



# תקשרות

## מטלה 1



# WIRESHARK

## INTRO

**1) List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.**

**2) How long did it take from when the HTTP GET message was sent until the HTTP**

**OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began.)**

**To display the Time field in time-of-day format, select the Wireshark View pull-down menu, then select Time Display Format, then select Time-of-day.)**

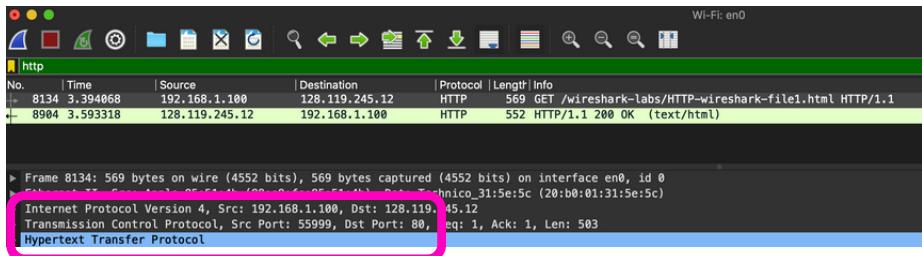
**3). What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer?)**

**4). Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the "Selected Packet Only" and "Print as displayed" radial buttons, and then click OK.**

# Question 1

**List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.**

# Answer 1



Here we can clearly see 3 different protocols

- Internet Protocol Version 4. "IPV4"
- Transmission Control Protocol "TCP"
- Hypertext Transfer Protocol "HTTP"

## Question 2

How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)

## Answer 2

Time
3.394068
3.593318

Time To execute 3.394068

## Question 3

3). What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)?

What is the Internet address of your computer?

## Answer 3

Source	Destination
192.168.1.100	128.119.245.12
128.119.245.12	192.168.1.100

Computer Internet address :

- Source Address      "**192.168.1.100**"

gaia.cs.umass.edu Internet address :

- Destination Address    "**128.119.245.12**"

# Question 4

Print the two HTTP messages (GET and OK) referred to in question 2 above.

To

do so, select Print from the Wireshark File command menu, and select the "Selected Packet Only" and "Print as displayed" radial buttons, and then

click

OK.

# Answer 4

```
/var/folders/2h/_cqkmpms0k91t9rl27l22nph0000gn/T/wireshark_Wi-Fi2QJU0.pcapng 14279 total packets, 2 shown
```

No.	Time	Source	Destination	Protocol	Length	Info
8134	3.394068	192.168.1.100	128.119.245.12	HTTP	569	GET / wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1 Frame 8134: 569 bytes on wire (4552 bits), 569 bytes captured (4552 bits) on interface en0, id 0 Ethernet II, Src: Apple_85:51:4b (88:e9:fe:85:51:4b), Dst: Technico_31:5e:5c (20:b0:01:31:5e: 5c) Internet Protocol Version 4, Src: 192.168.1.100, Dst: 128.119.245.12 Transmission Control Protocol, Src Port: 55999, Dst Port: 80, Seq: 1, Ack: 1, Len: 503 Hypertext Transfer Protocol

# WIRESHARK

## HTTP

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
2. What languages (if any) does your browser indicate that it can accept to the server?
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
4. What is the status code returned from the server to your browser?
5. When was the HTML file that you are retrieving last modified at the server?
6. How many bytes of content are being returned to your browser?
7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.
8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.
12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill of Rights?
13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
14. What is the status code and phrase in the response?
15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?
16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?
17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.
18. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?
19. When your browser’s sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

# Question 1

Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

# Answer 1

```
552 HTTP/1.1 200 OK (text/html)
```

My browser running HTTP version 1.1

# Question 2

What languages (if any) does your browser indicate that it can accept to the server?

# Answer 2

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,  
Accept-Encoding: gzip, deflate\r\n  
Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
```

French & English (US)

## Question 3

What is the IP address of your computer? Of the gaia.cs.umass.edu server?

## Answer 3

Source	Destination
192.168.1.100	128.119.245.12

Computer Internet address :

- Source Address        "**192.168.1.100**"

gaia.cs.umass.edu Internet address :

- Destination Address    "**128.119.245.12**"

## Question 4

What is the status code returned from the server to your browser?

## Answer 4

552 HTTP/1.1 200 OK (text/html)

**200 OK**

## Question 5

When was the HTML file that you are retrieving last modified at the server?

## Answer 5

**Last-Modified:** Sat, 14 Nov 2020 06:59:02 GMT\r\n

Saturday 14 November 2020 at 06:59:02

## Question 6

How many bytes of content are being returned to your browser?

## Answer 6

Accept-Ranges: bytes\r\n▼ Content-Length: 128\r\n[Content length: 128]  
Keep-Alive: timeout=5, max=1

Content-Length 128 Bytes

## Question 7

By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one. No. The raw data appears to match up exactly with what is shown in the packet-listing window.

## Answer 7

No, i don't see any header

## Question 8

Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?

## Answer 8

No, i don't see any "IF-MODIFIED-SINCE"

## Question 9

Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

## Answer 9

```
\n<html>\n\nCongratulations again! Now you've downloaded the file lab2-2.html. <br>\nThis file's last modification date will not change. <p>\nThus if you download this multiple times on your browser, a complete copy <br>\nwill only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\nfield in your browser's HTTP GET request to the server.\n\n</html>\n
```

Yes i can clearly see the contain html :  
"Congratulation. Again! ..."

## Question 10

Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?

## Answer 10

```
Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7\r\nIf-None-Match: "80-5b40bae1a9518"\r\nIf-Modified-Since: Sat, 14 Nov 2020 06:59:02 GMT\r\n\r\n
```

Sat, 14 Nov 2020

06:59:02

## Question 11

What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

## Answer 11

**304 HTTP/1.1 304 Not Modified**

▼ Hypertext Transfer Protocol  
    ▼ **HTTP/1.1 304 Not Modified\r\n**

The second HTTP GET returned 304 Not Modified because the request don't have to be renew the cash well know this address so it can be signified that nothing was modified since my last request .

## Question 12

How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

## Answer 12

1645	192.168.1.100	128.119.245.12	HTTP	569	GET /wireshark-labs/HTTP-wireshark-file3.htm
1652	128.119.245.12	192.168.1.100	HTTP	883	HTTP/1.1 200 OK (text/html)

My browser send 1 HTTP GET request message

## Question 13

Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

## Answer 13

43	6	336645	192.168.1.100	128.119.245.12	HTTP	569	GET /wireshark-labs/HTT
		883	533652	128.119.245.12	HTTP	883	HTTP/1.1 200 OK (text/

No. 43

## Question 14

What is the status code and phrase in the response?

## Answer 14

GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1

GET /wireshark-labs/HTPP-wireshark-file3.html HTTP/1.1

## Question 15

How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

## Answer 15

GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1  
HTTP/1.1 200 OK (text/html)

2 TCP segments     (1GET )(1 OK ).

## Question 16

How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

## Answer 16

No.	Time	Source	Destination	Protocol	Length	Info
52	2.834963	192.168.1.100	128.119.245.12	HTTP	569	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
75	3.038690	128.119.245.12	192.168.1.100	HTTP	1139	HTTP/1.1 200 OK (text/html)
77	3.057843	192.168.1.100	128.119.245.12	HTTP	581	GET /pearson.png HTTP/1.1
106	3.269795	128.119.245.12	192.168.1.100	HTTP	981	HTTP/1.1 200 OK (PNG)
133	3.478382	192.168.1.100	128.119.245.12	HTTP	475	GET /-kurose/cover_5th_ed.jpg HTTP/1.1
278	4.309361	128.119.245.12	192.168.1.100	HTTP	284	HTTP/1.1 200 OK (JPEG/JFIF image)

**1 destinations :**

- 128.119.245.12

## Question 17

Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel?  
Explain.

## Answer 17

### Picture 1

[3 Reassembled TCP Segments (3611 bytes): #103(1348), #104(1348), #106(915)]

### Picture 2

► [77 Reassembled TCP Segments (101318 bytes): #137(1348), #138(1348)]

both images have been downloaded in series

## Question 18

What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

## Answer 18

68 3.848689	192.168.1.100	128.119.245.12	HTTP	601	GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1
74 4.441301	128.119.245.12	192.168.1.100	HTTP	783	HTTP/1.1 401 Unauthorized (text/html)
319 32.771244	192.168.1.100	128.119.245.12	HTTP	660	GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1
324 33.791718	128.119.245.12	192.168.1.100	HTTP	586	HTTP/1.1 404 Not Found (text/html)

The server's response in the initial HTTP GET is the N°68  
GET/wireshark-labs/protected\_pages/HTTP-wireshark-  
HTTP/1.1

## Question 19

When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

## Answer 19

68 3.848689	192.168.1.100	128.119.245.12	HTTP	601	GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1
74 4.441301	128.119.245.12	192.168.1.100	HTTP	783	HTTP/1.1 401 Unauthorized (text/html)
319 32.771244	192.168.1.100	128.119.245.12	HTTP	660	GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1
324 33.791718	128.119.245.12	192.168.1.100	HTTP	586	HTTP/1.1 404 Not Found (text/html)

Unauthorized



# תקשרות

## מטלה נ

Nathanael Benichou



# WIRESHARK

## DNS

1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?

```
nathben97@nathben97-VirtualBox: ~
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
tsinghua.edu.cn nameserver = ns2.cuhk.hk.
tsinghua.edu.cn nameserver = dns.tsinghua.edu.cn.
tsinghua.edu.cn nameserver = dns2.tsinghua.edu.cn.
tsinghua.edu.cn nameserver = dns2.edu.cn.

Authoritative answers can be found from:

nathben97@nathben97-VirtualBox: ~$ nslookup www.apple.co.jp
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
www.apple.co.jp canonical name = apple.co.jp.
Name:  apple.co.jp
Address: 17.172.224.38
Name:  apple.co.jp
Address: 17.142.160.9
Name:  apple.co.jp
Address: 17.178.96.9
```

Adresses :

- 17.172.224.38
- 17.142.160.9
- 17.178.96.9

## 2. Run nslookup to determine the authoritative DNS servers for a university in Europe.

```
nathben97@nathben97-VirtualBox: ~
www.apple.co.jp canonical name = apple.co.jp.
Name: apple.co.jp
Address: 17.172.224.38
Name: apple.co.jp
Address: 17.142.160.9
Name: apple.co.jp
Address: 17.178.96.9

nathben97@nathben97-VirtualBox:~$ c
c : commande introuvable
nathben97@nathben97-VirtualBox:~$ nslookup -type=NS univ-amu.fr
nslookup: '-type=NS' is not a legal IDNA2008 name (string contains a disallowed character), use +noidn
nathben97@nathben97-VirtualBox:~$ nslookup -type=NS univ-amu.fr
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
univ-amu.fr      nameserver = ns1.univmed.fr.
univ-amu.fr      nameserver = cnudns.cines.fr.

Authoritative answers can be found from:
```

### Servers :

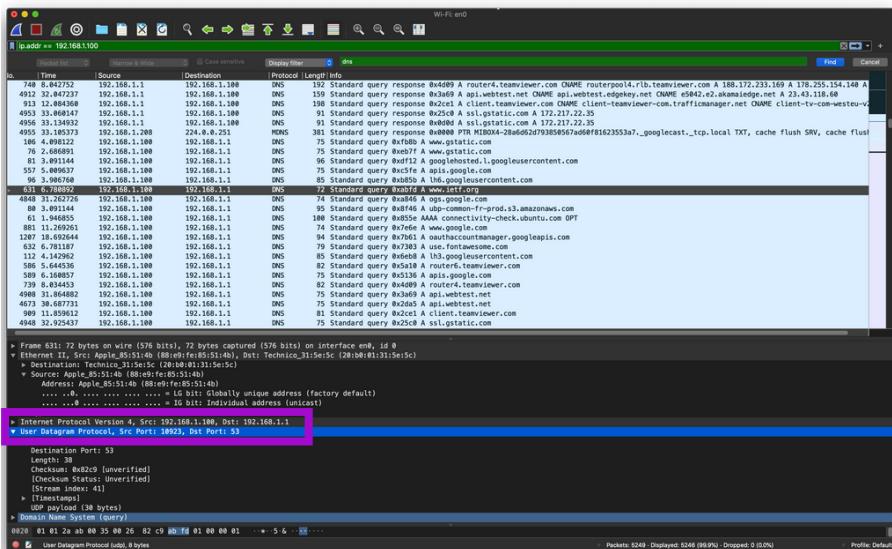
- ns1.univmed.fr
- cnudns.cines.fr

3.Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

```
nathben97@nathben97-VirtualBox:~$ nslookup univ-am.fr mail.yahoo.com  
;; connection timed out; no servers could be reached
```

```
nathben97@nathben97-VirtualBox:~$ █
```

Connection timed out no servers could be reached



## 4. Locate the DNS query and response messages. Are they sent over UDP or TCP?

UDP

## 5. What is the destination port for the DNS query message? What is the source port of DNS response message?

- Source port :10923
- Destination port :53

6 .To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

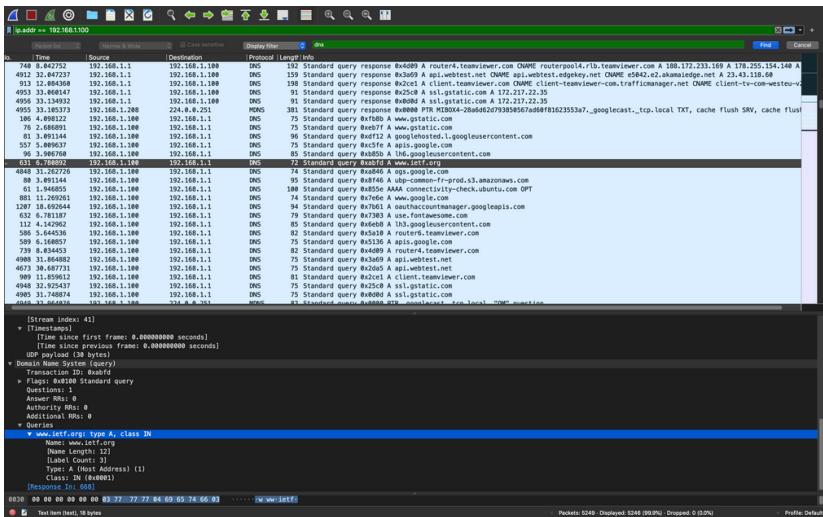
- Source :192.168.1.100
- Destination :192.168.1.1

```
status: inactive
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether 88:e9:fe:85:51:4b
    inet6 fe80::1ca9:cd24:91e4:6f82%en0 prefixlen 64 secured scopeid 0x6
        inet 192.168.1.100 netmask 0xffffffff broadcast 192.168.1.255
            nd6 options=201<PERFORMNUD,DAD>
            media: autoselect
            status: active
```

The MacOs (ipconfig /all) is "ifconfig" the inet show us that the destination feet with our DNS answer 192.168.100

## 7.Examine the DNS query message.

### What “Type” of DNS query is it? Does the query message contain any “answers”?



Standard Query ;  
Type of DNS Query : A;  
no answer.

## 8. Examine the DNS response message.

### How many “answers” are provided?

### What do each of these answers contain?

The screenshot shows a Wireshark capture of a DNS response message. The packet list pane shows many DNS queries and responses. A specific answer is highlighted in blue:

No.	Time	Source	Destination	Protocol	Length	Info
658	6.91952	192.168.1.1	192.168.1.100	DNS	149	Standard query response 0xbabfd A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 184.15.45.99 A 184.15.44.99
489	6.91953	192.168.1.1	192.168.1.100	DNS	143	Standard query response 0xbaf6 A upi-connectivity-prod-13.amazonaws.com CNAME www.upi-connectivity-central-1.amazonaws.com A 52.219.47.10
83	3.189540	192.168.1.1	192.168.1.100	DNS	104	Standard query response 0xb55e AAAA connectivity-check.ubuntu.com 0FFF
120	3.189548	192.168.1.1	192.168.1.100	DNS	104	Standard query response 0xb55e AAAA connectivity-check.ubuntu.com 0FFF
1222	18.24255	192.168.1.1	192.168.1.100	DNS	118	Standard query response 0xb761 A authaccountsmanager.googleapis.com A 23.54.89.42
1223	18.24256	192.168.1.1	192.168.1.100	DNS	118	Standard query response 0xb761 A authaccountsmanager.googleapis.com A 23.111.9.25
113	1.148989	192.168.1.1	192.168.1.100	DNS	130	Standard query response 0x8e8b A 13a.googleapiscontent.com CNAME googleapiscontent.com A 156.58.222.161
624	6.718818	192.168.1.1	192.168.1.100	DNS	206	Standard query response 0x8c38 A router6.teamviewer.com CNAME routerpool16.1b.teamviewer.com A 161.156.67.112 A 178.255.154.139 A
748	6.844742	192.168.1.1	192.168.1.100	DNS	130	Standard query response 0x8e8b A 13a.googleapiscontent.com CNAME googleapiscontent.com A 156.58.222.161
4953	33.149847	192.168.1.1	192.168.1.100	DNS	159	Standard query response 0x8d89 A router4.teamviewer.com CNAME routerpool4.1b.teamviewer.com A 180.172.233.160 A 178.255.154.148 A
4953	33.149848	192.168.1.1	192.168.1.100	DNS	159	Standard query response 0x8d89 A router4.teamviewer.com CNAME routerpool4.1b.teamviewer.com A 180.172.233.160 A 178.255.154.148 A
4953	33.149849	192.168.1.1	192.168.1.100	DNS	91	Standard query response 0x8258 A 1sl.gptatic.com A 172.272.2.25
4953	33.149850	192.168.1.1	192.168.1.100	DNS	242	Standard query response 0x8258 A 1sl.gptatic.com A 172.272.2.25
4953	33.149851	192.168.1.1	192.168.1.100	DNS	381	Standard query response 0x8000 PTR M1024x284662073852353a7..._googlecast_tcp.local TXT, cache flush SWP, cache flush SWP, cache flush SWP
180	4.035327	192.168.1.100	192.168.1.1	DNS	161	Standard-mnemo 0xb7bb \$ www.ietf.org

The details pane shows the structure of the DNS message, including the question and multiple answers. The bytes pane shows the raw hex and ASCII data of the message.

Answers :

3 answers contains :

( name, type, class, time to live, data  
,length ,adress)

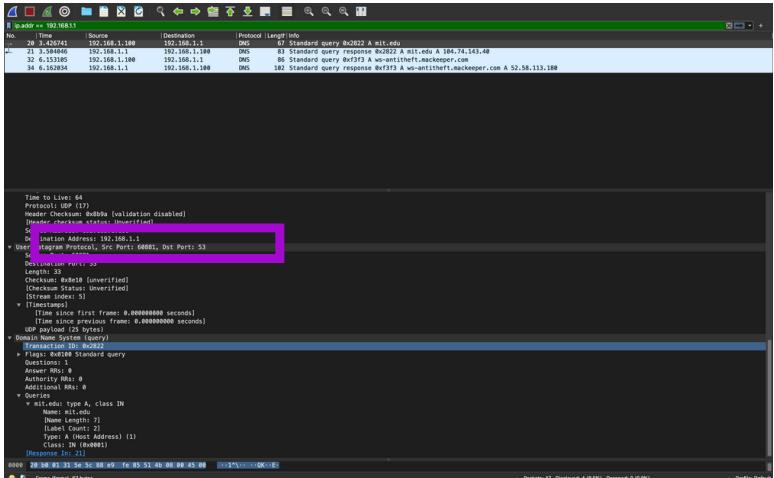
9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

Answer : adresse of provided by the DNS server of ietf.org is 104.16.44.99 as seen in the last screenshot

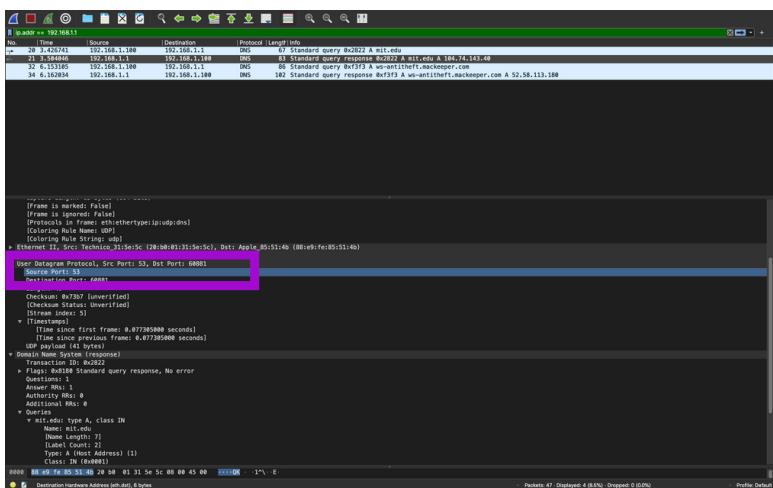
10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

All the images coming from ietf.org so no need to use a new DNS queries

# 11. What is the destination port for the DNS query message? What is the source port of DNS response message?

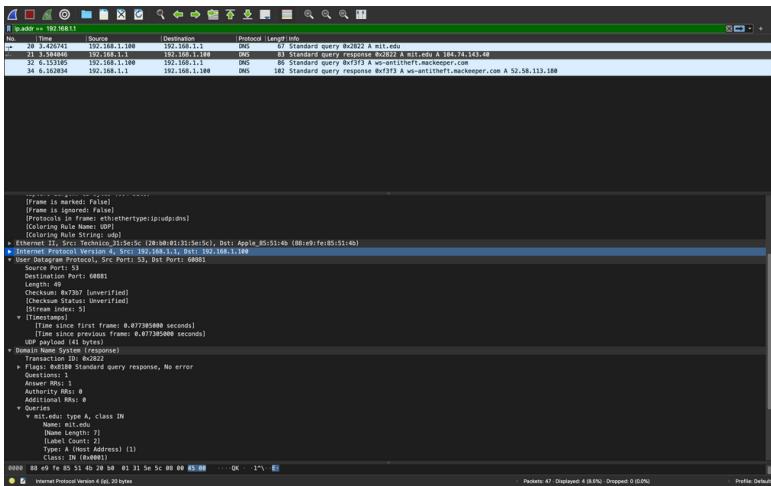


Request port 53



Answer port 53

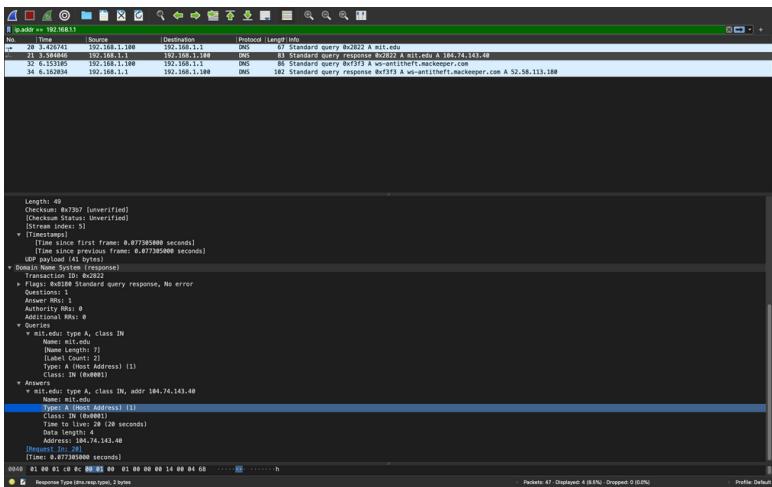
## 12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?



Destination is 192.168.1.100 its my Dns default ip as seen in the ifconfig screenshot

```
status: inactive
: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
options=400<CHANNEL_ID>
ether 88:e9:fe:85:51:4b
inet6 fe80::1ca9:c2d4:91e4:6f82%en0 prefixlen 64 secured scopeid 0x6
inet 192.168.1.100 netmask 0xffffffff broadcast 192.168.1.255
nd6 options=201<PERFORMNUD,DAD>
media: autoselect
status: active
```

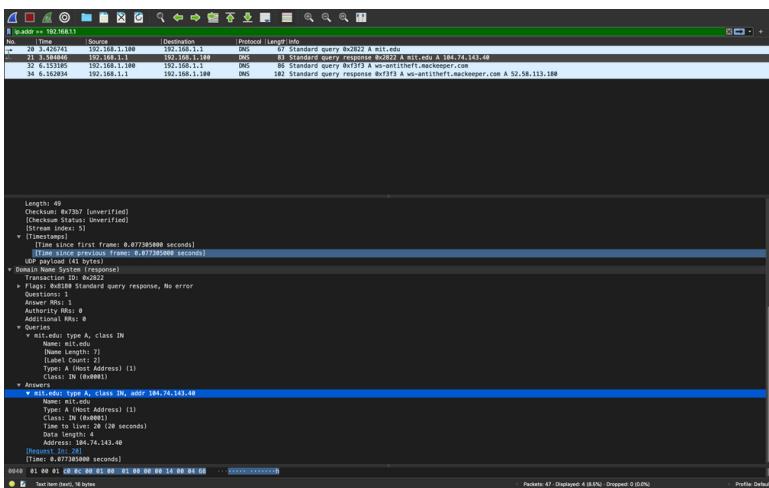
## 13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?



No answer /DNS type :A

14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

## 15.ScreenShot

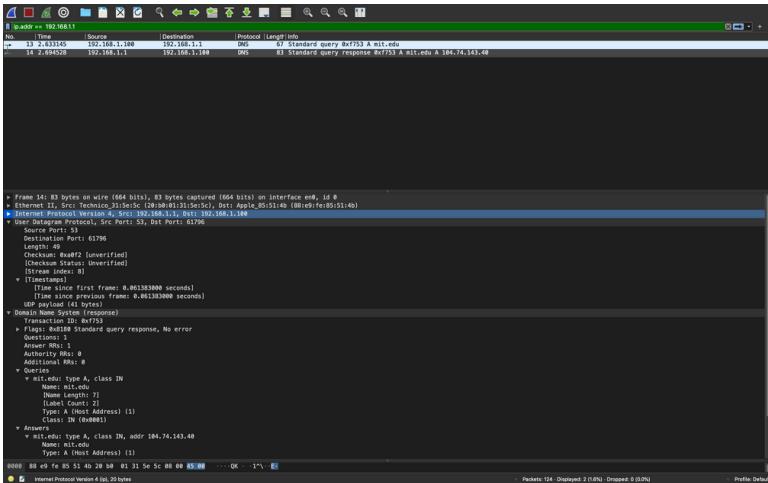


Answers :

1 answers contains :

( name, type, class, time to live, data ,length ,adress)

## 16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?



Destination is 192.168.1.100 its my Dns default ip as seen in the ifconfig screenshot

```
status: inactive
: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
  options=400<CHANNEL_IO>
  ether 88:e9:fe:85:51:4b
  inet6 fe80::1ca9:cd24:91e4:6f82%en0 prefixlen 64 secured scopeid 0x6
    inet 192.168.1.100 netmask 0xffffffff broadcast 192.168.1.255
      nd6 options=201<PERFORMNUD,DAD>
      media: autoselect
      status: active
```

## 17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

The screenshot shows a network traffic capture in Wireshark. A single DNS query frame is selected, with its details and bytes panes visible. The packet details pane shows:

Length	Checksum	Source	Destinations	Protocol	Length Info
49	Readf2	[unverified] [Content Status: Unverified]	[Stream index: 8]	DNS	67 Standard query 0x7f53 A mit.edu
48	0x0000	192.168.1.100	192.168.1.1	DNS	63 Standard query response 0x7f53 A mit.edu 104.74.143.40

The bytes pane shows the raw hex and ASCII data of the DNS message. The message structure is as follows:

- Header:** Length: 49, Checksum: Readf2 [unverified], Transaction ID: 0x7f53.
- Question:** Name: mit.edu, Type: A (Host Address), Class: IN.
- Answer:** Name: mit.edu, Type: A (Host Address), Class: IN, Data length: 71, TTL: 20, Time to live: 20 seconds.
- Additional:** None.
- Additional RR:** None.
- Queries:** None.

Below the packet details, the status bar indicates: Packets: 124 - Displayed: 2 (1%) - Dropped: 0 (0%).

Answer: Type A query, and no answer

```
nathanaelbenichou — bash — 80x22
Q Rechercher
Address: 104.74.143.40
MacBook-Pro-de-Nathanael:~ nathanaelbenichou$ nslookup mit.edu
Server:      192.168.1.1
Address:      192.168.1.1#53

Non-authoritative answer:
Name:  mit.edu
Address: 104.74.143.40

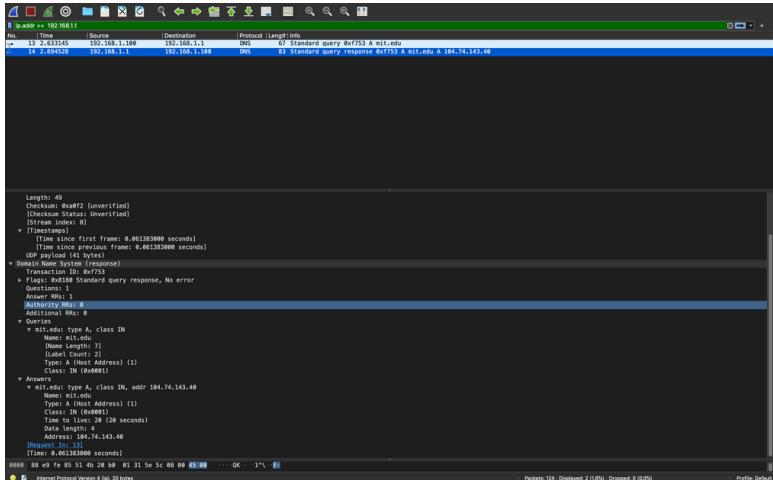
MacBook-Pro-de-Nathanael:~ nathanaelbenichou$ nslookup mit.edu
Server:      192.168.1.1
Address:      192.168.1.1#53

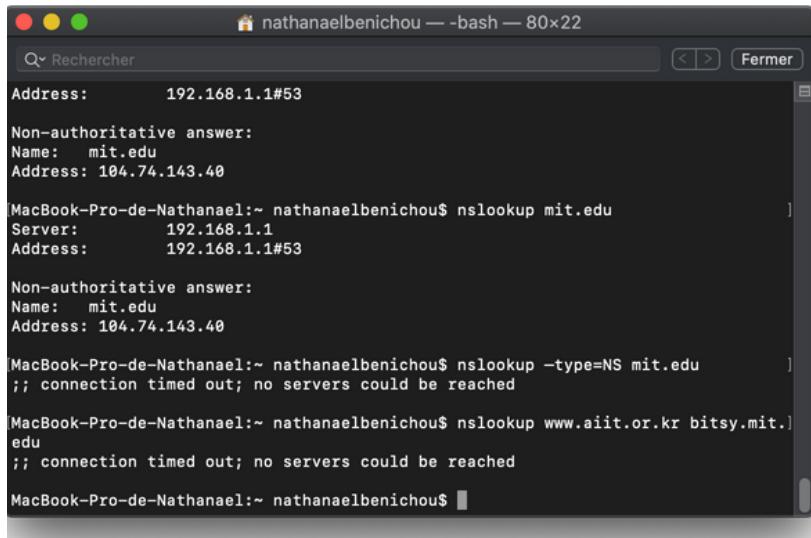
Non-authoritative answer:
Name:  mit.edu
Address: 104.74.143.40

MacBook-Pro-de-Nathanael:~ nathanaelbenichou$ nslookup -type=NS mit.edu
;; connection timed out; no servers could be reached
MacBook-Pro-de-Nathanael:~ nathanaelbenichou$
```

18. Examine the DNS response message.  
What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?

19. Provide a screenshot.





nathanaelbenichou — bash — 80x22

Q Rechercher Fermer

```
Address: 192.168.1.1#53
Non-authoritative answer:
Name: mit.edu
Address: 104.74.143.40

MacBook-Pro-de-Nathanael:~ nathanaelbenichou$ nslookup mit.edu
Server: 192.168.1.1
Address: 192.168.1.1#53

Non-authoritative answer:
Name: mit.edu
Address: 104.74.143.40

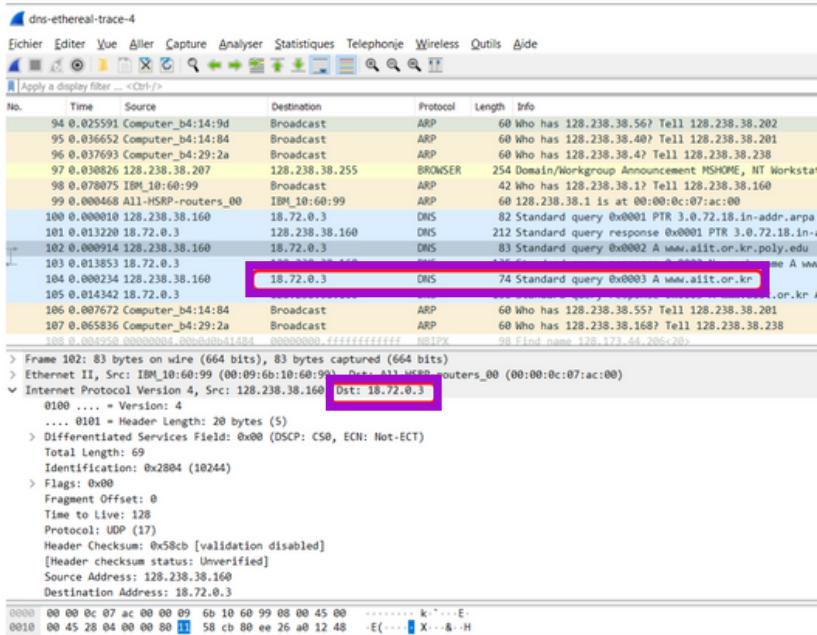
MacBook-Pro-de-Nathanael:~ nathanaelbenichou$ nslookup -type=NS mit.edu
;; connection timed out; no servers could be reached

MacBook-Pro-de-Nathanael:~ nathanaelbenichou$ nslookup www.aiit.or.kr bitsy.mit.edu
;; connection timed out; no servers could be reached

MacBook-Pro-de-Nathanael:~ nathanaelbenichou$
```

Doesn't work so i used the given pdf in  
this case

20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?



Answer: DNS send to 18.72.0.3  
the IP address of the wait response sender.

## 21. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

The screenshot shows a packet capture in Wireshark. The timeline pane at the bottom indicates the sequence of frames. Frame 102 is highlighted, showing a DNS query from an IBM computer (IP 128.238.38.160) to a broadcast address (128.238.38.255). The packet details pane shows the DNS request with the question 'www.ailt.or.kr.poly.edu' and type 'A'. The bytes pane shows the raw hex and ASCII data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
94	0.025591	Computer_b4:14:9d	Broadcast	ARP	60	Who has 128.238.38.56? Tell 128.238.38.202
95	0.036652	Computer_b4:14:84	Broadcast	ARP	60	Who has 128.238.38.40? Tell 128.238.38.201
96	0.037693	Computer_b4:29:2a	Broadcast	ARP	60	Who has 128.238.38.47 Tell 128.238.38.238
97	0.038826	128.238.38.207	128.238.38.255	BROWSER	254	Domain/Workgroup Announcement MSHOME, NT Workstation, Domain
98	0.078875	IBM_10:60:99	Broadcast	ARP	42	Who has 128.238.38.17 Tell 128.238.38.160
99	0.000468	All1-HSRP-routers_00	IBM_10:60:99	ARP	60	128.238.38.1 is at 00:00:0c:07:ac:00
100	0.000018	128.238.38.160	18.72.0.3	DNS	82	Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
101	0.013220	18.72.0.3	128.238.38.160	DNS	212	Standard query response 0x0001 PTR 3.0.72.18.in-addr.arpa PTR
102	0.000914	128.238.38.160	18.72.0.3	DNS	83	Standard query 0x0002 A www.ait.or.kr.poly.edu
103	0.013853	18.72.0.3	128.238.38.160	DNS	135	Standard query response 0x0002 No such name A www.ait.or.kr
104	0.000234	128.238.38.160	18.72.0.3	DNS	74	Standard query 0x0003 A www.ait.or.kr
105	0.014342	18.72.0.3	128.238.38.160	DNS	156	Standard query response 0x0003 A www.ait.or.kr A 218.36.94.2
106	0.007672	Computer_b4:14:84	Broadcast	ARP	60	Who has 128.238.38.55? Tell 128.238.38.201
107	0.065836	Computer_b4:29:2a	Broadcast	ARP	60	Who has 128.238.38.160? Tell 128.238.38.238
108	0.000454	00000004.000000-41484	00000000.ffffffffffff	NDIPX	98	Find name 128.173.44.20c<20>

> Frame 102: 83 bytes on wire (664 bits), 83 bytes captured (664 bytes)  
> Ethernet II, Src: IBM\_10:60:99 (00:09:60:10:60:99), Dst: All1-HSRP-routers\_00 (00:00:0c:07:ac:00)  
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 18.72.0.3  
> User Datagram Protocol, Src Port: 3752, Dst Port: 53

Domain Name System (query)  
  Transaction ID: 0x0002  
  Flags: 0x0100 Standard query  
  Questions: 1  
    Answer RRs: 0  
    Authority RRs: 0  
    Additional RRs: 0  
  Queries  
    www.ait.or.kr.poly.edu: type A, class IN  
      [Response In: 103]

Answer: Type of DNS : A  
Standard query  
no answer

22. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?

23. Provide a Screenshot:

The screenshot shows a Wireshark capture titled "dns-ethereal-trace-4". It displays a sequence of network frames. Frame 103 is a DNS query from host 18.72.0.3 to port 53, asking for the A record of www.alit.or.kr. Frame 135 is a DNS response from port 53 back to 18.72.0.3, indicating that no such name exists. The interface is set to "All" and the display filter is "`Apply a display filter ... <Ctrl-f>`".

No.	Time	Source	Destination	Protocol	Length	Info
94	0.025591	Computer_b4:14:9d	Broadcast	ARP	60	Who has 128.238.38.56? Tell 128.238.38.202
95	0.036652	Computer_b4:14:84	Broadcast	ARP	60	Who has 128.238.38.40? Tell 128.238.38.201
96	0.037693	Computer_b4:29:2a	Broadcast	ARP	60	Who has 128.238.38.47? Tell 128.238.38.238
97	0.038262	128.238.38.207	128.238.38.255	BROWSER	254	Domain/Workgroup Announcement MSHOME, NT Workstation, Domain Env
98	0.078075	IBM_10:60:99	Broadcast	ARP	42	Who has 128.238.38.17? Tell 128.238.38.160
99	0.080468	All-HSRP-routers_00	IBM_10:60:99	ARP	60	128.238.38.1 is at 00:00:0c:07:ac:00
100	0.080919	128.238.38.160	18.72.0.3	DNS	82	Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
101	0.013220	18.72.0.3	128.238.38.160	DNS	212	Standard query Response 0x0001 PTR 3.0.72.18.in-addr.arpa PTR B1
102	0.080914	128.238.38.160	18.72.0.3	DNS	83	Standard query 0x0002 A www.alit.or.kr.poly.edu
103	0.013220	18.72.0.3	128.238.38.160	DNS	135	Standard query response 0x0002 No such name A www.alit.or.kr.poly.edu
104	0.080234	128.238.38.160	18.72.0.3	DNS	74	Standard query 0x0003 A www.alit.or.kr
105	0.014342	18.72.0.3	128.238.38.160	DNS	156	Standard query response 0x0003 A www.alit.or.kr A 218.36.94.200
106	0.007672	Computer_b4:14:84	Broadcast	ARP	60	Who has 128.238.38.55? Tell 128.238.38.201
107	0.065836	Computer_b4:29:2a	Broadcast	ARP	60	Who has 128.238.38.168? Tell 128.238.38.238

> Frame 103: 135 bytes on wire (1080 bits), 135 bytes captured (1080 bits)  
> Ethernet II, Src: Cisco\_83:e4:54 (00:0b:8e:83:e4:54), Dst: IBM\_10:60:99 (00:09:6b:10:60:99)  
> Internet Protocol Version 4, Src: 18.72.0.3, Dst: 128.238.38.160  
> User Datagram Protocol, Src Port: 53, Dst Port: 3752  
▼ Domain Name System (response)  
    Transaction ID: 0x0002  
    > Flags: 0x0853 Standard query response, No such name  
        Questions: 1  
        Answers RRs: 0  
        Authority RRs: 1  
        Additional RRs: 0  
    ▼ Queries  
        > www.alit.or.kr.poly.edu: type A, class IN  
    > Authoritative nameservers  
        [Request In: 102]  
        [Time: 0.013853000 seconds]  
0000 00 09 6b 10 60 99 00 b0 8e 83 e4 54 08 00 45 00 ··k.·· ··T-E···  
0010 00 79 b5 42 40 08 f1 11 1a 58 12 48 00 03 88 ee ·v-BB·· ·X-H···

Answer: Type of DNS : A  
Standard query  
no answer



# תקשרות

Nathanael Benichou

JORDAN PEREZ



מטלה {

# PART I

## Question 1

הציגו יתרון אחד לשימוש ב-HoDo והסבירו אותו  
(כਮובן, מעבר לעובדה שהוא מאובטח ומצוון)

## Answer 1

מעבר להצפת הנתונים, ל- HoS יש יתרון  
בהגדלת הביצועים, גם במקרה של אובדן חבילות,  
הוא מהיר יותר בשילוח מיד.

## Question 2

הציגו והסבירו על שני חסרונות לשימוש בשיטת  
HoD לועמת DNS הרגיל

## Answer 2

(א)

HoD מונע מעקב אחר משתמשים.  
בחינת שאילות DNS יכולה להיות חשפנית מאוד וניתן  
להשתמש בה לטובה (גילוי פעילות של תוכנות זדוניות) או  
לروع (לאתור מי מבקר באיזה אתר). שוב, זו המטרה  
המשמעות של HoD להקשות על הניטור.

לפיכך, מפעיל רשות אינטראקטיבית יכולם לסנן את התוכן של  
אתרים לא רצויים מכיוון שאין שמי משתמש ב-HoD עוקף את  
רשת האבטחה הנו"ל, ומסכן את המשתמש.

(ב)

השימוש ב-HoD הופך את הרשות לאיטית ופחות  
יעילה מכיוון שהיא ייעוד עובר ברשות מרוחקת

## Question 3

בחרו אחד מהחסרונות משלה (2), הציעו דרך למתן\Lעקו\לפתרון חיסרונו זה והסבירו אותה.

## Answer 3

השימוש ב- GEODNS יכול להפוך את השימוש ב- HOD לאיי פחות, GeoDns משפר את חיפוש שמות הדומיינים על ידי רגולציה כתובת בהתבסס על המיקום הגיאוגרפי של הלוח.

## Answer 4

א) יישום ה- HoD בرمת היישום

יתרונות: ניתן לישם את פרוטוקול ה- DNS בישומים הנתמכים.  
חסרון - אם המשתמש מתעלם מבקשת, היישום לא יוכל להציג את המשתמש שהתעלם ממנו.

ב) יישום HoD בرمת שרת ה- \* Proxy - ברשות -

יתרון (אנונימיות): ה- proxy הוא נתיב המאפשר להפוך לאNONIMO. שימוש זה נותן אפשרות למשתמש כי IP שלהם, ולכן זהותו, נותר לא ידוע.

חסרון - למשתמשים שכנים המזוהים עם אותה רשות יש גישה למידע.

ג) יישום HoD של שרת ה- proxy המקומי -

יתרון  
גם אם המשתמשים מחוברים לאותה רשות הבקשות יוצפנו ולכן ההתקפה תהיה קשה יותר.

חסרון איקון  
התקנה כללית, באופן מקומי, עלולה ליצור עומס.

ד) התקן תוסף המישם את HoDo:

יתרונות:  
בניגוד ל-Proxy, בהיותו מודול תוסף, אין צורך להתקין אותו בכל המכונות בנפרד.

חסרון:  
לא כל מערכות הפעלה תומכות בתוסף

## מסקנות

נראה שהכי טוב הוא לחסוך זמן ולהימנע מכל סוג של עומס, הפתרון המועיל ביותר נראה לי הפלאגין.

## Question 5

נניח שאנו ברשות שקיים בה איבוד פקודות (packet loss) באחוז לא ידוע לנו רוצים לטעון דף שציריך 25 שאלות כדי לבדוק את כל המשאבים שבו. הציגו יתרון בhor שיש ל-Ho53 לעומת Ho53. (רמז: מנגן הקיים ב-TCP)

## Answer 5

בהתליר Ho53 משתמש בפרוטוקול UDP.

אין לו את אותם המאפיינים.

כאשר משתמשים ב-Ho53 במהלך אובדן מנות, מנגן שולח *acks*, מים לחכילה לפני זה שאבד, ולכן ניתן יהיה לשולח אותו שוב ללא בעיה.

# PART II

```
Jordan@Jordan-VirtualBox: ~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp
```

```
jordan@Jordan-VirtualBox:~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp$ ./measure
Socket successfully created..
Socket successfully binded..
Server listening..
server acccept the client...
```

Currently using cubic:

```
Received file 1 from client in 0.0000050 seconds
Received file 2 from client in 0.0000020 seconds
Received file 3 from client in 0.0000010 seconds
Received file 4 from client in 0.0000020 seconds
Received file 5 from client in 0.0000010 seconds
```

Average time: 0.0000022 seconds

Now using reno:

```
Received file 1 from client in 0.0000020 seconds
Received file 2 from client in 0.0000010 seconds
Received file 3 from client in 0.0000010 seconds
Received file 4 from client in 0.0000010 seconds
Received file 5 from client in 0.0000030 seconds
```

Average time: 0.0000016 seconds

```
Jordan@Jordan-VlrtualBox:~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp$
```

```
Jordan@Jordan-VirtualBox: ~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp
```

```
jordan@Jordan-VirtualBox:~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp$ ./sender
Socket successfully created..
Current: cubic
connected to the server..
New: reno
jordan@Jordan-VirtualBox:~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp$
```

# No Packet Loss

```
jordan@jordan-VirtualBox:~$ sudo tc qdisc add dev lo root netem loss 10%
jordan@jordan-VirtualBox:~$ █
```

```
Jordan@jordan-VirtualBox: ~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp
```

```
jordan@jordan-VirtualBox:~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp$ ./measure
Socket successfully created..
Socket successfully binded..
Server listening..
server acccept the client...
```

```
Currently using cubic:
Received file 1 from client in 0.0000040 seconds
Received file 2 from client in 0.00000170 seconds
Received file 3 from client in 0.0000010 seconds
Received file 4 from client in 0.0000020 seconds
Received file 5 from client in 0.0000020 seconds
```

Average time: 0.0000052 seconds

```
Now using reno:
Received file 1 from client in 0.0000020 seconds
Received file 2 from client in 0.0000020 seconds
Received file 3 from client in 0.0000020 seconds
Received file 4 from client in 0.0000010 seconds
Received file 5 from client in 0.0000020 seconds
```

Average time: 0.0000018 seconds

```
jordan@jordan-VirtualBox:~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp$ █
```

```
Jordan@Jordan-VirtualBox: ~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp
```

```
jordan@jordan-VirtualBox:~/Desktop/Tikchoret/Tikchoret 3/last verston/Tcp$ ./sender
Socket successfully created..
Current: cubic
connected to the server..
New: reno
jordan@jordan-VirtualBox:~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp$ █
```

# 10% Packet Loss

```
jordan@jordan-VirtualBox:~$ sudo tc qdisc add dev lo root netem loss 15%
jordan@jordan-VirtualBox:~$ █
```

```
jordan@jordan-VirtualBox: ~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp$ █
```

```
jordan@jordan-VirtualBox:~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp$ ./measure
```

```
Socket successfully created..
```

```
Socket successfully binded..
```

```
Server listening..
```

```
server acccept the client...
```

```
Currently using cubic:
```

```
Received file 1 from client in 0.0000190 seconds
```

```
Received file 2 from client in 0.0000020 seconds
```

```
Received file 3 from client in 0.0000020 seconds
```

```
Received file 4 from client in 0.0000020 seconds
```

```
Received file 5 from client in 0.0000020 seconds
```

```
Average time: 0.0000054 seconds
```

```
Now using reno:
```

```
Received file 1 from client in 0.0000220 seconds
```

```
Received file 2 from client in 0.0000020 seconds
```

```
Received file 3 from client in 0.0000020 seconds
```

```
Received file 4 from client in 0.0000010 seconds
```

```
Received file 5 from client in 0.0000030 seconds
```

```
Average time: 0.0000060 seconds
```

```
jordan@jordan-VirtualBox:~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp$ █
```

```
jordan@jordan-VirtualBox: ~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp$ ./sender
```

```
Socket successfully created..
```

```
Current: cubic
```

```
connected to the server..
```

```
New: reno
```

```
jordan@jordan-VirtualBox:~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp$ █
```

# 15% Packet Loss

jordan@jordan-VirtualBox: ~

```
jordan@jordan-VirtualBox:-$ sudo tc qdisc add dev lo root netem loss 20%
jordan@jordan-VirtualBox:-$ 
```

Jordan@jordan-VirtualBox: ~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp

```
jordan@jordan-VirtualBox:~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp$ ./measure
Socket successfully created..
Socket successfully binded..
Server listening..
server acccept the client...
```

Currently using cubic:  
Received file 1 from client in 0.0000060 seconds  
Received file 2 from client in 0.0000560 seconds  
Received file 3 from client in 0.0000030 seconds  
Received file 4 from client in 0.0000020 seconds  
Received file 5 from client in 0.0000010 seconds

Average time: 0.0000136 seconds

Now using reno:  
Received file 1 from client in 0.0000010 seconds  
Received file 2 from client in 0.0000010 seconds  
Received file 3 from client in 0.0000020 seconds  
Received file 4 from client in 0.0000020 seconds  
Received file 5 from client in 0.0000040 seconds

Average time: 0.0000020 seconds

```
jordan@jordan-VirtualBox:~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp$ 
```

Jordan@jordan-VirtualBox: ~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp

```
jordan@jordan-VirtualBox:~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp$ ./sender
Socket successfully created..
Current: cubic
connected to the server..
New: reno
jordan@jordan-VirtualBox:~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp$ 
```

# 20% Packet Loss

jordan@Jordan-VirtualBox: ~

```
jordan@jordan-VirtualBox:~$ sudo tc qdisc add dev lo root netem loss 25%
jordan@jordan-VirtualBox:~$
```

Jordan@Jordan-VirtualBox: ~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp

```
jordan@jordan-VirtualBox:~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp$ ./measure
Socket successfully created..
Socket successfully binded..
Server listening..
server acccept the client...
```

```
Currently using cubic:
Received file 1 from client in 0.0000070 seconds
Received file 2 from client in 0.0000020 seconds
Received file 3 from client in 0.0000010 seconds
Received file 4 from client in 0.0000010 seconds
Received file 5 from client in 0.0000020 seconds
```

Average time: 0.0000026 seconds

```
Now using reno:
Received file 1 from client in 0.0000010 seconds
Received file 2 from client in 0.0000030 seconds
Received file 3 from client in 0.0000570 seconds
Received file 4 from client in 0.0000050 seconds
Received file 5 from client in 0.0000250 seconds
```

Average time: 0.0000182 seconds

```
jordan@jordan-VirtualBox:~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp$
```

Jordan@Jordan-VirtualBox: ~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp

```
jordan@jordan-VirtualBox:~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp$ ./sender
Socket successfully created..
Current: cubic
connected to the server..
New: rno
jordan@jordan-VirtualBox:~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp$
```

# 25% Packet Loss

Jordan@Jordan-VirtualBox: ~

```
jordan@jordan-VirtualBox:~$ sudo tc qdisc add dev lo root netem loss 30%
jordan@jordan-VirtualBox:~$ 
```

Jordan@Jordan-VirtualBox: ~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp

```
jordan@jordan-VirtualBox:~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp$ ./measure
```

```
Socket successfully created..
```

```
Socket successfully binded..
```

```
Server listening..
```

```
server acccept the client...
```

```
Currently using cubic:
```

```
Received file 1 from client in 0.0000490 seconds
```

```
Received file 2 from client in 0.0000030 seconds
```

```
Received file 3 from client in 0.0000010 seconds
```

```
Received file 4 from client in 0.0000010 seconds
```

```
Received file 5 from client in 0.0000020 seconds
```

Average time: 0.0000112 seconds

```
Now using reno:
```

```
Received file 1 from client in 0.0000020 seconds
```

```
Received file 2 from client in 0.0000010 seconds
```

```
Received file 3 from client in 0.0000010 seconds
```

```
Received file 4 from client in 0.0000010 seconds
```

```
Received file 5 from client in 0.0000040 seconds
```

Average time: 0.0000018 seconds

Jordan@Jordan-VirtualBox: ~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp\$

Jordan@Jordan-VirtualBox: ~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp

```
jordan@jordan-VirtualBox:~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp$ ./sender
```

```
Socket successfully created..
```

```
Current: cubic
```

```
connected to the server..
```

```
New: reno
```

Jordan@Jordan-VirtualBox: ~/Desktop/Tikchoret/Tikchoret 3/last version/Tcp\$

# 30% Packet Loss



# תקשות מטלה

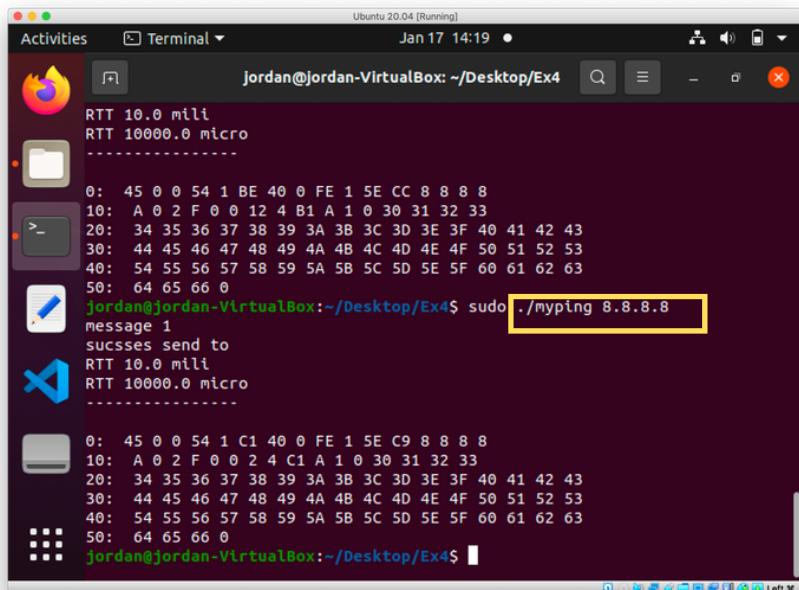
Nathanael Benichou-Jordan Perez



# PARTIE 1

אך חלון - *myping*

Send Ping with myping.c

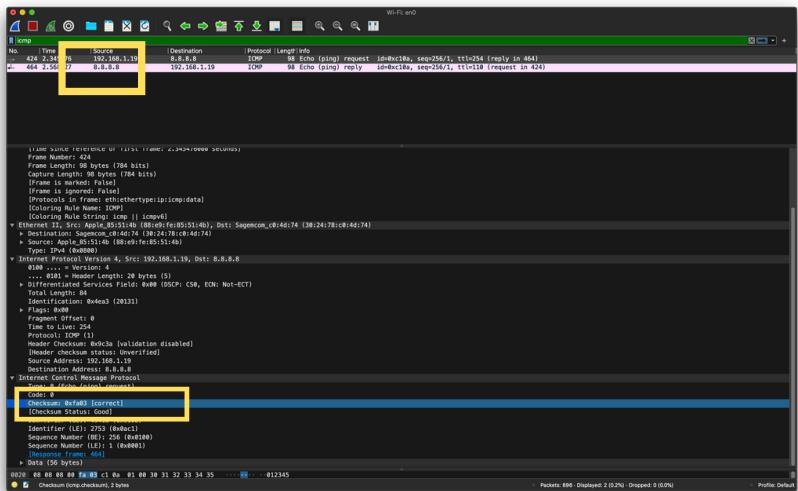


The screenshot shows a terminal window on an Ubuntu 20.04 desktop environment. The terminal title is "Terminal" and the prompt is "jordan@jordan-VirtualBox: ~/Desktop/Ex4\$". The user has run the command `./myping 8.8.8.8`, which outputs the following data:

```
RTT 10.0 mili
RTT 10000.0 micro
-----
0: 45 0 0 54 1 BE 40 0 FE 1 5E CC 8 8 8 8
10: A 0 2 F 0 0 12 4 B1 A 1 0 30 31 32 33
20: 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 40 41 42 43
30: 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50 51 52 53
40: 54 55 56 57 58 59 5A 5B 5C 5D 5E 5F 60 61 62 63
50: 64 65 66 0
jordan@jordan-VirtualBox:~/Desktop/Ex4$ sudo ./myping 8.8.8.8
message 1
succses send to
RTT 10.0 mili
RTT 10000.0 micro
-----
0: 45 0 0 54 1 C1 40 0 FE 1 5E C9 8 8 8 8
10: A 0 2 F 0 0 2 4 C1 A 1 0 30 31 32 33
20: 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 40 41 42 43
30: 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50 51 52 53
40: 54 55 56 57 58 59 5A 5B 5C 5D 5E 5F 60 61 62 63
50: 64 65 66 0
jordan@jordan-VirtualBox:~/Desktop/Ex4$
```

*Send ping to 8.8.8.8*

# Capture pacquets with WireShark



*Paquets ICMP well sniffed , CheckSum  
Correct ,Destination is 8.8.8.8*

## Send Ping\_(Another try)

```
Activities Terminal Jan 17 14:21
jordan@Jordan-VirtualBox: ~/Desktop/Ex4
20: 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 40 41 42 43
30: 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50 51 52 53
40: 54 55 56 57 58 59 5A 5B 5C 5D 5E 5F 60 61 62 63
50: 64 65 66 0
jordan@Jordan-VirtualBox: ~/Desktop/Ex4$ sudo ./myping 8.8.8.8
Message 1
succses send to
RTT 10.0 milli
RTT 10000.0 micro
-----
0: 45 0 0 54 1 C1 40 0 FE 1 5E C9 8 8 8 8
10: A 0 2 F 0 0 2 4 C1 A 1 0 30 31 32 33
20: 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 40 41 42 43
30: 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50 51 52 53
40: 54 55 56 57 58 59 5A 5B 5C 5D 5E 5F 60 61 62 63
50: 64 65 66 0
jordan@Jordan-VirtualBox: ~/Desktop/Ex4$ sudo ./myping 8.8.8.7
Message 1
succses send to
RTT 45.0 milli
RTT 45000.0 micro
^C
jordan@Jordan-VirtualBox: ~/Desktop/Ex4$
```

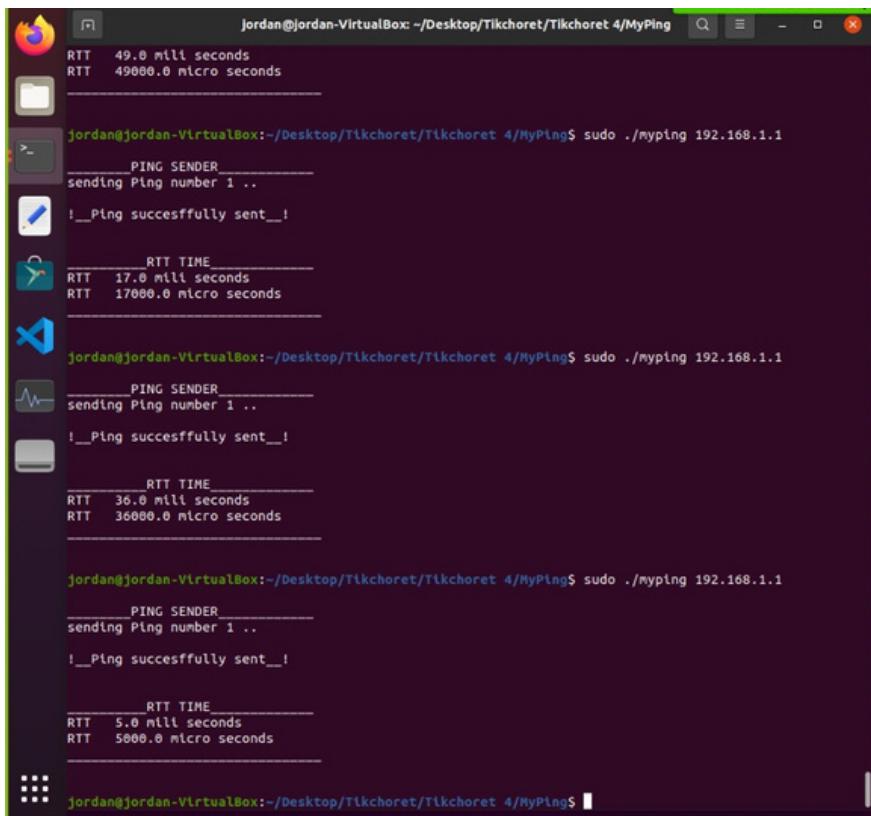
*Send ping to 8.8.8.7*

# *Well Recieved*

# PARTIE 2

## Sniffing – בְּמַלְחָקָה

*Send 7 Ping to the Same Adress*



```
Jordan@Jordan-VirtualBox: ~/Desktop/Tikchoret/Tikchoret 4/MyPing$ sudo ./myping 192.168.1.1
____ PING SENDER _____
sending Ping number 1 ..
!_Ping successfully sent_!

      RTT TIME
RTT  49.0 mill seconds
RTT 49000.0 micro seconds

____ PING SENDER _____
sending Ping number 1 ..
!_Ping successfully sent_!

      RTT TIME
RTT 17.0 mill seconds
RTT 17000.0 micro seconds

____ PING SENDER _____
sending Ping number 1 ..
!_Ping successfully sent_!

      RTT TIME
RTT 36.0 mill seconds
RTT 36000.0 micro seconds

____ PING SENDER _____
sending Ping number 1 ..
!_Ping successfully sent_!

      RTT TIME
RTT 5.0 mill seconds
RTT 5000.0 micro seconds

____ PING SENDER _____
sending Ping number 1 ..
!_Ping successfully sent_!

      RTT TIME
RTT 5.0 mill seconds
RTT 5000.0 micro seconds

____ PING SENDER _____
sending Ping number 1 ..
!_Ping successfully sent_!

      RTT TIME
RTT 5.0 mill seconds
RTT 5000.0 micro seconds

____ PING SENDER _____
sending Ping number 1 ..
!_Ping successfully sent_!

      RTT TIME
RTT 5.0 mill seconds
RTT 5000.0 micro seconds

jordan@Jordan-VirtualBox: ~/Desktop/Tikchoret/Tikchoret 4/MyPing$ sudo ./myping 192.168.1.1
```

# *Sniff The Ping Sent with Sniffer.c*

```
jordan@jordan-VirtualBox:~/Desktop/Tikchoret/Tikchoret 4/Or Sniffer
```

---

```
Available Devices are :
1. enp0s3 - (null)
2. enp0s8 - (null)
3. lo - (null)
4. any - Pseudo-device that captures on all interfaces
5. bluetooth-monitor - Bluetooth Linux Monitor
6. nflog - Linux netfilter log (NFLOG) interface
7. nfqueue - Linux netfilter queue (NFQUEUE) interface

Which device would you want to sniff ? 1
Opening device enp0s3 for sniffing ... Done
Number of Packet ICMP : 6
#Source IP      : 10.0.2.15
#Destination IP : 192.168.1.1
#Code : 0
#Type : 8

Number of Packet ICMP : 1
#Source IP      : 192.168.1.1
#Destination IP : 10.0.2.15
#Code : 0
#Type : 8

Number of Packet ICMP : 2
#Source IP      : 10.0.2.15
#Destination IP : 192.168.1.1
#Code : 0
#Type : 8

Number of Packet ICMP : 3
#Source IP      : 192.168.1.1
#Destination IP : 10.0.2.15
#Code : 0
#Type : 0

Number of Packet ICMP : 4
#Source IP      : 10.0.2.15
#Destination IP : 192.168.1.1
#Code : 0
#Type : 8

Number of Packet ICMP : 5
#Source IP      : 192.168.1.1
#Destination IP : 10.0.2.15
#Code : 0
#Type : 0
```



# Compare My Sniffer And WireShark

```
Jordan@Jordan-VirtualBox:~/Desktop/Tikshoret/Tikshoret 4$ ./MyPing
RTT TIME_
RTT 17.0 mill seconds
RTT 17000.0 micro seconds

Jordan@Jordan-VirtualBox:~/Desktop/Tikshoret/Tikshoret 4$ ./MyPing 192.168.1.1
PING SENDER
sending Ping number 1 ...
1..._Ping successfully sent_!

RTT TIME_
RTT 30.0 mill seconds
RTT 36000.0 micro seconds

Jordan@Jordan-VirtualBox:~/Desktop/Tikshoret/Tikshoret 4$ ./MyPing 192.168.1.1
PING SENDER
sending Ping number 1 ...
1..._Ping successfully sent_!

RTT TIME_
RTT 5.0 mill seconds
RTT 5800.0 micro seconds

Jordan@Jordan-VirtualBox:~/Desktop/Tikshoret/Tikshoret 4$ ./MyPing 192.168.1.1
PING SENDER
sending Ping number 1 ...
1..._Ping successfully sent_!

Jordan@Jordan-VirtualBox:~/Desktop/Tikshoret/Tikshoret 4$ ./Sniffer
which device would you want to sniff ? 2
Opening device mapped for sniffing... done
[["A-Chair"] *** [A-sniff] sniff) Interrupt
Jordan@Jordan-VirtualBox:~/Desktop/Tikshoret/Tikshoret 4$ ./Sniffer
sudo ./Sniffer
sudo ./Sniffer
Finding devices ... Success !
Available Device are :
1. enp0s3 (null)
2. enp0s8 (null)
3. enp0s9 (null)
4. any - Pseudo-device that captures on all interfaces
5. mon0 - Linux monitor log (MONITOR) Interface
6. alog - Linux netfilter log (NFLOG) Interface
7. nfqueue - Linux netfilter queue (NQUEUE) Interface

which device would you want to sniff ? 7
Opening device mapped for sniffing... done
Number of Packet ICMP : 0
#Source IP : 192.168.1.15
#Destination IP : 192.168.1.5
#Code : 0
#Type : 8

Number of Packet ICMP : 1
#Source IP : 192.168.1.5
#Destination IP : 192.168.1.15
#Code : 0
#Type : 8

Number of Packet ICMP : 2
#Source IP : 192.168.1.15
#Destination IP : 192.168.1.5
#Code : 0
#Type : 8

Number of Packet ICMP : 3
#Source IP : 192.168.1.5
#Destination IP : 192.168.1.15
#Code : 0
#Type : 8

Number of Packet ICMP : 4
#Source IP : 192.168.1.5
#Destination IP : 192.168.1.15
#Code : 0
#Type : 8
```



*Send 4 Ping to the Same Adresse  
Sniffe With sniffer.c & WireShark*

No.	Time	Source	Destination	Protocol	Length	Info
608	0.000174	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request 1d=0x00001, seq=1558/5639, ttl=254 (reply in 689)
609	0.000195	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply 1d=0x00001, seq=1558/5639, ttl=254 (request in 689)
610	0.000215	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) request 1d=0x00001, seq=1559/5894, ttl=254 (reply in 668)
605	0.000075	192.168.1.10	192.168.1.10	ICMP	98	Echo (ping) reply 1d=0x00001, seq=1559/5894, ttl=64 (request in 668)
744	0.000767	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request 1d=0x00001, seq=1560/6156, ttl=254 (reply in 745)
745	0.000547	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply 1d=0x00001, seq=1560/6156, ttl=64 (request in 745)
807	0.000250	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request 1d=0x00001, seq=1561/6400, ttl=254 (reply in 807)
808	0.000387	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply 1d=0x00001, seq=1561/6400, ttl=64 (request in 807)