

TP 1 : VMWare et Wireshark

Question 7 :

```
root@ChrysippusKali2016: ~  
File Edit View Search Terminal Help  
root@ChrysippusKali2016 Aurélien DUVAL ~#ifconfig -a  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.1.163 netmask 255.255.255.0 broadcast 192.168.1.255  
    inet6 fe80::20c:29ff:fe8a:7490 prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:8a:74:90 txqueuelen 1000 (Ethernet)  
    RX packets 76695 bytes 115001763 (109.6 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 29514 bytes 1783558 (1.7 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1 (Local Loopback)  
    RX packets 26 bytes 1458 (1.4 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 26 bytes 1458 (1.4 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
root@ChrysippusKali2016 Aurélien DUVAL ~#  
usbmon0  
usbmon1  
usbmon2  
Random packet generator: randpkt  
  
Learn  
User's Guides · Wiki · Questions and Answers · Mailing Lists  
You are running Wireshark 2.2.0 (Git Rev Unknown from unknown).  
  
Ready to load or capture No Packets Profile: Default
```

Question 11 :

```
Applications Places Wireshark Tue Sep 20, 17:10  
*eth0  
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help  
arp OR icmp  
No. Time Source Destination Protocol Length Info  
1 0.000000000 192.168.1.1 192.168.1.163 ICMP 98 Echo (ping) request id=0x0d2a, seq=1/256, ttl=64 (reply in 4)  
2 0.000041147 Vmware_8a:74:90 Broadcast ARP 42 Who has 192.168.1.1? Tell 192.168.1.163  
3 0.000101190 Vmware_c0:00:01 Vmware_8a:74:90 ARP 60 192.168.1.1 is at 00:50:56:c0:00:01  
4 0.000106159 192.168.1.163 192.168.1.1 ICMP 98 Echo (ping) reply id=0x0d2a, seq=1/256, ttl=64 (request in 1)  
5 0.999036517 192.168.1.1 192.168.1.163 ICMP 98 Echo (ping) request id=0x0d2a, seq=2/512, ttl=64 (reply in 6)  
6 0.999069933 192.168.1.163 192.168.1.1 ICMP 98 Echo (ping) reply id=0x0d2a, seq=2/512, ttl=64 (request in 5)  
7 1.998524379 192.168.1.1 192.168.1.163 ICMP 98 Echo (ping) request id=0x0d2a, seq=3/768, ttl=64 (reply in 8)  
8 1.998572130 192.168.1.163 192.168.1.1 ICMP 98 Echo (ping) reply id=0x0d2a, seq=3/768, ttl=64 (request in 7)  
9 2.998644496 192.168.1.1 192.168.1.163 ICMP 98 Echo (ping) request id=0x0d2a, seq=4/1024, ttl=64 (reply in 10)  
10 2.998699455 192.168.1.163 192.168.1.1 ICMP 98 Echo (ping) reply id=0x0d2a, seq=4/1024, ttl=64 (request in 9)  
11 3.998661296 192.168.1.1 192.168.1.163 ICMP 98 Echo (ping) request id=0x0d2a, seq=5/1280, ttl=64 (reply in 12)  
12 3.998731383 192.168.1.163 192.168.1.1 ICMP 98 Echo (ping) reply id=0x0d2a, seq=5/1280, ttl=64 (request in 11)  
13 4.998475646 192.168.1.1 192.168.1.163 ICMP 98 Echo (ping) request id=0x0d2a, seq=6/1536, ttl=64 (reply in 14)  
14 4.998509632 192.168.1.163 192.168.1.1 ICMP 98 Echo (ping) reply id=0x0d2a, seq=6/1536, ttl=64 (request in 13)  
15 5.998483701 192.168.1.1 192.168.1.163 ICMP 98 Echo (ping) request id=0x0d2a, seq=7/1792, ttl=64 (reply in 16)  
16 5.998510125 192.168.1.163 192.168.1.1 ICMP 98 Echo (ping) reply id=0x0d2a, seq=7/1792, ttl=64 (request in 15)  
  
Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0  
Ethernet II, Src: Vmware_c0:00:01 (00:50:56:c0:00:01), Dst: Vmware_8a:74:90 (00:0c:29:8a:74:90)  
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.163  
Internet Control Message Protocol  
  
0000 00 0c 29 8a 74 90 00 50 56 c0 00 01 08 00 45 00 .).t..P V.....E.  
0010 00 54 e8 5a 40 00 40 01 ce 59 c0 a8 01 01 c0 a8 .T.Z@..Y.....  
0020 01 a3 08 00 ed 0b 0d 2a 00 01 28 a5 e1 57 00 00 .....* ..(.W..  
0030 00 00 2c f9 08 00 00 00 00 00 11 12 13 14 15 .....  
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 ..... 1"#3%  
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,-./012345  
0060 36 37 67  
  
Invalid filter: "OR" was unexpected in this context. Packets: 30 · Displayed: 30 (100.0%) Profile: Default
```

Question 12 :

The screenshot shows a Wireshark capture of ICMP Echo (ping) traffic. The packet list shows 22 packets, alternating between requests and replies. The packet details pane shows the structure of an ICMP Echo request, including the type (8), code (0), identifier (0x0d2a), and sequence number (2512). The packet bytes pane shows the raw data of the ICMP Echo request, including the type, code, identifier, sequence number, and the payload (0x0d2a).

No.	Time	Source	Destination	Protocol	Length	Info
6	0.999069933	192.168.1.163	192.168.1.1	ICMP	98	Echo (ping) reply id=0x0d2a, seq=2/512, ttl=64 (request in 5)
7	1.998524379	192.168.1.1	192.168.1.163	ICMP	98	Echo (ping) request id=0x0d2a, seq=3/768, ttl=64 (reply in 7)
8	1.998572130	192.168.1.163	192.168.1.1	ICMP	98	Echo (ping) reply id=0x0d2a, seq=3/768, ttl=64 (request in 7)
9	2.998644496	192.168.1.1	192.168.1.163	ICMP	98	Echo (ping) request id=0x0d2a, seq=4/1024, ttl=64 (reply in 10)
10	2.998699455	192.168.1.163	192.168.1.1	ICMP	98	Echo (ping) reply id=0x0d2a, seq=4/1024, ttl=64 (request in 9)
11	3.998661296	192.168.1.1	192.168.1.163	ICMP	98	Echo (ping) request id=0x0d2a, seq=5/1280, ttl=64 (reply in 12)
12	3.998731383	192.168.1.163	192.168.1.1	ICMP	98	Echo (ping) reply id=0x0d2a, seq=5/1280, ttl=64 (request in 11)
13	4.998475646	192.168.1.1	192.168.1.163	ICMP	98	Echo (ping) request id=0x0d2a, seq=6/1536, ttl=64 (reply in 14)
14	4.998509632	192.168.1.163	192.168.1.1	ICMP	98	Echo (ping) reply id=0x0d2a, seq=6/1536, ttl=64 (request in 13)
15	5.998483701	192.168.1.1	192.168.1.163	ICMP	98	Echo (ping) request id=0x0d2a, seq=7/1792, ttl=64 (reply in 16)
16	5.998518426	192.168.1.163	192.168.1.1	ICMP	98	Echo (ping) reply id=0x0d2a, seq=7/1792, ttl=64 (request in 15)
17	6.998515678	192.168.1.1	192.168.1.163	ICMP	98	Echo (ping) request id=0x0d2a, seq=8/2048, ttl=64 (reply in 18)
18	6.998576833	192.168.1.163	192.168.1.1	ICMP	98	Echo (ping) reply id=0x0d2a, seq=8/2048, ttl=64 (request in 17)
19	7.998475070	192.168.1.1	192.168.1.163	ICMP	98	Echo (ping) request id=0x0d2a, seq=9/2304, ttl=64 (reply in 20)
20	7.998509972	192.168.1.163	192.168.1.1	ICMP	98	Echo (ping) reply id=0x0d2a, seq=9/2304, ttl=64 (request in 19)
21	8.998642553	192.168.1.1	192.168.1.163	ICMP	98	Echo (ping) request id=0x0d2a, seq=10/2560, ttl=64 (reply in 22)

Frame 6: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: Vmware_8a:74:90 (00:0c:29:8a:74:90), Dst: Vmware_c0:00:01 (00:50:56:c0:00:01)
Internet Protocol version 4, Src: 192.168.1.163, Dst: 192.168.1.1
Internet Control Message Protocol

0000 00 50 56 c0 00 01 00 0c 29 8a 74 90 08 00 45 00 .PV....).t...E.
0010 00 54 9a 99 00 00 40 01 5c 1b c0 a8 01 a3 c0 a8 .T...@. \.....
0020 01 01 00 00 da 0e 0d 2a 00 02 29 a5 e1 57 00 00*...).W..
0030 00 00 46 f5 08 00 00 00 00 00 10 11 12 13 14 15 .F.....
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25!#\$%&'()*+,-./012345
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,-./012345
0060 36 37 67

Question 15:

The screenshot shows a terminal window running an Nmap scan of 192.168.1.110. The output shows that the host is up and that the scan found several open ports (21/tcp, 22/tcp, 80/tcp, 631/tcp). The scan was completed in 0.29 seconds. The terminal also shows the command used to run the scan: `root@ChrysippusKali2016:~# nmap 192.168.1.110`.

```
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2016-09-20 17:29 EDT
mass dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.110
Host is up (0.00055s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
631/tcp   open  ipp
MAC Address: 00:0C:29:87:64:12 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
root@ChrysippusKali2016:~#
```

The screenshot also shows a Wireshark capture of the Nmap scan traffic. The packet list shows the Nmap scan request and the response. The packet details pane shows the structure of the Nmap scan request, including the type (0), code (0), identifier (0x0d2a), and sequence number (2512). The packet bytes pane shows the raw data of the Nmap scan request, including the type, code, identifier, sequence number, and the payload (0x0d2a).

Frame 6: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: Vmware_8a:74:90 (00:0c:29:8a:74:90), Dst: Vmware_c0:00:01 (00:50:56:c0:00:01)
Internet Protocol version 4, Src: 192.168.1.163, Dst: 192.168.1.1
Internet Control Message Protocol

0000 00 50 56 c0 00 01 00 0c 29 8a 74 90 08 00 45 00 .PV....).t...E.
0010 00 54 9a 99 00 00 40 01 5c 1b c0 a8 01 a3 c0 a8 .T...@. \.....
0020 01 01 00 00 da 0e 0d 2a 00 02 29 a5 e1 57 00 00*...).W..
0030 00 00 46 f5 08 00 00 00 00 00 10 11 12 13 14 15 .F.....
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25!#\$%&'()*+,-./012345
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,-./012345
0060 36 37 67

Question 16: [1]

The screenshot shows a Wireshark capture on interface eth0. The first packet is an ARP request (No. 1) from VMware_8a:74:90 to Broadcast, asking for the MAC of 192.168.1.110. This is followed by a series of TCP SYN packets (Nos. 2-16) from 192.168.1.110 to 192.168.1.163, all with Seq=0 and Win=1024. The capture ends with RST, ACK packets (Nos. 13-16) from 192.168.1.163 back to 192.168.1.110.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	Vmware_8a:74:90	Broadcast	ARP	42	Who has 192.168.1.110? Tell 192.168.1.163
2	0.000698996	Vmware_8a:74:90	Vmware_8a:74:90	ARP	60	192.168.1.110 is at 00:0c:29:87:64:12
3	0.067935231	192.168.1.163	192.168.1.110	TCP	58	52612->23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4	0.068031074	192.168.1.163	192.168.1.110	TCP	58	52612->113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
5	0.068066990	192.168.1.163	192.168.1.110	TCP	58	52612->1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	0.068096522	192.168.1.163	192.168.1.110	TCP	58	52612->143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7	0.068137605	192.168.1.163	192.168.1.110	TCP	58	52612->554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
8	0.068165695	192.168.1.163	192.168.1.110	TCP	58	52612->1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9	0.068205505	192.168.1.163	192.168.1.110	TCP	58	52612->111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10	0.068256899	192.168.1.163	192.168.1.110	TCP	58	52612->256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11	0.068285054	192.168.1.163	192.168.1.110	TCP	58	52612->80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12	0.068348754	192.168.1.163	192.168.1.110	TCP	58	52612->3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13	0.068347543	192.168.1.110	192.168.1.163	TCP	60	23->52612 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
14	0.068392192	192.168.1.110	192.168.1.163	TCP	60	113->52612 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15	0.069031280	192.168.1.110	192.168.1.163	TCP	60	1025->52612 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
16	0.069070554	192.168.1.110	192.168.1.163	TCP	60	143->52612 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: Vmware_8a:74:90 (00:0c:29:8a:74:90), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

0000 ff ff ff ff ff ff 00 29 8a 74 90 08 06 00 01).t....
0010 08 00 06 04 00 01 00 29 8a 74 90 c0 a8 01 a3).t....
0020 00 00 00 00 00 00 c0 a8 01 6en

[2]

Question 17: [1]

The screenshot shows the 'Wireshark - Protocol Hierarchy Statistics - BitTorrent' window. The statistics are as follows:

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End B
Frame	100.0	13	100.0	2222	480	0	0
Ethernet	100.0	13	8.2	182	39	0	0
Internet Protocol Version 4	100.0	13	11.7	260	56	0	0
Transmission Control Protocol	100.0	13	80.1	1780	384	3	264
Hypertext Transfer Protocol	15.4	2	32.1	714	154	2	714
BitTorrent	69.2	9	24.0	534	115	7	398
Aggregate Server Access Protocol	7.7	1	3.1	68	14	0	0
Short Frame	7.7	1	0.0	0	0	1	0

Frame 1: 127 bytes on wire (1016 bits), 127 bytes captured (1016 bits) on interface 0
Ethernet II, Src: Vmware_8a:74:90 (00:0c:29:8a:74:90), Dst: 192.168.1.110 (08:00:06:04:00:01)
Internet Protocol Version 4, Src: 192.168.1.110, Dst: 192.168.1.163
Transmission Control Protocol, Src Port: 52612, Dst Port: 80
Hypertext Transfer Protocol, GET / HTTP/1.1

[2]

Applications ▾Places ▾Wireshark ▾

Tue Sep 20, 18:54

1

fr ▾

⏻

BitTorrent.pcap

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

Wireshark

Expression...

No.	Time	Source	Destination	Protocol	Length	Info
2	0.027000000	213.122.214.127	213.202.193.43	BitTor...	122	Handshake
5	10.039000000	213.122.214.127	60.234.152.124	BitTor...	122	Handshake
6	10.093000000	213.122.214.127	80.37.9.37	BitTor...	122	Handshake
7	10.184000000	213.122.214.127	202.88.252.50	BitTor...	122	Handshake
8	15.774000000	60.234.152.124	213.122.214.127	BitTor...	151	Handshake Bitfield, Len:0x18
11	16.456000000	80.37.9.37	213.122.214.127	BitTor...	122	Handshake
12	20.499000000	202.88.252.50	213.122.214.127	BitTor...	151	Handshake Bitfield, Len:0x18

▶ Frame 2: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)

▶ Ethernet II, Src: XeroxCor_00:00:00 (00:00:01:00:00:00), Dst: bc:df:20:00:01:00 (bc:df:20:00:01:00)

▶ Internet Protocol Version 4, Src: 213.122.214.127, Dst: 213.202.193.43

▶ Transmission Control Protocol, Src Port: 3861, Dst Port: 14291, Seq: 1, Ack: 1, Len: 68

▶ BitTorrent

0000bcdf2000010000000100000008004500.....E.

0010006c550a400080066291d57ad67fd5ca..lU.@...b..z...

0020c12b0f1537d3e9995a499b04d3e45018+.7...Zl...P.

00302238ee8c000013426974546f7272656e"8....B itTorren

0040742070726f746f636f6c000000000000t protoc ol.....

005000000164fe7ef1105c57764170edf603...d~.. \wVAp...

0060c439d64214f1b86a737fe80caf680259.9.B...j s...h.Y

0070963724652756ee4d165b.7\$e'V.M .[

BitTorrent

Packets: 13 · Displayed: 7 (53.8%) · Load time: 0:0.17 · Profile: Default

[3]

Applications ▾Places ▾Wireshark ▾

Tue Sep 20, 18:58

1

fr ▾

⏻

Wireshark · Endpoints · BitTorrent

Ethernet · 2IPv4 · 8IPv6TCP · 15UDP

Address	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	City	Country	AS Number	Latitu
60.234.152.124	2	273	1	151	1	122	Auckland, E7	New Zealand	AS9790 CallPlus Services Limited	-36.8
69.44.153.178	2	822	0	0	2	822	San Antonio, TX	United States	AS3356 Level 3 Communications, Inc.	29.48
80.37.9.37	3	366	1	122	2	244	Sentmenat, 56	Spain	AS3352 TELEFONICA.DE.ESPANA	41.60
82.210.155.248	1	122	0	0	1	122	Bucharest, 10	Romania	AS6830 Liberty Global Operations B.V.	44.43
194.109.162.159	1	122	0	0	1	122	Maarssen, 09	Netherlands	AS3265 XS4ALL-NL Amsterdam	52.13
202.88.252.50	3	395	1	151	2	244	Manjeri, 13	India	AS17465 Cable ISP in India	11.11
213.122.214.127	13	2222	10	1798	3	424	Bexhill, E2	United Kingdom	AS2856 BTnet UK Regional network	50.84
213.202.193.43	1	122	0	0	1	122	—	Germany	AS13301 UNITEDCOLO-AS	51.25

☐ Name resolution

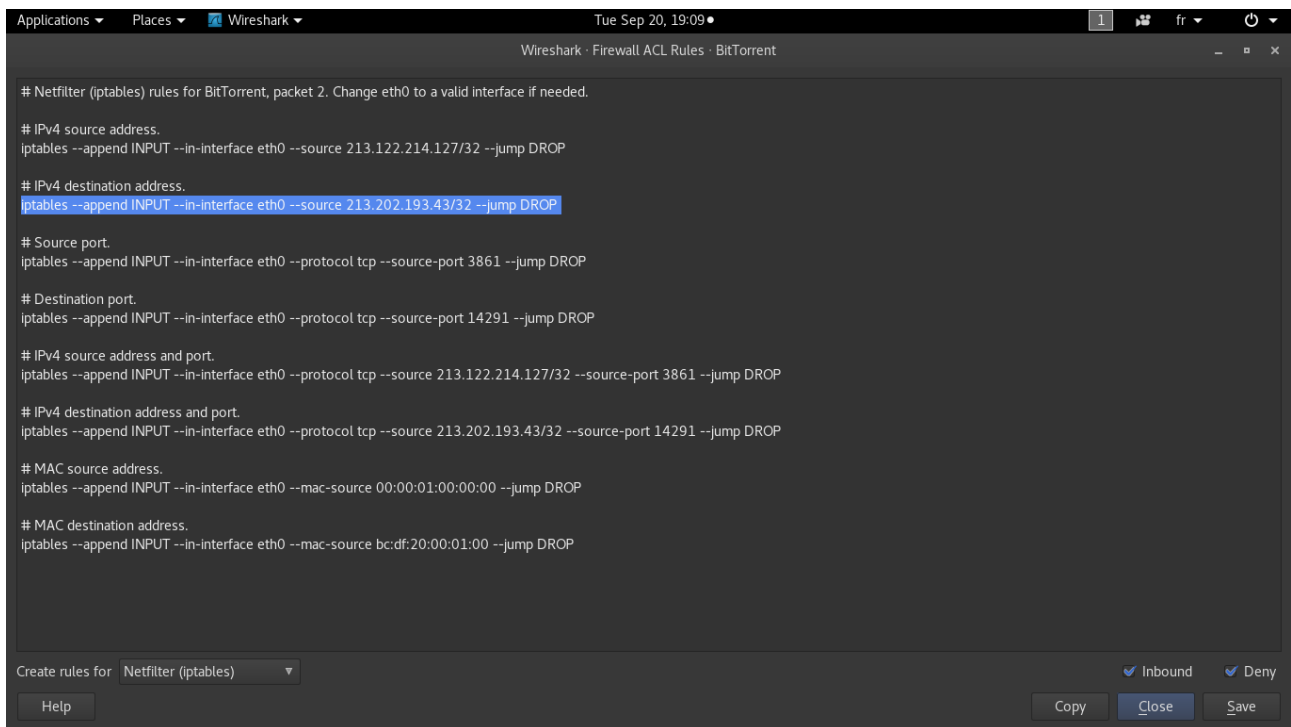
☐ Limit to display filter

Endpoint Types ▾

HelpCopyMapClose

"TPA-17.3.1.png" selected (68.3 kB)

Question 18:



The image shows the 'Firewall ACL Rules' dialog in Wireshark. It contains a list of iptables rules for BitTorrent, packet 2. The rules are for Netfilter (iptables) and are applied to the INPUT chain. The rules are as follows:

```
# Netfilter (iptables) rules for BitTorrent, packet 2. Change eth0 to a valid interface if needed.

# IPv4 source address.
iptables --append INPUT --in-interface eth0 --source 213.122.214.127/32 --jump DROP

# IPv4 destination address.
iptables --append INPUT --in-interface eth0 --source 213.202.193.43/32 --jump DROP

# Source port.
iptables --append INPUT --in-interface eth0 --protocol tcp --source-port 3861 --jump DROP

# Destination port.
iptables --append INPUT --in-interface eth0 --protocol tcp --source-port 14291 --jump DROP

# IPv4 source address and port.
iptables --append INPUT --in-interface eth0 --protocol tcp --source 213.122.214.127/32 --source-port 3861 --jump DROP

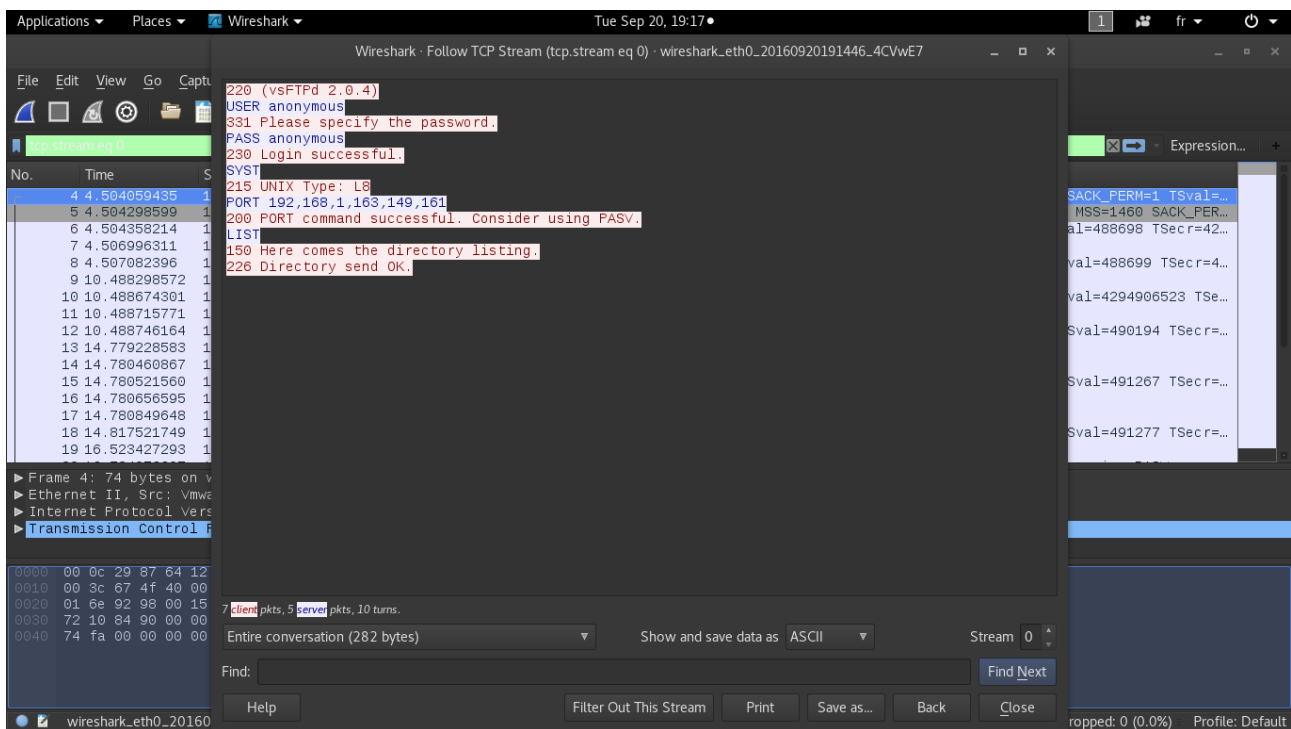
# IPv4 destination address and port.
iptables --append INPUT --in-interface eth0 --protocol tcp --source 213.202.193.43/32 --source-port 14291 --jump DROP

# MAC source address.
iptables --append INPUT --in-interface eth0 --mac-source 00:00:01:00:00:00 --jump DROP

# MAC destination address.
iptables --append INPUT --in-interface eth0 --mac-source bc:df:20:00:01:00 --jump DROP
```

At the bottom, there is a 'Create rules for' dropdown set to 'Netfilter (iptables)', and buttons for 'Help', 'Copy', 'Close', 'Save', 'Inbound', and 'Deny'.

Question 19:



The image shows the 'Follow TCP Stream' dialog in Wireshark. It displays a list of packets and their corresponding data. The packets are as follows:

No.	Time	S	D	Protocol	Length	Info
4	4.504059435	1	1	TCP	60	4.504059435 → 4.504298599 [RST] Seq=1921681163, Win=0, Len=0
5	4.504298599	1	1	TCP	60	4.504298599 → 4.504358214 [RST] Seq=1921681163, Win=0, Len=0
6	4.504358214	1	1	TCP	60	4.504358214 → 4.506996311 [RST] Seq=1921681163, Win=0, Len=0
7	4.506996311	1	1	TCP	60	4.506996311 → 4.507082396 [RST] Seq=1921681163, Win=0, Len=0
8	4.507082396	1	1	TCP	60	4.507082396 → 10.488298572 [RST] Seq=1921681163, Win=0, Len=0
9	10.488298572	1	1	TCP	60	10.488298572 → 10.488674301 [RST] Seq=1921681163, Win=0, Len=0
10	10.488674301	1	1	TCP	60	10.488674301 → 10.488715771 [RST] Seq=1921681163, Win=0, Len=0
11	10.488715771	1	1	TCP	60	10.488715771 → 10.488746164 [RST] Seq=1921681163, Win=0, Len=0
12	10.488746164	1	1	TCP	60	10.488746164 → 14.779228583 [RST] Seq=1921681163, Win=0, Len=0
13	14.779228583	1	1	TCP	60	14.779228583 → 14.780460867 [RST] Seq=1921681163, Win=0, Len=0
14	14.780460867	1	1	TCP	60	14.780460867 → 14.780521560 [RST] Seq=1921681163, Win=0, Len=0
15	14.780521560	1	1	TCP	60	14.780521560 → 14.780656595 [RST] Seq=1921681163, Win=0, Len=0
16	14.780656595	1	1	TCP	60	14.780656595 → 14.780849648 [RST] Seq=1921681163, Win=0, Len=0
17	14.780849648	1	1	TCP	60	14.780849648 → 14.817521749 [RST] Seq=1921681163, Win=0, Len=0
18	14.817521749	1	1	TCP	60	14.817521749 → 16.523427293 [RST] Seq=1921681163, Win=0, Len=0
19	16.523427293	1	1	TCP	60	16.523427293 → 220 (vsFTPD 2.0.4) [RST] Seq=1921681163, Win=0, Len=0

The dialog also shows a list of packets and their corresponding data. The packets are as follows:

- 220 (vsFTPD 2.0.4)
- USER anonymous
- 331 Please specify the password.
- PASS anonymous
- 230 Login successful.
- SYST
- 215 UNIX Type: L8
- PORT 192,168,1,163,149,161
- 200 PORT command successful. Consider using PASV.
- LIST
- 150 Here comes the directory listing.
- 226 Directory send OK.

At the bottom, there is a 'Find' field, a 'Filter Out This Stream' button, a 'Print' button, a 'Save as...' button, a 'Back' button, and a 'Close' button.

Question 20 : [1]

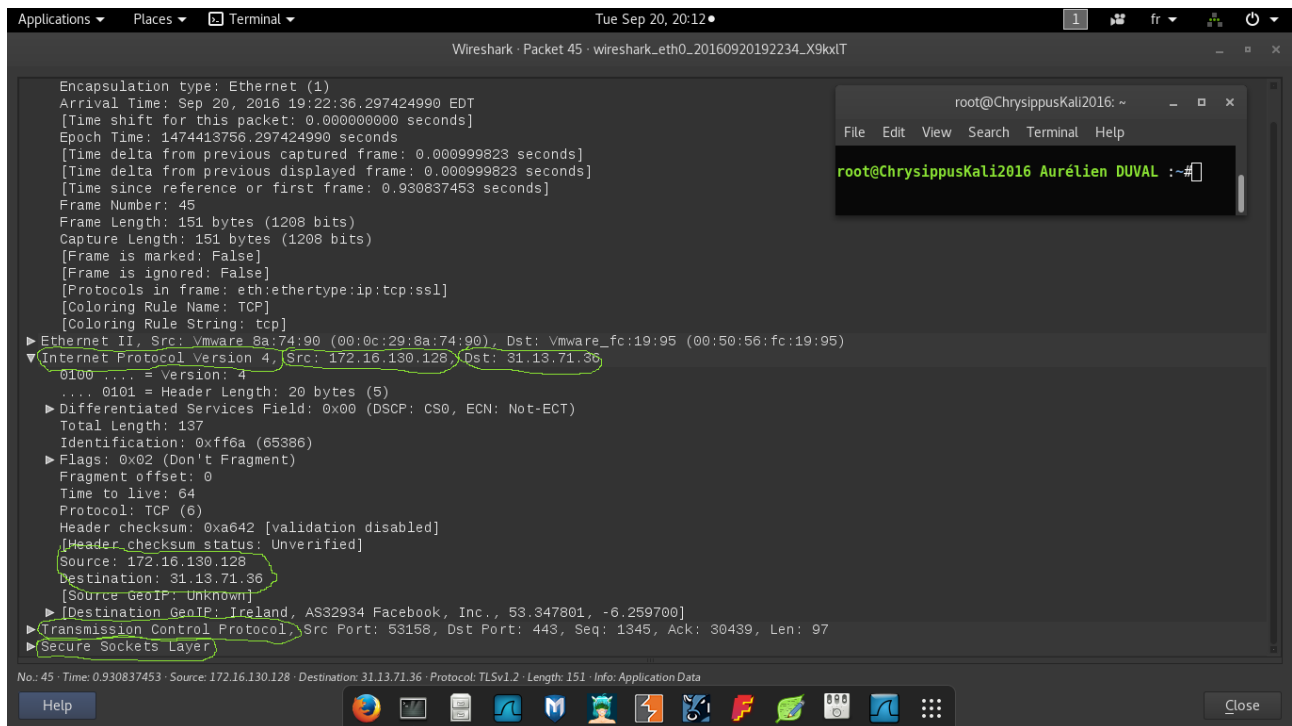
Ip locale 172.16.130.128

Ip du serveur hébergeant Facebook : 31.13.71.36

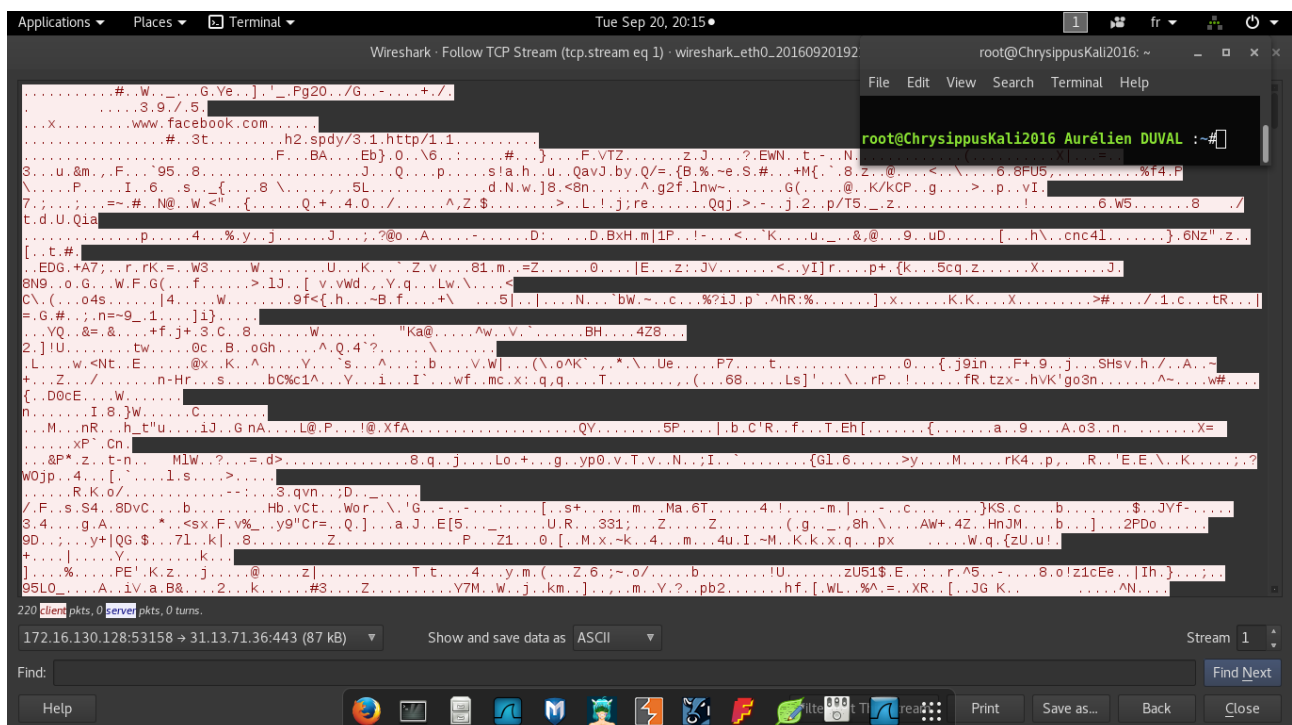
Protocole couche réseau : IPv4

Protocole couche transport : TCP

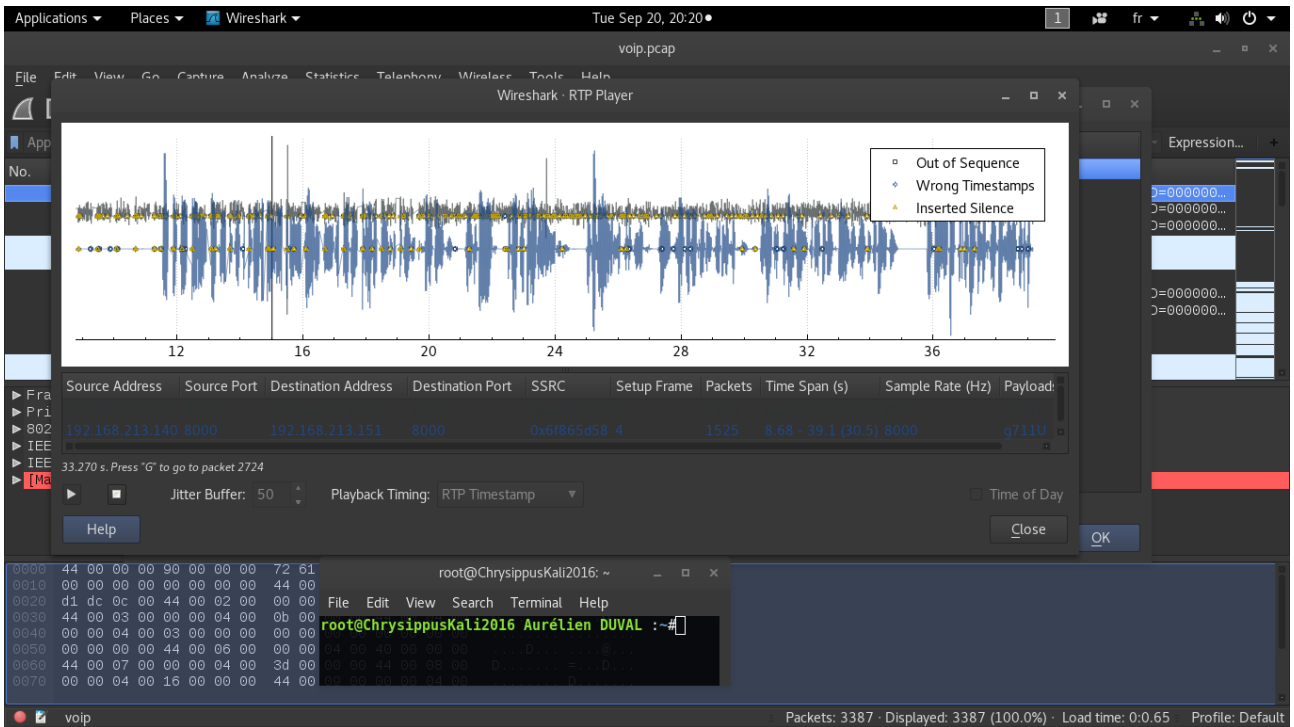
Protocole couche application : ssl / (http?)



[2] Le mot de passe n'est pas en clair!



Question 21 :



Question 22 : [1]

Wireshark · Conversations · capturerootkit

Ethernet · 5 IPv4 · 15 IPv6 TCP · 28 UDP · 87

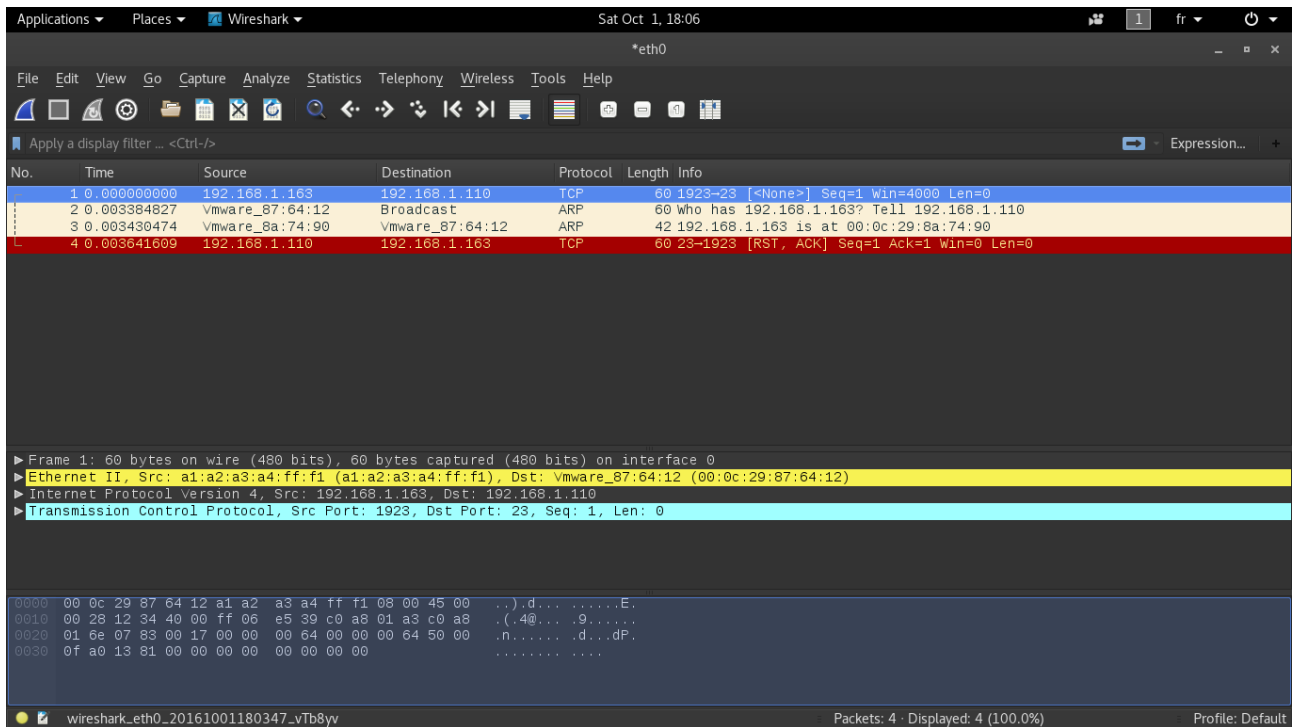
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bit
192.168.1.119	52998	54.186.108.54	80	11	2401	7	1338	4	1063	10.701958	428.2894	
192.168.1.119	52043	173.194.43.95	443	34	7316	19	1841	15	5475	33.939280	180.2994	
192.168.1.119	42283	206.167.212.106	80	8	990	5	784	3	206	35.934715	2.9400	
192.168.1.119	48017	132.203.187.106	80	8	900	5	694	3	206	67.698707	0.0284	
192.168.1.119	52046	173.194.43.95	443	356	300 k	138	13 k	218	287 k	70.859697	312.9348	
192.168.1.119	35154	206.167.212.91	443	106	81 k	59	24 k	47	56 k	71.736805	180.8704	
192.168.1.119	43740	206.167.212.101	443	1,685	2417 k	640	108 k	1,045	2308 k	72.506068	258.5762	
192.168.1.119	43155	132.203.210.120	80	6	412	4	272	2	140	78.834092	5.1950	
192.168.1.119	43156	132.203.210.120	80	32	3222	17	1665	15	1557	118.540623	116.0209	
192.168.1.119	43743	206.167.212.101	443	46	17 k	25	2836	21	14 k	118.697453	208.0682	
192.168.1.119	38119	206.167.212.80	443	92	61 k	47	4369	45	57 k	158.093690	221.2006	
192.168.1.119	43159	132.203.210.120	80	6	412	4	272	2	140	199.640886	5.0107	
192.168.1.119	48026	132.203.187.106	80	6	412	4	272	2	140	204.374991	5.6583	
192.168.1.119	43161	132.203.210.120	80	323	429 k	115	16 k	208	412 k	214.870215	149.3745	
192.168.1.119	59865	206.167.212.123	80	55	7916	29	4480	26	3436	238.241894	187.0983	
192.168.1.119	43163	132.203.210.120	80	474	773 k	162	19 k	312	754 k	238.342164	167.8829	
192.168.1.119	43164	132.203.210.120	80	181	198 k	68	11 k	113	187 k	238.342750	125.9138	
192.168.1.119	43165	132.203.210.120	80	134	206 k	57	4921	77	201 k	238.342969	0.0599	
192.168.1.119	43166	132.203.210.120	80	201	258 k	71	11 k	130	246 k	238.343692	125.9128	
192.168.1.119	43167	132.203.210.120	80	194	237 k	71	10 k	123	227 k	238.343959	125.9071	
192.168.1.119	43168	132.203.210.120	80	139	127 k	60	8964	79	118 k	238.402537	125.8540	
192.168.1.119	49429	63.245.216.134	443	16	4287	9	1046	7	3241	311.868762	8.8655	
192.168.1.119	49430	63.245.216.134	443	21	2786	11	1505	10	1201	322.873003	8.8655	
192.168.1.119	39627	72.21.91.29	80	6	412	4	272	2	140	323.873003	8.8655	

☐ Name resolution
 ☐ Limit to display filter
 ☐ Absolute start time

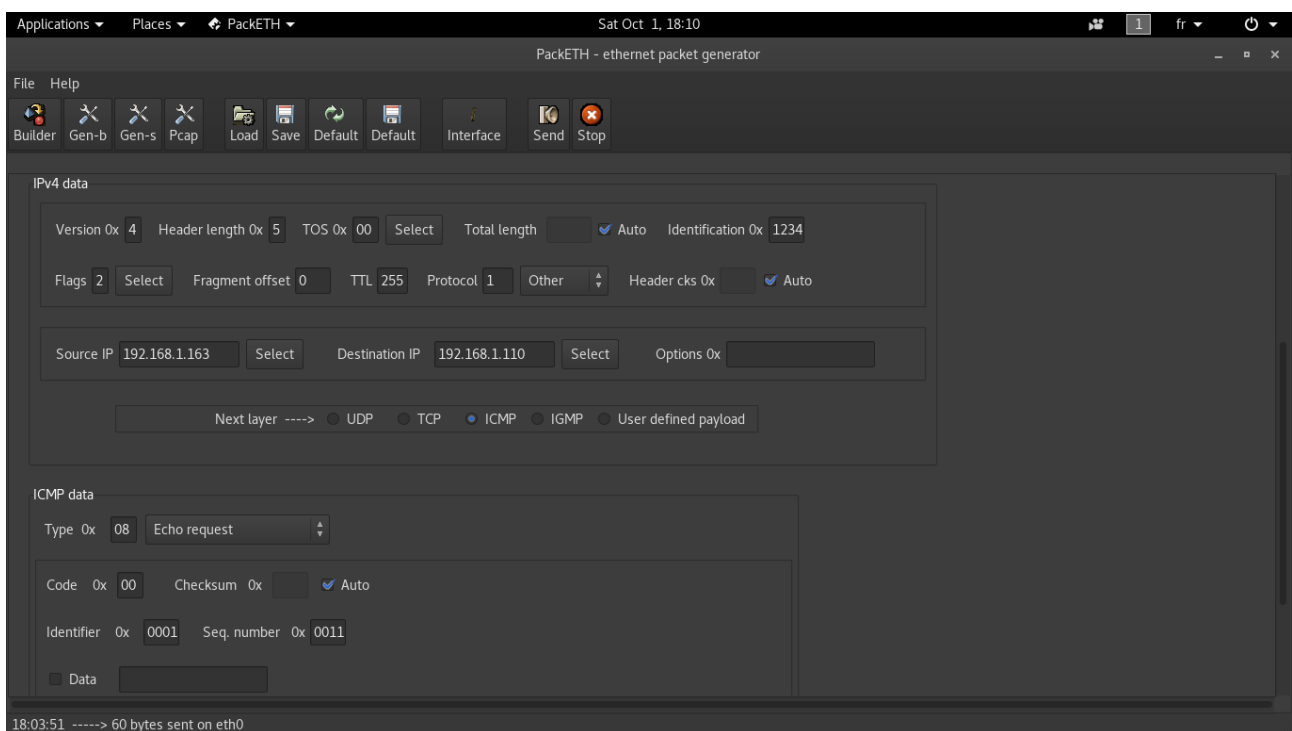
Help

[2] Je n'ai pas réussi à trouver d'informations sensibles

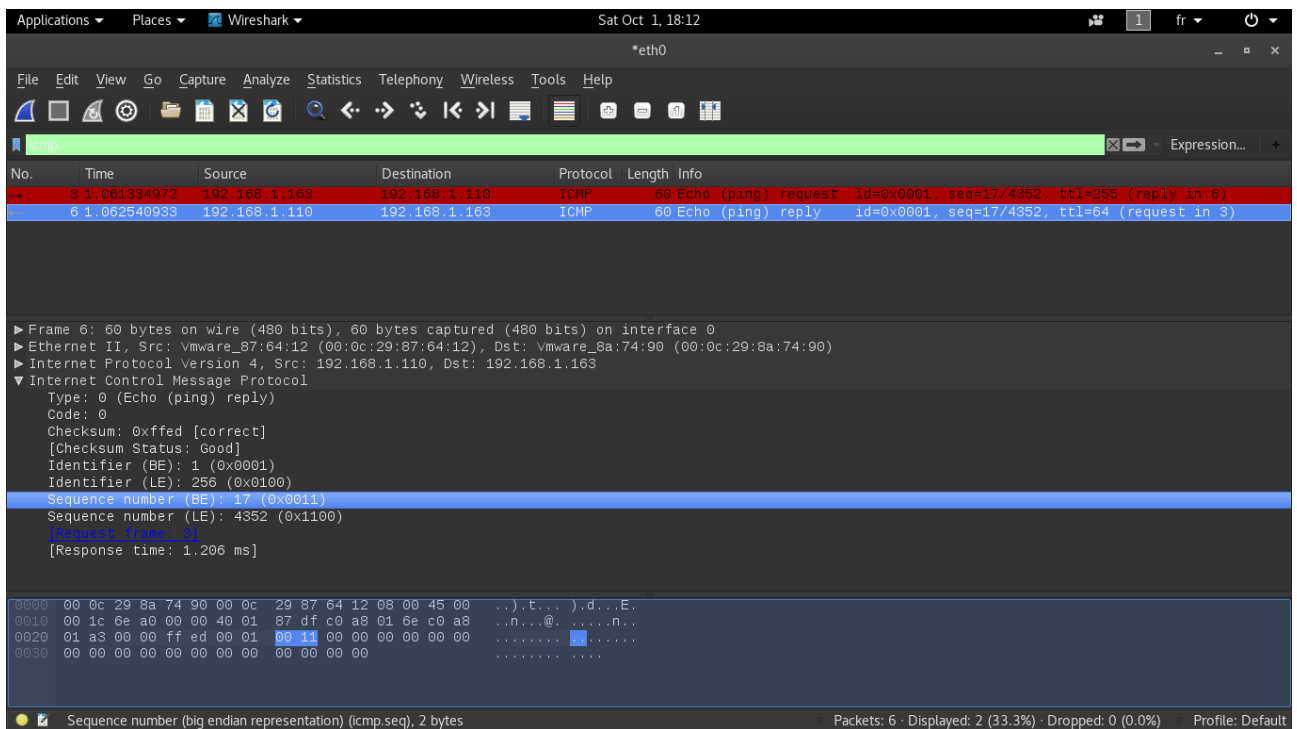
Question 23:



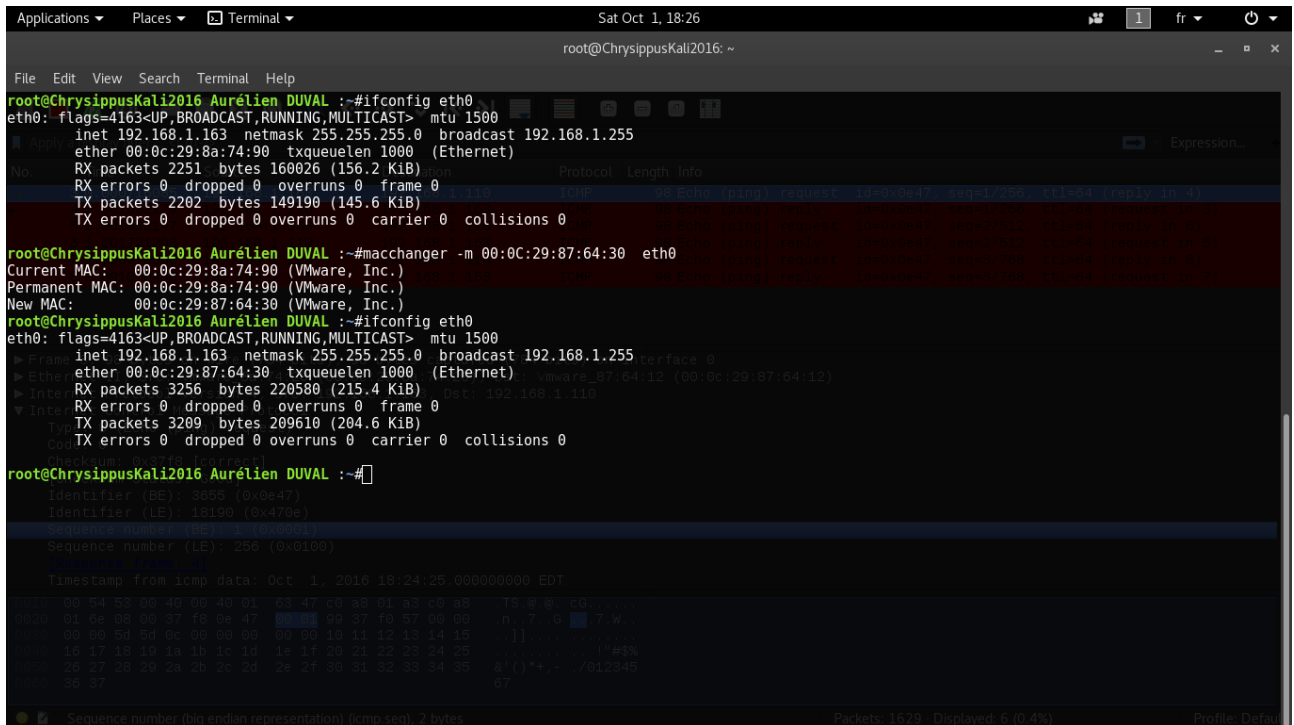
Question 24 : [1]



[2]



Question 25 : [1]



[2]

