Name : MOHAMMED TOUSIF
Roll: CB.EN.P2CYS22008

UNDERSTANDING NETWORK TRAFFIC ANALYSIS USING WIRESHARK

Date :- 22-10-2022

Aim :- To demonstrate the commands of networking and understanding network traffic analysis using wireshark

Tools Required :- Windows OS , CMD with Administrator privilege , Wireshark.

Procedure :-

PING

ping command is used to test the ability of the source computer to reach a specified destination.
The ping command operates by sending Internet Control Message Protocol (ICMP) echo requests messages to the destination and wait for the response.

a. Using ping on google.com and find IP address, TTL values, Round trip time value.

```
C:\WINDOWS\system32>ping google.com

Pinging google.com [2404:6800:4009:828::200e] with 32 bytes of data:
Reply from 2404:6800:4009:828::200e: time=93ms
Reply from 2404:6800:4009:828::200e: time=104ms
Reply from 2404:6800:4009:828::200e: time=69ms
Reply from 2404:6800:4009:828::200e: time=154ms

Ping statistics for 2404:6800:4009:828::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 69ms, Maximum = 154ms, Average = 105ms
```

1. IP address.
2. TTL value
3. Round trip time value

b. Sending 8 packets to check the output over google.com

```
C:\WINDOWS\system32>ping -n 8 google.com

Pinging google.com [2404:6800:4009:828::200e] with 32 bytes of data:
Reply from 2404:6800:4009:828::200e: time=118ms
Reply from 2404:6800:4009:828::200e: time=77ms
Reply from 2404:6800:4009:828::200e: time=80ms
Reply from 2404:6800:4009:828::200e: time=105ms
Reply from 2404:6800:4009:828::200e: time=76ms
Reply from 2404:6800:4009:828::200e: time=87ms
Reply from 2404:6800:4009:828::200e: time=88ms
Reply from 2404:6800:4009:828::200e: time=77ms

Ping statistics for 2404:6800:4009:828::200e:
    Packets: Sent = 8, Received = 8, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 76ms, Maximum = 118ms, Average = 88ms
```

-n option tells the ping command to send n no of requests so that to check the ping status of the desired no of packets.

c. Ping your local host. Explain what the purpose

```
C:\WINDOWS\system32>ping localhost

Pinging Tousif [::1] with 32 bytes of data:
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms

Ping statistics for ::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

ping localhost refers to the local machine currently making the request. localhost is useful for software testing and security purposes independent of a larger network.

TRACERT

Tracert is a network diagnostic tool used to track no of hops taken by a packet from source to destination.

It is used to determine response delays and routing loops present in a network pathway.

It also helps to locate any points of failure encountered in the pathway.

a. Try tracert over google.com

```
C:\WINDOWS\system32>tracert google.com

Tracing route to google.com [2404:6800:4009:830::200e]
over a maximum of 30 hops:

  1     3 ms     3 ms     2 ms  2409:4072:8e90:c724::9a
  2     *        *        *     Request timed out.
  3    68 ms    32 ms    38 ms  2405:200:394:eeee:20::52
  4    64 ms    42 ms    34 ms  2405:200:801:4f00::130
  5    76 ms    28 ms    52 ms  2405:200:801:4f00::133
  6    53 ms    38 ms    69 ms  2405:200:801:900::ce2
  7    65 ms    56 ms    66 ms  2001:4860:1:1::d10
  8    75 ms    44 ms    58 ms  2404:6800:8132::1
  9    93 ms    41 ms    56 ms  2001:4860:0:1::55d6
 10    71 ms    39 ms    55 ms  2001:4860:0:133f::a
 11    79 ms    74 ms    79 ms  2001:4860::9:4000:d773
 12    87 ms   106 ms   105 ms  2001:4860::9:4002:d931
 13    90 ms   133 ms    79 ms  2001:4860::1c:4000:d605
 14    81 ms    68 ms    77 ms  2001:4860:0:1::203b
 15   132 ms    98 ms    81 ms  bom12s20-in-x0e.1e100.net [2404:6800:4009:830::200e]

Trace complete.
```

b. Type tracert -d google.com

```
C:\WINDOWS\system32>tracert -d google.com

Tracing route to google.com [2404:6800:4009:830::200e]
over a maximum of 30 hops:

  1     2 ms     2 ms     4 ms  2409:4072:8e90:c724::9a
  2     *        *        *     Request timed out.
  3    53 ms    37 ms    38 ms  2405:200:394:eeee:20::52
  4    62 ms    51 ms    58 ms  2405:200:801:4f00::130
  5    72 ms    38 ms    38 ms  2405:200:801:4f00::133
  6    84 ms    63 ms    46 ms  2405:200:801:900::ce2
  7    82 ms    59 ms    59 ms  2001:4860:1:1::d10
  8   100 ms    34 ms    83 ms  2404:6800:8132::1
  9   101 ms    71 ms    60 ms  2001:4860:0:1::55d6
 10    56 ms    55 ms    53 ms  2001:4860:0:133f::a
 11   108 ms    88 ms    67 ms  2001:4860::9:4000:d773
 12   106 ms    87 ms    88 ms  2001:4860::9:4002:d931
 13   112 ms     *        *     2001:4860::1c:4000:d605
 14  1342 ms  1529 ms   879 ms  2001:4860:0:1::203b
 15   832 ms  1097 ms   974 ms  2404:6800:4009:830::200e

Trace complete.
```

1. How many hops is your machine away from google.com?

15 hops.

2. Wait for a while and execute the same command again. Is the output the same as the first time?

```
C:\WINDOWS\system32>tracert -d google.com

Tracing route to google.com [2404:6800:4009:830::200e]
over a maximum of 30 hops:

  1     3 ms     4 ms     3 ms  2409:4072:8e90:c724::9a
  2     *        *        *     Request timed out.
  3   197 ms   234 ms   204 ms  2405:200:394:eeee:20::52
  4    86 ms    90 ms    84 ms  2405:200:801:4f00::130
  5   162 ms   151 ms    69 ms  2405:200:801:4f00::133
  6   210 ms    99 ms   104 ms  2405:200:801:900::ce2
  7   120 ms     *       69 ms  2001:4860:1:1::d10
  8    49 ms    85 ms    55 ms  2404:6800:8132::1
  9    70 ms    75 ms    90 ms  2001:4860:0:1::55d6
 10   309 ms   246 ms    70 ms  2001:4860:0:133f::a
 11   170 ms   108 ms    94 ms  2001:4860::9:4000:d773
 12   126 ms    82 ms    73 ms  2001:4860::9:4002:d931
 13   269 ms   153 ms   274 ms  2001:4860::1c:4000:d605
 14    76 ms    70 ms    70 ms  2001:4860:0:1::203b
 15   161 ms   106 ms    61 ms  2404:6800:4009:830::200e

Trace complete.
```

Time values changed.

No of hops also may change because network may take several routes to the destination. Thus , the values differs everytime.

NETSTAT

a . Use netstat to display information about the routing table

-r command is used to display routing table information

```
C:\WINDOWS\system32>netstat -r
===========================================================================
Interface List
  6...08 8f c3 13 84 3c ......Realtek PCIe GbE Family Controller
 15...0a 00 27 00 00 0f ......VirtualBox Host-Only Ethernet Adapter
 16...a2 e7 0b 05 8c be ......Microsoft Wi-Fi Direct Virtual Adapter
  8...a0 e7 0b 05 8c bf ......Microsoft Wi-Fi Direct Virtual Adapter #3
  4...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 21...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
 17...a0 e7 0b 05 8c be ......Intel(R) Wi-Fi 6 AX201 160MHz
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.43.1   192.168.43.222     55
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
     192.168.38.0    255.255.255.0         On-link      192.168.38.1    291
     192.168.38.1  255.255.255.255         On-link      192.168.38.1    291
   192.168.38.255  255.255.255.255         On-link      192.168.38.1    291
     192.168.43.0    255.255.255.0         On-link    192.168.43.222    311
   192.168.43.222  255.255.255.255         On-link    192.168.43.222    311
   192.168.43.255  255.255.255.255         On-link    192.168.43.222    311
     192.168.56.0    255.255.255.0         On-link      192.168.56.1    281
     192.168.56.1  255.255.255.255         On-link      192.168.56.1    281
   192.168.56.255  255.255.255.255         On-link      192.168.56.1    281
```

```
IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 17     71 ::/0                     fe80::82ad:16ff:feca:e68c
  1    331 ::1/128                  On-link
 17     71 2409:4072:8e90:c724::/64 On-link
 17    311 2409:4072:8e90:c724:c9b:caf9:494:56fd/128
                                    On-link
 17    311 2409:4072:8e90:c724:917f:7ee5:5056:e141/128
                                    On-link
 15    281 fe80::/64                On-link
 17    311 fe80::/64                On-link
  4    291 fe80::/64                On-link
 21    291 fe80::/64                On-link
 17    311 fe80::917f:7ee5:5056:e141/128
                                    On-link
```

b. Use netstat to display about ethernet statistics.

-e is used to display the ethernet statistics.

```
C:\WINDOWS\system32>netstat -e
Interface Statistics

                           Received            Sent

Bytes                     233700960        28405192
Unicast packets              247584          141116
Non-unicast packets             224            4836
Discards                          0               0
Errors                            0               0
Unknown protocols                 0

C:\WINDOWS\system32>
```

NSLOOKUP

Name Server Lookup (NSLOOKUP) is used to get information from DNS server.
It is used to find the IP address that corresponds to a host, or the domain name that corresponds to an IP address.

a. Use nslookup to find out the internet address of the domain amrita.edu

```
C:\WINDOWS\system32>nslookup amrita.edu
Server:  prithvi.amritanet.edu
Address:  172.17.18.2

Non-authoritative answer:
Name:    amrita.edu
Addresses:  15.197.141.123
          3.33.154.67
```

15.197.141.123 and 3.33.154.67

b. What is the mail exchanger for the domain google.com.

```
C:\WINDOWS\system32>nslookup -q=mx google.com
Server:  prithvi.amritanet.edu
Address:  172.17.18.2

Non-authoritative answer:
google.com      MX preference = 10, mail exchanger = smtp.google.com

smtp.google.com internet address = 142.250.4.27
smtp.google.com internet address = 142.250.4.26
smtp.google.com internet address = 74.125.200.27
smtp.google.com internet address = 74.125.200.26
smtp.google.com internet address = 142.251.12.26
smtp.google.com AAAA IPv6 address = 2404:6800:4003:c00::1b
smtp.google.com AAAA IPv6 address = 2404:6800:4003:c11::1a
smtp.google.com AAAA IPv6 address = 2404:6800:4003:c00::1a
smtp.google.com AAAA IPv6 address = 2404:6800:4003:c06::1a
```

smtp.google.com

c. What is the name server for amrita.edu

```
C:\WINDOWS\system32>nslookup -type=ns amrita.edu
Server:  prithvi.amritanet.edu
Address:  172.17.18.2

Non-authoritative answer:
amrita.edu      nameserver = ns3.amrita.edu
amrita.edu      nameserver = ns4.amrita.edu
amrita.edu      nameserver = ns2.amrita.edu
amrita.edu      nameserver = ns1.amrita.edu

ns3.amrita.edu  internet address = 103.10.24.200
ns4.amrita.edu  internet address = 10.10.10.4
ns2.amrita.edu  internet address = 117.193.77.232
ns1.amrita.edu  internet address = 10.10.10.4
```

<u>ARP & RARP</u>

ARP stands for Address Resolution Protocol. It is a protocol that connects IP address to a fixed physical machine address which is known as Media Access Control (MAC) address.

RARP stands for Reverse Address Resolution Protocol. It retrieves logical address for a computer from the server.

a. Use arp command to find the gateway address and host systems hardware address.

```
C:\Users\TOUSIF>arp -a

Interface: 192.168.38.1 --- 0x4
  Internet Address      Physical Address      Type
  192.168.38.254        00-50-56-ee-4a-2d     dynamic
  192.168.38.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.56.1 --- 0xf
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 10.11.133.22 --- 0x11
  Internet Address      Physical Address      Type
  10.11.128.1           00-00-5e-00-01-fe     dynamic
  10.11.128.11          44-31-92-56-07-97     dynamic
```

The gateway address 192.168.38.254 and the host systems hardware address is 00-50-56-ee-4a-2d.

b. How do you find the arp entries for a particular interface?

-N flag is used to find arp entries for a particular interface.

```
C:\Users\TOUSIF>arp -aN 192.168.38.1

Interface: 192.168.38.1 --- 0x4
  Internet Address      Physical Address      Type
  192.168.38.254        00-50-56-ee-4a-2d     dynamic
  192.168.38.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\TOUSIF>
```

c. How do delete an arp entry?

-d is used to delete an arp entry.

```
C:\WINDOWS\system32>arp -d 192.168.53.134

C:\WINDOWS\system32>
```

d. How do you add an arp entry in arpcache?

-s is used to add an arp entry in arpcache

```
C:\WINDOWS\system32>arp -s 192.168.53.134 00-50-57-ea-a0-c1

C:\WINDOWS\system32>
```

<u>TCPDUMP</u>

a . Using tcpdump, get the information about the general incoming network traffic with names.

sudo tcpdump

```
tousif@TousifVM:~$ sudo tcpdump
[sudo] password for tousif:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:38:14.228409 IP 192.168.59.1.60067 > 239.255.255.250.1900: UDP, length 175
19:38:14.242208 IP TousifVM.60563 > _gateway.domain: 26693+ [1au] PTR? 250.255.255.239.in-addr.arpa. (57)
19:38:14.293217 IP _gateway.domain > TousifVM.60563: 26693 NXDomain 0/0/1 (57)
19:38:14.293377 IP TousifVM.60563 > _gateway.domain: 26693+ PTR? 250.255.255.239.in-addr.arpa. (46)
19:38:14.297661 IP _gateway.domain > TousifVM.60563: 26693 NXDomain 0/0/0 (46)
19:38:14.298301 IP TousifVM.40249 > _gateway.domain: 45155+ [1au] PTR? 1.59.168.192.in-addr.arpa. (54)
19:38:14.301875 IP _gateway.domain > TousifVM.40249: 45155 NXDomain 0/1/1 (89)
19:38:14.301923 IP TousifVM.40249 > _gateway.domain: 45155+ PTR? 1.59.168.192.in-addr.arpa. (43)
19:38:14.304598 IP _gateway.domain > TousifVM.40249: 45155 NXDomain 0/1/0 (78)
19:38:14.334628 IP TousifVM.42029 > _gateway.domain: 64177+ [1au] PTR? 2.59.168.192.in-addr.arpa. (54)
19:38:14.339470 IP _gateway.domain > TousifVM.42029: 64177 NXDomain 0/1/1 (89)
19:38:14.339548 IP TousifVM.42029 > _gateway.domain: 64177+ PTR? 2.59.168.192.in-addr.arpa. (43)
19:38:14.342233 IP _gateway.domain > TousifVM.42029: 64177 NXDomain 0/1/0 (78)
19:38:14.342584 IP TousifVM.56623 > _gateway.domain: 57689+ [1au] PTR? 128.59.168.192.in-addr.arpa. (56)
19:38:14.345046 IP _gateway.domain > TousifVM.56623: 57689 NXDomain 0/1/1 (91)
19:38:14.345096 IP TousifVM.56623 > _gateway.domain: 57689+ PTR? 128.59.168.192.in-addr.arpa. (45)
19:38:14.348392 IP _gateway.domain > TousifVM.56623: 57689 NXDomain 0/1/0 (80)
19:38:15.230899 IP 192.168.59.1.60067 > 239.255.255.250.1900: UDP, length 175
19:38:16.029663 IP6 TousifVM > ip6-allrouters: ICMP6, router solicitation, length 8
```

b. Using tcpdump, get the information about the general incoming network traffic with ip address on specific interface

```
tousif@TousifVM:~$ sudo tcpdump -i ens33
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:43:04.220333 IP TousifVM.37947 > _gateway.domain: 49845+ [1au] A? ntp.ubuntu.com. (43)
19:43:04.220813 IP TousifVM.44323 > _gateway.domain: 61188+ [1au] AAAA? ntp.ubuntu.com. (43)
19:43:04.223701 IP TousifVM.56794 > _gateway.domain: 50891+ [1au] PTR? 2.59.168.192.in-addr.arpa. (54)
19:43:04.227245 IP _gateway.domain > TousifVM.56794: 50891 NXDomain 0/1/1 (89)
19:43:04.227374 IP TousifVM.56794 > _gateway.domain: 50891+ PTR? 2.59.168.192.in-addr.arpa. (43)
19:43:04.230434 IP _gateway.domain > TousifVM.56794: 50891 NXDomain 0/1/0 (78)
19:43:04.230875 IP TousifVM.47925 > _gateway.domain: 24762+ [1au] PTR? 128.59.168.192.in-addr.arpa. (56)
19:43:04.233606 IP _gateway.domain > TousifVM.47925: 24762 NXDomain 0/1/1 (91)
19:43:04.233715 IP TousifVM.47925 > _gateway.domain: 24762+ PTR? 128.59.168.192.in-addr.arpa. (45)
19:43:04.238701 IP _gateway.domain > TousifVM.47925: 24762 NXDomain 0/1/0 (80)
19:43:04.284368 IP _gateway.domain > TousifVM.44323: 61188 3/0/1 AAAA 2620:2d:4000:1::40, AAAA 2620:2d:400
19:43:04.284410 IP _gateway.domain > TousifVM.37947: 49845 5/0/1 A 185.125.190.57, A 91.189.94.4, A 185.12
19:43:04.284821 IP TousifVM.54771 > prod-ntp-4.ntp4.ps5.canonical.com.ntp: NTPv4, Client, length 48
```

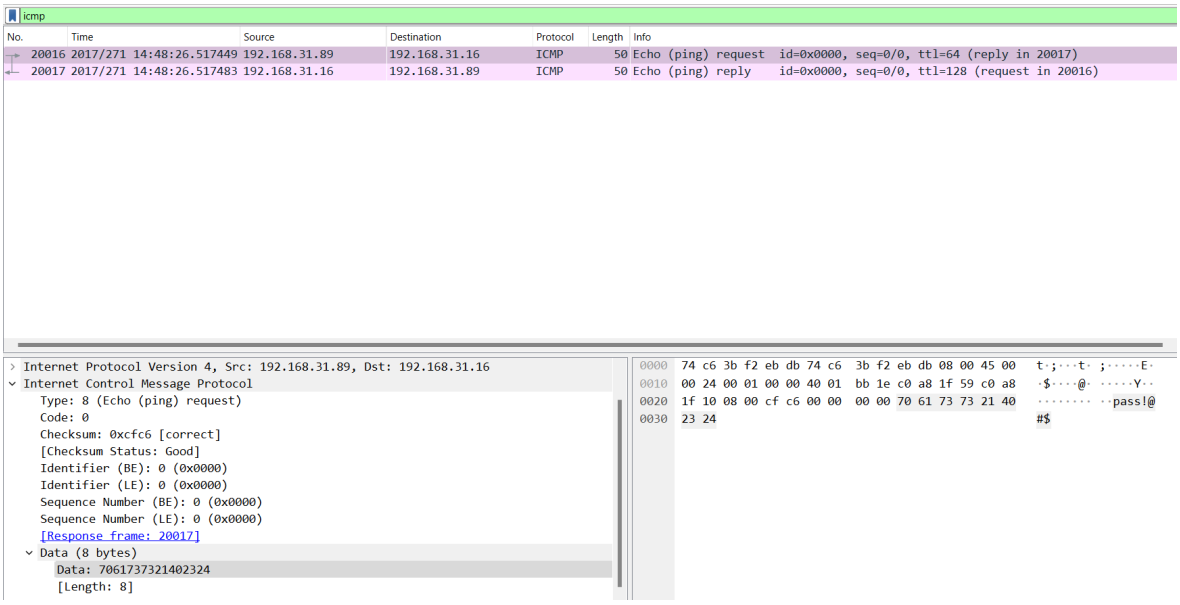
<u>WIRESHARK</u>

Using **Evidence.pcapng** as evidence

1. You, as a SOC analyst noted that someone try to send information (PING) to unknown IP address and you are suspecting some malicious information might transferred in it. Analyze the log file.

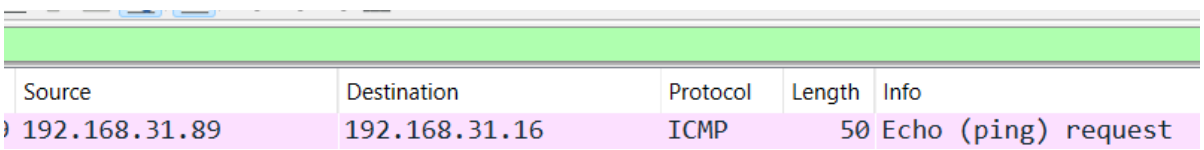
a. Find the data transferred.

As stated, found PING data of ICMP protocol.



The data is : **pass!@#$**

b. Find the source and destination IP of that log.



Source IP : **192.168.31.89**
Destination IP : **192.168.31.16**

c. Find the Data length (Bytes) and verify the checksum status on destination

Data length : **8 bytes**

Checksum status : **Good**

```
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xcfc6 [correct]
[Checksum Status: Good]
Identifier (BE): 0 (0x0000)
Identifier (LE): 0 (0x0000)
Sequence Number (BE): 0 (0x0000)
Sequence Number (LE): 0 (0x0000)
[Response frame: 20017]
Data (8 bytes)
    Data: 7061737321402324
    [Length: 8]
```

2. Now you have found that some kind of file is been downloaded by insider in unencrypted web traffic.

HTTP protocol is used to download the files. Thus , looking for HTTP files.

http

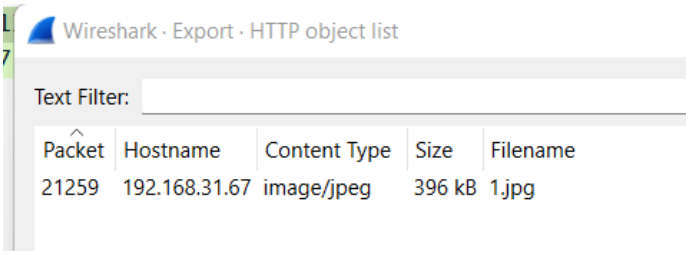
No.	Time	Source	Destination	Protocol	Length	Info
21175	2017/287 16:34:48.63788…	192.168.31.113	192.168.31.67	HTTP	209	GET /1.jpg HTTP/1.1
21259	2017/287 16:34:48.87179…	192.168.31.67	192.168.31.113	HTTP	22234	HTTP/1.1 200 OK (JPEG JFIF image)

a. Find the name and type of file.

	Info
9	GET /1.jpg HTTP/1.1
4	HTTP/1.1 200 OK (JPEG JFIF image)

Name : **1.jpg**
Type : **JPEG JFIF image**

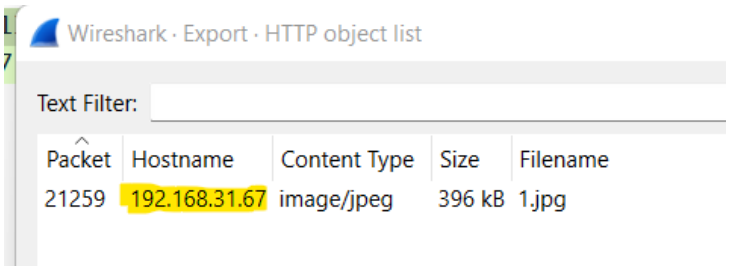
b. Export that file from that web traffic, then analyze the file for any secret information.


Wireshark · Export · HTTP object list
Text Filter:
Packet
Hostname
Content Type
Size
Filename
21259
192.168.31.67
image/jpeg
396 kB
1.jpg

The file :-

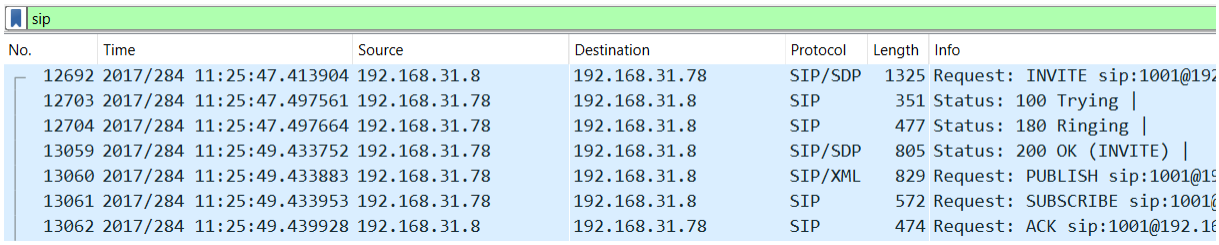

DESTINY

c. Find the hostname in which the file is stored.



3. Based upon their activities, auditing team has started investigation against them and found that the insider passed some sensitive information via call to someone. The traffic is been captured.

As we are looking for call data. SIP (Session Initiation Protocol) will be filtered.



sip

No.	Time	Source	Destination	Protocol	Length	Info
12692	2017/284 11:25:47.413904	192.168.31.8	192.168.31.78	SIP/SDP	1325	Request: INVITE sip:1001@192
12703	2017/284 11:25:47.497561	192.168.31.78	192.168.31.8	SIP	351	Status: 100 Trying |
12704	2017/284 11:25:47.497664	192.168.31.78	192.168.31.8	SIP	477	Status: 180 Ringing |
13059	2017/284 11:25:49.433752	192.168.31.78	192.168.31.8	SIP/SDP	805	Status: 200 OK (INVITE) |
13060	2017/284 11:25:49.433883	192.168.31.78	192.168.31.8	SIP/XML	829	Request: PUBLISH sip:1001@19
13061	2017/284 11:25:49.433953	192.168.31.78	192.168.31.8	SIP	572	Request: SUBSCRIBE sip:1001@
13062	2017/284 11:25:49.439928	192.168.31.8	192.168.31.78	SIP	474	Request: ACK sip:1001@192.16

a. Analyze the traffic and find those conversations and extract the sensitive information in it.

b. Find the call-ID when the status of the call is ringing.

```
From: "1002" <sip:1002@192.168.31.8>;tag=as1d95fb93
To: <sip:1001@192.168.31.78:57332;rinstance=fc3bc219541e9861;
Contact: <sip:1002@192.168.31.8:5060>
Call-ID: 01caab9b53b12efe00d3493a67ff695d@192.168.31.8:5060
CSeq: 102 INVITE
User-Agent: FPBX-2.11.0(11.13.0)
```

4.On further investigation, you have a suspect on some wireless device communications. List out the Bluetooth devices communications from this traffic and find the details about native Bluetooth adapter.

bluetooth

Packet list | Narrow & Wide | Case sensitive | Display filter

No.	Time	Source	Destination	Protocol	Length	Info
20020	2017/284 11:48:30.619695	host	controller	HCI_CMD	4	Sent Reset
20021	2017/284 11:48:32.624144	controller	host	HCI_EVT	7	Rcvd Command Complete (Reset)
20022	2017/284 11:48:32.624213	host	controller	HCI_CMD	4	Sent Read Local Supported Features
20023	2017/284 11:48:32.626822	controller	host	HCI_EVT	15	Rcvd Command Complete (Read Local Supported Features)
20024	2017/284 11:48:32.626873	host	controller	HCI_CMD	4	Sent Read Local Version Information
20025	2017/284 11:48:32.629429	controller	host	HCI_EVT	15	Rcvd Command Complete (Read Local Version Information)
20026	2017/284 11:48:32.629493	host	controller	HCI_CMD	4	Sent Read BD ADDR
20027	2017/284 11:48:32.632327	controller	host	HCI_EVT	13	Rcvd Command Complete (Read BD ADDR)
20028	2017/284 11:48:32.632398	host	controller	HCI_CMD	4	Sent Read Buffer Size
20029	2017/284 11:48:32.634779	controller	host	HCI_EVT	14	Rcvd Command Complete (Read Buffer Size)

<u>Result</u> :- Thus , network traffic analysis using wireshark is successfully done.