# Assignment #4: Lab on PCAP Analysis (4th Jan 2021)

In this assignment, we will complete our work with reading and reviewing PCAPs as it is essential for a security analyst to understand how to do this and to be very familiar with Wireshark. Additionally, students will set up a honeypot in their Kali Linux installation.

## Part #1

Situation: A Very Special One

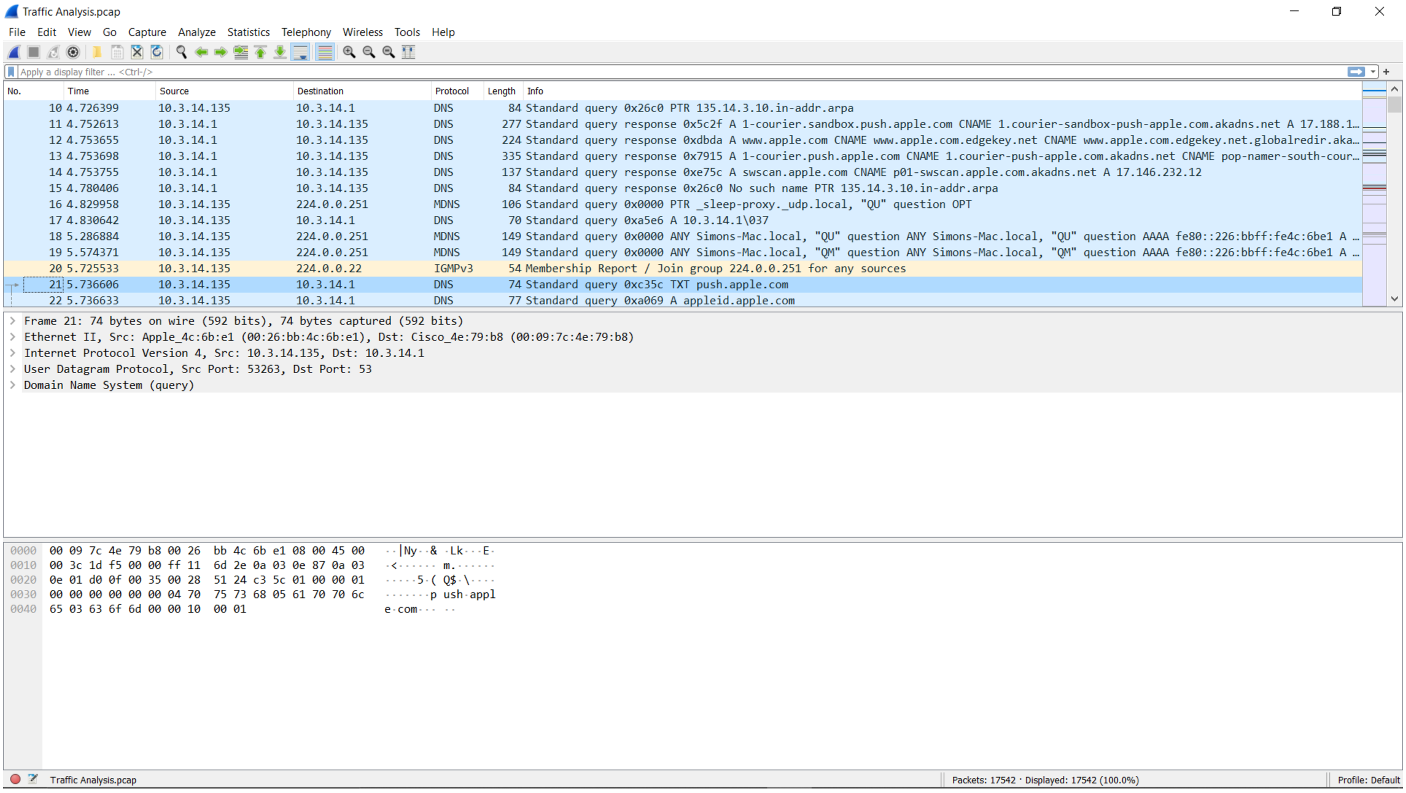
Students should:

1. Download this **PCAP file from Classwork**.

Task Done Till now:

I have downloaded wireshark in my windows and also downloaded pcap file from the classroom.

Opening PCAP file in wireshark



Traffic Analysis.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time      Source        Destination  Protocol Length Info
  10 4.726399  10.3.14.135   10.3.14.1    DNS       84 Standard query 0x26c0 PTR 135.14.3.10.in-addr.arpa
  11 4.752613  10.3.14.1     10.3.14.135  DNS      277 Standard query response 0x5c2f A 1-courier.sandbox.push.apple.com CNAME 1.courier-sandbox-push-apple.com.akadns.net A 17.188.1…
  12 4.753655  10.3.14.1     10.3.14.135  DNS      224 Standard query response 0xdbda A www.apple.com CNAME www.apple.com.edgekey.net CNAME www.apple.com.edgekey.net.globalredir.aka…
  13 4.753698  10.3.14.1     10.3.14.135  DNS      335 Standard query response 0x7915 A 1-courier.push.apple.com CNAME 1.courier-push-apple.com.akadns.net CNAME pop-namer-south-cour…
  14 4.753755  10.3.14.1     10.3.14.135  DNS      137 Standard query response 0xe75c A swscan.apple.com CNAME p01-swscan.apple.com.akadns.net A 17.146.232.12
  15 4.780406  10.3.14.1     10.3.14.135  DNS       84 Standard query response 0x26c0 No such name PTR 135.14.3.10.in-addr.arpa
  16 4.829958  10.3.14.135   224.0.0.251  MDNS     106 Standard query 0x0000 PTR _sleep-proxy._udp.local, "QU" question OPT
  17 4.830642  10.3.14.135   10.3.14.1    DNS       70 Standard query 0xa5e6 A 10.3.14.1\037
  18 5.286884  10.3.14.135   224.0.0.251  MDNS     149 Standard query 0x0000 ANY Simons-Mac.local, "QU" question ANY Simons-Mac.local, "QU" question AAAA fe80::226:bbff:fe4c:6be1 A …
  19 5.574371  10.3.14.135   224.0.0.251  MDNS     149 Standard query 0x0000 ANY Simons-Mac.local, "QM" question ANY Simons-Mac.local, "QM" question AAAA fe80::226:bbff:fe4c:6be1 A …
  20 5.725533  10.3.14.135   224.0.0.22   IGMPv3    54 Membership Report / Join group 224.0.0.251 for any sources
  21 5.736606  10.3.14.135   10.3.14.1    DNS       74 Standard query 0xc35c TXT push.apple.com
  22 5.736633  10.3.14.135   10.3.14.1    DNS       77 Standard query 0xa069 A appleid.apple.com
```

```
> Frame 21: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: Apple_4c:6b:e1 (00:26:bb:4c:6b:e1), Dst: Cisco_4e:79:b8 (00:09:7c:4e:79:b8)
> Internet Protocol Version 4, Src: 10.3.14.135, Dst: 10.3.14.1
> User Datagram Protocol, Src Port: 53263, Dst Port: 53
> Domain Name System (query)
```

```
0000  00 09 7c 4e 79 b8 00 26  bb 4c 6b e1 08 00 45 00   ··|Ny··& ·Lk···E·
0010  00 3c 1d f5 00 00 ff 11  6d 2e 0a 03 0e 87 0a 03   ·<······ m.······
0020  0e 01 d0 0f 00 35 00 28  51 24 c3 5c 01 00 00 01   ·····5·( Q$·\····
0030  00 00 00 00 00 00 04 70  75 73 68 05 61 70 70 6c   ·······p ush·appl
0040  65 03 63 6f 6d 00 00 10  00 01                     e·com··· ··
```

Traffic Analysis.pcap | Packets: 17542 · Displayed: 17542 (100.0%) | Profile: Default

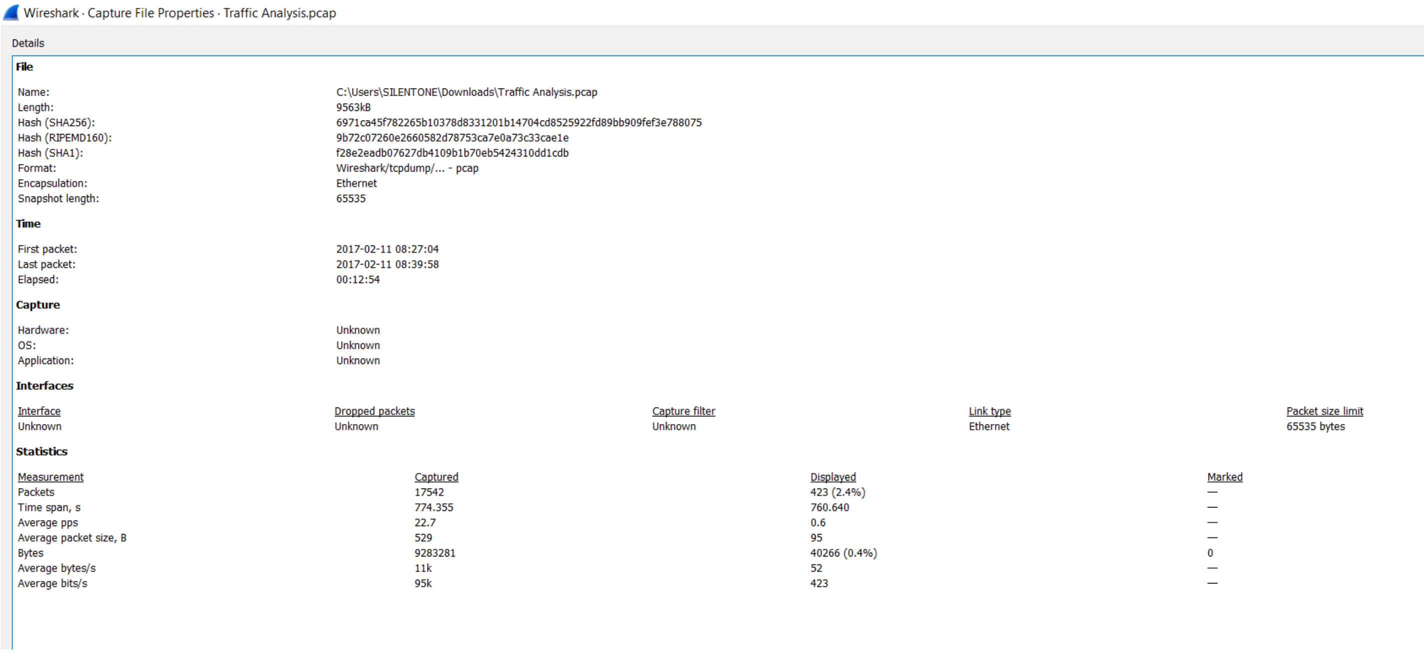
Complete a 1 page reflection for Part #1. Given these sample incident reports, write about what you learned, what you have questions about, what you researched as part of this review, and anything else you feel is relevant. Later in the course, you will be asked to complete an incident report on a given PCAP but this project is meant to mature the exercise of packet analysis and incident reporting.

2. Review the sample analysis discussing these questions:

i) Document the date, start time and end time of the pcap in UTC (GMT). ·

Ans: Date:2017-02-11 Start Time: 08:27:04 UTC End Time: 08:39:58 UTC

Steps: Statistics → Capture File Properties



Wireshark · Capture File Properties · Traffic Analysis.pcap

```
Details
File
Name:                    C:\Users\SILENTONE\Downloads\Traffic Analysis.pcap
Length:                  9563kB
Hash (SHA256):           6971ca45f782265b10378d8331201b14704cd8525922fd89bb909fef3e788075
Hash (RIPEMD160):        9b72c07260e2660582d78753ca7e0a73c33cae1e
Hash (SHA1):             f28e2eadb07627db4109b1b70eb5424310dd1cdb
Format:                  Wireshark/tcpdump/... - pcap
Encapsulation:           Ethernet
Snapshot length:         65535

Time
First packet:            2017-02-11 08:27:04
Last packet:             2017-02-11 08:39:58
Elapsed:                 00:12:54

Capture
Hardware:                Unknown
OS:                      Unknown
Application:             Unknown

Interfaces
Interface        Dropped packets     Capture filter      Link type     Packet size limit
Unknown          Unknown             Unknown             Ethernet      65535 bytes

Statistics
Measurement              Captured       Displayed       Marked
Packets                  17542          423 (2.4%)      —
Time span, s             774.355        760.640         —
Average pps              22.7           0.6             —
Average packet size, B   529            95              —
Bytes                    9283281        40266 (0.4%)    0
Average bytes/s          11k            52              —
Average bits/s           95k            423             —
```

Fig. Properties of pcap file

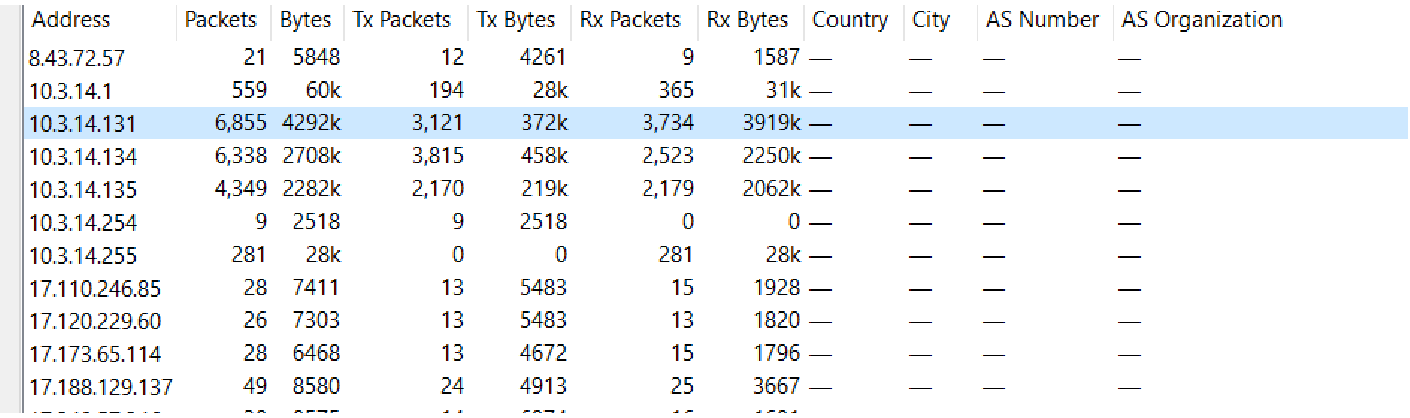
ii) Document the IP address of the three hosts in the pcap.

Ans: i) 10.3.14.131 ii) 10.3.14.134 iii) 10.3.14.135

Step: Statistics → Endpoints → IPv4

When looking into the source maximum transactions are found with the IP 10.3.14. Also we can observe that when source is not 10.3.14 then its destination is this. Hence we can say that 10.3.14 is the starting ip of the host.

There are 5 ip addresses in the IPv4 sections but out of those we know that 255 is used for the broadcasting and 254 for DHCP traffic. Hence remaining 3 are the required IP addresses.

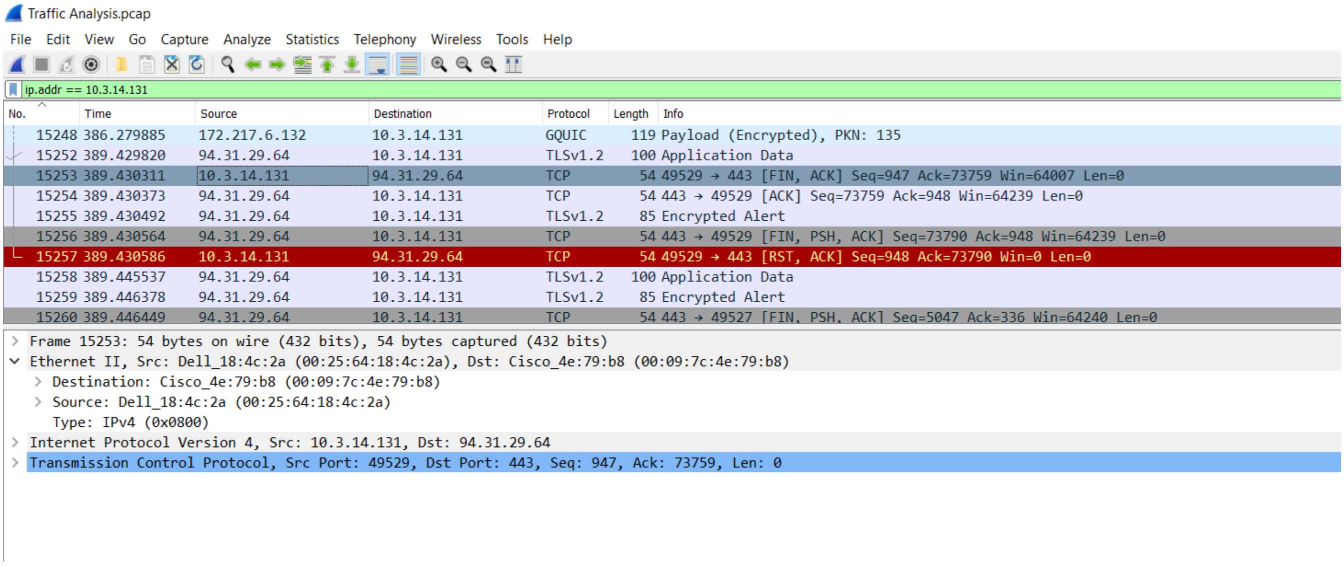


| Address | Packets | Bytes | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes | Country | City | AS Number | AS Organization |
|---|---|---|---|---|---|---|---|---|---|---|
| 8.43.72.57 | 21 | 5848 | 12 | 4261 | 9 | 1587 | — | — | — | — |
| 10.3.14.1 | 559 | 60k | 194 | 28k | 365 | 31k | — | — | — | — |
| 10.3.14.131 | 6,855 | 4292k | 3,121 | 372k | 3,734 | 3919k | — | — | — | — |
| 10.3.14.134 | 6,338 | 2708k | 3,815 | 458k | 2,523 | 2250k | — | — | — | — |
| 10.3.14.135 | 4,349 | 2282k | 2,170 | 219k | 2,179 | 2062k | — | — | — | — |
| 10.3.14.254 | 9 | 2518 | 9 | 2518 | 0 | 0 | — | — | — | — |
| 10.3.14.255 | 281 | 28k | 0 | 0 | 281 | 28k | — | — | — | — |
| 17.110.246.85 | 28 | 7411 | 13 | 5483 | 15 | 1928 | — | — | — | — |
| 17.120.229.60 | 26 | 7303 | 13 | 5483 | 13 | 1820 | — | — | — | — |
| 17.173.65.114 | 28 | 6468 | 13 | 4672 | 15 | 1796 | — | — | — | — |
| 17.188.129.137 | 49 | 8580 | 24 | 4913 | 25 | 3667 | — | — | — | — |

Fig.: IPv4 address of Endpoints

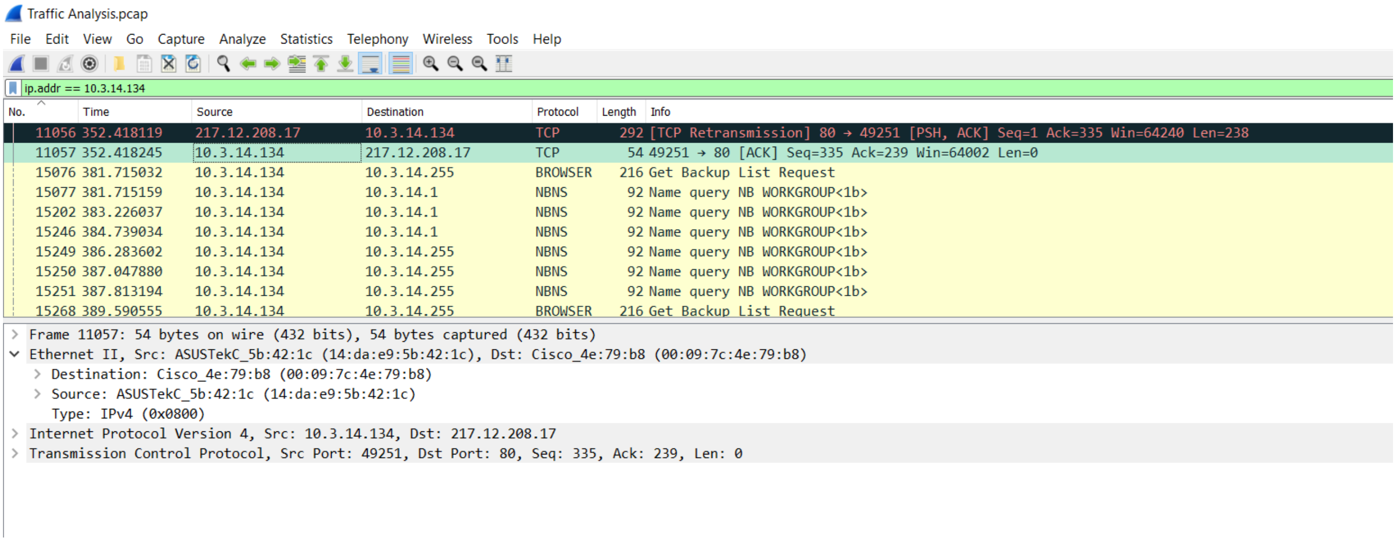
## iii) Document the mac address of the three hosts in the pcap.

Ans: MAC Address of 10.3.14.131 is 00:25:64:18:4c:2a
MAC Address of 10.3.14.134 is 14:da:e9:5b:42:1c
MAC Address of 10.3.14.135 is 00:26:bb:4c:6b:e1


Traffic Analysis.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

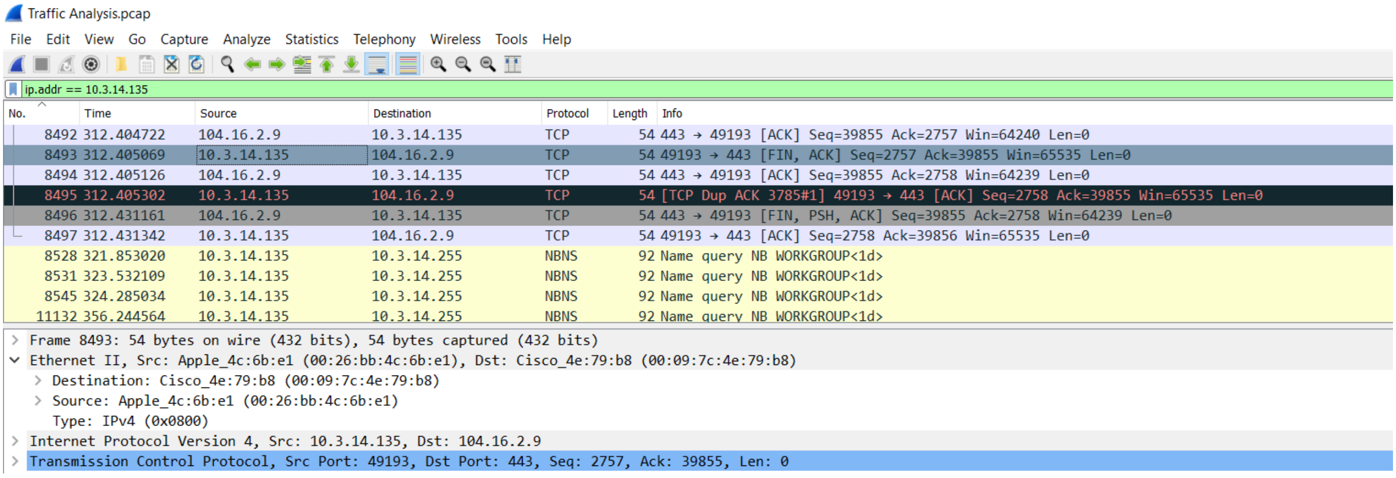
```
ip.addr == 10.3.14.131

No.    Time        Source         Destination    Protocol  Length Info
15248 386.279885  172.217.6.132  10.3.14.131    GQUIC     119 Payload (Encrypted), PKN: 135
15252 389.429820  94.31.29.64    10.3.14.131    TLSv1.2   100 Application Data
15253 389.430311  10.3.14.131    94.31.29.64    TCP        54 49529 → 443 [FIN, ACK] Seq=947 Ack=73759 Win=64007 Len=0
15254 389.430373  94.31.29.64    10.3.14.131    TCP        54 443 → 49529 [ACK] Seq=73759 Ack=948 Win=64239 Len=0
15255 389.430492  94.31.29.64    10.3.14.131    TLSv1.2    85 Encrypted Alert
15256 389.430564  94.31.29.64    10.3.14.131    TCP        54 443 → 49529 [FIN, PSH, ACK] Seq=73790 Ack=948 Win=64239 Len=0
15257 389.430586  10.3.14.131    94.31.29.64    TCP        54 49529 → 443 [RST, ACK] Seq=948 Ack=73790 Win=0 Len=0
15258 389.445537  94.31.29.64    10.3.14.131    TLSv1.2   100 Application Data
15259 389.446378  94.31.29.64    10.3.14.131    TLSv1.2    85 Encrypted Alert
15260 389.446449  94.31.29.64    10.3.14.131    TCP        54 443 → 49527 [FIN, PSH, ACK] Seq=5047 Ack=336 Win=64240 Len=0

> Frame 15253: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
v Ethernet II, Src: Dell_18:4c:2a (00:25:64:18:4c:2a), Dst: Cisco_4e:79:b8 (00:09:7c:4e:79:b8)
  > Destination: Cisco_4e:79:b8 (00:09:7c:4e:79:b8)
  > Source: Dell_18:4c:2a (00:25:64:18:4c:2a)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 10.3.14.131, Dst: 94.31.29.64
> Transmission Control Protocol, Src Port: 49529, Dst Port: 443, Seq: 947, Ack: 73759, Len: 0
```

Fig. Mac Address for 10.3.14.131


Traffic Analysis.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 10.3.14.134

No.    Time        Source         Destination    Protocol  Length Info
11056 352.418119  217.12.208.17  10.3.14.134    TCP       292 [TCP Retransmission] 80 → 49251 [PSH, ACK] Seq=1 Ack=335 Win=64240 Len=238
11057 352.418245  10.3.14.134    217.12.208.17  TCP        54 49251 → 80 [ACK] Seq=335 Ack=239 Win=64002 Len=0
15076 381.715032  10.3.14.134    10.3.14.255    BROWSER   216 Get Backup List Request
15077 381.715159  10.3.14.134    10.3.14.1      NBNS       92 Name query NB WORKGROUP<1b>
15202 383.226037  10.3.14.134    10.3.14.1      NBNS       92 Name query NB WORKGROUP<1b>
15246 384.739034  10.3.14.134    10.3.14.1      NBNS       92 Name query NB WORKGROUP<1b>
15249 386.283602  10.3.14.134    10.3.14.255    NBNS       92 Name query NB WORKGROUP<1b>
15250 387.047880  10.3.14.134    10.3.14.255    NBNS       92 Name query NB WORKGROUP<1b>
15251 387.813194  10.3.14.134    10.3.14.255    NBNS       92 Name query NB WORKGROUP<1b>
15268 389.590555  10.3.14.134    10.3.14.255    BROWSER   216 Get Backup List Request

> Frame 11057: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
v Ethernet II, Src: ASUSTekC_5b:42:1c (14:da:e9:5b:42:1c), Dst: Cisco_4e:79:b8 (00:09:7c:4e:79:b8)
  > Destination: Cisco_4e:79:b8 (00:09:7c:4e:79:b8)
  > Source: ASUSTekC_5b:42:1c (14:da:e9:5b:42:1c)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 10.3.14.134, Dst: 217.12.208.17
> Transmission Control Protocol, Src Port: 49251, Dst Port: 80, Seq: 335, Ack: 239, Len: 0
```

Fig. Mac Address for 10.3.14.134

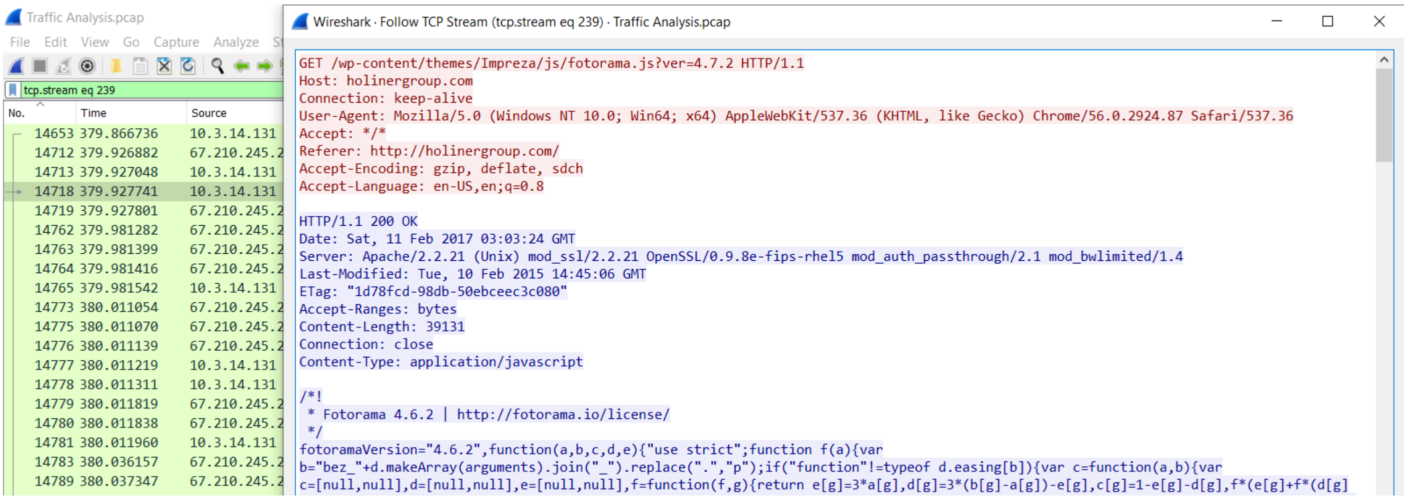

Traffic Analysis.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 10.3.14.135

No.    Time        Source         Destination    Protocol  Length Info
 8492 312.404722  104.16.2.9     10.3.14.135    TCP        54 443 → 49193 [ACK] Seq=39855 Ack=2757 Win=64240 Len=0
 8493 312.405069  10.3.14.135    104.16.2.9     TCP        54 49193 → 443 [FIN, ACK] Seq=2757 Ack=39855 Win=65535 Len=0
 8494 312.405126  104.16.2.9     10.3.14.135    TCP        54 443 → 49193 [ACK] Seq=39855 Ack=2758 Win=64239 Len=0
 8495 312.405302  10.3.14.135    104.16.2.9     TCP        54 [TCP Dup ACK 3785#1] 49193 → 443 [ACK] Seq=2758 Ack=39855 Win=65535 Len=0
 8496 312.431161  104.16.2.9     10.3.14.135    TCP        54 443 → 49193 [FIN, PSH, ACK] Seq=39855 Ack=2758 Win=64239 Len=0
 8497 312.431342  10.3.14.135    104.16.2.9     TCP        54 49193 → 443 [ACK] Seq=2758 Ack=39856 Win=65535 Len=0
 8528 321.853020  10.3.14.135    10.3.14.255    NBNS       92 Name query NB WORKGROUP<1d>
 8531 323.532109  10.3.14.135    10.3.14.255    NBNS       92 Name query NB WORKGROUP<1d>
 8545 324.285034  10.3.14.135    10.3.14.255    NBNS       92 Name query NB WORKGROUP<1d>
11132 356.244564  10.3.14.135    10.3.14.255    NBNS       92 Name query NB WORKGROUP<1d>

> Frame 8493: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
v Ethernet II, Src: Apple_4c:6b:e1 (00:26:bb:4c:6b:e1), Dst: Cisco_4e:79:b8 (00:09:7c:4e:79:b8)
  > Destination: Cisco_4e:79:b8 (00:09:7c:4e:79:b8)
  > Source: Apple_4c:6b:e1 (00:26:bb:4c:6b:e1)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 10.3.14.135, Dst: 104.16.2.9
> Transmission Control Protocol, Src Port: 49193, Dst Port: 443, Seq: 2757, Ack: 39855, Len: 0
```

Fig. Mac Address for 10.3.14.135

iv)Document the type of computer (Windows,Mac,Android, etc) for each of the three hosts in the pcap.

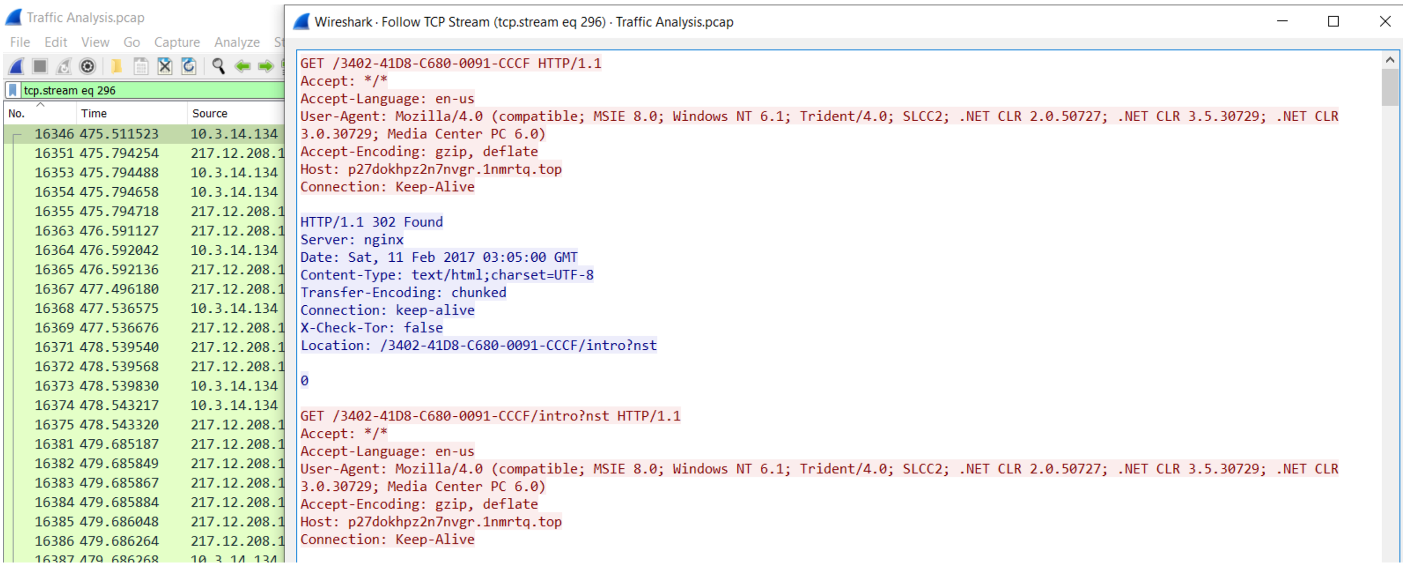
Ans: Type of Computer of 10.3.14.131 is Mozilla 5 running on Windows 10.0
Type of Computer of 10.3.14.134 is Mozilla 4 running on Windows 6.1
Type of Computer of 10.3.14.135 is Apple computer running OS X.


Traffic Analysis.pcap
File Edit View Go Capture Analyze S
tcp.stream eq 239
Wireshark · Follow TCP Stream (tcp.stream eq 239) · Traffic Analysis.pcap

```
No.   Time       Source
14653 379.866736 10.3.14.131
14712 379.926882 67.210.245.2
14713 379.927048 10.3.14.131
14718 379.927741 10.3.14.131
14719 379.927801 67.210.245.2
14762 379.981282 67.210.245.2
14763 379.981399 67.210.245.2
14764 379.981416 67.210.245.2
14765 379.981542 10.3.14.131
14773 380.011054 67.210.245.2
14775 380.011070 67.210.245.2
14776 380.011139 67.210.245.2
14777 380.011219 10.3.14.131
14778 380.011311 10.3.14.131
14779 380.011819 67.210.245.2
14780 380.011838 67.210.245.2
14781 380.011960 10.3.14.131
14783 380.036157 67.210.245.2
14789 380.037347 67.210.245.2
```

```
GET /wp-content/themes/Impreza/js/fotorama.js?ver=4.7.2 HTTP/1.1
Host: holinergroup.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
Accept: */*
Referer: http://holinergroup.com/
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8

HTTP/1.1 200 OK
Date: Sat, 11 Feb 2017 03:03:24 GMT
Server: Apache/2.2.21 (Unix) mod_ssl/2.2.21 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4
Last-Modified: Tue, 10 Feb 2015 14:45:06 GMT
ETag: "1d78fcd-98db-50ebceec3c080"
Accept-Ranges: bytes
Content-Length: 39131
Connection: close
Content-Type: application/javascript

/*!
 * Fotorama 4.6.2 | http://fotorama.io/license/
 */
fotoramaVersion="4.6.2",function(a,b,c,d,e){"use strict";function f(a){var
b="bez_"+d.makeArray(arguments).join("_").replace(".","p");if("function"!=typeof d.easing[b]){var c=function(a,b){var
c=[null,null],d=[null,null],e=[null,null],f=function(f,g){return e[g]=3*a[g],d[g]=3*(b[g]-a[g])-e[g],c[g]=1-e[g]-d[g],f*(e[g]+f*(d[g]
```

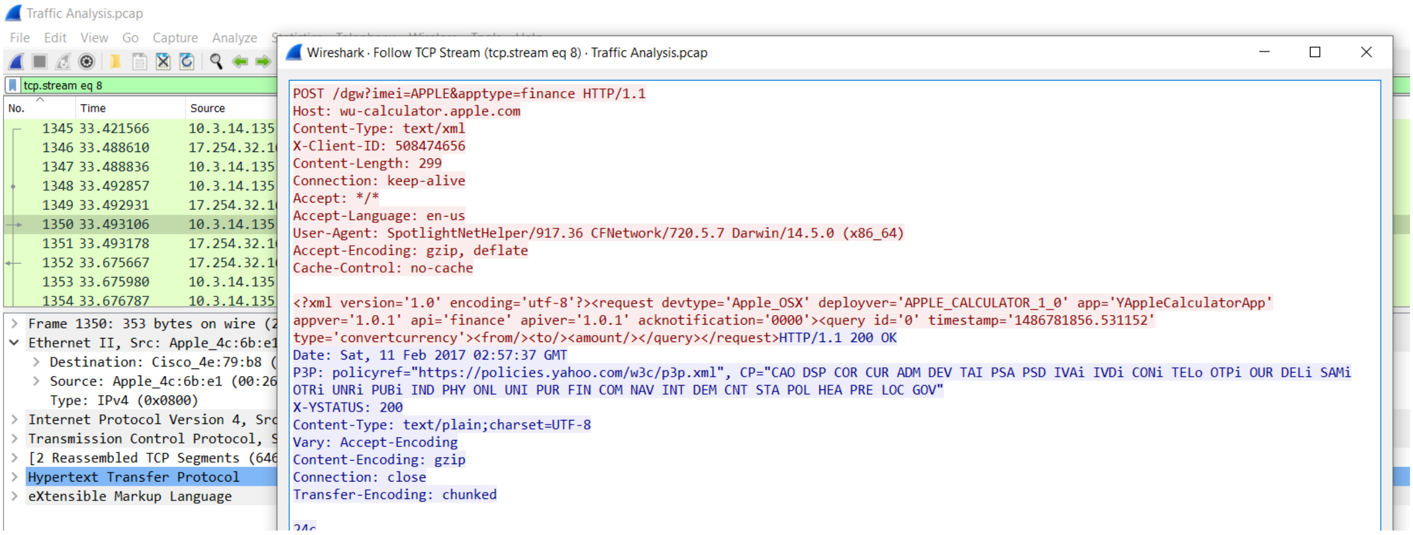
Fig. Mac Address for 10.3.14.131


Traffic Analysis.pcap
File Edit View Go Capture Analyze S
tcp.stream eq 296
Wireshark · Follow TCP Stream (tcp.stream eq 296) · Traffic Analysis.pcap

```
No.   Time       Source
16346 475.511523 10.3.14.134
16351 475.794254 217.12.208.1
16353 475.794488 10.3.14.134
16354 475.794658 10.3.14.134
16355 475.794718 217.12.208.1
16363 476.591127 217.12.208.1
16364 476.592042 10.3.14.134
16365 476.592136 217.12.208.1
16367 477.496180 217.12.208.1
16368 477.536575 10.3.14.134
16369 477.536676 217.12.208.1
16371 478.539540 217.12.208.1
16372 478.539568 217.12.208.1
16373 478.539830 10.3.14.134
16374 478.543217 10.3.14.134
16375 478.543320 217.12.208.1
16381 479.685187 217.12.208.1
16382 479.685849 217.12.208.1
16383 479.685867 217.12.208.1
16384 479.685884 217.12.208.1
16385 479.686048 217.12.208.1
16386 479.686264 217.12.208.1
16387 479.686268 10.3.14.134
```

```
GET /3402-41D8-C680-0091-CCCF HTTP/1.1
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR
3.0.30729; Media Center PC 6.0)
Accept-Encoding: gzip, deflate
Host: p27dokhpz2n7nvgr.1nmrtq.top
Connection: Keep-Alive

HTTP/1.1 302 Found
Server: nginx
Date: Sat, 11 Feb 2017 03:05:00 GMT
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Check-Tor: false
Location: /3402-41D8-C680-0091-CCCF/intro?nst

0

GET /3402-41D8-C680-0091-CCCF/intro?nst HTTP/1.1
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR
3.0.30729; Media Center PC 6.0)
Accept-Encoding: gzip, deflate
Host: p27dokhpz2n7nvgr.1nmrtq.top
Connection: Keep-Alive
```

Fig. Mac Address for 10.3.14.134


Traffic Analysis.pcap
File Edit View Go Capture Analyze S
tcp.stream eq 8
Wireshark · Follow TCP Stream (tcp.stream eq 8) · Traffic Analysis.pcap

```
No.  Time      Source
1345 33.421566 10.3.14.135
1346 33.488610 17.254.32.1
1347 33.488836 10.3.14.135
1348 33.492857 10.3.14.135
1349 33.492931 17.254.32.1
1350 33.493106 10.3.14.135
1351 33.493178 17.254.32.1
1352 33.675667 17.254.32.1
1353 33.675980 10.3.14.135
1354 33.676787 10.3.14.135
```

```
> Frame 1350: 353 bytes on wire (2
v Ethernet II, Src: Apple_4c:6b:e1
  > Destination: Cisco_4e:79:b8 (
  > Source: Apple_4c:6b:e1 (00:26
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src
> Transmission Control Protocol, S
> [2 Reassembled TCP Segments (646
> Hypertext Transfer Protocol
> eXtensible Markup Language
```

```
POST /dgw?imei=APPLE&apptype=finance HTTP/1.1
Host: wu-calculator.apple.com
Content-Type: text/xml
X-Client-ID: 508474656
Content-Length: 299
Connection: keep-alive
Accept: */*
Accept-Language: en-us
User-Agent: SpotlightNetHelper/917.36 CFNetwork/720.5.7 Darwin/14.5.0 (x86_64)
Accept-Encoding: gzip, deflate
Cache-Control: no-cache

<?xml version='1.0' encoding='utf-8'?><request devtype='Apple_OSX' deployver='APPLE_CALCULATOR_1_0' app='YAppleCalculatorApp'
appver='1.0.1' api='finance' apiver='1.0.1' acknotification='0000'><query id='0' timestamp='1486781856.531152'
type='convertcurrency'><from/><to/><amount/></query></request>HTTP/1.1 200 OK
Date: Sat, 11 Feb 2017 02:57:37 GMT
P3P: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELi SAMi
OTRi UNRi PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV"
X-YSTATUS: 200
Content-Type: text/plain;charset=UTF-8
Vary: Accept-Encoding
Content-Encoding: gzip
Connection: close
Transfer-Encoding: chunked

24c
```

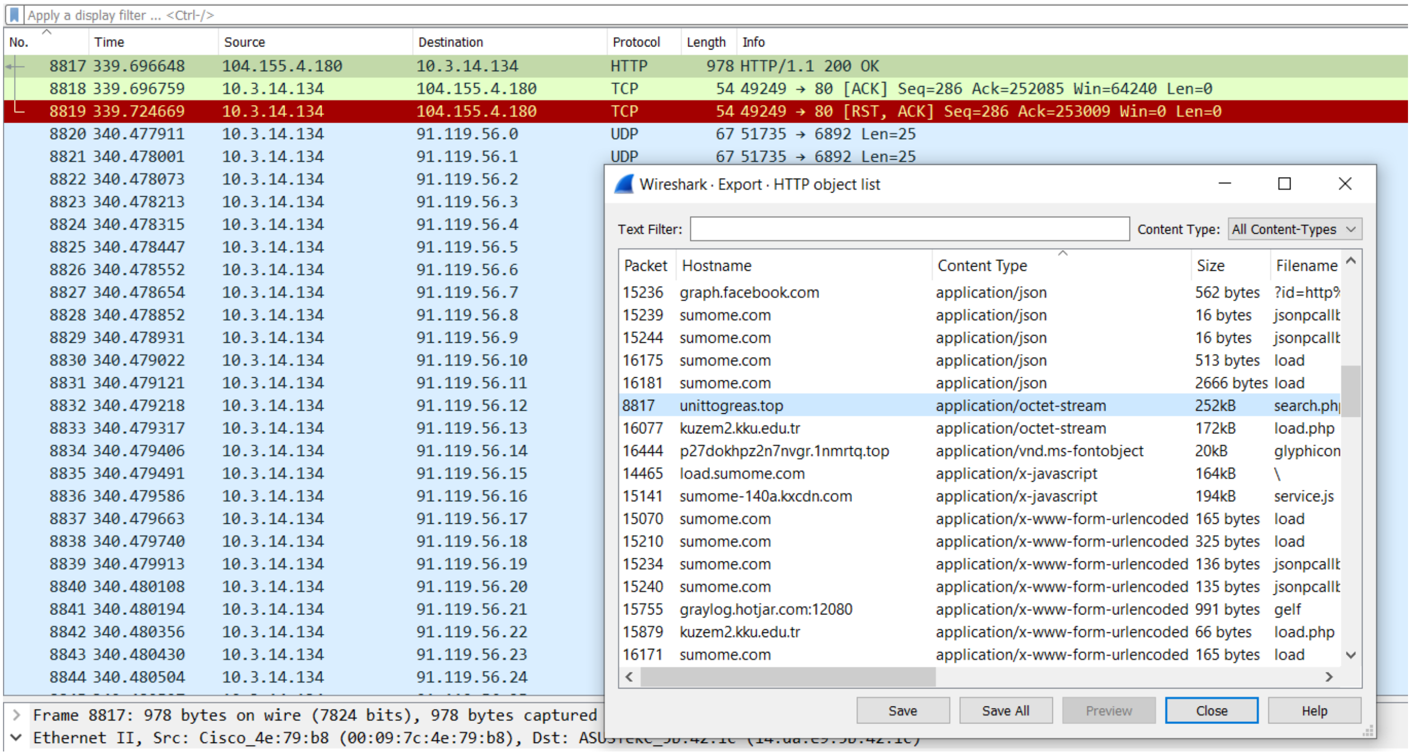
Fig. Mac Address for 10.3.14.134

v) Determine which host(s) were infected.

Ans: 10.3.14.134 and 10.3.14.131 are infected.

Reason: On exporting the object in http format we find out octet-stream content type. Octet-stream consists of random binary data which indicated that file is infected.

On clicking this infected ip is reflected in the wireshark. Hence we found out two IP’s to be infected and they are mentioned above.



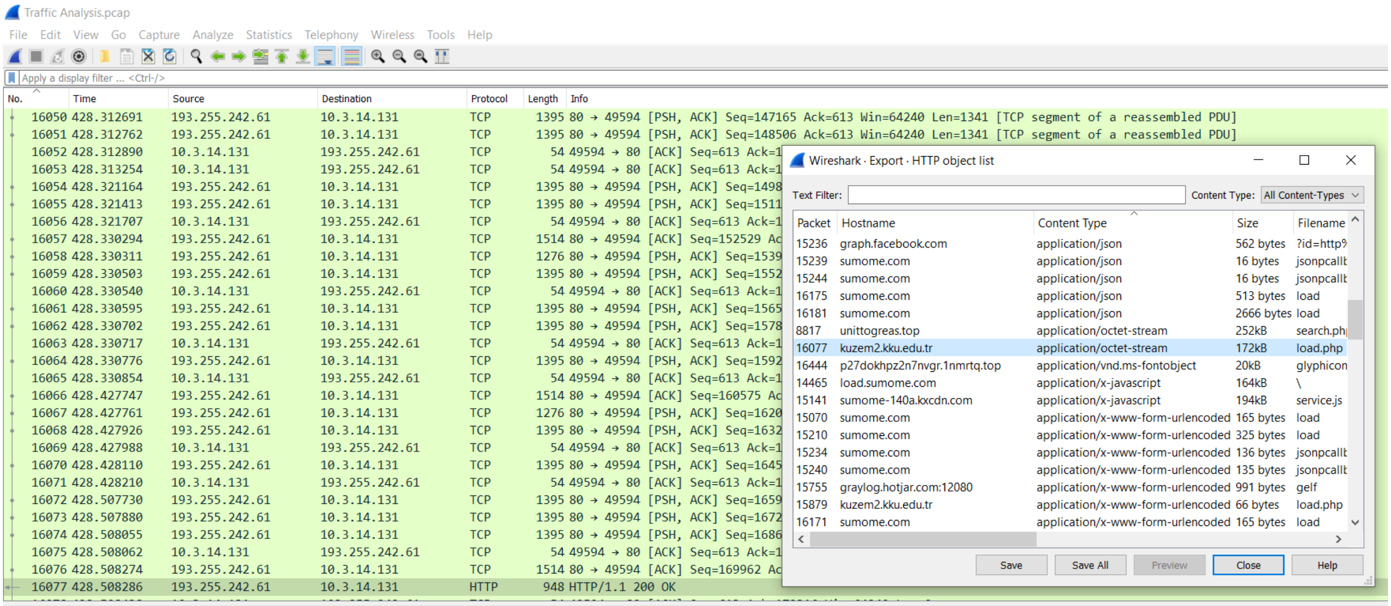
```
No.     Time        Source          Destination     Protocol  Length  Info
 8817 339.696648   104.155.4.180   10.3.14.134     HTTP       978 HTTP/1.1 200 OK
 8818 339.696759   10.3.14.134     104.155.4.180   TCP         54 49249 → 80 [ACK] Seq=286 Ack=252085 Win=64240 Len=0
 8819 339.724669   10.3.14.134     104.155.4.180   TCP         54 49249 → 80 [RST, ACK] Seq=286 Ack=253009 Win=0 Len=0
 8820 340.477911   10.3.14.134     91.119.56.0     UDP         67 51735 → 6892 Len=25
 8821 340.478001   10.3.14.134     91.119.56.1     UDP         67 51735 → 6892 Len=25
 8822 340.478073   10.3.14.134     91.119.56.2
 8823 340.478213   10.3.14.134     91.119.56.3
 8824 340.478315   10.3.14.134     91.119.56.4
 8825 340.478447   10.3.14.134     91.119.56.5
 8826 340.478552   10.3.14.134     91.119.56.6
 8827 340.478654   10.3.14.134     91.119.56.7
 8828 340.478852   10.3.14.134     91.119.56.8
 8829 340.478931   10.3.14.134     91.119.56.9
 8830 340.479022   10.3.14.134     91.119.56.10
 8831 340.479121   10.3.14.134     91.119.56.11
 8832 340.479218   10.3.14.134     91.119.56.12
 8833 340.479317   10.3.14.134     91.119.56.13
 8834 340.479406   10.3.14.134     91.119.56.14
 8835 340.479491   10.3.14.134     91.119.56.15
 8836 340.479586   10.3.14.134     91.119.56.16
 8837 340.479663   10.3.14.134     91.119.56.17
 8838 340.479740   10.3.14.134     91.119.56.18
 8839 340.479913   10.3.14.134     91.119.56.19
 8840 340.480108   10.3.14.134     91.119.56.20
 8841 340.480194   10.3.14.134     91.119.56.21
 8842 340.480356   10.3.14.134     91.119.56.22
 8843 340.480430   10.3.14.134     91.119.56.23
 8844 340.480504   10.3.14.134     91.119.56.24

> Frame 8817: 978 bytes on wire (7824 bits), 978 bytes captured
v Ethernet II, Src: Cisco_4e:79:b8 (00:09:7c:4e:79:b8), Dst: ASU
```

Wireshark · Export · HTTP object list

Text Filter: 　Content Type: All Content-Types

| Packet | Hostname | Content Type | Size | Filename |
|---|---|---|---|---|
| 15236 | graph.facebook.com | application/json | 562 bytes | ?id=http% |
| 15239 | sumome.com | application/json | 16 bytes | jsonpcallk |
| 15244 | sumome.com | application/json | 16 bytes | jsonpcallk |
| 16175 | sumome.com | application/json | 513 bytes | load |
| 16181 | sumome.com | application/json | 2666 bytes | load |
| 8817 | unittogreas.top | application/octet-stream | 252kB | search.ph |
| 16077 | kuzem2.kku.edu.tr | application/octet-stream | 172kB | load.php |
| 16444 | p27dokhpz2n7nvgr.1nmrtq.top | application/vnd.ms-fontobject | 20kB | glyphicon |
| 14465 | load.sumome.com | application/x-javascript | 164kB | \ |
| 15141 | sumome-140a.kxcdn.com | application/x-javascript | 194kB | service.js |
| 15070 | sumome.com | application/x-www-form-urlencoded | 165 bytes | load |
| 15210 | sumome.com | application/x-www-form-urlencoded | 325 bytes | load |
| 15234 | sumome.com | application/x-www-form-urlencoded | 136 bytes | jsonpcallk |
| 15240 | sumome.com | application/x-www-form-urlencoded | 135 bytes | jsonpcallk |
| 15755 | graylog.hotjar.com:12080 | application/x-www-form-urlencoded | 991 bytes | gelf |
| 15879 | kuzem2.kku.edu.tr | application/x-www-form-urlencoded | 66 bytes | load.php |
| 16171 | sumome.com | application/x-www-form-urlencoded | 165 bytes | load |

Fig. IP infected from host unittogreas.top is 10.3.14.134



Traffic Analysis.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.     Time        Source           Destination      Protocol  Length  Info
16050 428.312691   193.255.242.61   10.3.14.131      TCP       1395 80 → 49594 [PSH, ACK] Seq=147165 Ack=613 Win=64240 Len=1341 [TCP segment of a reassembled PDU]
16051 428.312762   193.255.242.61   10.3.14.131      TCP       1395 80 → 49594 [PSH, ACK] Seq=148506 Ack=613 Win=64240 Len=1341 [TCP segment of a reassembled PDU]
16052 428.312890   10.3.14.131      193.255.242.61   TCP         54 49594 → 80 [ACK] Seq=613 Ack=1
16053 428.313254   10.3.14.131      193.255.242.61   TCP         54 49594 → 80 [ACK] Seq=613 Ack=1
16054 428.321164   193.255.242.61   10.3.14.131      TCP       1395 80 → 49594 [PSH, ACK] Seq=1498
16055 428.321413   193.255.242.61   10.3.14.131      TCP       1395 80 → 49594 [PSH, ACK] Seq=1511
16056 428.321707   10.3.14.131      193.255.242.61   TCP         54 49594 → 80 [ACK] Seq=613 Ack=1
16057 428.330294   193.255.242.61   10.3.14.131      TCP       1514 80 → 49594 [ACK] Seq=152529 Ac
16058 428.330311   193.255.242.61   10.3.14.131      TCP       1276 80 → 49594 [PSH, ACK] Seq=1539
16059 428.330503   193.255.242.61   10.3.14.131      TCP       1395 80 → 49594 [PSH, ACK] Seq=1552
16060 428.330540   10.3.14.131      193.255.242.61   TCP         54 49594 → 80 [ACK] Seq=613 Ack=1
16061 428.330595   193.255.242.61   10.3.14.131      TCP       1395 80 → 49594 [PSH, ACK] Seq=1565
16062 428.330702   193.255.242.61   10.3.14.131      TCP       1395 80 → 49594 [PSH, ACK] Seq=1578
16063 428.330717   10.3.14.131      193.255.242.61   TCP         54 49594 → 80 [ACK] Seq=613 Ack=1
16064 428.330776   193.255.242.61   10.3.14.131      TCP       1395 80 → 49594 [PSH, ACK] Seq=1592
16065 428.330854   10.3.14.131      193.255.242.61   TCP         54 49594 → 80 [ACK] Seq=613 Ack=1
16066 428.427747   193.255.242.61   10.3.14.131      TCP       1514 80 → 49594 [ACK] Seq=160575 Ac
16067 428.427761   193.255.242.61   10.3.14.131      TCP       1276 80 → 49594 [PSH, ACK] Seq=1620
16068 428.427926   193.255.242.61   10.3.14.131      TCP       1395 80 → 49594 [PSH, ACK] Seq=1632
16069 428.427988   10.3.14.131      193.255.242.61   TCP         54 49594 → 80 [ACK] Seq=613 Ack=1
16070 428.428110   193.255.242.61   10.3.14.131      TCP       1395 80 → 49594 [PSH, ACK] Seq=1645
16071 428.428210   10.3.14.131      193.255.242.61   TCP         54 49594 → 80 [ACK] Seq=613 Ack=1
16072 428.507730   193.255.242.61   10.3.14.131      TCP       1395 80 → 49594 [PSH, ACK] Seq=1659
16073 428.507880   193.255.242.61   10.3.14.131      TCP       1395 80 → 49594 [PSH, ACK] Seq=1672
16074 428.508055   193.255.242.61   10.3.14.131      TCP       1395 80 → 49594 [PSH, ACK] Seq=1686
16075 428.508062   10.3.14.131      193.255.242.61   TCP         54 49594 → 80 [ACK] Seq=613 Ack=1
16076 428.508274   193.255.242.61   10.3.14.131      TCP       1514 80 → 49594 [ACK] Seq=169962 Ac
16077 428.508286   193.255.242.61   10.3.14.131      HTTP       948 HTTP/1.1 200 OK
```

Wireshark · Export · HTTP object list

Text Filter: 　Content Type: All Content-Types

| Packet | Hostname | Content Type | Size | Filename |
|---|---|---|---|---|
| 15236 | graph.facebook.com | application/json | 562 bytes | ?id=http% |
| 15239 | sumome.com | application/json | 16 bytes | jsonpcallk |
| 15244 | sumome.com | application/json | 16 bytes | jsonpcallk |
| 16175 | sumome.com | application/json | 513 bytes | load |
| 16181 | sumome.com | application/json | 2666 bytes | load |
| 8817 | unittogreas.top | application/octet-stream | 252kB | search.ph |
| 16077 | kuzem2.kku.edu.tr | application/octet-stream | 172kB | load.php |
| 16444 | p27dokhpz2n7nvgr.1nmrtq.top | application/vnd.ms-fontobject | 20kB | glyphicon |
| 14465 | load.sumome.com | application/x-javascript | 164kB | \ |
| 15141 | sumome-140a.kxcdn.com | application/x-javascript | 194kB | service.js |
| 15070 | sumome.com | application/x-www-form-urlencoded | 165 bytes | load |
| 15210 | sumome.com | application/x-www-form-urlencoded | 325 bytes | load |
| 15234 | sumome.com | application/x-www-form-urlencoded | 136 bytes | jsonpcallk |
| 15240 | sumome.com | application/x-www-form-urlencoded | 135 bytes | jsonpcallk |
| 15755 | graylog.hotjar.com:12080 | application/x-www-form-urlencoded | 991 bytes | gelf |
| 15879 | kuzem2.kku.edu.tr | application/x-www-form-urlencoded | 66 bytes | load.php |
| 16171 | sumome.com | application/x-www-form-urlencoded | 165 bytes | load |

Fig. IP infected from host kuzem2.kku.edu.tr is 10.3.14.131

vi) Document the family (or families) of malware based on indicators from the pcap. ·

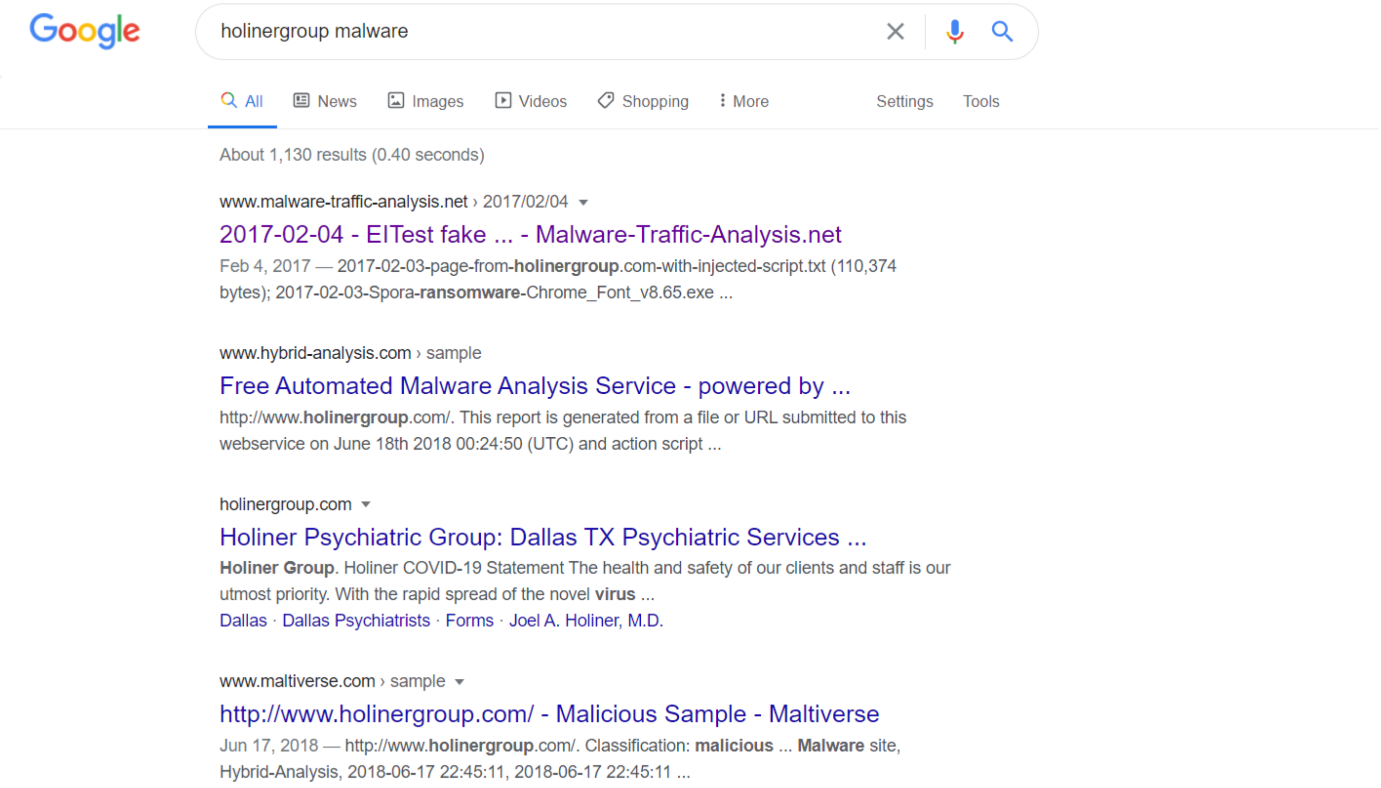
Ans: 10.3.14.131 was infected with Spora ransomware.
10.3.14.134 was infected with Cerber ransomware.

Host of the infections are found in the last sections as:

i) unittogreas.top
ii) kuzem2.kku.edu.tr

The root cause for kuzem2.kku.edu.tr is http://holinergroup.com (It is found using he follow tcp stream of that IP). Hence we come to know tis malware is found from this link.

On google search holinergroup malware we come to know that Spora-Ransomware is the malware associated with it.
Similarly we found host of other IP as unittogreas.top and on google searching it we found it associated with the Cerber ransomware.



holinergroup malware

About 1,130 results (0.40 seconds)

www.malware-traffic-analysis.net › 2017/02/04
2017-02-04 - EITest fake ... - Malware-Traffic-Analysis.net
Feb 4, 2017 — 2017-02-03-page-from-**holinergroup**.com-with-injected-script.txt (110,374 bytes); 2017-02-03-Spora-**ransomware**-Chrome_Font_v8.65.exe ...

www.hybrid-analysis.com › sample
Free Automated Malware Analysis Service - powered by ...
http://www.**holinergroup**.com/. This report is generated from a file or URL submitted to this webservice on June 18th 2018 00:24:50 (UTC) and action script ...

holinergroup.com
Holiner Psychiatric Group: Dallas TX Psychiatric Services ...
**Holiner Group**. Holiner COVID-19 Statement The health and safety of our clients and staff is our utmost priority. With the rapid spread of the novel **virus** ...
Dallas · Dallas Psychiatrists · Forms · Joel A. Holiner, M.D.

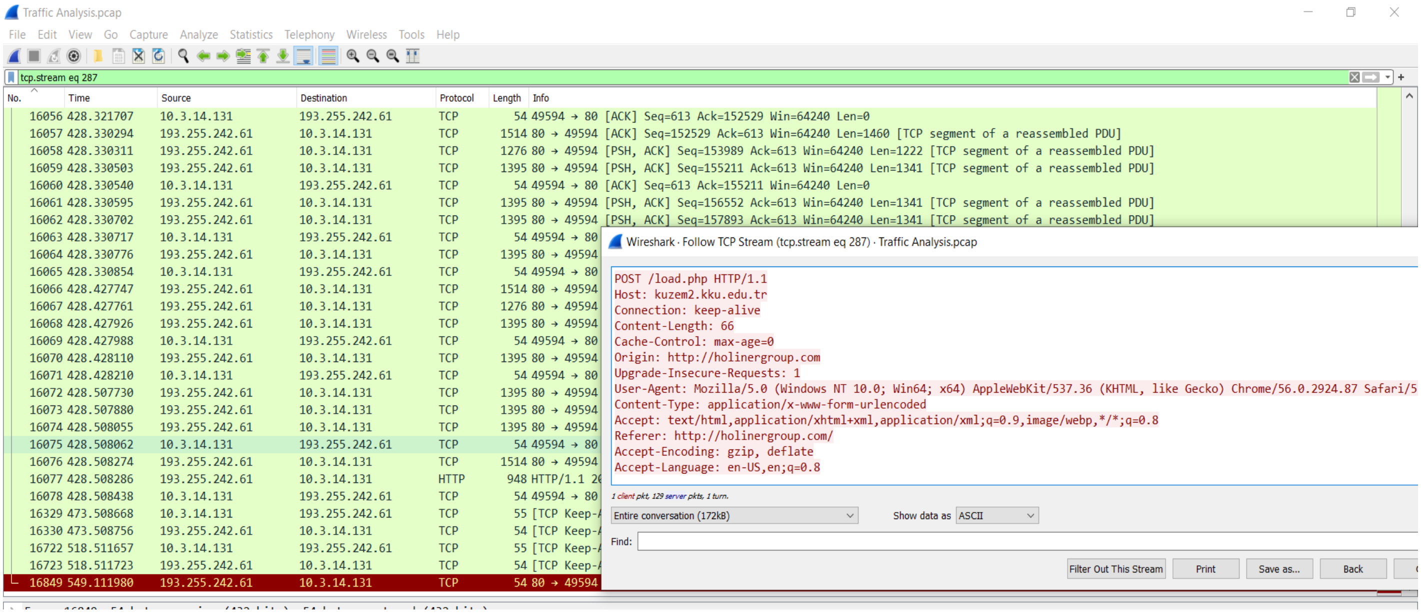
www.maltiverse.com › sample
http://www.holinergroup.com/ - Malicious Sample - Maltiverse
Jun 17, 2018 — http://www.**holinergroup**.com/. Classification: **malicious** ... **Malware** site, Hybrid-Analysis, 2018-06-17 22:45:11, 2018-06-17 22:45:11 ...

Fig. Google search of “holineargroup malware”

vii) Document the root cause for any infections noted in the pcap.

Ans: Root cause for the IP 10.3.14.131 is http://holinergroup.com.

Reason: On finding the IP through the object report we follow the TCP stream of it and find the origin to be the above mentioned link.


Traffic Analysis.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 287

```
No.   Time       Source          Destination     Protocol Length Info
16056 428.321707 10.3.14.131     193.255.242.61  TCP        54 49594 → 80 [ACK] Seq=613 Ack=152529 Win=64240 Len=0
16057 428.330294 193.255.242.61  10.3.14.131     TCP      1514 80 → 49594 [ACK] Seq=152529 Ack=613 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
16058 428.330311 193.255.242.61  10.3.14.131     TCP      1276 80 → 49594 [PSH, ACK] Seq=153989 Ack=613 Win=64240 Len=1222 [TCP segment of a reassembled PDU]
16059 428.330503 193.255.242.61  10.3.14.131     TCP      1395 80 → 49594 [PSH, ACK] Seq=155211 Ack=613 Win=64240 Len=1341 [TCP segment of a reassembled PDU]
16060 428.330540 10.3.14.131     193.255.242.61  TCP        54 49594 → 80 [ACK] Seq=613 Ack=155211 Win=64240 Len=0
16061 428.330595 193.255.242.61  10.3.14.131     TCP      1395 80 → 49594 [PSH, ACK] Seq=156552 Ack=613 Win=64240 Len=1341 [TCP segment of a reassembled PDU]
16062 428.330702 193.255.242.61  10.3.14.131     TCP      1395 80 → 49594 [PSH, ACK] Seq=157893 Ack=613 Win=64240 Len=1341 [TCP segment of a reassembled PDU]
16063 428.330717 10.3.14.131     193.255.242.61  TCP        54 49594 → 80
16064 428.330776 193.255.242.61  10.3.14.131     TCP      1395 80 → 49594
16065 428.330854 10.3.14.131     193.255.242.61  TCP        54 49594 → 80
16066 428.427747 193.255.242.61  10.3.14.131     TCP      1514 80 → 49594
16067 428.427761 193.255.242.61  10.3.14.131     TCP      1276 80 → 49594
16068 428.427926 193.255.242.61  10.3.14.131     TCP      1395 80 → 49594
16069 428.427988 10.3.14.131     193.255.242.61  TCP        54 49594 → 80
16070 428.428110 193.255.242.61  10.3.14.131     TCP      1395 80 → 49594
16071 428.428210 10.3.14.131     193.255.242.61  TCP        54 49594 → 80
16072 428.507730 193.255.242.61  10.3.14.131     TCP      1395 80 → 49594
16073 428.507880 193.255.242.61  10.3.14.131     TCP      1395 80 → 49594
16074 428.508055 193.255.242.61  10.3.14.131     TCP      1395 80 → 49594
16075 428.508062 10.3.14.131     193.255.242.61  TCP        54 49594 → 80
16076 428.508274 193.255.242.61  10.3.14.131     TCP      1514 80 → 49594
16077 428.508286 193.255.242.61  10.3.14.131     HTTP      948 HTTP/1.1 2
16078 428.508438 10.3.14.131     193.255.242.61  TCP        54 49594 → 80
16329 473.508668 10.3.14.131     193.255.242.61  TCP        55 [TCP Keep-
16330 473.508756 193.255.242.61  10.3.14.131     TCP        54 [TCP Keep-
16722 518.511657 10.3.14.131     193.255.242.61  TCP        55 [TCP Keep-
16723 518.511723 193.255.242.61  10.3.14.131     TCP        54 [TCP Keep-
16849 549.111980 193.255.242.61  10.3.14.131     TCP        54 80 → 49594
```

Wireshark · Follow TCP Stream (tcp.stream eq 287) · Traffic Analysis.pcap

```
POST /load.php HTTP/1.1
Host: kuzem2.kku.edu.tr
Connection: keep-alive
Content-Length: 66
Cache-Control: max-age=0
Origin: http://holinergroup.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/5
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://holinergroup.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
```

1 client pkt, 129 server pkts, 1 turn.

Entire conversation (172kB) Show data as ASCII

Find:

Fig. Root casue of infected IP 10.3.14.131

# Learning:

1) Wireshark is the packet network analyser. It can brief about all our incoming and outgoing packets. It is an open-source software which is available for both UNIX and Windows.

2) We have analysed the given pcap file to us name Traffic Analyser. We came to many conclusions such as host ips, there OS and mac address. We also analysed the infected one among them and their origin. We can also figure out the connections of the host with other machines.

3) Besides this project we came to know about many feature of wireshark and how it can be useful to analyse our network and secure it from various malware. There are lot of feature in Wireshark that can be used to closly determine the flow of our network.

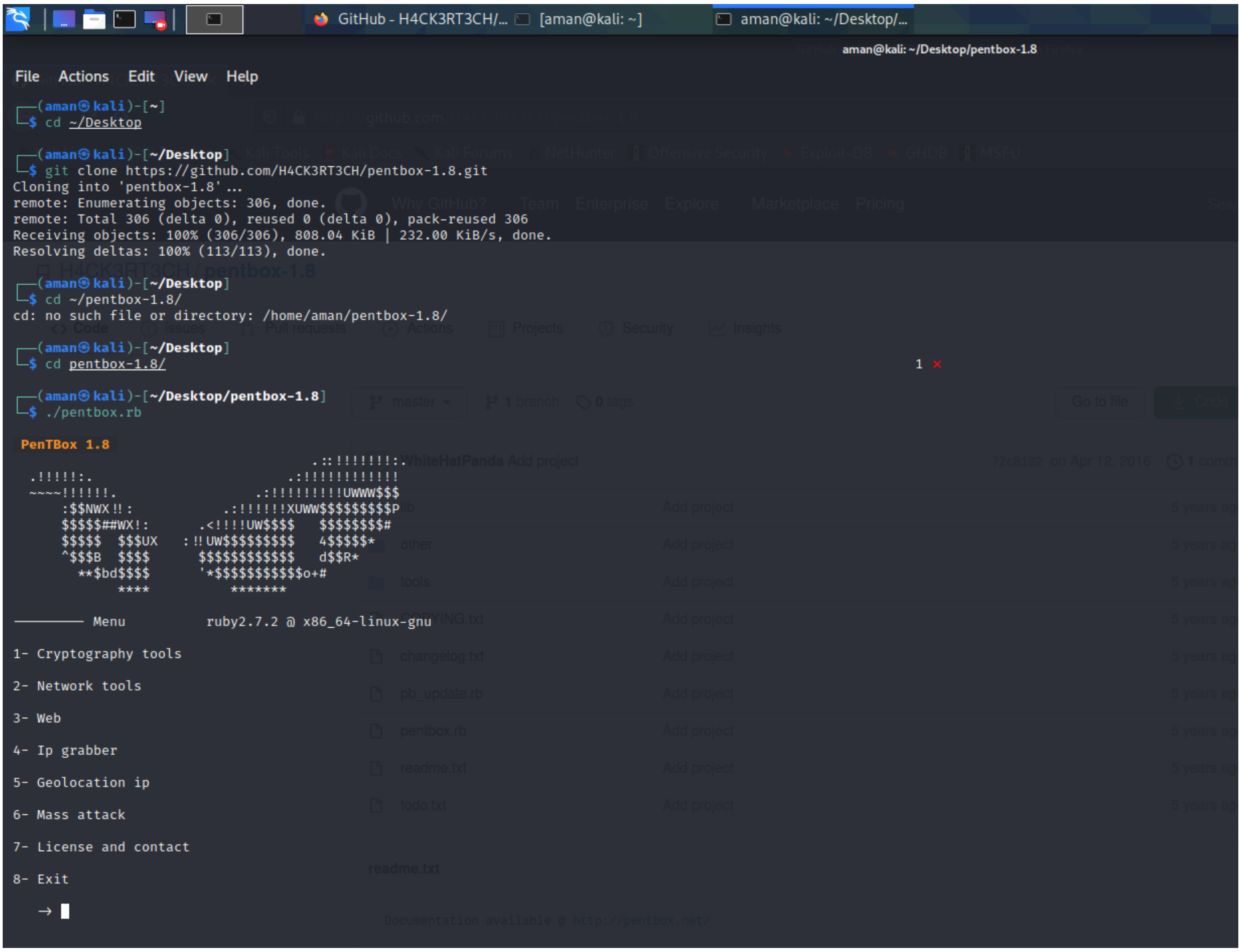
4) Wireshark is not helpful in stopping the activities that can harm our network. Hence it cannot act as intrusion detection system. It can only help in figure out what going in the system.

-----------------------------------------------------------------------------------------------

## Part #2

In Part #2 this assignment, students are to follow the guidance in your book and in the  video below on how to create a honeypot within Kali Linux. Students should provide  screen shots as needed showing the setup process of the honeypot and that the honeypot  is working. Finally, students should write about what you learned in this part.

### Step1: Installation of Pentbox 1.8



```
┌──(aman㉿kali)-[~]
└─$ cd ~/Desktop

┌──(aman㉿kali)-[~/Desktop]
└─$ git clone https://github.com/H4CK3RT3CH/pentbox-1.8.git
Cloning into 'pentbox-1.8' ...
remote: Enumerating objects: 306, done.
remote: Total 306 (delta 0), reused 0 (delta 0), pack-reused 306
Receiving objects: 100% (306/306), 808.04 KiB | 232.00 KiB/s, done.
Resolving deltas: 100% (113/113), done.

┌──(aman㉿kali)-[~/Desktop]
└─$ cd ~/pentbox-1.8/
cd: no such file or directory: /home/aman/pentbox-1.8/

┌──(aman㉿kali)-[~/Desktop]
└─$ cd pentbox-1.8/

┌──(aman㉿kali)-[~/Desktop/pentbox-1.8]
└─$ ./pentbox.rb

 PenTBox 1.8
                                      .::!!!!!!!:.
  .!!!!!:.                        .:!!!!!!!!!!!!
  ~~~~!!!!!!.                 .:!!!!!!!!!UWWW$$$
      :$$NWX!!:           .:!!!!!!XUWW$$$$$$$$$P
      $$$$$##WX!:      .<!!!!UW$$$$   $$$$$$$$#
      $$$$$  $$$UX   :!!UW$$$$$$$$$   4$$$$$*
      ^$$$B  $$$$      $$$$$$$$$$$$   d$$R*
        **$bd$$$$      '*$$$$$$$$$$$o+#
             ****          *******

──────── Menu          ruby2.7.2 @ x86_64-linux-gnu

1- Cryptography tools

2- Network tools

3- Web

4- Ip grabber

5- Geolocation ip

6- Mass attack

7- License and contact

8- Exit

   ->
```

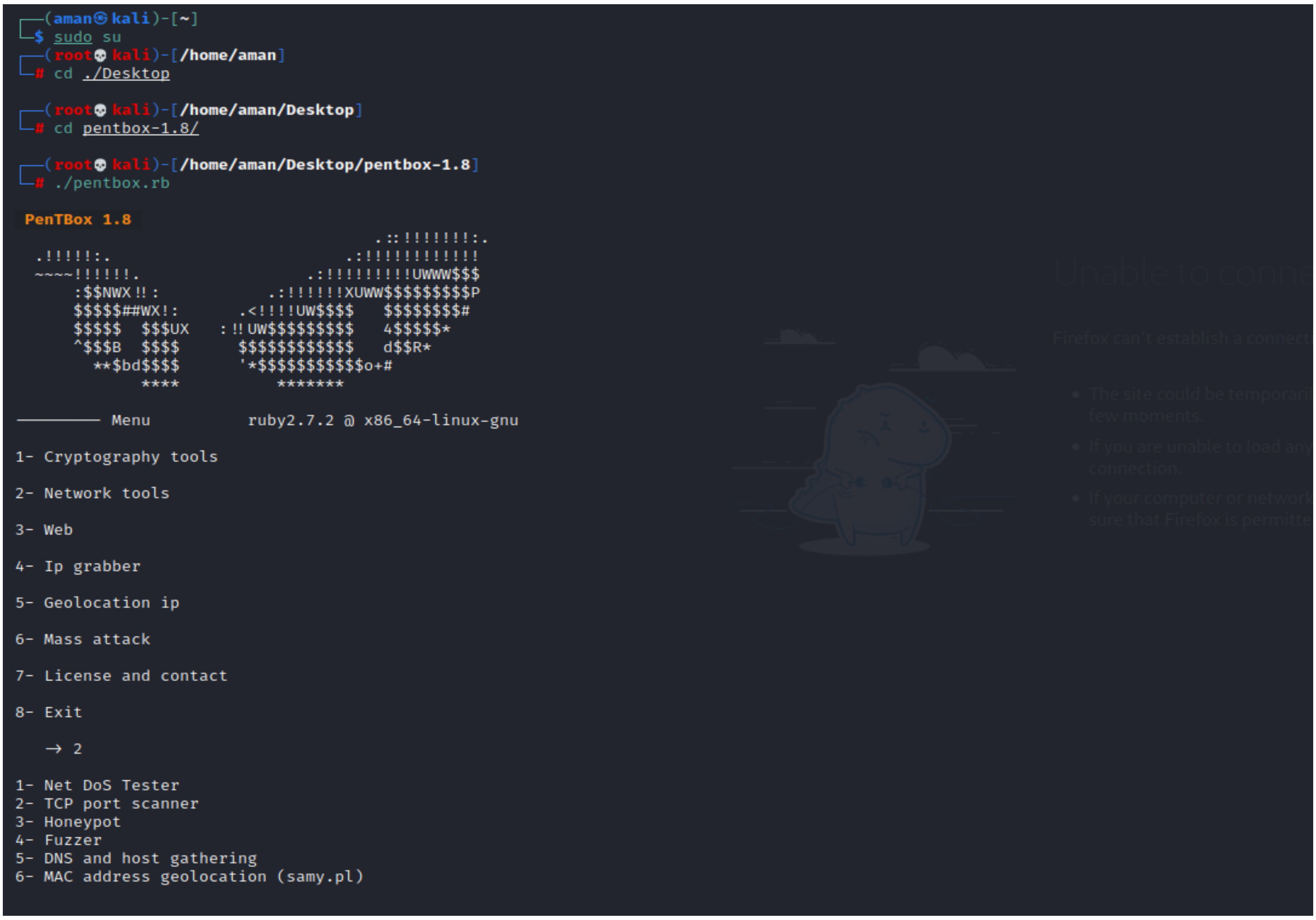
### Step2: Finding IP Address of Linux Machine

CMD: ifconfig

### Step 3: Setting up honey pot

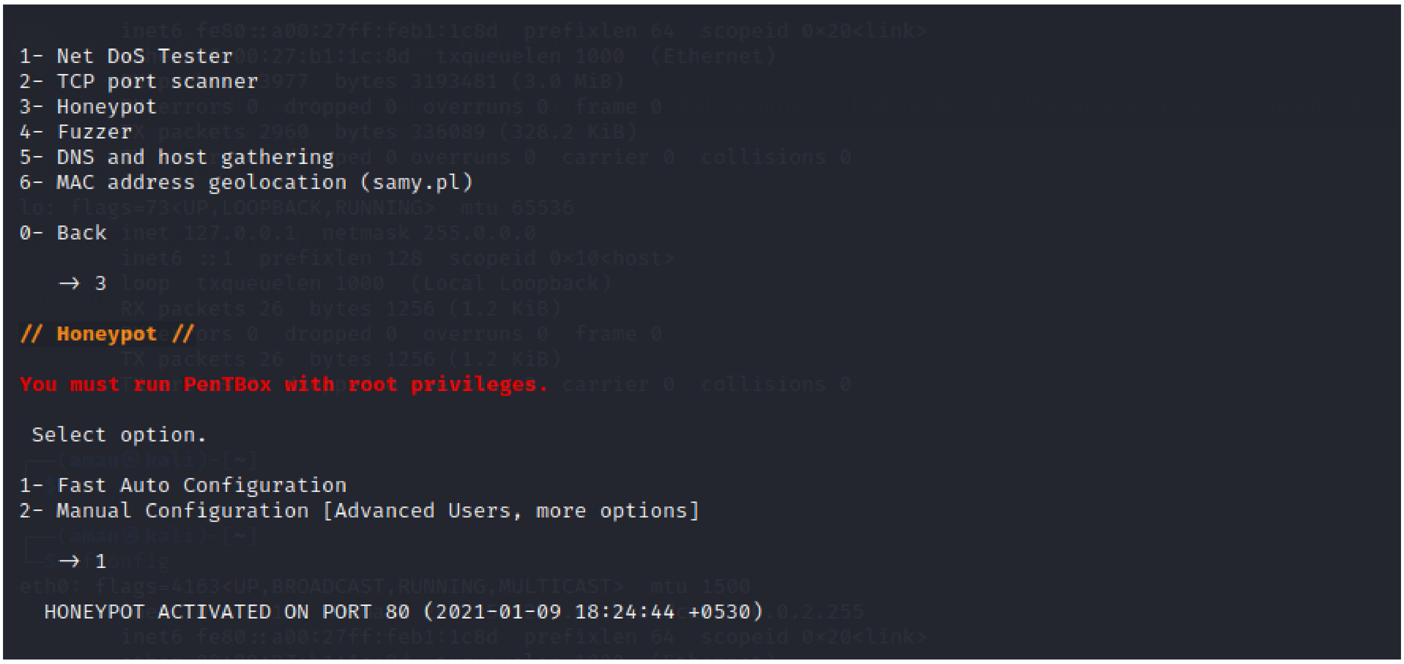
**Error faced: Honeypot requires root privilege.**

It is solved by becoming the super user. It is shown in the screenshot.



```
┌──(aman㉿kali)-[~]
└─$ sudo su
┌──(root💀kali)-[/home/aman]
└─# cd ./Desktop

┌──(root💀kali)-[/home/aman/Desktop]
└─# cd pentbox-1.8/

┌──(root💀kali)-[/home/aman/Desktop/pentbox-1.8]
└─# ./pentbox.rb

 PenTBox 1.8
                                          .::!!!!!!!:.
  .!!!!!:.                            .:!!!!!!!!!!!!
  ~~~~!!!!!!.                      .:!!!!!!!!!UWWW$$$
      :$$NWX!!:                .:!!!!!!XUWW$$$$$$$$$P
      $$$$$##WX!:           .<!!!!UW$$$$   $$$$$$$$#
      $$$$$  $$$UX      :!!UW$$$$$$$$$$   4$$$$$*
      ^$$$B  $$$$         $$$$$$$$$$$$   d$$R*
        **$bd$$$$         '*$$$$$$$$$$$o+#
             ****             *******

──────── Menu          ruby2.7.2 @ x86_64-linux-gnu

1- Cryptography tools

2- Network tools

3- Web

4- Ip grabber

5- Geolocation ip

6- Mass attack

7- License and contact

8- Exit

   → 2

1- Net DoS Tester
2- TCP port scanner
3- Honeypot
4- Fuzzer
5- DNS and host gathering
6- MAC address geolocation (samy.pl)
```

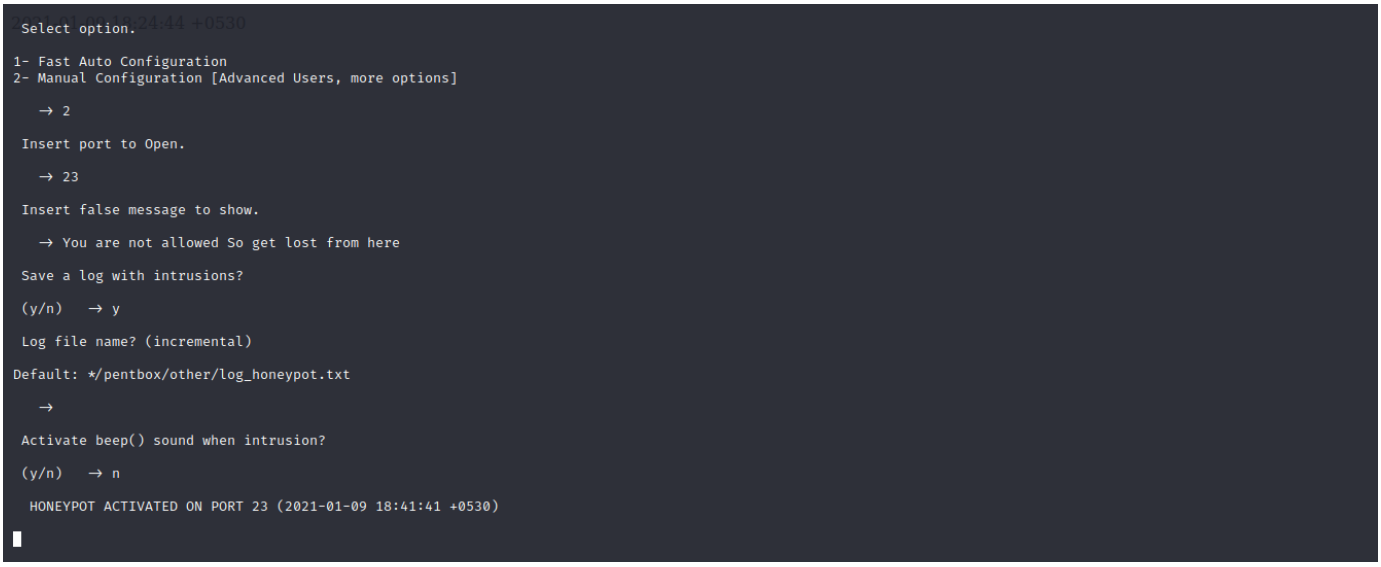
## I: Using Fast Auto Configuration



```
1- Net DoS Tester
2- TCP port scanner
3- Honeypot
4- Fuzzer
5- DNS and host gathering
6- MAC address geolocation (samy.pl)

0- Back

   → 3

// Honeypot //

You must run PenTBox with root privileges.

 Select option.

1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]

   → 1

  HONEYPOT ACTIVATED ON PORT 80 (2021-01-09 18:24:44 +0530)
```

## Step 4 : Login from the browser

## II: Using Manual Configuration

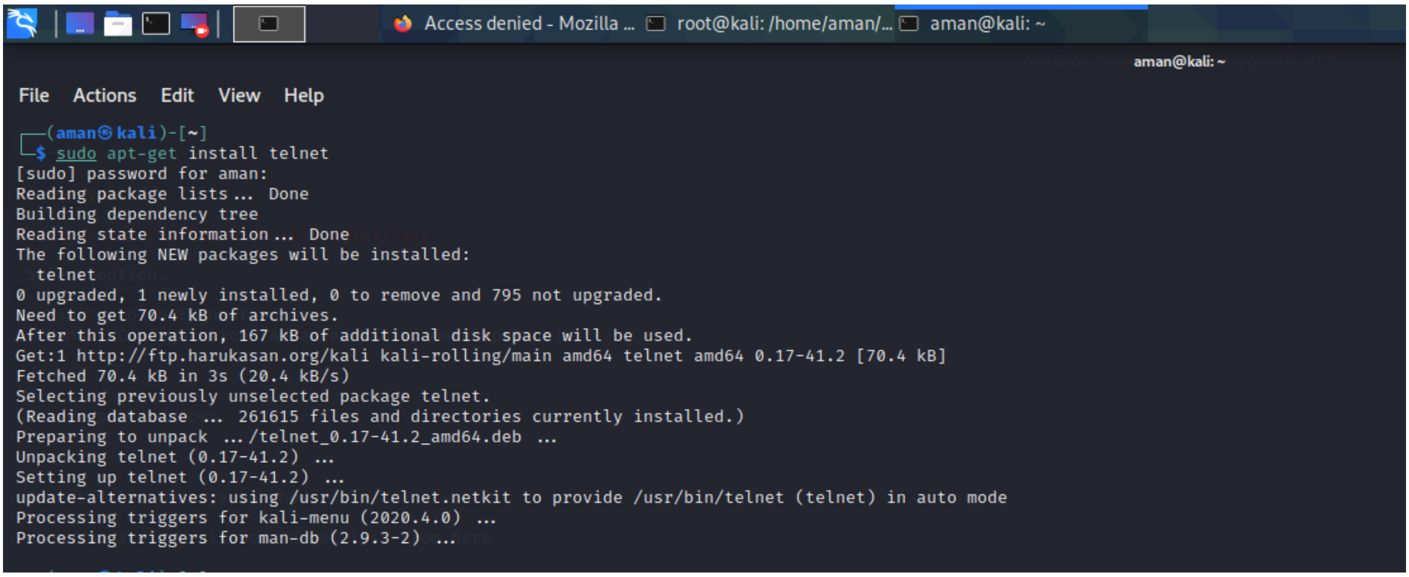


```
 Select option.

1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]

   → 2

 Insert port to Open.

   → 23

 Insert false message to show.

   → You are not allowed So get lost from here

 Save a log with intrusions?

 (y/n)   → y

 Log file name? (incremental)

Default: */pentbox/other/log_honeypot.txt

   →

 Activate beep() sound when intrusion?

 (y/n)   → n

  HONEYPOT ACTIVATED ON PORT 23 (2021-01-09 18:41:41 +0530)
```

Step 4 : Login From Browser

**Error faced: Telnet command not found.**

It solved by installing telnet in linux machine.



```
┌──(aman㉿kali)-[~]
└─$ sudo apt-get install telnet
[sudo] password for aman:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  telnet
0 upgraded, 1 newly installed, 0 to remove and 795 not upgraded.
Need to get 70.4 kB of archives.
After this operation, 167 kB of additional disk space will be used.
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 telnet amd64 0.17-41.2 [70.4 kB]
Fetched 70.4 kB in 3s (20.4 kB/s)
Selecting previously unselected package telnet.
(Reading database ... 261615 files and directories currently installed.)
Preparing to unpack .../telnet_0.17-41.2_amd64.deb ...
Unpacking telnet (0.17-41.2) ...
Setting up telnet (0.17-41.2) ...
update-alternatives: using /usr/bin/telnet.netkit to provide /usr/bin/telnet (telnet) in auto mode
Processing triggers for kali-menu (2020.4.0) ...
Processing triggers for man-db (2.9.3-2) ...
```

# Learning:

It is security mechanism in which attacker can be easily traced. As its name suggest pot of honey means a trap to lure attacker. It is mentioned in the video that it basically hacking the hacker.

We have installed honeypot from the Pentbox 1.8 which is basically a security suite that can be used in penetration testing to do various activities.

Honeypot is one of the features of Pentbox. We can set it up by two ways:

1) By Using Fast Auto Configuration in which it is setup automatically with the default port 80.

2) By Manual Configuration in which we can set up the port for the honeypot.

In the end whenever we try to enter into our IP is blocks it and also directs IP address of the attacking user.

-----------------------------------------------------------------------------------------------------------