

Lab 2

Mohammed Alom

R00144214

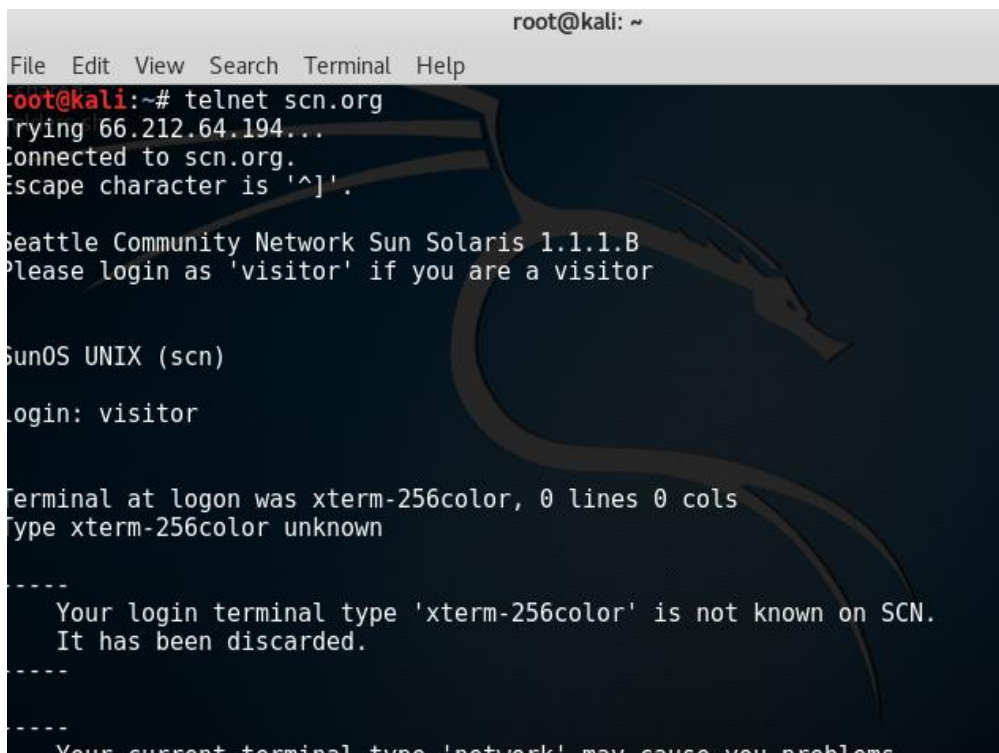
Date – 13/11/2018

Part 1: Using Telnet, SSH, and FTP

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



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# telnet scn.org
Trying 66.212.64.194...
Connected to scn.org.
Escape character is '^]'.

Seattle Community Network Sun Solaris 1.1.1.B
Please login as 'visitor' if you are a visitor

SunOS UNIX (scn)

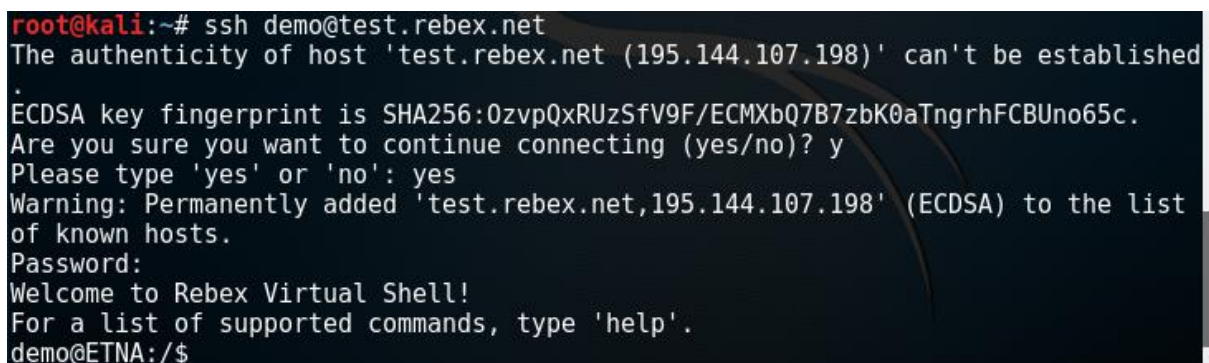
login: visitor

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
-----
```

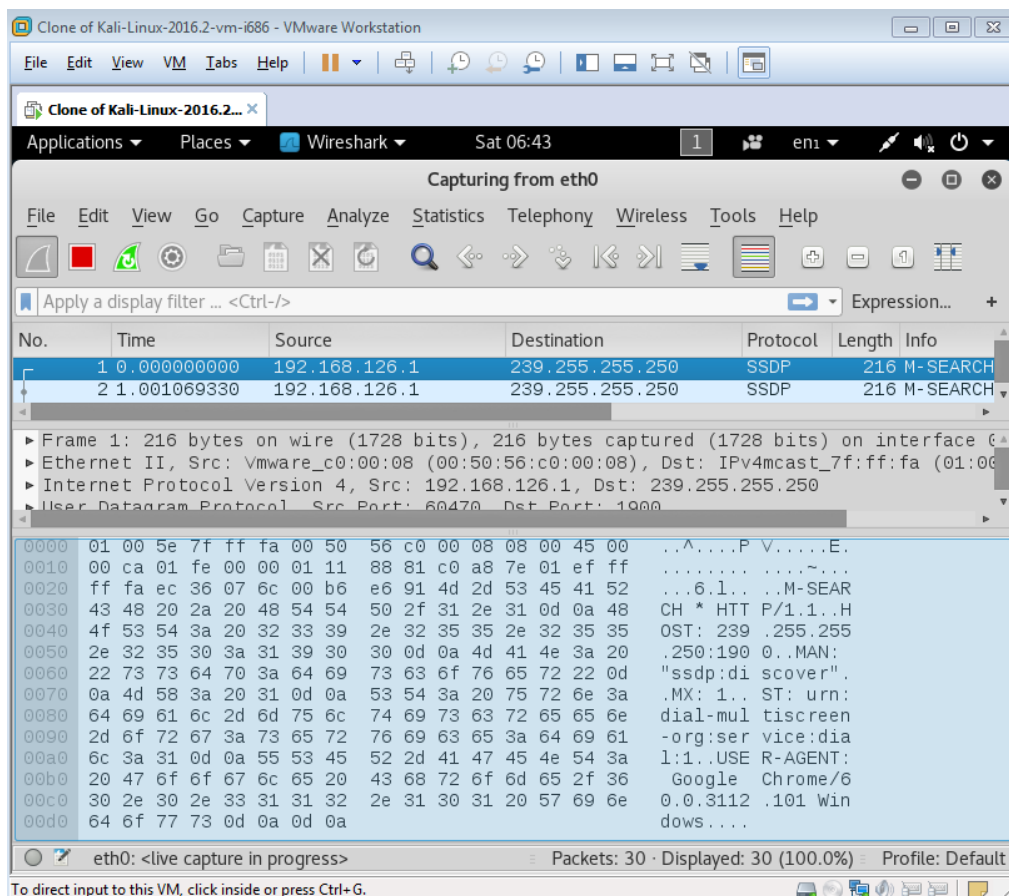
Ssh screenshot



```
root@kali:~# ssh demo@test.rebex.net
The authenticity of host 'test.rebex.net (195.144.107.198)' can't be established
ECDSA key fingerprint is SHA256:0zvpQxRUzSfV9F/ECMXbQ7B7zbK0aTngrhFCBUno65c.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added 'test.rebex.net,195.144.107.198' (ECDSA) to the list
of known hosts.
Password:
Welcome to Rebex Virtual Shell!
For a list of supported commands, type 'help'.
demo@ETNA:/$
```

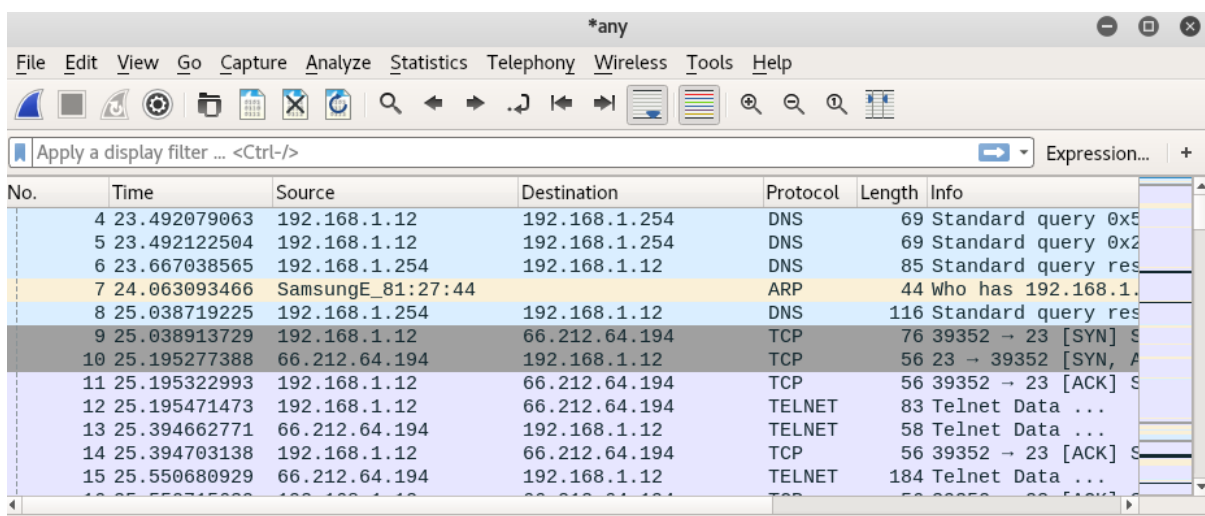
Part 2: Capturing and analysing traffic using Wireshark (50%)

Wireshark screenshot



Capturing Telnet and SSH Traffic

Telnet Data Traffic



*any						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Apply a display filter ... <Ctrl-/> Expression...						
No.	Time	Source	Destination	Protocol	Length	Info
76	38.976063654	66.212.64.194	192.168.1.12	TCP	133	[TCP Retransmission]
77	38.976100948	192.168.1.12	66.212.64.194	TCP	56	[TCP ACKed unseen]
78	42.460525001	192.168.1.12	66.212.64.194	TELNET	58	Telnet Data ...
79	42.656346339	66.212.64.194	192.168.1.12	TELNET	104	Telnet Data ...
80	42.656386428	192.168.1.12	66.212.64.194	TCP	56	39352 → 23 [ACK] S
81	44.966795308	192.168.1.12	66.212.64.194	TELNET	58	Telnet Data ...
82	45.163985440	66.212.64.194	192.168.1.12	TELNET	140	Telnet Data ...
83	45.164023153	192.168.1.12	66.212.64.194	TCP	56	39352 → 23 [ACK] S
84	45.319076160	66.212.64.194	192.168.1.12	TELNET	143	Telnet Data ...
85	45.319106401	192.168.1.12	66.212.64.194	TCP	56	39352 → 23 [ACK] S
86	45.474262771	66.212.64.194	192.168.1.12	TELNET	328	Telnet Data ...
87	45.474300066	192.168.1.12	66.212.64.194	TCP	56	39352 → 23 [ACK] S

telnet						
Expression...						
No.	Time	Source	Destination	Protocol	Length	Info
12	25.195471473	192.168.1.12	66.212.64.194	TELNET	83	Telnet Data ...
13	25.394662771	66.212.64.194	192.168.1.12	TELNET	58	Telnet Data ...
15	25.550680929	66.212.64.194	192.168.1.12	TELNET	184	Telnet Data ...
17	25.550815441	192.168.1.12	66.212.64.194	TELNET	76	Telnet Data ...
18	25.719826935	66.212.64.194	192.168.1.12	TELNET	90	Telnet Data ...
19	25.719913188	192.168.1.12	66.212.64.194	TELNET	62	Telnet Data ...
20	25.875305857	66.212.64.194	192.168.1.12	TELNET	63	Telnet Data ...
22	26.070805755	66.212.64.194	192.168.1.12	TELNET	59	Telnet Data ...

▶ 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

0000	00 00 00 01 00 06 58 d7	59 1e 40 b2 00 00 08 00X. Y.@....
0010	45 00 01 4c 4e af 00 00	2e 06 f7 b2 42 d4 40 c2	E..LN.B.@.
0020	c0 a8 01 0c 00 17 99 b8	35 c1 bc 43 63 fc 1c 3d 5..Cc.==
0030	50 18 10 00 84 88 00 00	20 20 20 20 20 53 43 4e	P..... SCN
0040	20 41 73 73 6f 63 69 61	74 69 6f 6e 0d 0a 20 20	Associa tion..
0050	20 20 20 20 20 20 50 4f	20 42 6f 78 20 39 34 37	PO Box 947
0060	0d 0a 20 20 20 20 20 20	20 20 53 65 61 74 74 6c	.. Seattl
0070	65 2c 20 57 41 20 39 38	31 31 31 2d 30 39 34 37	e, WA 98 111-0947
0080	0d 0a 0d 0a 54 68 65 20	53 43 4e 20 63 6f 6e 6e	...The SCN conn
0090	65 63 74 69 6f 6e 20 79	6f 75 20 61 72 65 20 6e	ection y ou are n
00a0	6f 77 20 75 73 69 6e 67	20 69 73 20 63 6f 75 72	ow using is cour
00b0	74 65 73 79 20 6f 68 3a	6d 0a 0d 0a 53 65 61 74	tesy of: Seatt

SSH Capturing Data Traffic

*any						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Apply a display filter ... <Ctrl-/> Expression...						
No.	Time	Source	Destination	Protocol	Length	Info
226	150.005694482	192.168.1.12	195.144.107.198	SSHv2	84	Client: New Keys
227	150.259497010	195.144.107.198	192.168.1.12	TCP	68	22 → 39802 [ACK] S
228	150.259533955	192.168.1.12	195.144.107.198	SSHv2	132	Client: Encrypted
229	150.316092177	195.144.107.198	192.168.1.12	SSHv2	132	Server: Encrypted
230	150.316105726	192.168.1.12	195.144.107.198	TCP	68	39802 → 22 [ACK] S
231	150.316188067	192.168.1.12	195.144.107.198	SSHv2	148	Client: Encrypted
232	150.377184415	195.144.107.198	192.168.1.12	SSHv2	164	Server: Encrypted
233	150.377295111	192.168.1.12	195.144.107.198	SSHv2	180	Client: Encrypted
234	150.431401318	195.144.107.198	192.168.1.12	SSHv2	148	Server: Encrypted
235	150.472252931	192.168.1.12	195.144.107.198	TCP	68	39802 → 22 [ACK] S
236	150.939303402	192.168.1.10	192.168.1.255	DB-LSP...	190	Dropbox LAN sync D
237	154.626691486	HuaweiTe_1e:40:b2	195.144.107.198	ARP	62	Who has 192.168.1.1

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 Prev]		
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: ...vviissitttoorr  
.  
  
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  
technology
```

34 client pkts, 66 server pkts, 65 turns.

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

Find: Find Next

```

<<< 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
17 25.550815444	192.168.1.12	66.212.64.194	TELNET	76 Telnet Data ...

- ▶ 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...@curve25519-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-
sha2-nistp256,diffie-hellman-group16-sha512,diffie-hellman-
```

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


```
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  
$.C.'.....=.h(s.E+=C..h!x.<..|....  
... ]3a..`>.>..~...|..... ..HC..s...*b....mE..  
6W...o.L...#... _J  
...;.....|.. \r./.% .MC9...f....{. @..@).282...T.t..  
aMd=>.nw.Yf...F..."..v .&S....l.sk.t0.....T8^..._..mmI...G...[....  
2=.2s....._..n..Y..NO.G .F..Ft](....U~(w.({..@....bc..5.M|..?<.ZWz&..`.....0:|. #.,...uL.o.../...N..Lc.>..P.0...V.cj#..  
+..H....}$....n..s..\.=P{b.q..>..?..x....  
4...:gf...~*...../..Rz.Y.....o.o.)..8..02....H.k4...B%.  
3...>..Z.f..  
MT_d
```

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%)

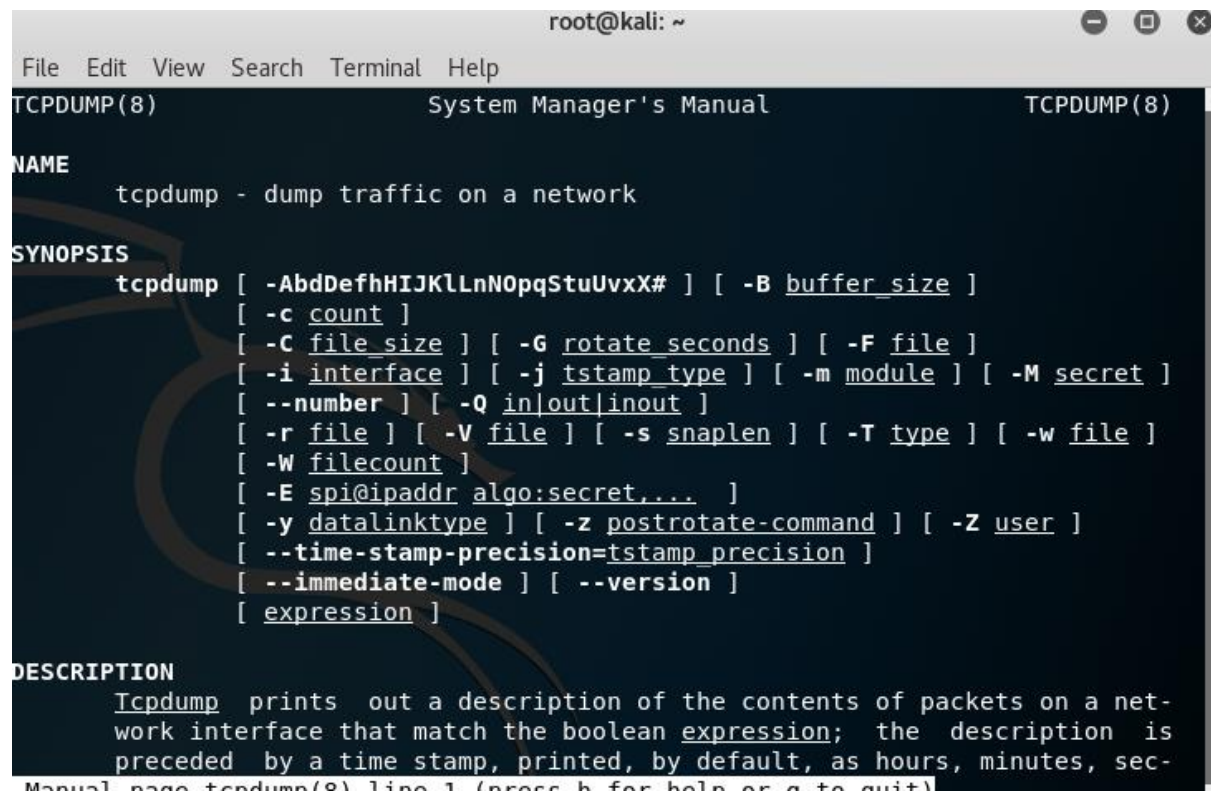
Running Tcpdump

```
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  
32 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



The screenshot shows a terminal window titled "root@kali: ~" with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal displays the man page for "TCPDUMP(8)". The page content includes:

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 network interface that match the boolean expression; the description is preceded by a time stamp, printed, by default, as hours, minutes, seconds.

Manual page tcpdump(8) line 1 (press h for help or q to quit)

Tcpdump -i lo screenshot

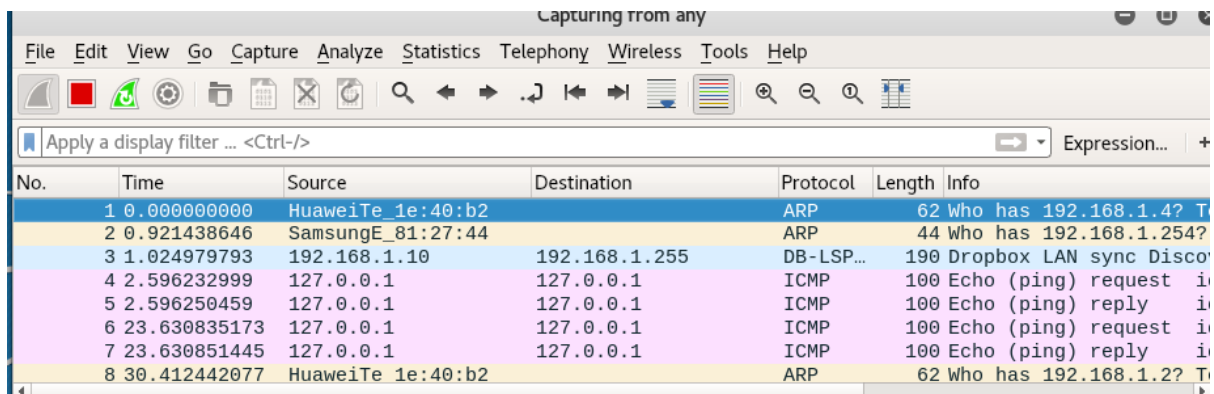
```
root@kali:~# tcpdump -i lo
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Ping command screenshot

```
root@kali:~# ping -c1 127.0.0.1
PING 127.0.0.1 (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

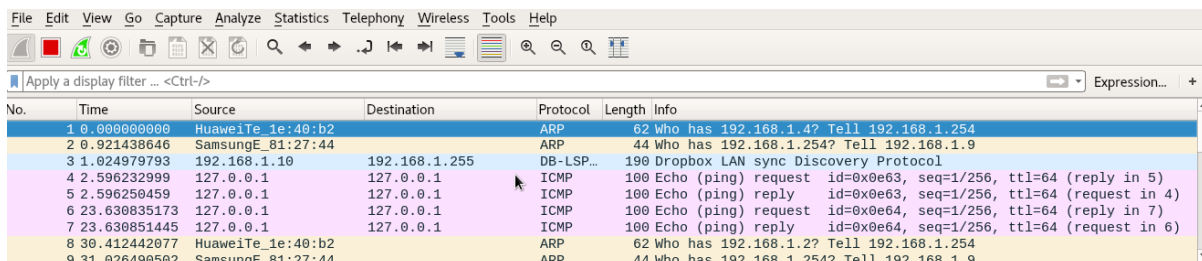
--- 127.0.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.048/0.048/0.048/0.000 ms
root@kali:~#
```

Capturing ping in the Wireshark



Wireshark packet capture showing network traffic. The interface is 'Capturing from any'. The packet list shows 8 packets. The first two are ARP requests from Huawei and Samsung interfaces. The next three are ICMP Echo (ping) requests from 192.168.1.10 to 127.0.0.1. The last three are ICMP Echo (ping) replies from 127.0.0.1 to 192.168.1.10 and an ARP request from Huawei.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	HuaweiTe_1e:40:b2		ARP	62	Who has 192.168.1.4? Tell 192.168.1.254
2	0.921438646	SamsungE_81:27:44		ARP	44	Who has 192.168.1.254? Tell 192.168.1.9
3	1.024979793	192.168.1.10	192.168.1.255	DB-LSP...	190	Dropbox LAN sync Discovery Protocol
4	2.596232999	127.0.0.1	127.0.0.1	ICMP	100	Echo (ping) request id=0x0e63, seq=1/256, ttl=64 (request in 5)
5	2.596250459	127.0.0.1	127.0.0.1	ICMP	100	Echo (ping) reply id=0x0e63, seq=1/256, ttl=64 (request in 4)
6	23.630835173	127.0.0.1	127.0.0.1	ICMP	100	Echo (ping) request id=0x0e64, seq=1/256, ttl=64 (request in 7)
7	23.630851445	127.0.0.1	127.0.0.1	ICMP	100	Echo (ping) reply id=0x0e64, seq=1/256, ttl=64 (request in 6)
8	30.412442077	HuaweiTe_1e:40:b2		ARP	62	Who has 192.168.1.2? Tell 192.168.1.254



Wireshark packet capture showing network traffic. The interface is 'Capturing from any'. The packet list shows 8 packets. The first two are ARP requests from Huawei and Samsung interfaces. The next three are ICMP Echo (ping) requests from 192.168.1.10 to 127.0.0.1. The last three are ICMP Echo (ping) replies from 127.0.0.1 to 192.168.1.10 and an ARP request from Huawei.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	HuaweiTe_1e:40:b2		ARP	62	Who has 192.168.1.4? Tell 192.168.1.254
2	0.921438646	SamsungE_81:27:44		ARP	44	Who has 192.168.1.254? Tell 192.168.1.9
3	1.024979793	192.168.1.10	192.168.1.255	DB-LSP...	190	Dropbox LAN sync Discovery Protocol
4	2.596232999	127.0.0.1	127.0.0.1	ICMP	100	Echo (ping) request id=0x0e63, seq=1/256, ttl=64 (request in 5)
5	2.596250459	127.0.0.1	127.0.0.1	ICMP	100	Echo (ping) reply id=0x0e63, seq=1/256, ttl=64 (request in 4)
6	23.630835173	127.0.0.1	127.0.0.1	ICMP	100	Echo (ping) request id=0x0e64, seq=1/256, ttl=64 (request in 7)
7	23.630851445	127.0.0.1	127.0.0.1	ICMP	100	Echo (ping) reply id=0x0e64, seq=1/256, ttl=64 (request in 6)
8	30.412442077	HuaweiTe_1e:40:b2		ARP	62	Who has 192.168.1.2? Tell 192.168.1.254
9	31.026498502	SamsungE_81:27:44		ARP	44	Who has 192.168.1.254? Tell 192.168.1.9

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

Wireshark packet capture showing a list of packets. The selected packet (No. 9) is a TCP segment from 172.245.130.175 to 192.168.79.128, sequence number 1, acknowledgment number 439. The packet details pane shows the following information:

- Frame 9: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
- Linux cooked capture
- Internet Protocol Version 4, Src: 172.245.130.175, Dst: 192.168.79.128
- Transmission Control Protocol, Src Port: 80, Dst Port: 35240, Seq: 1, Ack: 439, Len: 0
- Source Port: 80
- Destination Port: 35240
- [Stream index: 0]
- [TCP Segment Len: 0]
- Sequence number: 1 (relative sequence number)
- [Next sequence number: 1 (relative sequence number)]
- Acknowledgment number: 439 (relative ack number)

Wireshark packet capture showing a list of packets. The selected packet (No. 8) is a TCP segment from 192.168.79.128 to 172.245.130.175, sequence number 1, acknowledgment number 1. The packet details pane shows the following information:

- Frame 8: 494 bytes on wire (3952 bits), 494 bytes captured (3952 bits) on interface 0
- Linux cooked capture
- Internet Protocol Version 4, Src: 192.168.79.128, Dst: 172.245.130.175
- Transmission Control Protocol, Src Port: 35240, Dst Port: 80, Seq: 1, Ack: 1, Len: 438
- Source Port: 35240
- Destination Port: 80
- [Stream index: 0]
- [TCP Segment Len: 438]
- Sequence number: 1 (relative sequence number)
- [Next sequence number: 439 (relative sequence number)]
- Acknowledgment number: 1 (relative ack number)
- 0101 = Header Length: 20 bytes (5)
- Flags: 0x018 (PSH, ACK)
- 000. = Reserved: Not set
- ...0 = Nonce: Not set
- ... 0... = Congestion Window Reduced (CWR): Not set
-0.. = ECN-Echo: Not set

The packet bytes pane shows the raw data of the SYN packet:

```
0000 00 04 00 01 00 06 00 0c 29 a2 e0 19 00 00 08 00 ..... ).....
0010 45 00 01 de 7b bf 40 00 40 06 7d 8d c0 a8 4f 80 E...{.:@.@}...0.
0020 ac f5 82 af 89 a8 00 50 0d 82 04 4b 02 12 1f 75 .....P...K...u
0030 50 18 72 10 41 9e 00 00 47 45 54 20 2f 6c 61 73 P-r-A... GET /las
0040 74 70 61 67 65 2f 20 48 54 54 50 2f 31 2e 31 0d tpage/ H TTP/1.1.
0050 0a 48 6f 73 74 3a 20 77 77 77 2e 31 31 31 32 2e .Host: w ww.1112.
```

Tcp stream

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.....{0/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 verv last page of the Internet.</p>
    </center>
  </body>
</html>
```

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

Wireshark interface showing a network capture filtered by `tcp.stream eq 2`. The packet list displays several packets, with the selected packet (No. 17) showing details in the packet details pane.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
16	0.531301070	104.17.129.9	192.168.79.128	TLSv1.2	1447	Application Data
17	0.531348677	192.168.79.128	104.17.129.9	TCP	56	51288 → 443 [ACK] Seq=1 Ack=1392 Win=33384 Len=0
18	0.532689681	104.17.129.9	192.168.79.128	TLSv1.2	1447	Application Data
19	0.532736646	192.168.79.128	104.17.129.9	TCP	56	51288 → 443 [ACK] Seq=1 Ack=2783 Win=36166 Len=0
20	0.532881772	104.17.129.9	192.168.79.128	TLSv1.2	4229	Application Data, Application Data, Application Data
21	0.533039965	192.168.79.128	104.17.129.9	TCP	56	51288 → 443 [ACK] Seq=1 Ack=6956 Win=45260 Len=0
22	0.533085523	104.17.129.9	192.168.79.128	TLSv1.2	4229	Application Data, Application Data, Application Data
23	0.533122975	192.168.79.128	104.17.129.9	TCP	56	51288 → 443 [ACK] Seq=1 Ack=11129 Win=52560 Len=0
24	0.533149746	104.17.129.9	192.168.79.128	TLSv1.2	1447	Application Data
25	0.533182675	192.168.79.128	104.17.129.9	TCP	56	51288 → 443 [ACK] Seq=1 Ack=12520 Win=55480 Len=0
26	0.533207320	104.17.129.9	192.168.79.128	TLSv1.2	1447	Application Data
27	0.533237533	192.168.79.128	104.17.129.9	TCP	56	51288 → 443 [ACK] Seq=1 Ack=13911 Win=58422 Len=0
28	0.533263160	104.17.129.9	192.168.79.128	TLSv1.2	1933	Application Data, Application Data, Application Data
29	0.533294003	192.168.79.128	104.17.129.9	TCP	56	51288 → 443 [ACK] Seq=1 Ack=15788 Win=62780 Len=0

Packet Details (Frame 17):

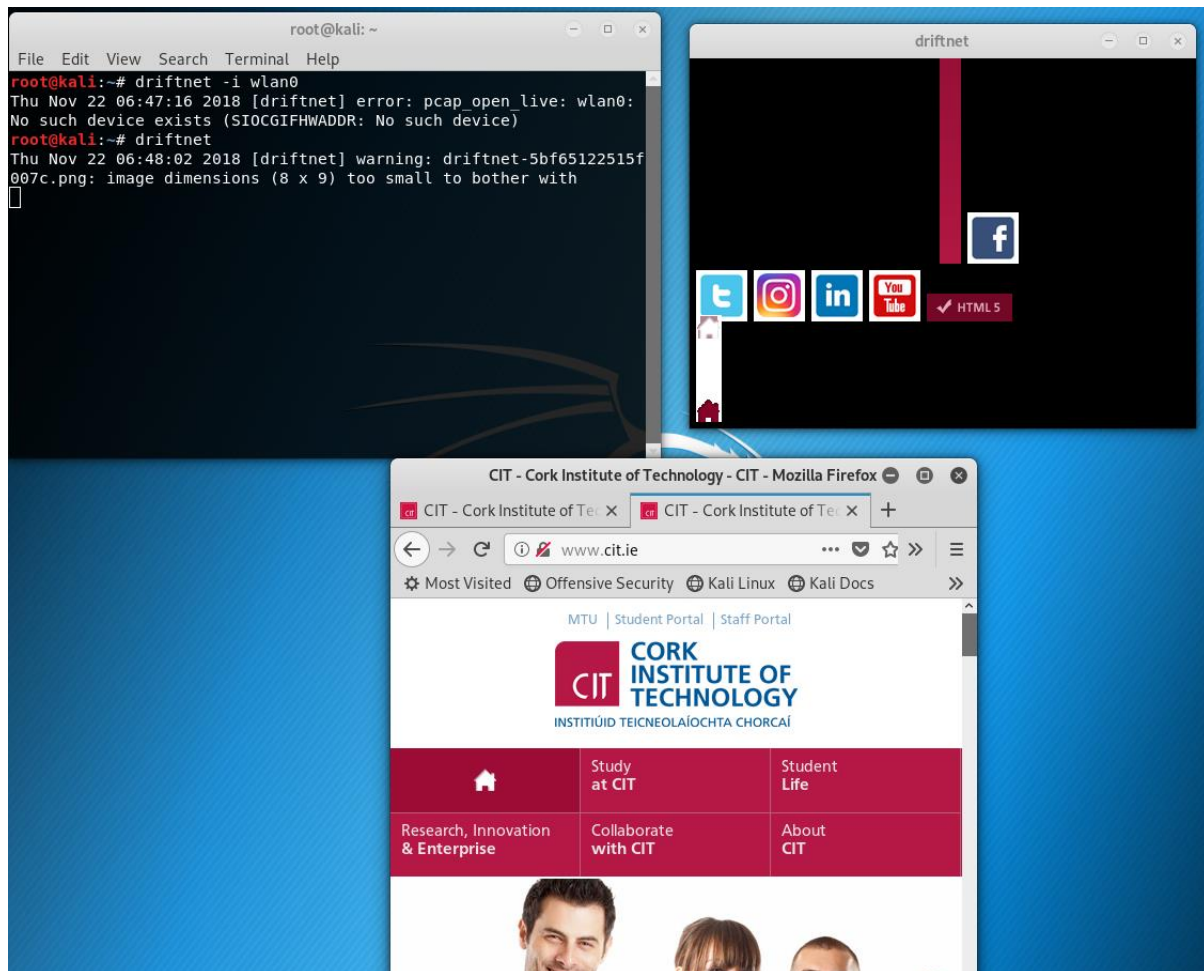
- Linux cooked capture
- Internet Protocol Version 4, Src: 192.168.79.128, Dst: 104.17.129.9
- Transmission Control Protocol, Src Port: 51288, Dst Port: 443, Seq: 1, Ack: 1392, Len: 0
 - Source Port: 51288
 - Destination Port: 443
 - [Stream index: 2]
 - [TCP Segment Len: 0]
 - Sequence number: 1 (relative sequence number)
 - [Next sequence number: 1 (relative sequence number)]
 - Acknowledgment number: 1392 (relative ack number)
 - 0101 = Header Length: 20 bytes (5)
 - Flags: 0x010 (ACK)
 - 000. = Reserved: Not set
 - ...0 = Nonce: Not set
 -0... = Congestion Window Reduced (CWR): Not set
 -0... = ECN-Echo: Not set
 -0... = Urgent: Not set
 -1... = Acknowledgment: Set
 -1... = Push: Not set
 -0... = Reset: Not set
 -0... = SYN: Not set

Packet Bytes:

Offset	Hex	ASCII
0000	00 04 00 01 00 06 00 0c 29 a2 e0 19 00 00 08 00).....
0010	45 00 00 28 62 32 40 00 40 06 df 5a c0 a8 4f 80	E..(b2@ @.Z..0.
0020	68 11 81 09 c8 58 01 bb c4 07 63 9c 7f 7d 1b cf	h...X...c...}..
0030	50 10 82 68 f9 5d 00 00	P..h]..

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.