

מטלה 5

סטודנט ראשון : אילן מאיר סופיר, ת"ז : 342615648

סטודנט שני : בן כהן , ת"ז : 207029786

חלק א :

צירפנו את הקובץ part_1.pcapng לחלק הזה.

הכתובת שלי ב Ubuntu זה :

```
ilansouffir@ilansouffir-VirtualBox: ~  
ilansouffir@ilansouffir-VirtualBox:~$ ip addr  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:47:37:89 brd ff:ff:ff:ff:ff:ff  
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3  
        valid_lft 85348sec preferred_lft 85348sec  
    inet6 fe80::1605:77f:dc72:533c/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
ilansouffir@ilansouffir-VirtualBox:~$
```

הרצנו `mytcping.cpp` לכתובת `google 192.168.1.1` עם הדפסת חישובי `rtt`.

הרצת `mytcping` תוך כדי `wireshark` מופעל עם פילטר `icmp (echo request)`.

ניתן לראות שנשלחו שתי חבילות `ICMP request` ו`reply` ושהכתובת של ה `source` היא שלי וה`destination` היא `192.168.1.1` כמו שציינו בקוד. בנוסף רואים שה`checksum` ה`correct`.

The image shows a Wireshark packet capture of an ICMP echo request and its corresponding reply. The packet list shows two packets: a request (No. 10) and a reply (No. 11). The packet details for the request (No. 10) are expanded, showing the ICMP header and the data field. The checksum is highlighted as correct. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
10	5.442364490	10.0.2.15	192.168.1.1	ICMP	62	Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 11)
11	5.452910224	192.168.1.1	10.0.2.15	ICMP	62	Echo (ping) reply id=0x1200, seq=0/0, ttl=63 (request in 10)

Frame 10: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu47:37:89 (08:00:27:47:37:89), Dst: RealtekU12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.1.1
... = Version: 4
... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 48
Identification: 0xad0 (56016)
Flags: 0x40, Don't Fragment
Fragment Offset: 0
Time to Live: 64
Protocol: ICMP (1)
Header Checksum: 0x9244 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.0.2.15
Destination Address: 192.168.1.1
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xa420 [correct]
[Checksum Status: Good]
Identifier (BE): 4608 (0x1200)
Identifier (LE): 18 (0x0012)
Sequence Number (BE): 0 (0x0000)
Sequence Number (LE): 0 (0x0000)
[Response frame: 11]
Data (20 bytes)

```
ilansouffir@ilansouffir-VirtualBox: ~/Desktop/Ex5
ilansouffir@ilansouffir-VirtualBox:~/Desktop/Ex5$ sudo ./myping
Sending ping to ip address 192.168.1.1 .....
Ping successfully received by ip address 192.168.1.1 !

RTT: 10.561000 milliseconds
RTT: 10561 microseconds

(Data received was = 'This is the ping.
')
ilansouffir@ilansouffir-VirtualBox:~/Desktop/Ex5$
```

0000 52 54 00 12 35 02 08 00 27 47 37 89 08 00 45 00 RTT: 5...G7...E-
0010 00 30 da d0 40 00 40 01 92 44 0a 00 02 0f c0 a8 -0-...D-...
0020 01 01 08 00 a4 20 12 00 00 00 54 68 69 73 20 69This i
0030 73 20 74 68 65 20 70 69 6e 67 2e 20 0a 00 s the pi ng. ...

פה ניתן לראות את תוכן ה `reply echo` שהתקבל. ניתן לראות שקבלנו את ה `msg` :

The image shows a Wireshark packet capture of an ICMP echo reply. The packet list shows two packets: a request (No. 10) and a reply (No. 11). The packet details for the reply (No. 11) are expanded, showing the ICMP header and the data field. The checksum is highlighted as correct. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
10	5.442364490	10.0.2.15	192.168.1.1	ICMP	62	Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 11)
11	5.452910224	192.168.1.1	10.0.2.15	ICMP	62	Echo (ping) reply id=0x1200, seq=0/0, ttl=63 (request in 10)

Frame 11: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface enp0s3, id 0
Ethernet II, Src: RealtekU12:35:02 (52:54:00:12:35:02), Dst: PcsCompu47:37:89 (08:00:27:47:37:89)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 10.0.2.15
... = Version: 4
... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 48
Identification: 0x02d1 (721)
Flags: 0x00
Fragment Offset: 0
Time to Live: 63
Protocol: ICMP (1)
Header Checksum: 0xab44 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.1
Destination Address: 10.0.2.15
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0xac20 [correct]
[Checksum Status: Good]
Identifier (BE): 4608 (0x1200)
Identifier (LE): 18 (0x0012)
Sequence Number (BE): 0 (0x0000)
Sequence Number (LE): 0 (0x0000)
[Request frame: 10]
[Response time: 10.546 ms]
Data (20 bytes)

```
ilansouffir@ilansouffir-VirtualBox: ~/Desktop/Ex5
ilansouffir@ilansouffir-VirtualBox:~/Desktop/Ex5$ sudo ./myping
Sending ping to ip address 192.168.1.1 .....
Ping successfully received by ip address 192.168.1.1 !

RTT: 10.561000 milliseconds
RTT: 10561 microseconds

(Data received was = 'This is the ping.
')
ilansouffir@ilansouffir-VirtualBox:~/Desktop/Ex5$
```

0000 08 00 27 47 37 89 52 54 00 12 35 02 08 00 45 00 --'G7-RT--5---E-
0010 00 30 02 d1 00 00 3f 01 ab 44 0a a8 01 01 0a 00 -0-...2...D-...
0020 02 0f 00 00 ac 20 12 00 00 00 54 68 69 73 20 69This i
0030 73 20 74 68 65 20 70 69 6e 67 2e 20 0a 00 s the pi ng. ...

חלק ב :

צירפנו את הקובץ ה part_2.pcapng ו-part_2.pcapng לחלק הזה.

הרצנו sniffer, מציגים את הsrc, הdst, הטיפוס והקוד של החבילה שהוסנפה.
כאן ניתן לראות את הפלט באשריט, ניתן לבדוק שהתשובות שקיבלנו נכונות:
src, dst, type, code

The image displays a Wireshark capture of an ICMP echo request and response between 10.0.2.15 and 192.168.1.1. The packet list shows two packets: a request (No. 1) and a reply (No. 2). The packet details for the request are expanded, showing the Internet Control Message Protocol (ICMP) section with Type 8 (Echo (ping) request) and Code 0. The packet bytes pane shows the raw data. A terminal window shows the execution of a ping command and a sniffer script that captures the packet and displays its details.

```
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	192.168.1.1	ICMP	62	Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 2)
2	0.005780875	192.168.1.1	10.0.2.15	ICMP	62	Echo (ping) reply id=0x1200, seq=0/0, ttl=63 (request in 1)

Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu.47:37:89 (08:00:27:47:37:89), Dst: RealtekU.12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.1.1
0100 = Version: 4
... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 48
Identification: 0xe63f (58943)
Flags: 0x40, Don't fragment
Fragment Offset: 0
Time to Live: 64
Protocol: ICMP (1)
Header Checksum: 0x86d5 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.0.2.15
Destination Address: 192.168.1.1
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xa420 [correct]
[Checksum Status: Good]
Identifier (BE): 4608 (0x1200)
Identifier (LE): 18 (0x0012)
Sequence Number (BE): 0 (0x0000)
Sequence Number (LE): 0 (0x0000)
[Response frame: 2]
Data (20 bytes)

```
llansouffir@llansouffir-VirtualBox: ~/Desktop/Ex5$ sudo ./sniffer
ICMP PACKET SNIFFED
IP_SRC : 10.0.2.15
IP_DST : 192.168.1.1
TYPE : 8 Echo request
CODE : 0
```

The image displays a Wireshark capture of an ICMP echo request and response between 192.168.1.1 and 10.0.2.15. The packet list shows two packets: a request (No. 1) and a reply (No. 2). The packet details for the request are expanded, showing the Internet Control Message Protocol (ICMP) section with Type 8 (Echo (ping) request) and Code 0. The packet bytes pane shows the raw data. A terminal window shows the execution of a ping command and a sniffer script that captures the packet and displays its details.

```
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	192.168.1.1	ICMP	62	Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 2)
2	0.005780875	192.168.1.1	10.0.2.15	ICMP	62	Echo (ping) reply id=0x1200, seq=0/0, ttl=63 (request in 1)

Frame 2: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface enp0s3, id 0
Ethernet II, Src: RealtekU.12:35:02 (52:54:00:12:35:02), Dst: PcsCompu.47:37:89 (08:00:27:47:37:89)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 10.0.2.15
0100 = Version: 4
... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 48
Identification: 0x02d5 (725)
Flags: 0x00
Fragment Offset: 0
Time to Live: 63
Protocol: ICMP (1)
Header Checksum: 0xab40 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.1
Destination Address: 10.0.2.15
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xac20 [correct]
[Checksum Status: Good]
Identifier (BE): 4608 (0x1200)
Identifier (LE): 18 (0x0012)
Sequence Number (BE): 0 (0x0000)
Sequence Number (LE): 0 (0x0000)
[Request frame: 1]
[Response time: 5.781 ms]
Data (20 bytes)

```
llansouffir@llansouffir-VirtualBox: ~/Desktop/Ex5$ sudo ./sniffer
ICMP PACKET SNIFFED
IP_SRC : 10.0.2.15
IP_DST : 192.168.1.1
TYPE : 8 Echo request
CODE : 0
```

כמובן שניתן לבדוק את הקוד ביחד עם הפקודה ping, הנה פלט של הרצת sniffer ביחד עם ping :

The image displays a network analysis setup. On the left, Wireshark shows a list of captured ICMP packets. The selected packet (No. 11) is expanded, showing its details: Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol (Echo (ping) request). The packet data is shown in hexadecimal and ASCII.

In the center, a terminal window shows the command `llansouffir@llansouffir-VirtualBox: ~/Desktop/Ex5$ sudo ./sniffer` and its output, which lists the sniffed ICMP packets with their source and destination addresses, sequence numbers, and timestamps.

On the right, another terminal window shows the command `llansouffir@llansouffir-VirtualBox: ~/Desktop/Ex5$ ping 192.168.1.1` and its output, which displays the ping statistics, including the number of packets transmitted, received, and the round-trip time (RTT).