Lab 2

Mohammed Alom

R00144214

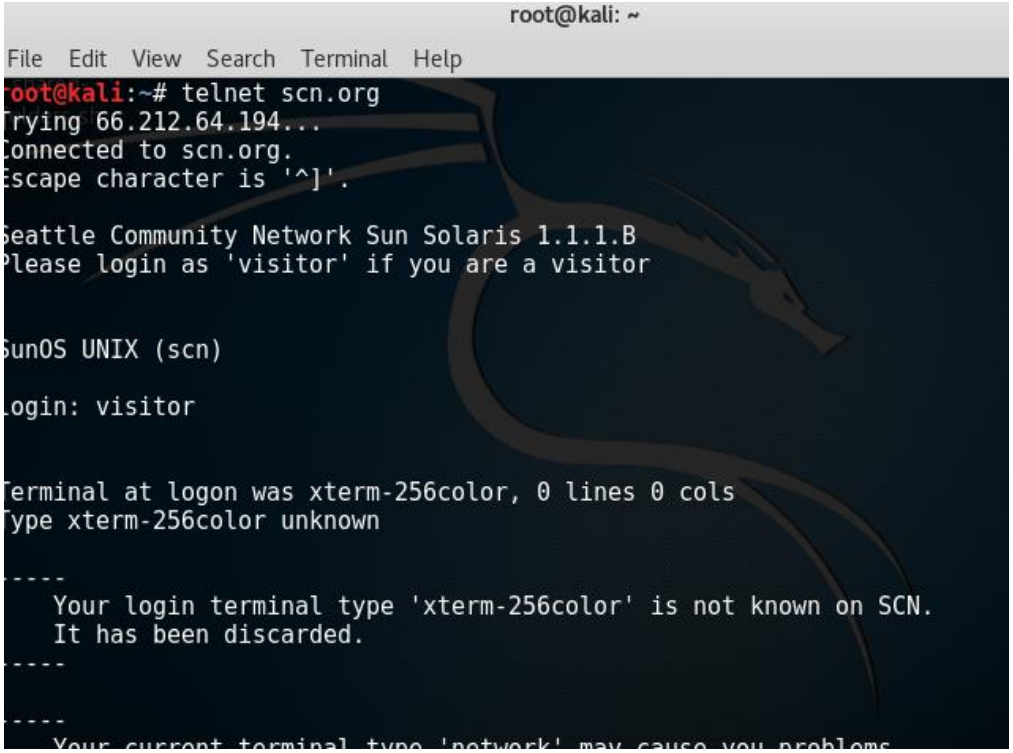
Date – 13/11/2018

Part 1: Using Telnet, SSH, and FTP

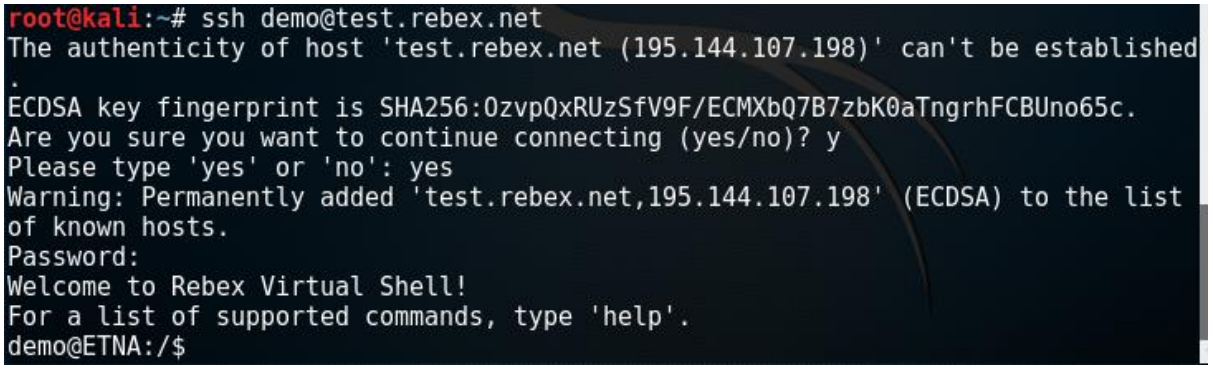
I was able to use kali linux and through command prompt I checked Telnel and SSH service as per lab instruction. I have attached screenshot for both telnet ant ssh.

In the terminal when I typed – telnet scn.org it took me to that website which I used in the dos mode and logged in as a visitor. Here is the screenshot.

Using telnet screenshot—

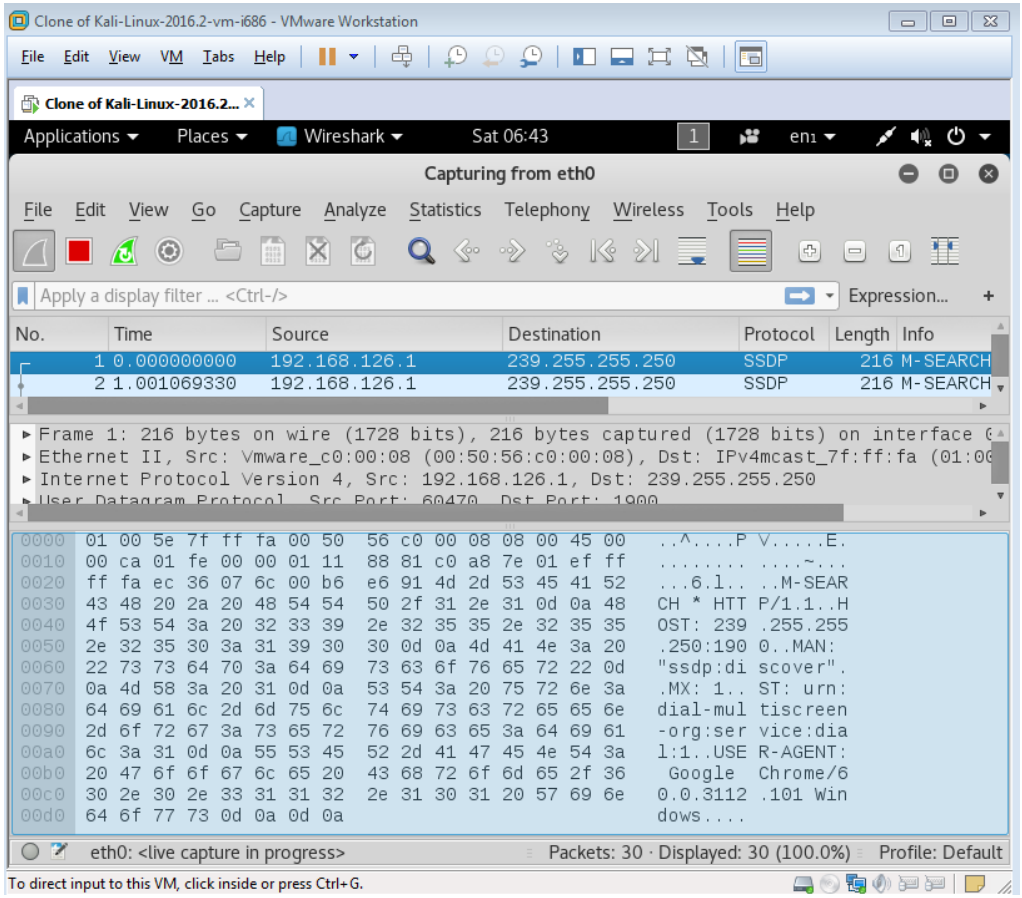


Ssh screenshot



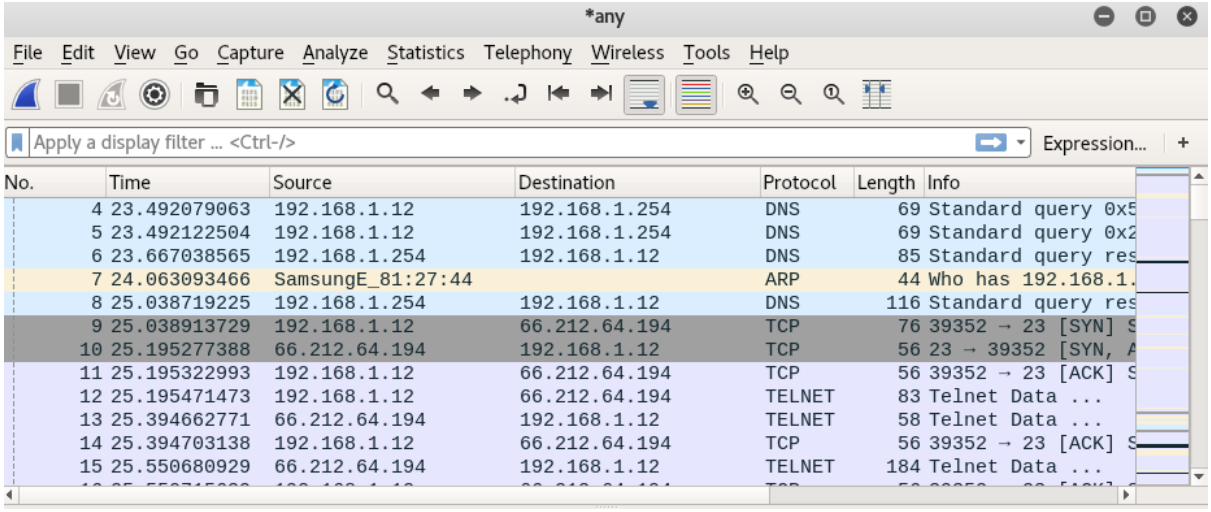
Part 2: Capturing and analysing traffic using Wireshark (50%)

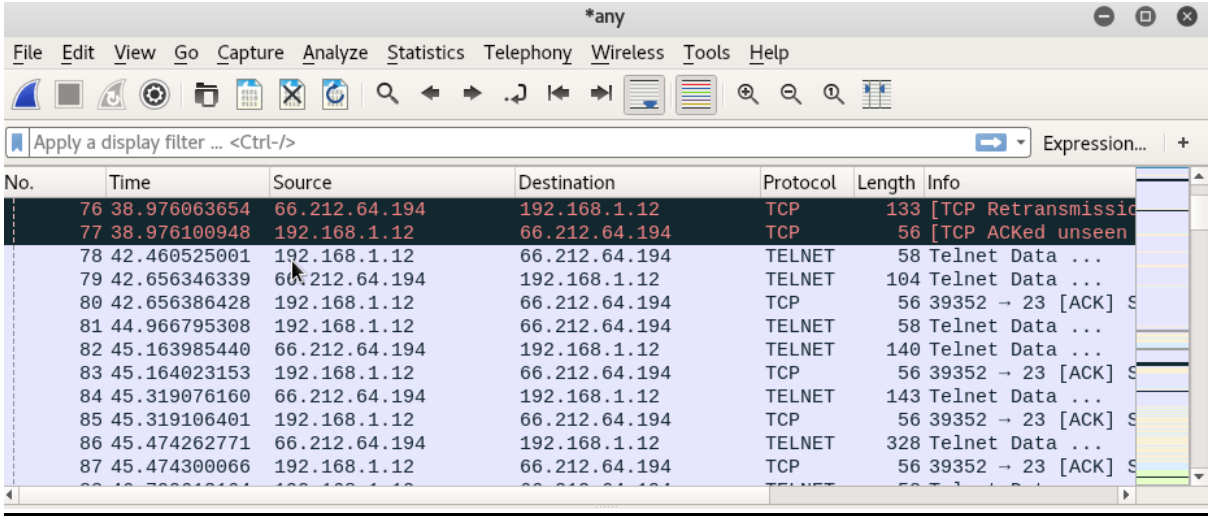
Wireshark screenshot

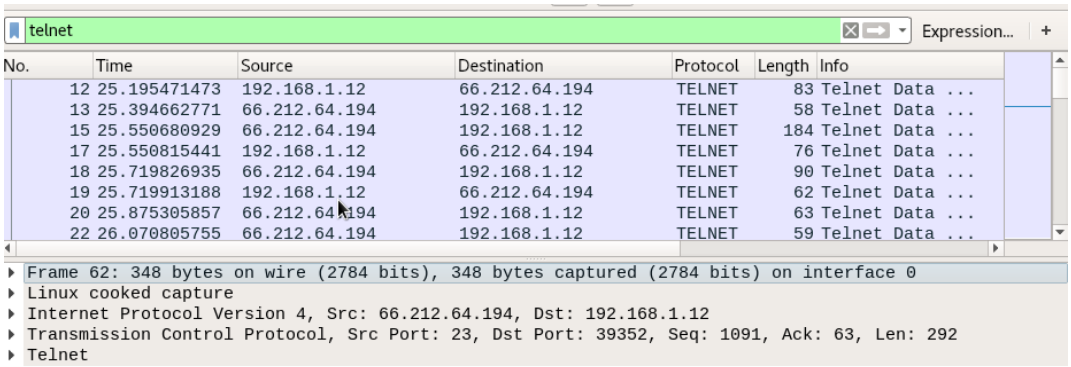


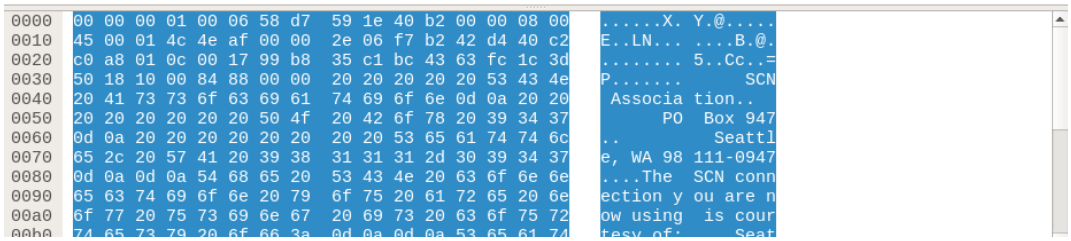
Capturing Telnet and SSH Traffic

Telnet Data Traffic

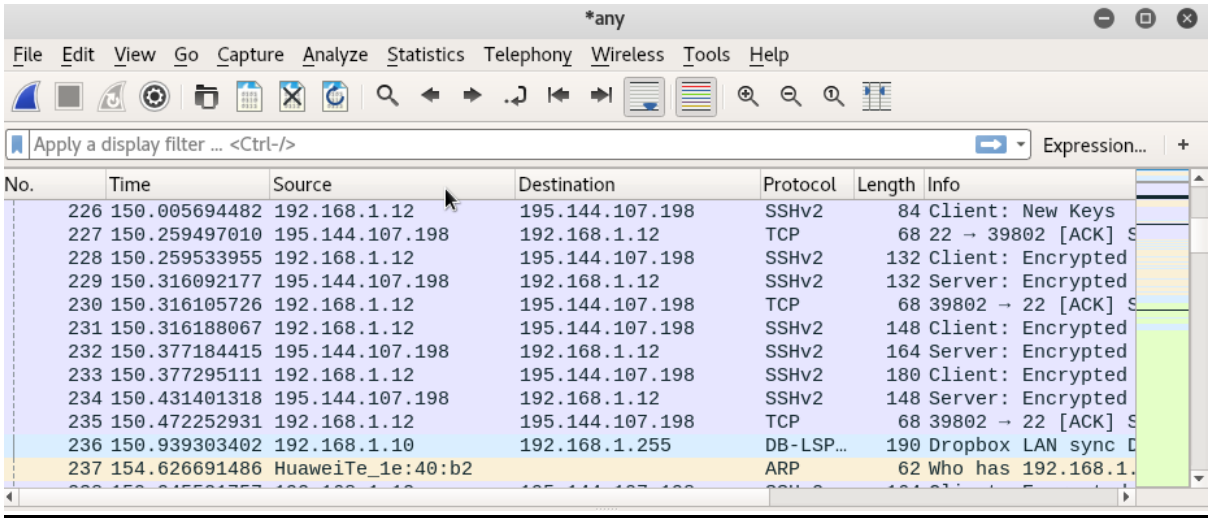








SSH Capturing Data Traffic



SSH Filtering Traffic

ssh

Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
209	140.404872955	192.168.1.12	195.144.107.198	SSHv2	100	Client: Protocol (
210	140.459229682	195.144.107.198	192.168.1.12	SSHv2	94	Server: Protocol (
212	140.459538654	192.168.1.12	195.144.107.198	SSHv2	1428	Client: Key Exchar
213	140.460816937	195.144.107.198	192.168.1.12	SSHv2	724	Server: Key Exchar
216	140.713313611	192.168.1.12	195.144.107.198	SSHv2	116	Client: Elliptic C
217	140.777160903	195.144.107.198	192.168.1.12	SSHv2	84	Server: [TCP Previ
226	150.005694482	192.168.1.12	195.144.107.198	SSHv2	84	Client: New Keys
228	150.259533955	192.168.1.12	195.144.107.198	SSHv2	132	Client: Encrypted

```
▸ Frame 209: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 192.168.1.12, Dst: 195.144.107.198
▸ Transmission Control Protocol, Src Port: 39802, Dst Port: 22, Seq: 1, Ack: 1, Len: 32
▸ SSH Protocol
```

```
0000  00 04 00 01 00 06 00 24  21 d4 7a eb 08 00 08 00   .......$ !.z.....
0010  45 00 00 54 a2 e3 40 00  40 06 a6 b5 c0 a8 01 0c   E..T..@. @.......
0020  c3 90 6b c6 9b 7a 00 16  9d 68 2e 0d 42 2c ec 3d   ..k..z.. .h..B,.=
0030  80 18 00 e5 e3 03 00 00  01 01 08 0a c7 96 b9 c8   ........ ........
0040  01 19 5a 11 53 53 48 2d  32 2e 30 2d 4f 70 65 6e   ..Z.SSH- 2.0-Open
0050  53 53 48 5f 37 2e 36 70  31 20 44 65 62 69 61 6e   SSH_7.6p 1 Debian
0060  2d 34 0d 0a                                       -4..
```

Telnet Packet Data Analysis

Wireshark · Follow TCP Stream (tcp.stream eq 0) · wireshark_any_201811200...

```
........... ..!.."..'.....#
Seattle Community Network Sun Solaris 1.1.1.B
Please login as 'visitor' if you are a visitor
........... ..!.."..'.....#.........xterm-256color.......

SunOS UNIX (scn)

.

.......login: ...vviissiittoorr
.


Terminal at logon was xterm-256color, 0 lines 0 cols
Type xterm-256color unknown
.
-----
    Your login terminal type 'xterm-256color' is not known on
SCN.
    It has been discarded.
-----
.
-----
    Your current terminal type 'network' may cause you problems
    using SCN. If possible, set your terminal type to a
    supported terminal type ('go term' at the prompt).
-----
SEATTLE COMMUNITY NETWORK - Powering our communities with
```

34 client pkts, 66 server pkts, 65 turns.

Entire conversation (8947 bytes) | Show and save data as ASCII | Stream 0

Find: | Find Next

Help | Filter Out This Stream | Print | Save as... | Back | Close

Wireshark · Follow TCP Stream (tcp.stream eq 0) · wireshark_any_201811200...

```
                        <<< SEATTLE COMMUNITY NETWORK >>>
                               Main Menu (press M)

  1 Visitor and Information...     (registration, FAQ, donating,
volunteer...)

  2 Help Menu...                   (confused? look here before
you ask!)

  3 Seattle Public Library...       (our good friends)

  4 E-mail Menu...                 (read and send mail, mail
forwarding...)

  5 World Wide Web...              (and local community web
pages)

  6 Work with Your Files...        (file transfer, download comm
programs...)

  7 Settings and Utilities...      (terminal types, user lookup,
Free-Nets...)

  8 Information Provider, Test, and Staff Menus
-------------------------------------------------------------
m = Main Menu        pine = Pine E-mail         h = Help
p = Previous Menu    lynx = Lynx Web Browser    x = Exit SCN
```

34 client pkts, 66 server pkts, 65 turns.

Entire conversation (8947 bytes) | Show and save data as ASCII | Stream 0

Find: | Find Next

Help | Filter Out This Stream | Print | Save as... | Back | Close

Telnet Data Analysis

15	25.550680929	66.212.64.194	192.168.1.12	TELNET	184 Telnet Data ...
16	25.550715639	192.168.1.12	66.212.64.194	TCP	56 39352 → 23 [ACK] S

```
▸ Frame 15: 184 bytes on wire (1472 bits), 184 bytes captured (1472 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 66.212.64.194, Dst: 192.168.1.12
▸ Transmission Control Protocol, Src Port: 23, Dst Port: 39352, Seq: 3, Ack: 28, Len: 128
▾ Telnet
    Data: Seattle Community Network Sun Solaris 1.1.1.B\r\n
    Data: Please login as 'visitor' if you are a visitor\r\n
  ▸ Do Terminal Type
  ▸ Will Suppress Go Ahead
  ▸ Don't Negotiate About Window Size
  ▸ Don't Terminal Speed
  ▸ Don't Remote Flow Control
  ▸ Don't Linemode
  ▸ Don't New Environment Option
  ▸ Won't Status
  ▸ Don't X Display Location
  ▸ Suboption Terminal Type
  ▸ Suboption End
```

62	34.894110346	66.212.64.194	192.168.1.12	TELNET	348 Telnet Data ...
63	34.894141705	192.168.1.12	66.212.64.194	TCP	56 39352 → 23 [ACK] S

```
▸ Frame 62: 348 bytes on wire (2784 bits), 348 bytes captured (2784 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 66.212.64.194, Dst: 192.168.1.12
▸ Transmission Control Protocol, Src Port: 23, Dst Port: 39352, Seq: 1091, Ack: 63, Len: 292
▾ Telnet
    Data:      SCN Association\r\n
    Data:         PO Box 947\r\n
    Data:         Seattle, WA 98111-0947\r\n
    Data: \r\n
    Data: The SCN connection you are now using is courtesy of:\r\n
    Data: \r\n
    Data: Seattle Community Network Association\r\n
    Data: \r\n
    Data: Over 1000 Strong - Join Today\r\n
    Data: $25 Annual Membership Fee\r\n
    Data: Democratic Technology for All\r\n
    Data: \r\n
    Data: \r
    Data: Press RETURN to Continue:
```

SSH Packet Data Analysis

Wireshark · Follow TCP Stream (tcp.stream eq 1) · wireshark_any_201811200...

```
SSH-2.0-OpenSSH_7.6p1 Debian-4
SSH-2.0-RebexSSH_1.0.0.0
...L...m[*>...k....)w....0curve25519-sha256,curve25519-
sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-
sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-
hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-
hellman-group-exchange-sha1,diffie-hellman-group14-sha256,diffie-
hellman-group14-sha1,ext-info-c..."ecdsa-sha2-nistp256-cert-
v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-
sha2-nistp521-cert-v01@openssh.com,ssh-ed25519-cert-
v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ecdsa-sha2-
nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-ed25519,rsa-
sha2-512,rsa-sha2-256,ssh-rsa...lchacha20-
poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-
gcm@openssh.com,aes256-gcm@openssh.com...lchacha20-
poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-
gcm@openssh.com,aes256-gcm@openssh.com...umac-64-
etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-
etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-
etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-
sha2-256,hmac-sha2-512,hmac-sha1....umac-64-
etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-
etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-
etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-
sha2-256,hmac-sha2-512,hmac-
sha1....none,zlib@openssh.com,zlib....none,zlib@openssh.com,zlib.
.............................:....;'Mi.c......curve25519-
sha256@libssh.org,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-
```

22 client pkts, 26 server pkts, 35 turns.

Entire conversation (5610 bytes) | Show and save data as ASCII | Stream 1

Find: | Find Next

Help | Filter Out This Stream | Print | Save as... | Back | Close

Wireshark · Follow TCP Stream (tcp.stream eq 1) · wireshark_any_201811200...

```
hellman-group14-sha256...Xssh-ed25519,ecdsa-sha2-nistp256,rsa-
sha2-512,ssh-rsa-sha256@ssh.com,rsa-sha2-256,ssh-rsa...naes256-
ctr,aes256-cbc,aes192-ctr,aes192-cbc,aes128-ctr,aes128-
cbc,twofish256-ctr,twofish192-ctr,twofish128-ctr...naes256-
ctr,aes256-cbc,aes192-ctr,aes192-cbc,aes128-ctr,aes128-
cbc,twofish256-ctr,twofish192-ctr,twofish128-ctr....hmac-
sha2-512,hmac-sha2-256....hmac-sha2-512,hmac-
sha2-256....none....none.....,.....
....VK...w.....C..`)U...n
....7Z......[264 bytes missing in capture file].....
.............
............      5.x..'.Q.}...../...........c...H<w8....
{...g...{@..J.........}$(....Q....6.y:...."...*....V..=s
.
.K.-..C4...Za..zZVB..Vb.X.s.V....-
w...jE.K....."S...B>_......rZ7..EA.w.$gd.H..........9.Iggr_.
4...e.|. .|;........
}...z.;..[.7......(..# 2......vP(7;....3......t
$.C.'.....=..h(s.E=+C..h!x.<..|....
...]3a..`.>.>..~...|.....         ..HC..s..*b....mE..
6W...o.L...#... _J
..;........|..\r./.%.MC9...f....{.@..@).282...T.t..
aMd=>.nw.Yf...F.."..v .&S....l.sk.tO.....T8^..._..mmI...G..[....
2=.2s....._..n..Y..NO.G .F..Ft](....U~(w.({..@....bc..5.M|..?
<.ZWz&..`......0:|.#.,...uL.o.../...N..Lc.>..P.0...V.cj#..
+..H....}$....n..s..\.=P{b.q..>..?..x....
4..:gf..,~*........./.Rz.Y...........o.o.)..8..O2....H.k4...B%.
3..>..Z.f..
```

22 client pkts, 26 server pkts, 35 turns.

Entire conversation (5610 bytes) | Show and save data as ASCII | Stream 1

Find: | Find Next

Help | Filter Out This Stream | Print | Save as... | Back | Close

Part 3: Using Tcpdump (30%)

Running Tcpdump

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlan0, link-type EN10MB (Ethernet), capture size 262144 bytes
01:24:05.726746 ARP, Request who-has 192.168.1.4 tell _gateway, length 46
01:24:05.727331 IP kali.57973 > _gateway.domain: 52409+ PTR? 4.1.168.192.in-addr
.arpa. (42)
01:24:05.829127 ARP, Request who-has kali tell _gateway, length 28
01:24:05.829138 ARP, Reply kali is-at 00:24:21:d4:7a:eb (oui Unknown), length 28
01:24:05.830973 IP _gateway.domain > kali.57973: 52409 NXDomain* 0/1/0 (94)
01:24:05.831443 IP kali.60956 > _gateway.domain: 34998+ PTR? 254.1.168.192.in-ad
dr.arpa. (44)
01:24:05.857131 IP _gateway.domain > kali.60956: 34998 NXDomain* 0/1/0 (96)
01:24:05.858426 IP kali.40375 > _gateway.domain: 9220+ PTR? 12.1.168.192.in-addr
.arpa. (43)
01:24:06.648333 ARP, Request who-has 192.168.1.4 tell _gateway, length 46
01:24:10.759616 ARP, Request who-has _gateway tell kali, length 28
01:24:10.761628 ARP, Reply _gateway is-at 58:d7:59:1e:40:b2 (oui Unknown), lengt
h 28
01:24:11.768390 ARP, Request who-has 192.168.1.4 tell _gateway, length 46
01:24:12.587411 ARP, Request who-has _gateway tell 192.168.1.9, length 28
01:24:12.587563 IP kali.50409 > _gateway.domain: 31122+ PTR? 9.1.168.192.in-addr
.arpa. (42)
01:24:12.615044 IP _gateway.domain > kali.50409: 31122 NXDomain* 0/1/0 (94)
01:24:15.046262 IP 192.168.1.10.17500 > 192.168.1.255.17500: UDP, length 146
```

```
01:27:44.552036 ARP, Request who-has _gateway tell 192.168.1.9, length 28
01:27:44.655361 ARP, Request who-has _gateway tell 192.168.1.9, length 28
01:27:46.191313 IP 192.168.1.10.17500 > 192.168.1.255.17500: UDP, length 146
^C
78 packets captured
82 packets received by filter
4 packets dropped by kernel
root@kali:~#
```

Screenshot of the tcpdump –help

```
root@kali:~# tcpdump --help
tcpdump version 4.9.2
libpcap version 1.8.1
OpenSSL 1.1.0h  27 Mar 2018
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqStuUvxX#] [ -B size ] [ -c count ]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -i interface ] [ -j tstamptype ] [ -M secret ] [ --number ]
                [ -Q in|out|inout ]
                [ -r file ] [ -s snaplen ] [ --time-stamp-precision precision ]
                [ --immediate-mode ] [ -T type ] [ --version ] [ -V file ]
                [ -w file ] [ -W filecount ] [ -y datalinktype ] [ -z postrotate
-command ]
                [ -Z user ] [ expression ]
root@kali:~#
```

Man tcpdump screenshot

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
TCPDUMP(8)                System Manager's Manual                TCPDUMP(8)

NAME
       tcpdump - dump traffic on a network

SYNOPSIS
       tcpdump [ -AbdDefhHIJKlLnNOpqStuUvxX# ] [ -B buffer_size ]
               [ -c count ]
               [ -C file_size ] [ -G rotate_seconds ] [ -F file ]
               [ -i interface ] [ -j tstamp_type ] [ -m module ] [ -M secret ]
               [ --number ] [ -Q in|out|inout ]
               [ -r file ] [ -V file ] [ -s snaplen ] [ -T type ] [ -w file ]
               [ -W filecount ]
               [ -E spi@ipaddr algo:secret,...  ]
               [ -y datalinktype ] [ -z postrotate-command ] [ -Z user ]
               [ --time-stamp-precision=tstamp_precision ]
               [ --immediate-mode ] [ --version ]
               [ expression ]

DESCRIPTION
       Tcpdump  prints  out a description of the contents of packets on a net-
       work interface that match the boolean expression;  the  description  is
       preceded  by a time stamp, printed, by default, as hours, minutes, sec-
 Manual page tcpdump(8) line 1 (press h for help or q to quit)
```

Tcpdump -I lo screenshot

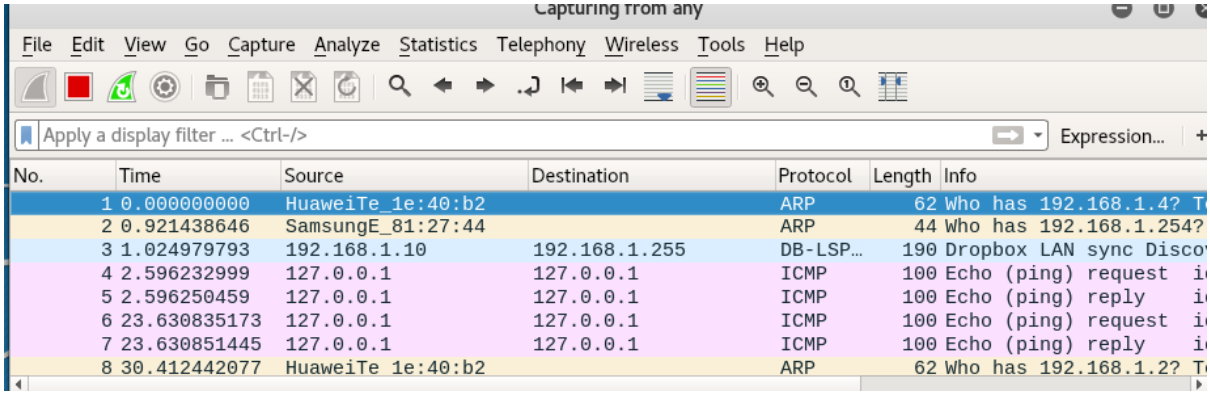
```
root@kali:~# tcpdump -i lo
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
```

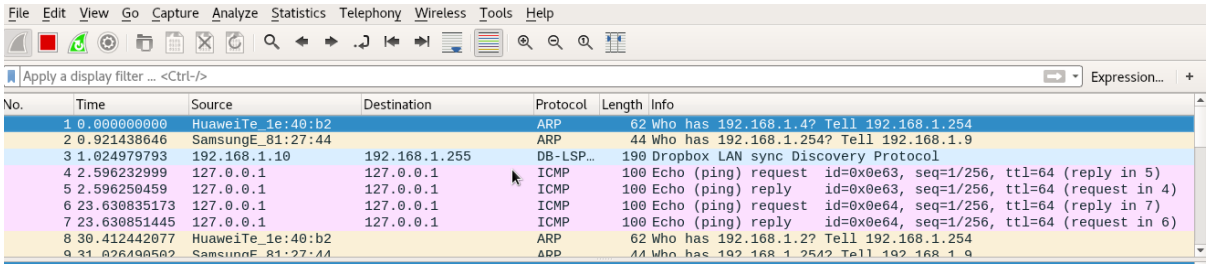
Ping command screenshot

```
root@kali:~# ping -c1 127.0.01
PING 127.0.01 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.048 ms

--- 127.0.01 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.048/0.048/0.048/0.000 ms
root@kali:~#
```

Capturing ping in he wireshark

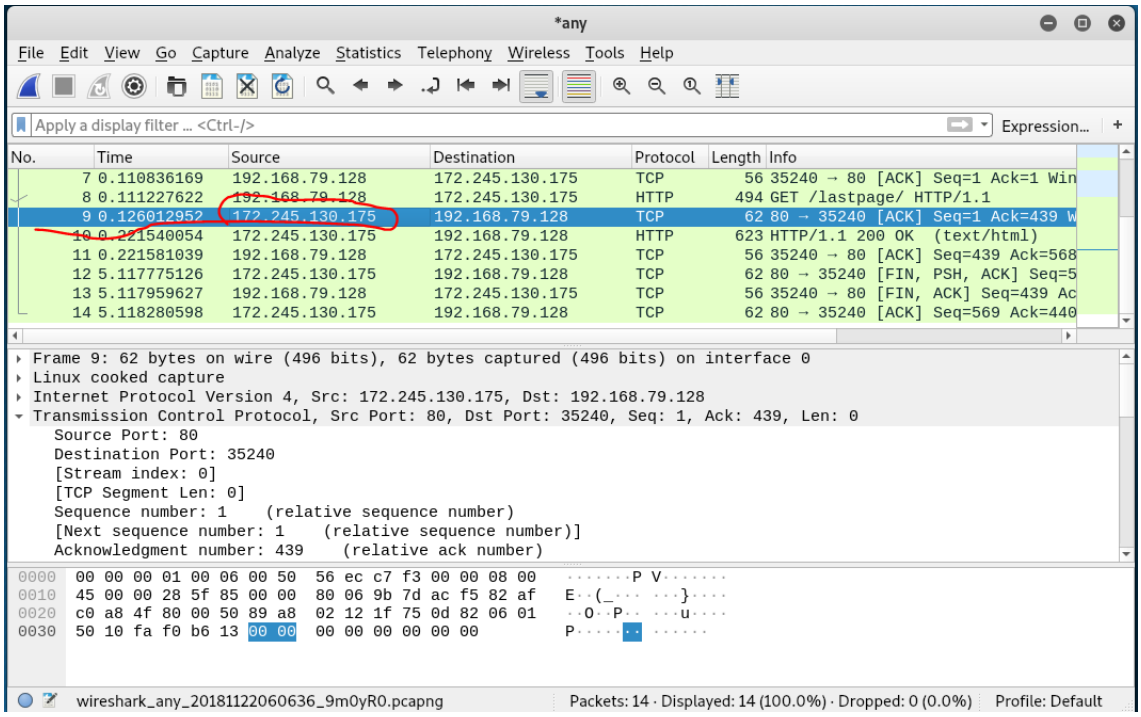


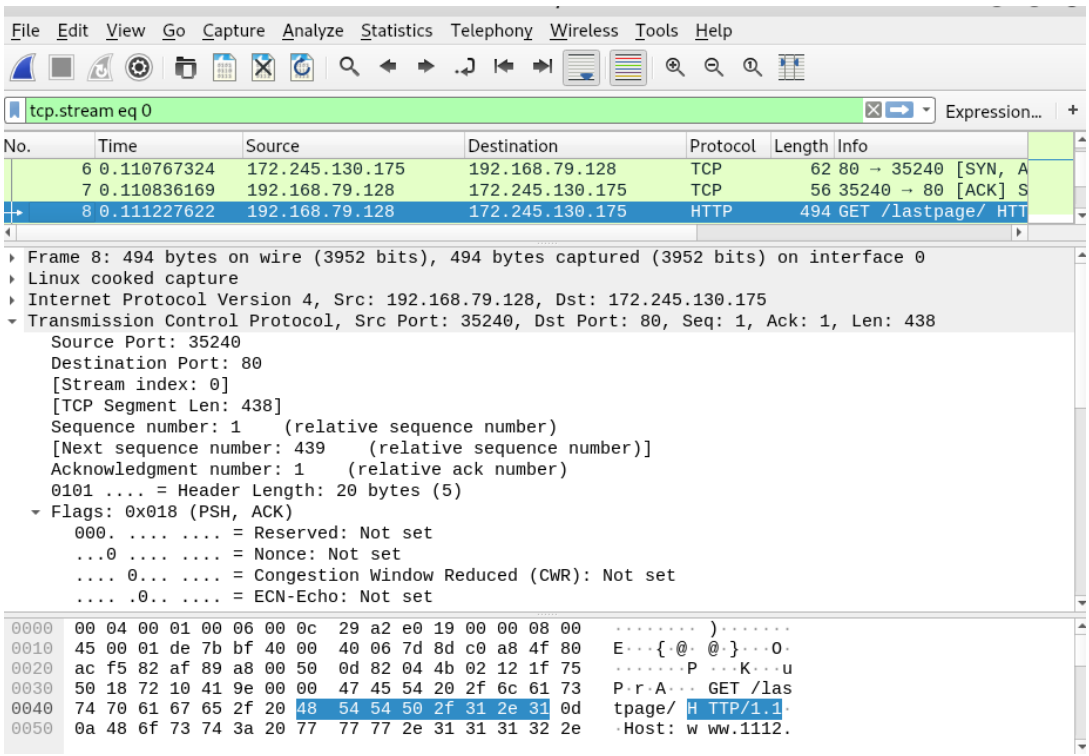


Part 4: (Challenge) Secure Web Browsing (20%)

Capturing Data through Wireshark for -www.1112.net/lastpage screenshot

www.1112.net its ip address is – 172.245.130.175





Tcp steam

Wireshark · Follow TCP Stream (tcp.stream eq 0) · any

```
GET /lastpage/ HTTP/1.1
Host: www.1112.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
If-Modified-Since: Mon, 07 Nov 2011 12:57:40 GMT
If-None-Match: "19a-4b124998df900-gzip"
Cache-Control: max-age=0

HTTP/1.1 200 OK
Date: Thu, 22 Nov 2018 16:15:48 GMT
Server: Apache/2.4.7 (Ubuntu)
Last-Modified: Mon, 07 Nov 2011 12:57:40 GMT
ETag: "19a-4b124998df900-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 231
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

...............0.D..
}A.^.a.caYzX(=:.....q.....IC/-.M.f.........@..AG.e .....(pt.._@tq.B9..YE.i6+6......
\...a..X...^z..h.E.K..M.T.-..9v..\ .. .k..%.Dy..&K/...<.h.;.. p".7>.
+...E.&.}.c./...AJ.....[...a.E.....{O/hh.5i.K{Z..%..V......
```

Packet 8. 1 client pkt(s), 1 server pkt(s), 1 turn(s). Click to select.

Entire conversation (1,005 bytes) | Show and save data as ASCII | Stream 0

Find: | Find Next

Help | Filter Out This Stream | Print | Save as... | Back | Close

http stream

Wireshark · Follow HTTP Stream (tcp.stream eq 0) · any

```
GET /lastpage/ HTTP/1.1
Host: www.1112.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
If-Modified-Since: Mon, 07 Nov 2011 12:57:40 GMT
If-None-Match: "19a-4b124998df900-gzip"
Cache-Control: max-age=0

HTTP/1.1 200 OK
Date: Thu, 22 Nov 2018 16:15:48 GMT
Server: Apache/2.4.7 (Ubuntu)
Last-Modified: Mon, 07 Nov 2011 12:57:40 GMT
ETag: "19a-4b124998df900-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 231
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<html>
  <head>
    <title>The Last Page of the Internet</title>
  </head>
  <body>
    <center>
      <h1><b><u>Attention:</u></b></h1>
      <p><br><strong> You have reached the very last page of the Internet.</
```

1 client pkt(s), 1 server pkt(s), 1 turn(s).

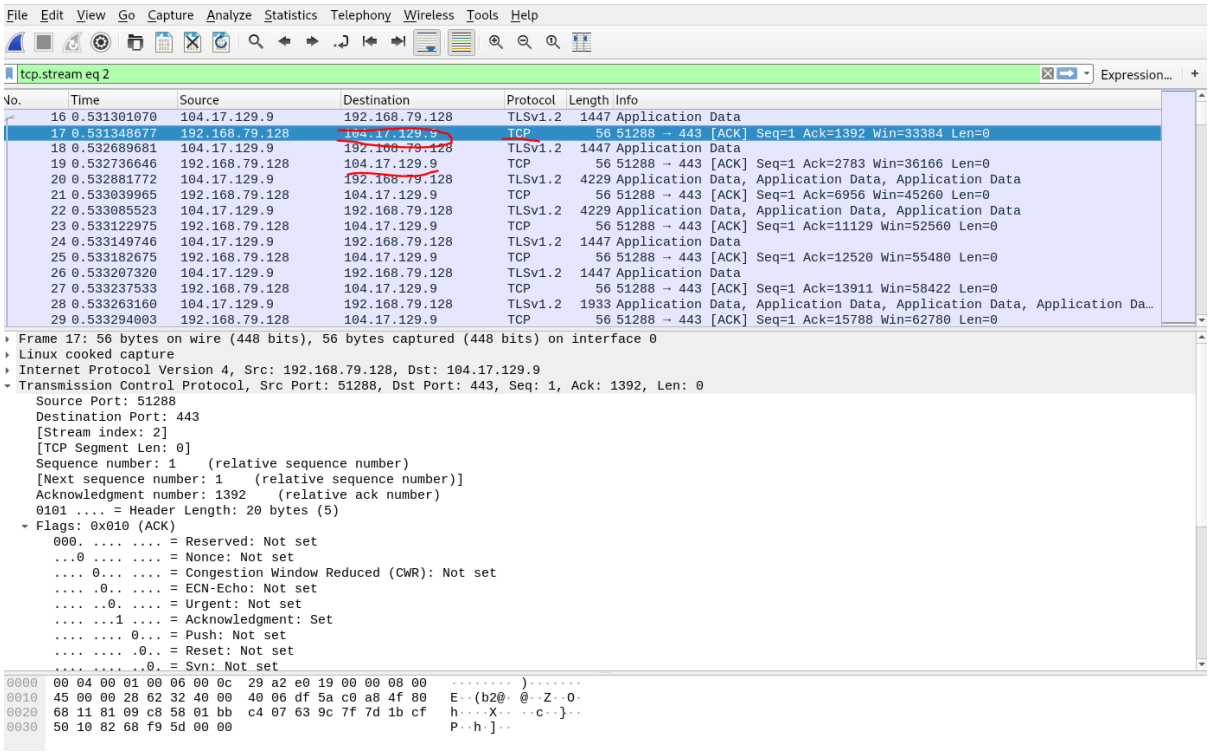
Entire conversation (1,184 bytes) | Show and save data as ASCII

Find: | Find Next

Help | Filter Out This Stream | Print | Save as... | Back | Close

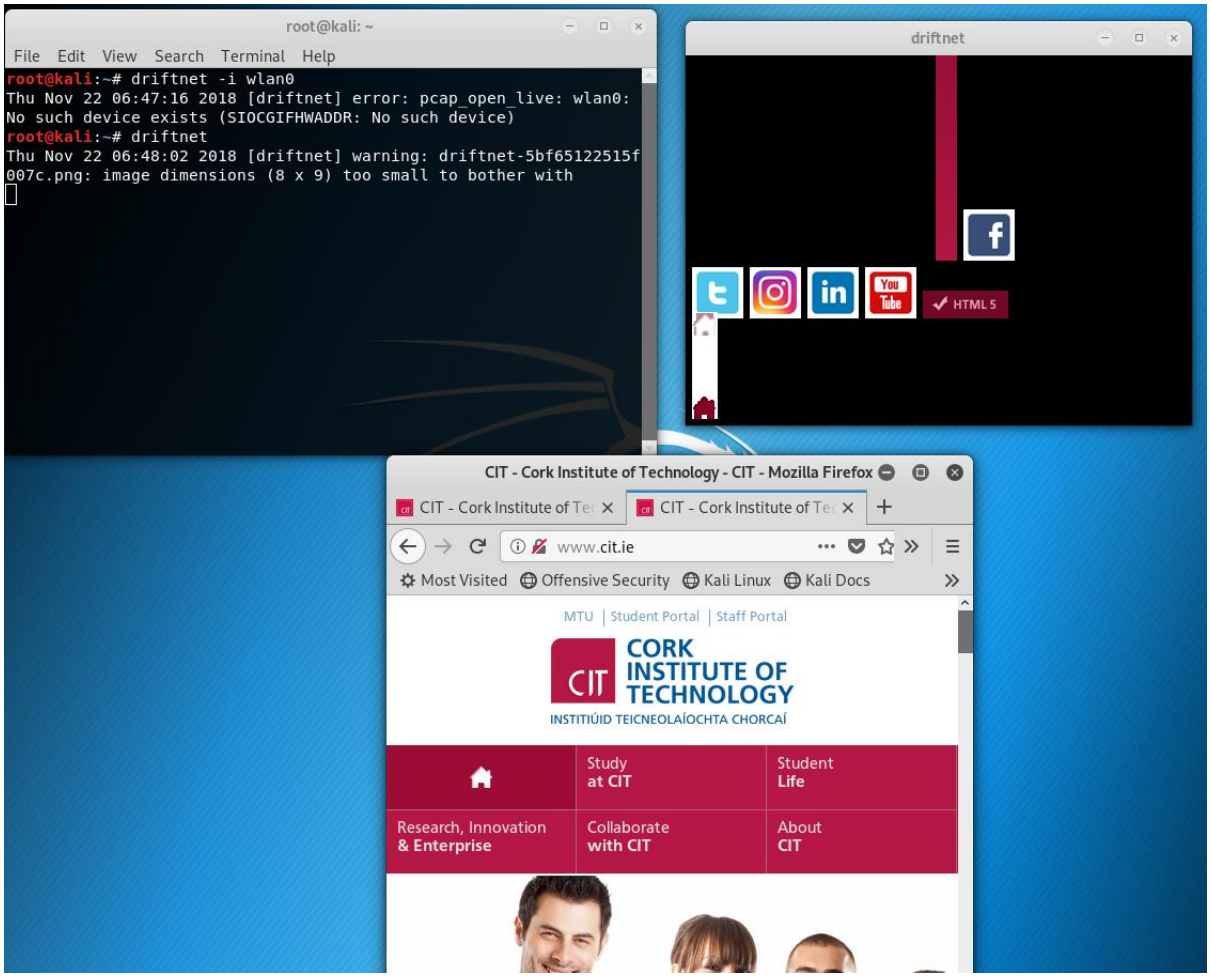
I have used http to find out the above address and its data capture filter.

Capturing Data through Wireshark for -www.warnerbros.com screenshot



I used TCP stream to filter the www.warnerbros.com web site.

Using www.cit.ie driftnet



I tried with www.rte.ie website and it did not work on driftnet for image. It's because you can only browse Google over https only and not http. Even if you force http, the response for that request will be a redirect to https. Cit website is not https secure. So that I can see the picture on driftnet.