NAME: S.PRIYADHARSHINI

ROLL NO.: CB.EN.P2CYS22010

DATE: 22.10.2022

INTERNET PROTOCOL LAB – II

AIM:

To analyze the network traffic using Wireshark and implementing some commands in cmd.

TOOLS REQUIRED:

Wireshark, CMD.

PROCEDURE:

1. Understand PING and document it, then answer the following question:

a. Use ping on google.com and document your results on the output you received. [Find the IP address, Time to live value, and round trip time value from the results you got].

```
C:\Users\priya>ping google.com

Pinging google.com [142.250.71.46] with 32 bytes of data:
Reply from 142.250.71.46: bytes=32 time=7ms TTL=118
Reply from 142.250.71.46: bytes=32 time=7ms TTL=118
Reply from 142.250.71.46: bytes=32 time=7ms TTL=118
Reply from 142.250.71.46: bytes=32 time=7ms TTL=118

Ping statistics for 142.250.71.46:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 7ms, Average = 7ms

C:\Users\priya>
```

IP address: 142.250.71.46

TTL: 118

Round trip time value: 7ms

b. By default, ping will send 4 packets to check the details, here you have to send 8 packets to check the output over google.com. Explain what the purpose of this doing is.

To send specific number of packets the flag -n is used. The command is ping -n 8 google.com.

```
C:\Users\priya>ping -n 8 google.com

Pinging google.com [142.250.71.46] with 32 bytes of data:
Reply from 142.250.71.46: bytes=32 time=7ms TTL=118
Reply from 142.250.71.46: bytes=32 time=7ms TTL=118
Reply from 142.250.71.46: bytes=32 time=9ms TTL=118
Reply from 142.250.71.46: bytes=32 time=7ms TTL=118
Reply from 142.250.71.46: bytes=32 time=7ms TTL=118
Reply from 142.250.71.46: bytes=32 time=7ms TTL=118
Reply from 142.250.71.46: bytes=32 time=11ms TTL=118
Reply from 142.250.71.46: bytes=32 time=9ms TTL=118

Ping statistics for 142.250.71.46:
    Packets: Sent = 8, Received = 8, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 11ms, Average = 8ms

C:\Users\priya>
```

c. Ping your local host. Explain what the purpose is.

Localhost refers to the system we are working on. Pinging localhost will check whether our system protocols are active and running.

```
C:\Users\priya>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\priya>
```

2. Read the Unix manual page for traceroute OR help for tracert. Experiment with the various options.

a. Try tracert over google.com

```
C:\Users\priya>tracert google.com

Tracing route to google.com [142.250.71.46]
over a maximum of 30 hops:

  1    73 ms     5 ms     5 ms  192.168.0.1
  2     9 ms     6 ms     6 ms  10.213.0.1
  3     *        *        *     Request timed out.
  4   120 ms    99 ms   100 ms  10.200.150.30
  5     7 ms    22 ms     6 ms  72.14.242.244
  6     7 ms     7 ms     8 ms  216.239.43.137
  7    32 ms     7 ms    38 ms  142.250.233.145
  8     8 ms     6 ms    61 ms  maa03s35-in-f14.1e100.net [142.250.71.46]

Trace complete.
```

b.Type tracert -d google.com

-d flag is used to display the ip address instead of the hostnames.

```
C:\Users\priya>tracert -d google.com

Tracing route to google.com [142.250.71.46]
over a maximum of 30 hops:

  1     5 ms     4 ms     4 ms  192.168.0.1
  2     7 ms     6 ms     8 ms  10.213.0.1
  3     *        *        *     Request timed out.
  4    10 ms     6 ms    14 ms  10.200.150.30
  5     7 ms     6 ms    65 ms  72.14.242.244
  6     8 ms     7 ms    49 ms  216.239.43.137
  7     8 ms     7 ms     7 ms  142.250.233.145
  8     7 ms     6 ms   118 ms  142.250.71.46

Trace complete.
```

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

8 Hops.

2. Wait for a while and execute the same command again. Is the output the same as the first time? Observe and compare the difference and explain the reason.

The output may differ from the previous one because the packet may take a different route to reach the destination if it is the shortest distance. So, the number of hops may vary. In the output below the number of hops is same as the one above.

```
C:\Users\priya>tracert google.com

Tracing route to google.com [142.250.71.46]
over a maximum of 30 hops:

  1     5 ms     4 ms     5 ms  192.168.0.1
  2     7 ms     6 ms    40 ms  10.213.0.1
  3     *        *        *     Request timed out.
  4   137 ms    99 ms    99 ms  10.200.150.30
  5     7 ms     6 ms    69 ms  72.14.242.244
  6     8 ms     6 ms    35 ms  216.239.43.137
  7     8 ms     7 ms    65 ms  142.250.233.145
  8     8 ms     7 ms    44 ms  maa03s35-in-f14.1e100.net [142.250.71.46]

Trace complete.
```

3. You have to read about NETSTAT from the manual page or help before answering the below questions:

a.Use netstat to display information about the routing table.

```
C:\Users\priya>netstat -r
===========================================================================
Interface List
 11...0a 00 27 00 00 0b ......VirtualBox Host-Only Ethernet Adapter
  8...2a 39 26 24 12 09 ......Microsoft Wi-Fi Direct Virtual Adapter
 17...aa 39 26 05 02 01 ......Microsoft Wi-Fi Direct Virtual Adapter #2
  9...28 39 26 63 33 5b ......Realtek 8821CE Wireless LAN 802.11ac PCI-E NIC
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.0.1      192.168.0.7     50
        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
      192.168.0.0    255.255.255.0         On-link       192.168.0.7    306
      192.168.0.7  255.255.255.255         On-link       192.168.0.7    306
    192.168.0.255  255.255.255.255         On-link       192.168.0.7    306
     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
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link       192.168.0.7    306
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      192.168.56.1    281
  255.255.255.255  255.255.255.255         On-link       192.168.0.7    306
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  9    306 ::/0                    fe80::1e5f:2bff:feda:adc6
  1    331 ::1/128                 On-link
 11    281 fe80::/64               On-link
  9    306 fe80::/64               On-link
 11    281 fe80::5885:a919:6378:5fe3/128
                                   On-link
  9    306 fe80::b1a0:bdf6:6ebf:32d7/128
                                   On-link
  1    331 ff00::/8                On-link
 11    281 ff00::/8                On-link
  9    306 ff00::/8                On-link
```

b.Use netstat to display about ethernet statistics.

```
C:\Users\priya>netstat -e
Interface Statistics

                           Received            Sent

Bytes                    1935742760       159193360
Unicast packets             1711592         1058256
Non-unicast packets           20504           19568
Discards                          0               0
Errors                            0               0
Unknown protocols                 0

C:\Users\priya>
```

4. What is the purpose of nslookup ?

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

```
C:\Users\priya>nslookup google.com
Server:  183.82.243.66.actcorp.in
Address:  183.82.243.66

Non-authoritative answer:
Name:    google.com.domain.name
Address:  78.47.226.171
```

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

mail.parktons.com

```
C:\Users\priya>nslookup -q=MX google.com
Server:  183.82.243.66.actcorp.in
Address:  183.82.243.66

Non-authoritative answer:
google.com.domain.name  MX preference = 10, mail exchanger = mail.parktons.com

mail.parktons.com       internet address = 88.99.210.161
```

c. What is the name server for amrita.edu.

```
C:\Users\priya>nslookup -type=ns google.com
Server:  183.82.243.66.actcorp.in
Address:  183.82.243.66

Non-authoritative answer:
google.com.domain.name  nameserver = dns1.domain.name
google.com.domain.name  nameserver = dns2.domain.name

dns1.domain.name        internet address = 46.4.68.165
dns2.domain.name        internet address = 195.201.58.83

C:\Users\priya>
```

5. What are ARP and RARP?

ARP – Address Resolution Protocol (helps in mapping the IP address to it's respective MAC address)

RARP – Reverse Address Resolution Protocol (helps in mapping the MAC address to it's respective IP address)

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

the gateway address = 192.168.0.1

host system hardware address = 1c-5f-2b-da-ad-c6

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

Interface: 192.168.0.7 --- 0x9
  Internet Address      Physical Address      Type
  192.168.0.1           1c-5f-2b-da-ad-c6     dynamic
  192.168.0.2           7c-27-bc-8d-92-eb     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.250           01-00-5e-00-00-fa     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
  239.255.255.251       01-00-5e-7f-ff-fb     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.56.1 --- 0xb
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.250           01-00-5e-00-00-fa     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
  239.255.255.251       01-00-5e-7f-ff-fb     static

C:\Users\priya>
```

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

To find the arp entries for a particular interface -n flag is used.

```
C:\Users\priya>arp -a -n 192.168.0.7

Interface: 192.168.0.7 --- 0x9
  Internet Address      Physical Address      Type
  192.168.0.1           1c-5f-2b-da-ad-c6     dynamic
  192.168.0.2           7c-27-bc-8d-92-eb     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.250           01-00-5e-00-00-fa     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
  239.255.255.251       01-00-5e-7f-ff-fb     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

c. How to delete an arp entry?

To delete an arp entry -d flag is used followed by the specific ip address to be deleted.

```
C:\Users\priya>arp -d 192.168.0.7
The ARP entry deletion failed: The requested operation requires elevation.
```

d. How do you add and arp entry in arp cache?

To add an entry in arp cache -s flag is used followed by the ip address and mac address.

```
C:\Users\priya>arp -s 192.168.43.160 00-aa-00-62-c6-09
The ARP entry addition failed: The requested operation requires elevation.
```

6. Read about TCPDUMP tool.

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

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

7. Use Wireshark to solve the below scenarios:

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.

To find the data transferred in display filter ICMP is used. The data transferred is pass!@#$.

```
0000  74 c6 3b f2 eb db 74 c6  3b f2 eb db 08 00 45 00   t·;···t· ;·····E·
0010  00 24 00 01 00 00 40 01  bb 1e c0 a8 1f 59 c0 a8   ·$····@· ·····Y··
0020  1f 10 08 00 cf c6 00 00  00 00 70 61 73 73 21 40   ···••••• ••pass!@
0030  23 24                                             #$
```

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

Source IP address : 192.168.31.89

Destination IP address : 192.168.31.89

Source	Destination
192.168.31.89	192.168.31.16
192.168.31.16	192.168.31.89

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

```
Data (8 bytes)
    Data: 7061737321402324
    [Length: 8]
```

```
Internet Protocol Version 4, Src: 192.168.31.89, Dst: 192.168.31.16
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 36
   Identification: 0x0001 (1)
 > 000. .... = Flags: 0x0
   ...0 0000 0000 0000 = Fragment Offset: 0
   Time to Live: 64
   Protocol: ICMP (1)
   Header Checksum: 0xbb1e [validation disabled]
   [Header checksum status: Unverified]
   Source Address: 192.168.31.89
   Destination Address: 192.168.31.16
```

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

Hypertext Transfer Protocol	0.0	2	6.8	397343	2	1	143	0	2
JPEG File Interchange Format	0.0	1	6.8	396909	2	1	396909	2	1
Data	0.2	44	1.1	61354	0	44	61354	0	44

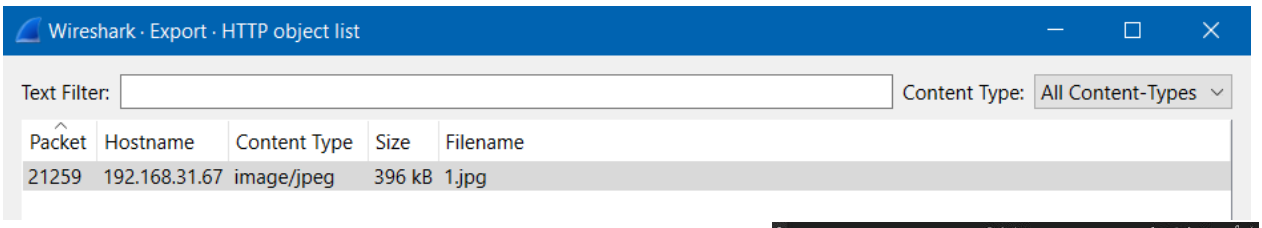
No.	Time	Source port	Source	Destination	Destn port	Protocol	Length	Info
21175	2017/287 16:34:48.63788…	59380	192.168.31.113	192.168.31.67	80	HTTP	209	GET /1.jpg HTTP/1.1
21259	2017/287 16:34:48.87179…	80	192.168.31.67	192.168.31.113	59380	HTTP	22234	HTTP/1.1 200 OK (JPEG JFIF image)

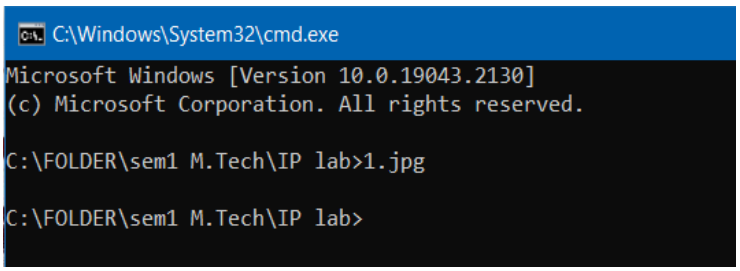
a.Find the name and type of file.

Name: 1

Type: .jpg file

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





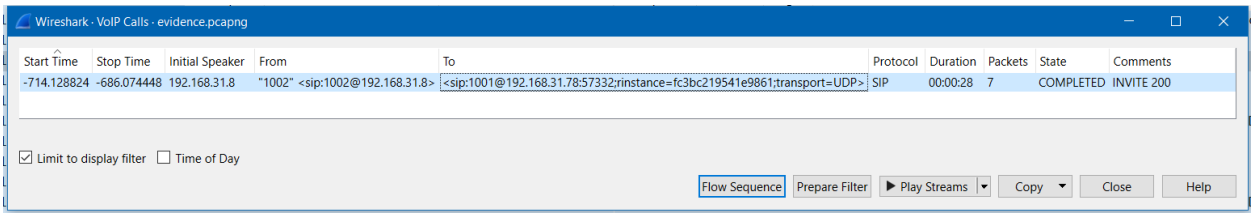
c. Find the hostname in which the file is stored.

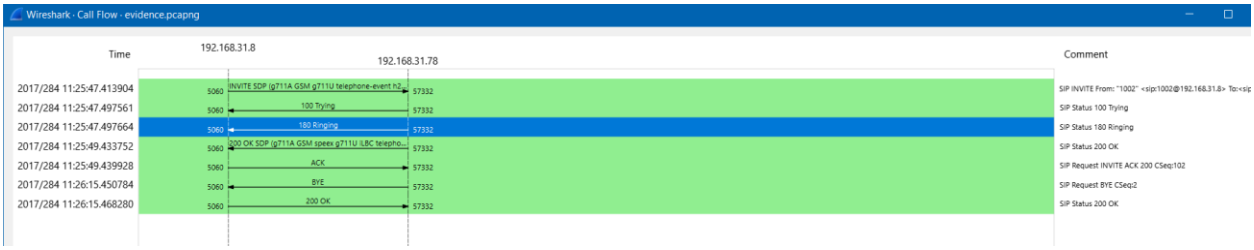
Hostname = 192.168.31.113

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.

SIP – Session Initiation Protocol (supports voice calls by managing the actual elements of a call)

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.

```
12692 2017/284 11:25:47.413904    5060 192.168.31.8    192.168.31.78    57332 SIP/SDP  1325 Request: INVITE sip:1001@192.168.31.78:57332;rinstan
12703 2017/284 11:25:47.497561   57332 192.168.31.78   192.168.31.8      5060 SIP       351 Status: 100 Trying |
12704 2017/284 11:25:47.497664   57332 192.168.31.78   192.168.31.8      5060 SIP       477 Status: 180 Ringing |
13059 2017/284 11:25:49.433752   57332 192.168.31.78   192.168.31.8      5060 SIP/SDP   805 Status: 200 OK (INVITE) |
```

```
INVITE sip:1001@192.168.31.78:57332;rinstance=fc3bc219541e9861;transport=UDP SIP/2.0
Via: SIP/2.0/UDP 192.168.31.8:5060;branch=z9hG4bK30e63862
Max-Forwards: 70
From: "1002" <sip:1002@192.168.31.8>;tag=as1d95fb93
To: <sip:1001@192.168.31.78:57332;rinstance=fc3bc219541e9861;transport=UDP>
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)
Date: Tue, 10 Oct 2017 16:25:46 GMT
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH, MESSAGE
Supported: replaces, timer
Content-Type: application/sdp
Content-Length: 627
```

```
Call-ID: 01caab9b53b12efe00d3493a67ff695d@192.168.31.8:5060
```

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.

a.Analyze the captured WPA handshake from this traffic and report in detail about it to your administrator.

b. Geo locate all the endpoint of wireless devices.

c. Analyze the protocol level information transfer between wireless devices

RESULT:

The commands like ping, tracert, nslookup, netstat were implemented and the network traffic was analyzed successfully using Wireshark.