

Majeure Info Barberot_Bach_Bonnevialle

The screenshot displays a terminal window on the left and a Wireshark packet capture window on the right. The terminal shows the execution of a server program named 'MajorsignalTp' which is listening on port 1069. It lists available files and then receives a connection from 127.0.0.1. The Wireshark window shows a packet capture on the 'eth0' interface. A red box highlights a DNS query from 127.0.0.1 to 127.0.0.1, which is a standard query response for 'www.google.com'.

Terminal Output:

```
ensea@StudentLab: ~/Desktop/MajorsignalTp/serveur
ensea@StudentLab:~/Desktop/MajorsignalTp/serveur$ ./go.sh
Demarrage du serveur TFTP en écoute sur le port 1069
Liste des fichiers disponibles:
-rw-rw-r-- 1 ensea ensea 256 déc. 17 2017 alt256
-rw-rw-r-- 1 ensea ensea 21410 déc. 17 2017 ensea.png
-rw-rw-r-- 1 ensea ensea 1044 janv. 15 18:26 ones1024
-rw-rw-r-- 1 ensea ensea 2048 janv. 29 2018 ones2048
-rw-rw-r-- 1 ensea ensea 256 janv. 6 2019 ones256
-rw-rw-r-- 1 ensea ensea 512 janv. 6 2019 ones512
-rw-rw-r-- 1 ensea ensea 1024 déc. 17 2017 zeros1024
-rw-rw-r-- 1 ensea ensea 2048 déc. 17 2017 zeros2048
-rw-rw-r-- 1 ensea ensea 256 déc. 17 2017 zeros256
-rw-rw-r-- 1 ensea ensea 512 déc. 17 2017 zeros512
Ctrl-C pour arrêter...
```

Wireshark Packet Capture:

No.	Time	Source	Destination	Protocol	Length	Info
53	0.053646447	10.0.2.15	142.250.179.100	TCP	56	41700 → 443 [ACK] Seq=518 Ack=1431 Win=8179200 Len=0
54	0.055705208	142.250.179.100	10.0.2.15	TCP	3036	[TCP Retransmission] 443 → 41700 [PSH, ACK] Seq=1431 Ack=518 Win=65535 Len=2980
55	0.055792337	10.0.2.15	142.250.179.100	TCP	56	41700 → 443 [ACK] Seq=518 Ack=4411 Win=7997440 Len=0
56	0.056404006	10.0.2.15	142.250.179.100	TCP	136	[TCP Retransmission] 41700 → 443 [PSH, ACK] Seq=518 Ack=4411 Win=8179200 Len=74
57	0.056810209	142.250.179.100	10.0.2.15	TCP	62	443 → 41700 [ACK] Seq=4411 Ack=592 Win=65535 Len=0
58	0.057152242	142.250.179.100	10.0.2.15	TCP	1486	[TCP Retransmission] 443 → 41702 [PSH, ACK] Seq=1 Ack=518 Win=65535 Len=1430
59	0.057161419	10.0.2.15	142.250.179.100	TCP	56	41702 → 443 [ACK] Seq=518 Ack=1431 Win=8179200 Len=0
60	0.057429356	142.250.179.100	10.0.2.15	TCP	1486	[TCP Retransmission] 443 → 41702 [PSH, ACK] Seq=1431 Ack=518 Win=65535 Len=1430
61	0.057438023	10.0.2.15	142.250.179.100	TCP	56	41702 → 443 [ACK] Seq=518 Ack=2861 Win=8179200 Len=0
62	0.058592200	142.250.179.100	10.0.2.15	TCP	1486	[TCP Retransmission] 443 → 41702 [PSH, ACK] Seq=592 Ack=518 Win=65535 Len=1430
63	0.058601659	10.0.2.15	142.250.179.100	TCP	56	41702 → 443 [ACK] Seq=518 Ack=4291 Win=8179200 Len=0
64	0.058621718	142.250.179.100	10.0.2.15	TCP	176	[TCP Retransmission] 443 → 41702 [PSH, ACK] Seq=4291 Ack=518 Win=65535 Len=120
65	0.058626685	10.0.2.15	142.250.179.100	TCP	56	41702 → 443 [ACK] Seq=518 Ack=4411 Win=8163840 Len=0
66	0.059422391	142.250.179.100	10.0.2.15	TCP	136	[TCP Retransmission] 41700 → 443 [PSH, ACK] Seq=518 Ack=4411 Win=8163840 Len=74
67	0.059422391	142.250.179.100	10.0.2.15	TCP	62	443 → 41702 [ACK] Seq=4411 Ack=592 Win=65535 Len=0
68	0.015459256	127.0.0.1	127.0.0.1	DNS	101	Standard query response 0xac59 A www.google.com A 142.250.179.100 OPT
69	1.067766536	10.0.2.15	66.102.1.188	TCP	56	34688 → 5228 [ACK] Seq=1 Ack=1 Win=63900 Len=0
70	1.067899414	66.102.1.188	10.0.2.15	TCP	62	[TCP ACKed unseen segment] 5228 → 34688 [ACK] Seq=1 Ack=2 Win=65535 Len=0
71	1.067766536	10.0.2.15	66.102.1.188	TCP	54	[TCP Dup ACK 69#1] 34688 → 5228 [ACK] Seq=1 Ack=1 Win=63900 Len=0
72	1.067899414	66.102.1.188	10.0.2.15	TCP	60	[TCP Dup ACK 70#1] [TCP ACKed unseen segment] 5228 → 34688 [ACK] Seq=1 Ack=2 Win=65535
73	5.196264275	PcsCompu ac:9f:1e	RealtekU 12:35:03	ARP	44	Who has 10.0.2.3? Tell 10.0.2.15
74	5.196611388	RealtekU 12:35:03	RealtekU 12:35:03	ARP	62	10.0.2.3 is at 52:54:00:12:35:03
75	5.196264275	PcsCompu ac:9f:1e	RealtekU 12:35:03	ARP	42	Who has 10.0.2.3? Tell 10.0.2.15
76	5.196611388	RealtekU 12:35:03	PcsCompu ac:9f:1e	ARP	60	10.0.2.3 is at 52:54:00:12:35:03
77	10.057680795	142.250.179.100	10.0.2.15	TCP	62	443 → 41702 [FIN, ACK] Seq=4411 Ack=592 Win=65535 Len=0
78	10.067260917	142.250.179.100	10.0.2.15	TCP	62	443 → 41700 [FIN, ACK] Seq=4411 Ack=592 Win=65535 Len=0
79	10.057680795	142.250.179.100	10.0.2.15	TCP	60	[TCP Out-Of-Order] 443 → 41702 [FIN, ACK] Seq=4411 Ack=592 Win=65535 Len=0
80	10.067260917	142.250.179.100	10.0.2.15	TCP	60	[TCP Out-Of-Order] 443 → 41700 [FIN, ACK] Seq=4411 Ack=592 Win=65535 Len=0
81	10.099144151	10.0.2.15	142.250.179.100	TCP	54	41702 → 443 [ACK] Seq=592 Ack=4412 Win=8163840 Len=0
82	10.111796816	10.0.2.15	142.250.179.100	TCP	54	41700 → 443 [ACK] Seq=592 Ack=4412 Win=8179200 Len=0
83	10.099144151	10.0.2.15	142.250.179.100	TCP	56	[TCP Dup ACK 81#1] 41702 → 443 [ACK] Seq=592 Ack=4412 Win=8163840 Len=0
84	10.111796816	10.0.2.15	142.250.179.100	TCP	56	[TCP Dup ACK 82#1] 41700 → 443 [ACK] Seq=592 Ack=4412 Win=8179200 Len=0

Wireshark Packet Details:

- Frame 1: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 2
- Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
- Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
- User Datagram Protocol, Src Port: 35957, Dst Port: 53
- Domain Name System (query)

On lance un terminal avec le serveur de l'ENSEA ; on lance également wireshark et la commande qui s'exécute bien...

On lit bien le fichier « zeros1024 » comme noté dans le code.

Sur l'écran des captures wireshark, on a bien une requête à l'adresse 127.0.0.1 l'adresse du serveur de l'ensea ce qui correspond à la requête RRQ lancée.

The image displays three screenshots from a Linux environment. The top screenshot is a Wireshark packet capture window titled 'Capturing from 5 interfaces'. It shows a list of network packets. Two packets are highlighted with a red box:

No.	Time	Source	Destination	Protocol	Length	Info
9	35.793612106	127.0.0.1	127.0.0.1	ICMP	76	Destination unreachable (Port unreachable)
10	35.793612106	127.0.0.1	127.0.0.1	ICMP	74	Destination unreachable (Port unreachable)

The bottom-left screenshot shows a terminal window with the following output:

```

ensea@StudentLab: ~/Desktop/MajorSignalTp
$ ./go.sh
No such file or directory
ensea@StudentLab:~/Desktop/MajorSignalTp$ ./go.sh
Démarrage du serveur TFTP en écoute sur le port 1069
Liste des fichiers disponibles:
-rw-rw-r-- 1 ensea ensea 256 déc. 17 2017 alt256
-rw-rw-r-- 1 ensea ensea 21418 déc. 17 2017 ensea.png
-rw-rw-r-- 1 ensea ensea 1844 janv. 15 18:26 ones1024
-rw-rw-r-- 1 ensea ensea 2848 janv. 29 2018 ones2048
-rw-rw-r-- 1 ensea ensea 256 janv. 6 2019 ones256
-rw-rw-r-- 1 ensea ensea 512 janv. 6 2019 ones512
-rw-rw-r-- 1 ensea ensea 1024 déc. 17 2017 zeros1024
-rw-rw-r-- 1 ensea ensea 2048 déc. 17 2017 zeros2048
-rw-rw-r-- 1 ensea ensea 256 déc. 17 2017 zeros256
-rw-rw-r-- 1 ensea ensea 512 déc. 17 2017 zeros512
$

```

The bottom-right screenshot shows a terminal window with the following output:

```

ensea@StudentLab:~/Desktop/MajorSignalTp$ make enseash
make: Nothing to be done for 'enseash'.
ensea@StudentLab:~/Desktop/MajorSignalTp$ ./main5 127.0.0.1
Segmentation fault (core dumped)
ensea@StudentLab:~/Desktop/MajorSignalTp$ ./main5 127.0.0.1 ones1024
ones1024octet
ensea@StudentLab:~/Desktop/MajorSignalTp$

```

Pour la question 5, on réitère la même manipulation.

On se connecte bien au serveur car on arrive à lire le nombre d'octet que contient le fichier « ones1024 », mais le code contient des problèmes au niveau de la requête wrq (écriture) ou du ACK car le port est dit « inatteignable » comme le montre la partie encadrée