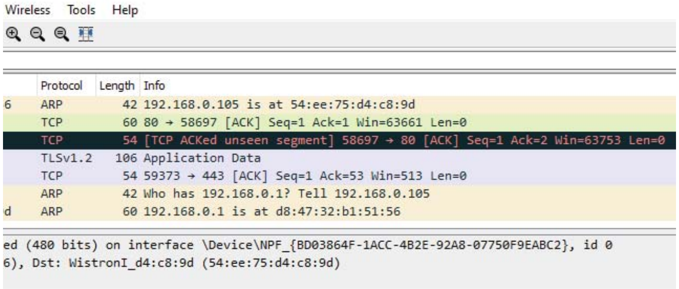
Fig. 2. Wireshark Network Analyzer


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wi
Apply a display filter ... <Ctrl-/>

```
No.   Time        Source              Destination
    2 0.000053    WistronI_d4:c8:9d   Tp-LinkT_b1:51:56
    3 1.482913    51.83.238.200       192.168.0.105
    4 1.483077    192.168.0.105       51.83.238.200
    5 1.532600    74.125.68.189       192.168.0.105
    6 1.584388    192.168.0.105       74.125.68.189
    7 3.593239    WistronI_d4:c8:9d   Broadcast
    8 3.594237    Tp-LinkT_b1:51:56   WistronI_d4:c8:9d

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured
> Ethernet II, Src: Tp-LinkT_b1:51:56 (d8:47:32:b1:51:56),
> Address Resolution Protocol (request)
```

Fig. 3. Traffic on Ethernet Interface

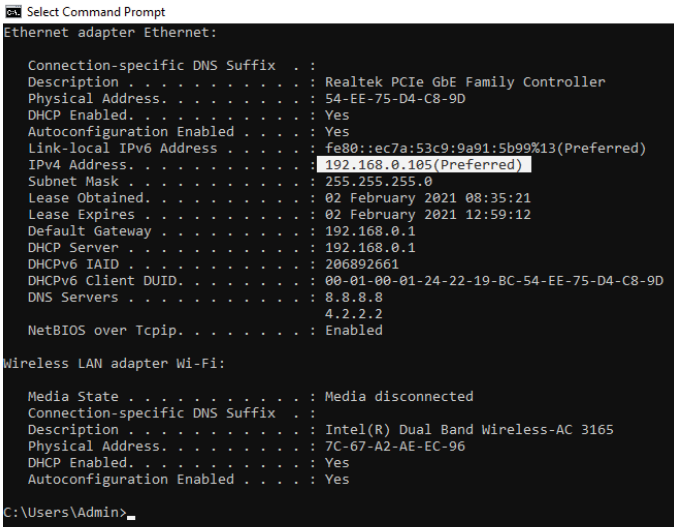
The ethernet and adapter for loopback traffic capture is being utilized [10]. The network traffic on ethernet interface is captured as shown in figure 3. As per figure 4, the various protocols in the network are ARP, TCP and TLSv1.2 (Transport layer Security).



```
   Protocol  Length Info
6  ARP           42 192.168.0.105 is at 54:ee:75:d4:c8:9d
   TCP           60 80 → 58697 [ACK] Seq=1 Ack=1 Win=63661 Len=0
   TCP           54 [TCP ACKed unseen segment] 58697 → 80 [ACK] Seq=1 Ack=2 Win=63753 Len=0
   TLSv1.2      106 Application Data
   TCP           54 59373 → 443 [ACK] Seq=1 Ack=53 Win=513 Len=0
   ARP           42 Who has 192.168.0.1? Tell 192.168.0.105
d  ARP           60 192.168.0.1 is at d8:47:32:b1:51:56

ed (480 bits) on interface \Device\NPF_{BD03864F-1ACC-4B2E-92A8-07750F9EABC2}, id 0
6), Dst: WistronI_d4:c8:9d (54:ee:75:d4:c8:9d)
```

Fig. 4. TCP Filter

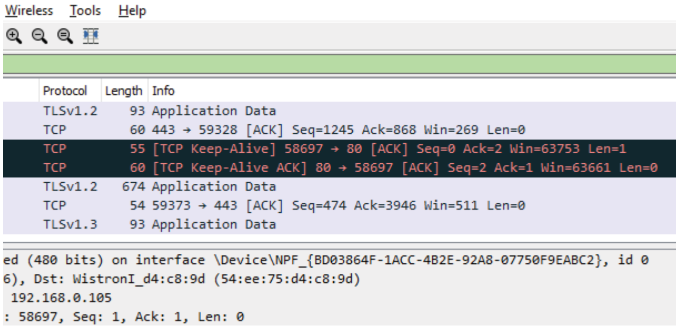
Figure 5 displays the physical address (MAC) and logical address (IP) of the source originating the transfer of data.



```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : 54-EE-75-D4-C8-9D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::ec7a:53c9:9a91:5b99%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.105(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 02 February 2021 08:35:21
   Lease Expires . . . . . . . . . . : 02 February 2021 12:59:12
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 206892661
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-22-19-BC-54-EE-75-D4-C8-9D
   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       4.2.2.2
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Wi-Fi:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 3165
   Physical Address. . . . . . . . . : 7C-67-A2-AE-EC-96
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

C:\Users\Admin>_
```

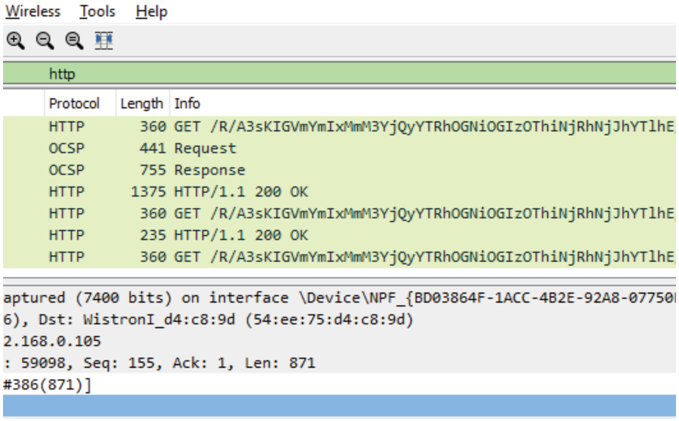
Fig. 5. IP Address of source

After the application of TCP filter [11], the TCP traffic alone is isolated with the frame sequence number and acknowledgement number as shown in figure 6.



```
   Protocol  Length Info
   TLSv1.2       93 Application Data
   TCP           60 443 → 59328 [ACK] Seq=1245 Ack=868 Win=269 Len=0
   TCP           55 [TCP Keep-Alive] 58697 → 80 [ACK] Seq=0 Ack=2 Win=63753 Len=1
   TCP           60 [TCP Keep-Alive ACK] 80 → 58697 [ACK] Seq=2 Ack=1 Win=63661 Len=0
   TLSv1.2      674 Application Data
   TCP           54 59373 → 443 [ACK] Seq=474 Ack=3946 Win=511 Len=0
   TLSv1.3       93 Application Data

ed (480 bits) on interface \Device\NPF_{BD03864F-1ACC-4B2E-92A8-07750F9EABC2}, id 0
6), Dst: WistronI_d4:c8:9d (54:ee:75:d4:c8:9d)
 192.168.0.105
: 58697, Seq: 1, Ack: 1, Len: 0
```

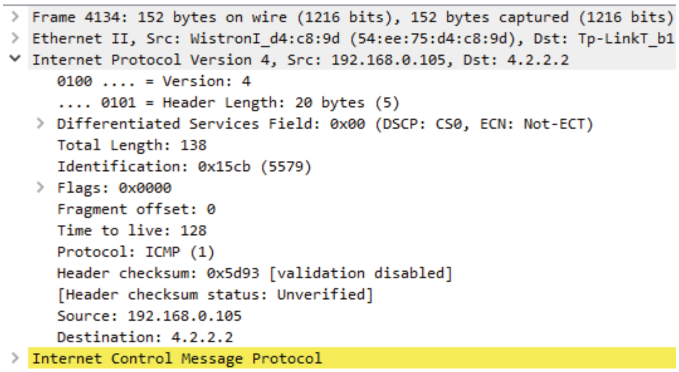
Fig. 6. TCP Filter



```
http
Protocol  Length Info
HTTP         360 GET /R/A3sKIGVmYmIxMmM3YjQyYTRhOGNiOGIzOThiNjRhNjJhYTlhE
OCSP         441 Request
OCSP         755 Response
HTTP        1375 HTTP/1.1 200 OK
HTTP         360 GET /R/A3sKIGVmYmIxMmM3YjQyYTRhOGNiOGIzOThiNjRhNjJhYTlhE
HTTP         235 HTTP/1.1 200 OK
HTTP         360 GET /R/A3sKIGVmYmIxMmM3YjQyYTRhOGNiOGIzOThiNjRhNjJhYTlhE

aptured (7400 bits) on interface \Device\NPF_{BD03864F-1ACC-4B2E-92A8-07750
6), Dst: WistronI_d4:c8:9d (54:ee:75:d4:c8:9d)
2.168.0.105
: 59098, Seq: 155, Ack: 1, Len: 871
#386(871)]
```

Fig. 7. HTTP Filter

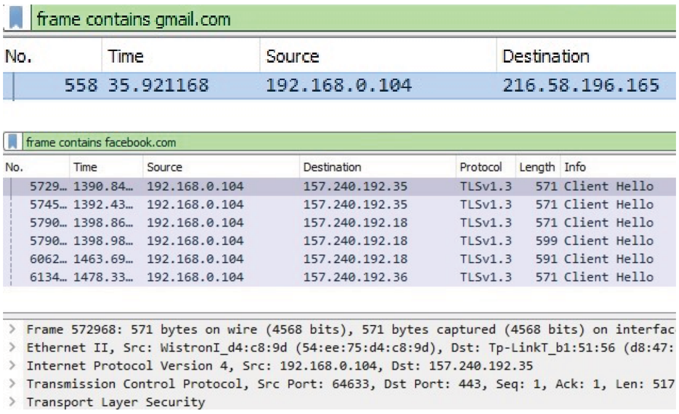
After the application of HTTP filter, the request and response messages are displayed. The Online Certificate Status Protocol (OCSP) codes are 441 and 755 as shown in figure 7.



```
> Frame 4134: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits)
> Ethernet II, Src: WistronI_d4:c8:9d (54:ee:75:d4:c8:9d), Dst: Tp-LinkT_b1
v Internet Protocol Version 4, Src: 192.168.0.105, Dst: 4.2.2.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 138
    Identification: 0x15cb (5579)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x5d93 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.105
    Destination: 4.2.2.2
> Internet Control Message Protocol
```

Fig. 8. ICMP

As per figure 8, the packet fields such as source ip address, destination ip address, source MAC address, destination MAC address, total length, TTL (Time To Live) and header checksum are displayed in the second window pane [12]. The ICMP (Internet Control Message Protocol) echo request is generated by the PING (Packet Internet Groper) command used to check reachability between the two hosts.

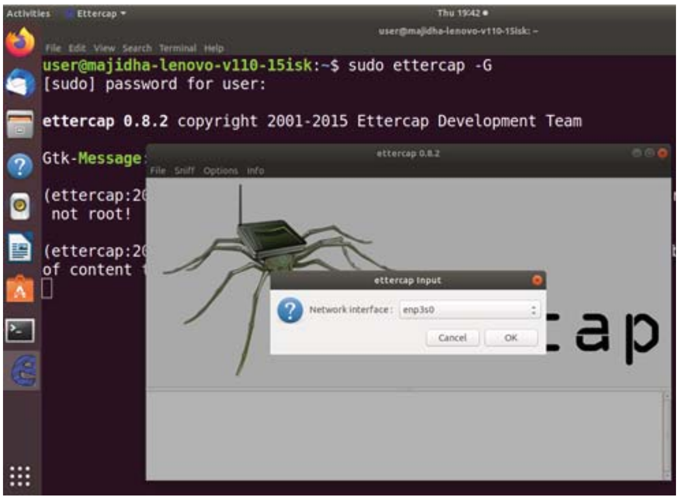


```
frame contains gmail.com
No.     Time          Source           Destination
    558 35.921168     192.168.0.104    216.58.196.165

frame contains facebook.com
No.     Time      Source          Destination      Protocol  Length Info
  5729… 1390.84…  192.168.0.104   157.240.192.35   TLSv1.3     571 Client Hello
  5745… 1392.43…  192.168.0.104   157.240.192.35   TLSv1.3     571 Client Hello
  5790… 1398.86…  192.168.0.104   157.240.192.18   TLSv1.3     571 Client Hello
  5790… 1398.98…  192.168.0.104   157.240.192.18   TLSv1.3     599 Client Hello
  6062… 1463.69…  192.168.0.104   157.240.192.18   TLSv1.3     591 Client Hello
  6134… 1478.33…  192.168.0.104   157.240.192.36   TLSv1.3     571 Client Hello

> Frame 572968: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interfac
> Ethernet II, Src: WistronI_d4:c8:9d (54:ee:75:d4:c8:9d), Dst: Tp-LinkT_b1:51:56 (d8:47:
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 157.240.192.35
> Transmission Control Protocol, Src Port: 64633, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
> Transport Layer Security
```

Fig. 9. Gmail and Facebook Traffic

If gmail and facebook web pages are accessed, the respective data flow is captured with transmission of hello messages as shown in figure 9.

B. Ettercap



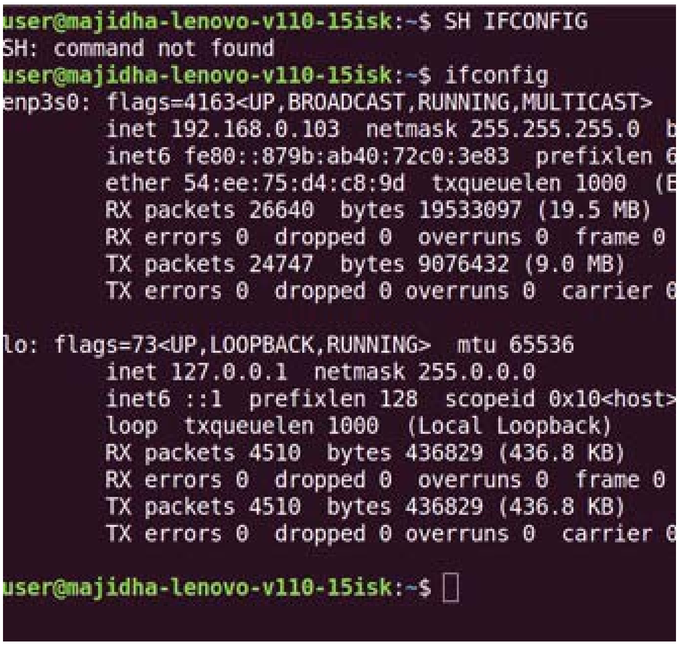
```
user@majidha-lenovo-v110-15isk:~$ sudo ettercap -G
[sudo] password for user:

ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team

Gtk-Message:

(ettercap:2
 not root!

(ettercap:2
of content
```

Network interface : enp3s0

Fig. 10. Ettercap Launch

As per figure 10, the host's interface enp3s0 with IP Address 192.168.0.103 is being sniffed by selecting

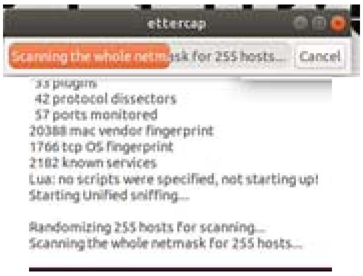
Sniff -> Unified Sniffing -> Network Interface : enp3s0



```
user@majidha-lenovo-v110-15isk:~$ SH IFCONFIG
SH: command not found
user@majidha-lenovo-v110-15isk:~$ ifconfig
enp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>
        inet 192.168.0.103  netmask 255.255.255.0  b
        inet6 fe80::879b:ab40:72c0:3e83  prefixlen 6
        ether 54:ee:75:d4:c8:9d  txqueuelen 1000  (E
        RX packets 26640  bytes 19533097 (19.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24747  bytes 9076432 (9.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4510  bytes 436829 (436.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4510  bytes 436829 (436.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0

user@majidha-lenovo-v110-15isk:~$ ▯
```

Fig. 11. Ifconfig on Linux

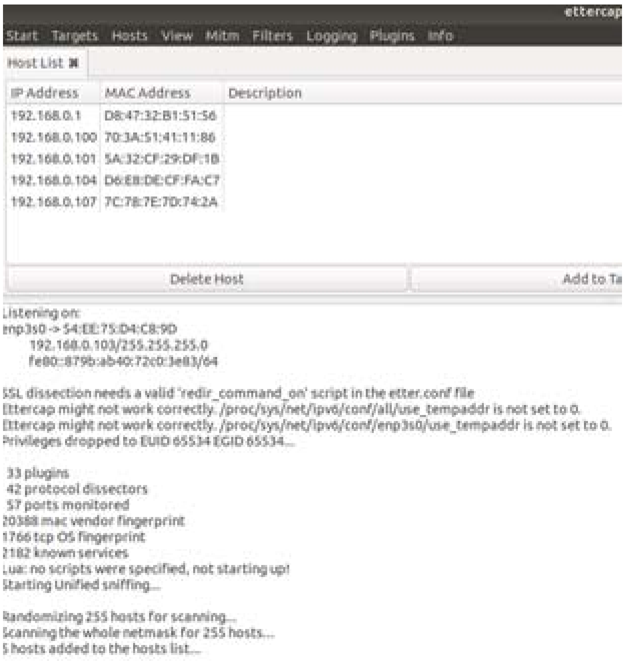
The network traffic for ip address 192.168.0.103 and loopback ip 127.0.0.1 with mask 255.255.255.0 and 255.0.0.0 respectively are being displayed in linux system [13]. The number of packets in bytes sent and received are shown in figure 11.



```
 33 plugins
 42 protocol dissectors
 57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
```

Fig. 12. Scanning the hosts

The options Host -> Scan for host -> Host list are chosen [14]. It scans the whole netmask for 255 hosts. 33 plugins, 42 protocol dissectors, 57 ports, 20388 mac vendor fingerprint, tcp OS fingerprint, known services are sniffed in unified sniffing as per figure 12.

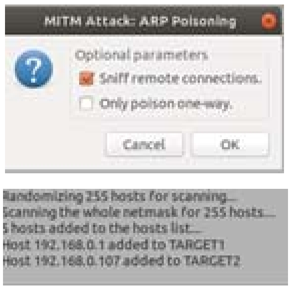


IP Address	MAC Address	Description
192.168.0.1	D8:47:32:B1:51:56	
192.168.0.100	70:3A:51:41:11:86	
192.168.0.101	5A:32:CF:29:DF:1B	
192.168.0.104	D6:E8:DE:CF:FA:C7	
192.168.0.107	7C:78:7E:7D:74:2A	

```
Listening on:
enp3s0 -> 54:EE:75:D4:C8:9D
      192.168.0.103/255.255.255.0
      fe80::879b:ab40:72c0:3e83/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/all/use_tempaddr is not set to 0.
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/enp3s0/use_tempaddr is not set to 0.
Privileges dropped to EUID 65534 EGID 65534...

 33 plugins
 42 protocol dissectors
 57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
5 hosts added to the hosts list...
```

Fig. 13. Target hosts

Click on first host -> Add to Target 1, Click on second host -> Add to Target 2. As per figure 13, the first host is added to target 1. Then the second host is added to target 2. Totally 5 hosts are added to the hosts list.

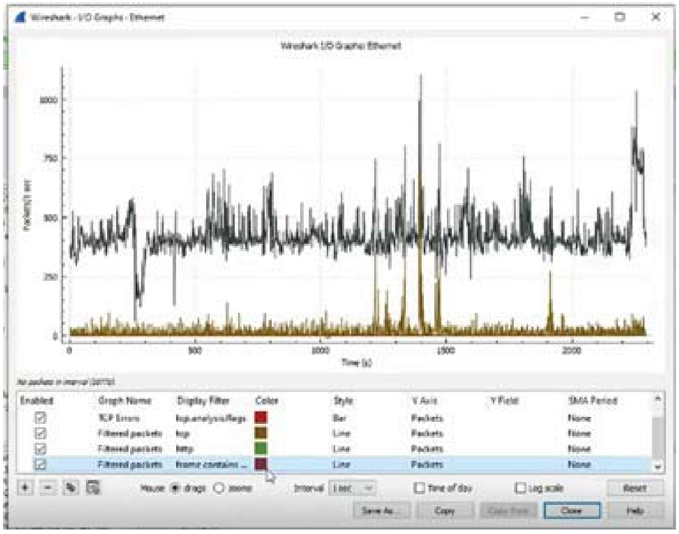


```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
5 hosts added to the hosts list...
Host 192.168.0.1 added to TARGET1
Host 192.168.0.107 added to TARGET2
```

Fig. 14. MITM and ARP

The path is MITM -> ARP poisoning -> Sniff Remote Connection. MITM (Man in The Middle attack) and ARP poisoning spurious traffic are being observed. As per figure 14, when an intruder intrudes in the middle between sender and receiver, his IP is being captured [15]. The hosts in a LAN suddenly starts sending enormous ARP requests and response messages thus poisoning the network with flooding ARP broadcasts.

IV. RESULTS AND DISCUSSION



Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
☑	TCP Errors	tcp.analysis.flags	🟥	Bar	Packets		None
☑	Filtered packets	tcp	🟫	Line	Packets		None
☑	Filtered packets	http	🟩	Line	Packets		None
☑	Filtered packets	frame contains ...	🟥	Line	Packets		None

Fig. 15. Input and Output Traffic

The statistics of the I/O Graph of wireshark is generated as shown in figure 15. It consists of capture file properties, resolved addresses, protocol hierarchy, conversations, end points, packet length, service response time, DHCP, ONC-RPC programs, 29West, ANCP, BACNet, Collectd, DNS flow graph, HART-IP, HPFEEDS, HTTP, HTTP2, UDP multicast streams, F5, IPv4 statistics and IPV6 statistics.

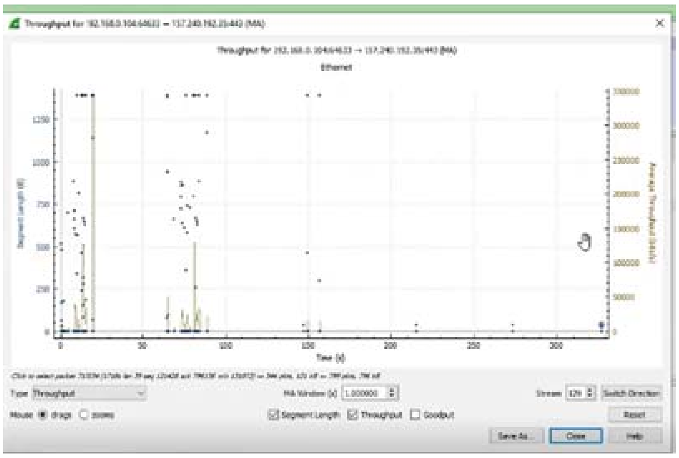
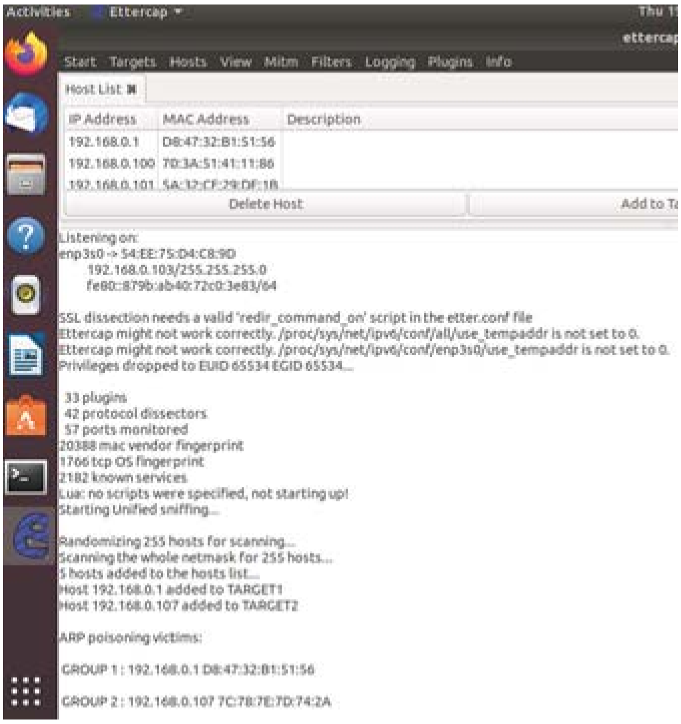


Fig. 16. TCP Throughput

The throughput for TCP Stream Graph is shown in figure 16. It comprises Time Sequence (Stevens), Time Sequence (tcptrace), round trip time and window scaling.



IP Address	MAC Address	Description
192.168.0.1	D8:47:32:B1:51:56	
192.168.0.100	70:3A:51:41:11:86	
192.168.0.101	5A:32:CF:29:DF:1B	

```
Listening on:
enp3s0 -> 54:EE:75:D4:C8:9D
      192.168.0.103/255.255.255.0
      fe80::879b:ab40:72c0:3e83/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/all/use_tempaddr is not set to 0.
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/enp3s0/use_tempaddr is not set to 0.
Privileges dropped to EUID 65534 EGID 65534...

 33 plugins
 42 protocol dissectors
 57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
5 hosts added to the hosts list...
Host 192.168.0.1 added to TARGET1
Host 192.168.0.107 added to TARGET2

ARP poisoning victims:

 GROUP 1 : 192.168.0.1 D8:47:32:B1:51:56

 GROUP 2 : 192.168.0.107 7C:78:7E:7D:74:2A
```

Fig. 17. ARP Poisoning Victims.

The protocol dissectors, ports monitored and known services are captured by ettercap as per figure 17. Group 1 with IP address 192.168.0.1 and MAC D8:47:32:B1:51:56 belong to 1st victim. IP address 192.168.0.107 with MAC 7C:78:7E:7D:74:2A represents Group 2 victim.

.

V. CONCLUSION

Thus the network is monitored through the performance monitoring tools like wireshark and ettercap. Wireshark analyzes each packet that passes through a switch, router or firewall. Ettercap analyzes the ARP poisoning attack by examining the packets from source to destination and poisoning victims. Through such observation, if there is sudden spike in the link utilization or suspicious generation of packets in a specific path, that particular traffic can be isolated and inspected for any spurious traffic or malware attack. The work can be extended to analyze the OS fingerprint pattern by identifying all the commands executed in the particular operating system of the victim under consideration.

ACKNOWLEDGEMENT

I express my sincere thanks to the Management, Principal, HOD, Faculty and my Supervisor for their extended support and encouragement in doing this work.

REFERENCES

[1] Vudipi Manohar, “Comparative Study on Network Monitoring Tools “, International Research Journal of Engineering and Technology, 2020, pp. 299-301

[2] Deepak Chahal, Latika Kharb, Deepanshu Choudhary , “Performance Analytics of Network Monitoring Tools “,International Journal of Innovative Technology and Exploring Engineering (IJITEE) , 2019, vol.8, pp.2572-2577.

[3] Bhavya Jani, Kajal Jain, Narendra Vishwakarma, “Network Monitoring Tools and Technologies”, International Journal of Creative Research Thoughts, 2018, vol.6, pp. 1295-1297

[4] Sakshi Singh, Suresh Kumar, “Capability of Wireshark as Intrusion Detection System”, International Journal of Recent Technology and Engineering, 2020, vol.8, pp. 4574-4578

[5] Haroon Iqbal, Sameena Naaz, “Wireshark as a tool for detection of various LAN attacks”, International Journal of Computer Science and Engineering, 2019, vol. 7, 833-837.

[6] Alia yahia, Eric Atwell, “Evaluation of Capabilities of Wireshark as Intrusion Detection System”, Journal of Global Research in Computer Science, 2018, vol.9, pp.1-8.

[7] V. Rohatgi and S. Goyal, "A Detailed Survey for Detection and Mitigation Techniques against ARP Spoofing," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2020, pp. 352-356.

[8] Robert A. Sowah, Kwadwo B. Ofori-Amanfo, Godfrey A. Mills, Koudjo M. Koumadi, "Detection and Prevention of Man-in-the-Middle Spoofing Attacks in MANETs Using Predictive Techniques in Artificial Neural Networks (ANN)", Journal of Computer Networks and Communications, 2019, pp.1-14.

[9] S. Prudhviraj, C. Sudha, “Command line and Graphical interface comparative analysis for ARP Poisoning through Ettercap”, International Journal of Computer Sciences and Engineering”, 2018, pp. 679-683.

[10] https://www.caida.org/tools/taxonomy/worktaxonomy.xml

[11]http://citeseer.ist.psu.edu/viewdoc/citations;jsessionid=A48300FFC94511A53587F7F6F122B5C6?doi=10.1.1.381.98

[12] https://core.ac.uk/download/pdf/219374674.pdf

[13] https://www.academia.edu/38701557/Cybercrime_and_Network_Traffic_Investigations

[14] Argha Ghosh, Dr. A.Senthilrajan, “Research on Packet Inspection Techniques”, International Journal Of Scientific & Technology Research 2019, vol.8, pp. 2068-2073

[15] Z. Cheng, M. Beshley, H. Beshley, O. Kochan and O. Urikova, "Development of Deep Packet Inspection System for Network Traffic Analysis and Intrusion Detection," IEEE 15th International Conference on Advanced Trends in Radio electronics, Telecommunications and Computer Engineering (TCSET), 2020, pp. 877-881