



Δρ. Άννα Κεφάλια

WireShark
(a network protocol analyser)

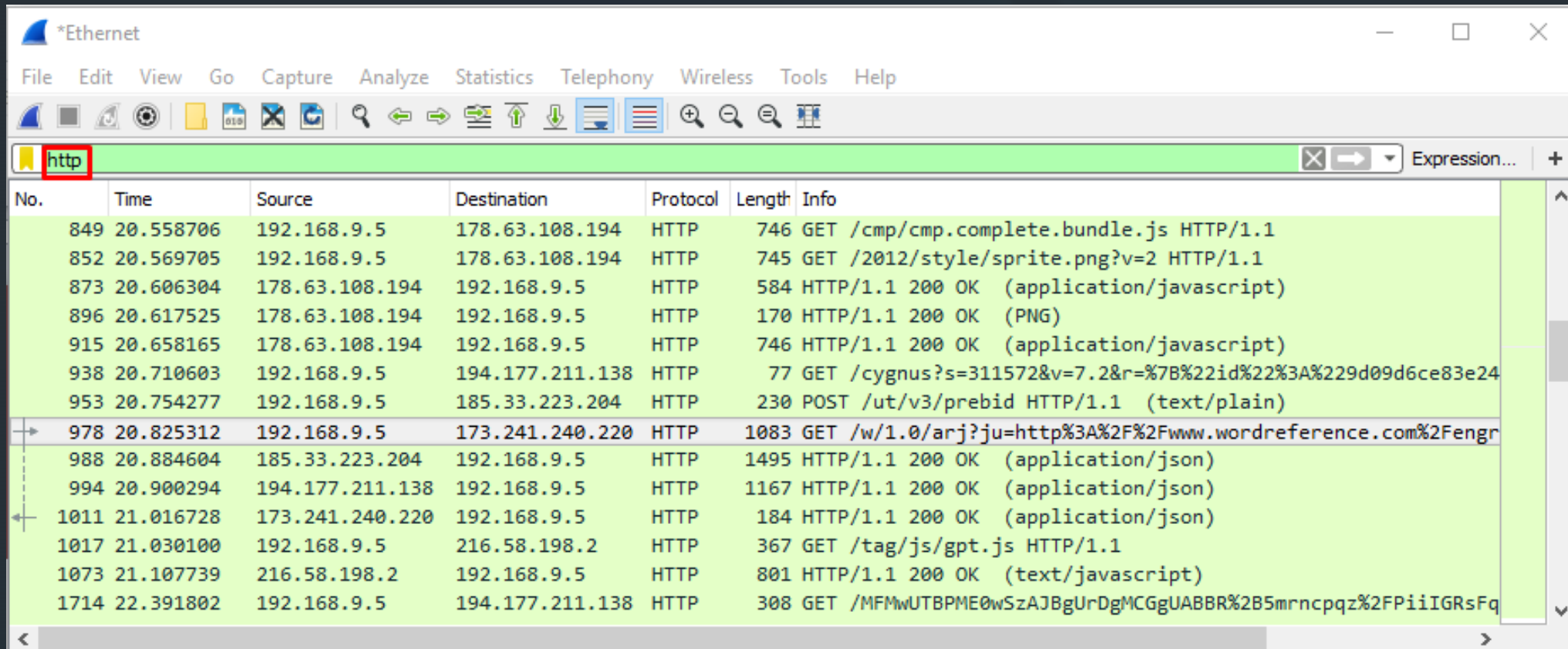
WireShark Web Browsing Demo

Try it out!

- Ξεκινήστε τον Browser
- Ξεκινήστε το WireShark
- Επιλέξτε το interface για ανίχνευση
- Ξεκινήστε την ανίχνευση 
- Visit <http://ccslab.aueb.gr/> ή κάποιο άλλο URL
- Σταματήστε την ανίχνευση 
- Ανάμεσα στα πακέτα που ανιχνεύθηκαν υπάρχει και η ανταλλαγή των HTTP μηνυμάτων...

Filtering

Filter HTTP κίνηση



The screenshot shows the Wireshark interface with a network capture filtered for HTTP traffic. The filter expression 'http' is entered in the filter field. The packet list pane displays several HTTP packets, with packet 978 selected. The packet details pane shows the structure of the selected packet, including the Ethernet II header, Internet Protocol Version 4 header, and Hypertext Transfer Protocol header.

No.	Time	Source	Destination	Protocol	Length	Info
849	20.558706	192.168.9.5	178.63.108.194	HTTP	746	GET /cmp/cmp.complete.bundle.js HTTP/1.1
852	20.569705	192.168.9.5	178.63.108.194	HTTP	745	GET /2012/style/sprite.png?v=2 HTTP/1.1
873	20.606304	178.63.108.194	192.168.9.5	HTTP	584	HTTP/1.1 200 OK (application/javascript)
896	20.617525	178.63.108.194	192.168.9.5	HTTP	170	HTTP/1.1 200 OK (PNG)
915	20.658165	178.63.108.194	192.168.9.5	HTTP	746	HTTP/1.1 200 OK (application/javascript)
938	20.710603	192.168.9.5	194.177.211.138	HTTP	77	GET /cygnus?s=311572&v=7.2&r=%7B%22id%22%3A%229d09d6ce83e24
953	20.754277	192.168.9.5	185.33.223.204	HTTP	230	POST /ut/v3/prebid HTTP/1.1 (text/plain)
978	20.825312	192.168.9.5	173.241.240.220	HTTP	1083	GET /w/1.0/arj?ju=http%3A%2F%2Fwww.wordreference.com%2Fengr
988	20.884604	185.33.223.204	192.168.9.5	HTTP	1495	HTTP/1.1 200 OK (application/json)
994	20.900294	194.177.211.138	192.168.9.5	HTTP	1167	HTTP/1.1 200 OK (application/json)
1011	21.016728	173.241.240.220	192.168.9.5	HTTP	184	HTTP/1.1 200 OK (application/json)
1017	21.030100	192.168.9.5	216.58.198.2	HTTP	367	GET /tag/js/gpt.js HTTP/1.1
1073	21.107739	216.58.198.2	192.168.9.5	HTTP	801	HTTP/1.1 200 OK (text/javascript)
1714	22.391802	192.168.9.5	194.177.211.138	HTTP	308	GET /MFMwUTBPME0wSzAJBgUrDgMCGGUABBR%2B5mrncpqz%2FPiiIGRsFq

- Επιλέξτε ένα HTTP GET πακέτο

The screenshot displays the Wireshark network traffic analysis tool. The main pane shows a list of captured packets. Packet 978 is highlighted with a red box. The packet details pane shows the Hypertext Transfer Protocol section expanded, and the packet bytes pane shows the raw data.

No.	Time	Source	Destination	Protocol	Length	Info
849	20.558706	192.168.9.5	178.63.108.194	HTTP	746	GET /cmp/cmp.complete.bundle.js HTTP/1.1
852	20.569705	192.168.9.5	178.63.108.194	HTTP	745	GET /2012/style/sprite.png?v=2 HTTP/1.1
873	20.606304	178.63.108.194	192.168.9.5	HTTP	584	HTTP/1.1 200 OK (application/javascript)
896	20.617525	178.63.108.194	192.168.9.5	HTTP	170	HTTP/1.1 200 OK (PNG)
915	20.658165	178.63.108.194	192.168.9.5	HTTP	746	HTTP/1.1 200 OK (application/javascript)
938	20.710603	192.168.9.5	194.177.211.138	HTTP	77	GET /cygnus?s=311572&v=7.2&r=%7B%22id%22%3A%2229d09d6ce83e246%
953	20.754277	192.168.9.5	185.33.223.204	HTTP	230	POST /ut/v3/prebid HTTP/1.1 (text/plain)
978	20.825312	192.168.9.5	173.241.240.220	HTTP	1083	GET /w/1.0/arj?ju=http%3A%2F%2Fwww.wordreference.com%2Fengr%2
988	20.884604	185.33.223.204	192.168.9.5	HTTP	1495	HTTP/1.1 200 OK (application/json)
994	20.900294	194.177.211.138	192.168.9.5	HTTP	1167	HTTP/1.1 200 OK (application/json)
1011	21.016728	173.241.240.220	192.168.9.5	HTTP	184	HTTP/1.1 200 OK (application/json)
1017	21.030100	192.168.9.5	216.58.198.2	HTTP	367	GET /tag/js/gpt.js HTTP/1.1
1073	21.107730	216.58.198.2	192.168.9.5	HTTP	801	HTTP/1.1 200 OK (text/javascript)

Frame 978: 1083 bytes on wire (8664 bits), 1083 bytes captured (8664 bits) on interface 0
> Ethernet II, Src: Giga-Byt_48:19:9f (fc:aa:14:48:19:9f), Dst: Fortinet_09:00:25 (00:09:0f:09:00:25)
> Internet Protocol Version 4, Src: 192.168.9.5, Dst: 173.241.240.220
> Transmission Control Protocol, Src Port: 54334, Dst Port: 80, Seq: 1, Ack: 1, Len: 1029
> Hypertext Transfer Protocol

```
0030  01 00 54 ef 00 00 47 45 54 20 2f 77 2f 31 2e 30  ..T...GET /w/1.0
0040  2f 61 72 6a 3f 6a 75 3d 68 74 74 70 25 33 41 25  /arj?ju= http%3A%
0050  32 46 25 32 46 77 77 77 2e 77 6f 72 64 72 65 66  2F%2Fwww .wordref
0060  65 72 65 6e 63 65 2e 63 6f 6d 25 32 46 65 6e 67  erence.c om%2Feng
```

Hypertext Transfer Protocol (http), 1029 bytes | Packets: 3551 · Displayed: 67 (1.9%) · Dropped: 0 (0.0%) | Profile: Default

- Communicating peers

Analyzing IP

The screenshot shows a Wireshark capture of network traffic on an Ethernet interface. The main pane displays a list of captured packets, with packet 978 selected. The packet list pane shows the following details:

No.	Time	Source	Destination	Protocol	Length	Info
896	20.617525	178.63.108.194	192.168.9.5	HTTP	170	HTTP/1.1 200 OK (PNG)
915	20.658165	178.63.108.194	192.168.9.5	HTTP	746	HTTP/1.1 200 OK (application/javascript)
938	20.710603	192.168.9.5	194.177.211.138	HTTP	77	GET /cygnus?s=311572&v=7.2&r=%7B%22id%22%3A%229d09d6ce83e246%
953	20.754277	192.168.9.5	185.33.223.204	HTTP	230	POST /ut/v3/prebid HTTP/1.1 (text/plain)
978	20.825312	192.168.9.5	173.241.240.220	HTTP	1083	GET /w/1.0/arj?ju=http%3A%2F%2Fwww.wordreference.com%2Fengr%2
988	20.884604	185.33.223.204	192.168.9.5	HTTP	1495	HTTP/1.1 200 OK (application/json)
994	20.900294	194.177.211.138	192.168.9.5	HTTP	1167	HTTP/1.1 200 OK (application/json)
1011	21.016728	173.241.240.220	192.168.9.5	HTTP	184	HTTP/1.1 200 OK (application/json)

The packet details pane for packet 978 shows the following structure:

- Frame 978: 1083 bytes on wire (8664 bits), 1083 bytes captured (8664 bits) on interface 0
- Ethernet II, Src: Giga-Byt_48:19:9f (fc:aa:14:48:19:9f), Dst: Fortinet_09:00:25 (00:09:0f:09:00:25)
- Internet Protocol Version 4, Src: 192.168.9.5, Dst: 173.241.240.220
 - Version: 4
 - Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 1069
 - Identification: 0x187f (6271)
 - Flags: 0x4000, Don't fragment
 - Time to live: 128
 - Protocol: TCP (6)
 - Header checksum: 0x75d0 [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 192.168.9.5
 - Destination: 173.241.240.220
- Transmission Control Protocol, Src Port: 54334, Dst Port: 80, Seq: 1, Ack: 1, Len: 1029

The packet bytes pane shows the raw data of the HTTP request:

```

0030  01 00 54 ef 00 00 47 45 54 20 2f 77 2f 31 2e 30  ..T...GE T /w/1.0
0040  2f 61 72 6a 3f 6a 75 3d 68 74 74 70 25 33 41 25  /arj?ju= http%3A%
0050  32 46 25 32 46 77 77 77 2e 77 6f 72 64 72 65 66  2F%2Fwww .wordref
0060  65 72 65 6e 63 65 2e 63 6f 6d 25 32 46 65 6e 67  erence.c om%2Feng
0070  72 25 32 46 6c 6f 6f 6b 25 32 35 32 30 66 6f 72  r%2Flook %2520for
  
```

The status bar at the bottom indicates: Hypertext Transfer Protocol (http), 1029 bytes | Packets: 3551 · Displayed: 67 (1.9%) · Dropped: 0 (0.0%) | Profile: Default

Analyzing Transportation Level

- TCP, well-known port for HTTP?

The screenshot shows a Wireshark capture of network traffic on an Ethernet interface. The packet list pane displays several HTTP packets. Packet 978 is selected, showing a GET request to `/w/1.0/arj?ju=http%3A%2F%2Fwww.wordreference.com%2Fengr%2Flook%2520for`. The packet details pane for this packet shows the following information:

- Frame 978: 1083 bytes on wire (8664 bits), 1083 bytes captured (8664 bits) on interface 0
- Ethernet II, Src: Giga-Byt_48:19:9f (fc:aa:14:48:19:9f), Dst: Fortinet_09:00:25 (00:09:0f:09:00:25)
- Internet Protocol Version 4, Src: 192.168.9.5, Dst: 173.241.240.220
- Transmission Control Protocol, Src Port: 54334, **Dst Port: 80**, Seq: 1, Ack: 1, Len: 1029
 - Source Port: 54334
 - Destination Port: 80
 - [Stream index: 32]
 - [TCP Segment Len: 1029]
 - Sequence number: 1 (relative sequence number)
 - [Next sequence number: 1030 (relative sequence number)]
 - Acknowledgment number: 1 (relative ack number)
 - 0101 = Header Length: 20 bytes (5)
 - Flags: 0x018 (PSH, ACK)
 - Window size value: 256
 - [Calculated window size: 65536]
 - [Window size scaling factor: 256]

The packet bytes pane shows the raw data of the TCP segment, starting with `0030 01 00 54 ef 00 00 47 45 54 20 2f 77 2f 31 2e 30`.

Analyzing HTTP GET message

The image shows a Wireshark packet capture window titled '*Ethernet'. The main pane displays a list of captured packets. Packet 978 is selected, showing an HTTP GET request. The details pane below shows the structure of the request, including the Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Referer, Content-Type, Origin, Connection, and Cookie headers. The Cookie header is highlighted in green.

No.	Time	Source	Destination	Protocol	Length	Info
953	20.754277	192.168.9.5	185.33.223.204	HTTP	230	POST /ut/v3/prebid HTTP/1.1 (text/plain)
978	20.825312	192.168.9.5	173.241.240.220	HTTP	1083	GET /w/1.0/arj?ju=http%3A%2F%2Fwww.wordreference.com%2Fengr%2
988	20.884604	185.33.223.204	192.168.9.5	HTTP	1495	HTTP/1.1 200 OK (application/json)
994	20.900294	194.177.211.138	192.168.9.5	HTTP	1167	HTTP/1.1 200 OK (application/json)
1011	21.016728	173.241.240.220	192.168.9.5	HTTP	184	HTTP/1.1 200 OK (application/json)
1017	21.030100	192.168.9.5	216.58.198.2	HTTP	367	GET /tag/is/gpt.is HTTP/1.1

> Frame 978: 1083 bytes on wire (8664 bits), 1083 bytes captured (8664 bits) on interface 0
> Ethernet II, Src: Giga-Byt_48:19:9f (fc:aa:14:48:19:9f), Dst: Fortinet_09:00:25 (00:09:0f:09:00:25)
> Internet Protocol Version 4, Src: 192.168.9.5, Dst: 173.241.240.220
> Transmission Control Protocol, Src Port: 54334, Dst Port: 80, Seq: 1, Ack: 1, Len: 1029
> Hypertext Transfer Protocol
 > [truncated]GET /w/1.0/arj?ju=http%3A%2F%2Fwww.wordreference.com%2Fengr%2Flook%2520for&jr=http%3A%2F%2Fwww.wordreference.com%2...
 Host: wordreference-d.openx.net\r\n
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0\r\n
 Accept: */*\r\n
 Accept-Language: en-US,en;q=0.5\r\n
 Accept-Encoding: gzip, deflate\r\n
 Referer: http://www.wordreference.com/engr/look%20for\r\n
 Content-Type: text/plain\r\n
 Origin: http://www.wordreference.com\r\n
 Connection: keep-alive\r\n
 Cookie: i=bbc7b46b-1d73-4c88-2250-44f0bed7a473|1441350232; p_synced=j0.pp.ph.oX.px.pw.oL.jQ.oT.ma.im.ie.mS.pF.ns.t9.ku.qH.sj; ...
 \r\n
 [Full request URI [truncated]: http://wordreference-d.openx.net/w/1.0/arj?ju=http%3A%2F%2Fwww.wordreference.com%2Fengr%2Flook%...
 [HTTP request 1/1]
 Response in frame: 1011

Analyzing HTTP response message

The screenshot displays the Wireshark interface with a packet capture of an HTTP response. The packet list pane shows several packets, with packet 1011 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol.


No.	Time	Source	Destination	Protocol	Length	Info
953	20.754277	192.168.9.5	185.33.223.204	HTTP	230	POST /ut/v3/prebid HTTP/1.1 (text/plain)
978	20.825312	192.168.9.5	173.241.240.220	HTTP	1083	GET /w/1.0/arj?ju=http%3A%2F%2Fwww.wordreference.com%2Fengr%2
988	20.884604	185.33.223.204	192.168.9.5	HTTP	1495	HTTP/1.1 200 OK (application/json)
994	20.900294	194.177.211.138	192.168.9.5	HTTP	1167	HTTP/1.1 200 OK (application/json)
1011	21.016728	173.241.240.220	192.168.9.5	HTTP	184	HTTP/1.1 200 OK (application/json)
1017	21.030100	192.168.9.5	216.58.198.2	HTTP	367	GET /tao/is/ent is HTTP/1.1

Frame 1011: 184 bytes on wire (1472 bits), 184 bytes captured (1472 bits) on interface 0
 Ethernet II, Src: Fortinet_09:00:25 (00:09:0f:09:00:25), Dst: Giga-Byt_48:19:9f (fc:aa:14:48:19:9f)
 Internet Protocol Version 4, Src: 173.241.240.220, Dst: 192.168.9.5
 Transmission Control Protocol, Src Port: 80, Dst Port: 54334, Seq: 4381, Ack: 1030, Len: 130
 [4 Reassembled TCP Segments (4510 bytes): #1007(1460), #1009(1460), #1010(1460), #1011(130)]
 Hypertext Transfer Protocol
 HTTP/1.1 200 OK\r\n
 Vary: Accept\r\n
 Set-Cookie: p_synced=j0.pp.ph.oX.px.pw.oL.jQ.oT.ma.im.ie.mS.pF.ns.t9.ku.qH.sj; Version=1; Expires=Wed, 21-Nov-2018 14:50:21 GM
 Set-Cookie: i=bbc7b46b-1d73-4c88-2250-44f0bed7a473|1441350232; Version=1; Expires=Wed, 06-Nov-2019 14:50:21 GMT; Max-Age=31536
 Server: OXGW/16.103.1\r\n
 Pragma: no-cache\r\n
 P3P: CP="CUR ADM OUR NOR STA NID"\r\n
 Expires: Mon, 26 Jul 1997 05:00:00 GMT\r\n
 Date: Tue, 06 Nov 2018 14:50:21 GMT\r\n
 Content-Type: application/json\r\n
 Cache-Control: private, max-age=0, no-cache\r\n
 Access-Control-Allow-Origin: http://www.wordreference.com\r\n
 Access-Control-Allow-Credentials: true\r\n
 Transfer-Encoding: chunked\r\n
 Content-Encoding: gzip\r\n
 \r\n
 [HTTP response 1/1]
 [Time since request: 0.191416000 seconds]
 [Request in frame: 978]

Wireshark

FTP (File Transfer Protocol) Demo

Try it out!

- Ξεκινήστε το Wireshark
- Επιλέξτε το interface για ανίχνευση
- Ξεκινήστε την ανίχνευση 
- Ανοίξτε ένα command-line παράθυρο

FTP command-line

- ftp [ftp.hellug.gr](ftp://ftp.hellug.gr) (user: anonymous, pass: email address)

```
Command Prompt - ftp ftp.hellug.gr
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

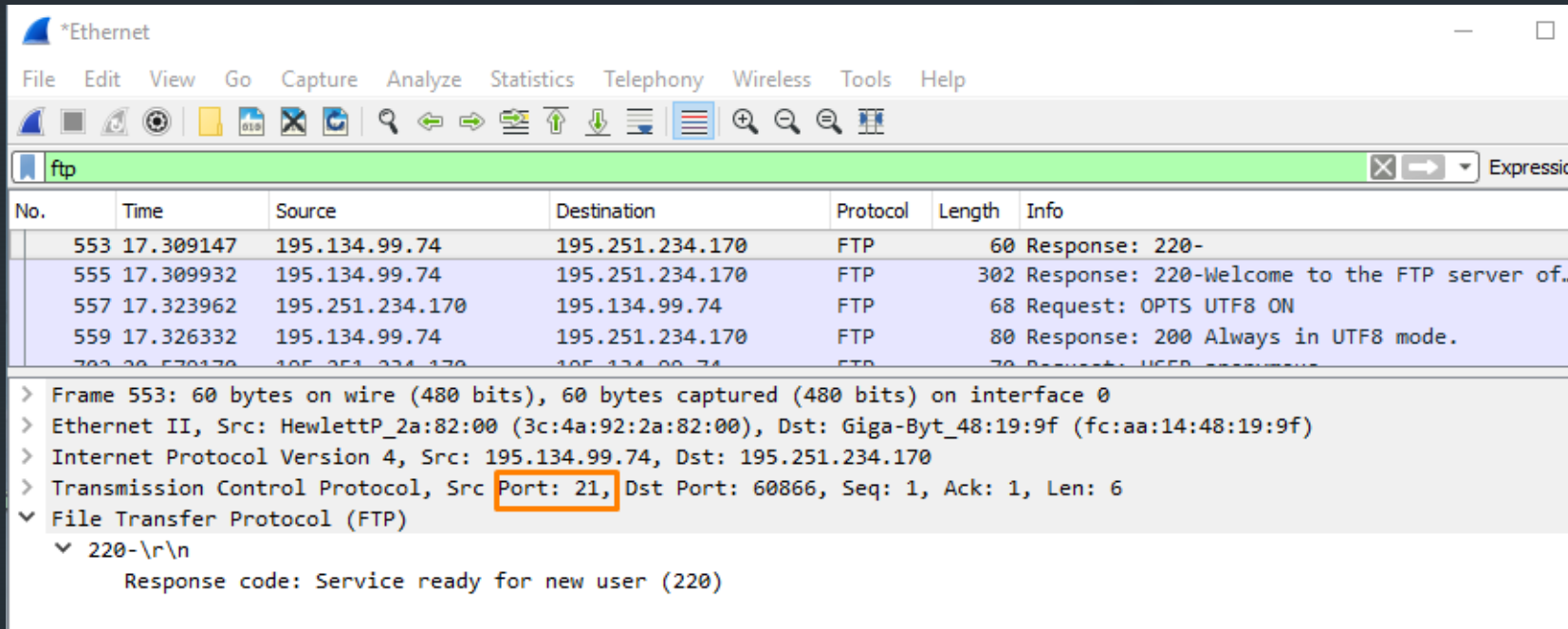
C:\Users\anna>ftp ftp.hellug.gr
Connected to tux-cave.hellug.gr.
220-
220-Welcome to the FTP server of HEL.L.U.G. (http://www.hellug.gr)
220-
220-Contact ftpadmin[*] for problems and/or suggestions.
220-
220-
220-[*] contact address is at hellug dot gr domain,
220-   username as you see it above
220-
220
200 Always in UTF8 mode.
User (tux-cave.hellug.gr:(none)): anonymous
331 Please specify the password.
Password:
230 Login successful.
ftp>
```

FTP | Get a file

- cd pub/gnutls (change directory)
- get README (file)
- stop capturing

```
ftp>  
ftp> cd pub/gnutls  
250-More information on GnuTLS can be found at http://www.gnutls.org/  
250-  
250 Directory successfully changed.  
ftp> get README  
200 PORT command successful. Consider using PASV.  
150 Opening BINARY mode data connection for README (67 bytes).  
226 Transfer complete.  
ftp: 67 bytes received in 0.00Seconds 67000.00Kbytes/sec.  
ftp>
```


Filter: ftp



The image shows a Wireshark capture window titled '*Ethernet'. The filter bar at the top contains the text 'ftp'. Below the filter bar is a table of captured packets. The table has columns for No., Time, Source, Destination, Protocol, Length, and Info. The first four rows are highlighted in blue. The first row (No. 553) shows an FTP response with code 220. The second row (No. 555) shows an FTP response with code 220 and a welcome message. The third row (No. 557) shows an FTP request for UTF8 mode. The fourth row (No. 559) shows an FTP response with code 200 and a confirmation message. Below the table, the details pane for the selected packet (No. 553) is expanded, showing the following information:

- > Frame 553: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
- > Ethernet II, Src: HewlettP_2a:82:00 (3c:4a:92:2a:82:00), Dst: Giga-Byt_48:19:9f (fc:aa:14:48:19:9f)
- > Internet Protocol Version 4, Src: 195.134.99.74, Dst: 195.251.234.170
- > Transmission Control Protocol, Src Port: 21, Dst Port: 60866, Seq: 1, Ack: 1, Len: 6
- ▼ File Transfer Protocol (FTP)
 - ▼ 220-\r\n
 - Response code: Service ready for new user (220)

TCP port 21
(well known)

FTP login: username

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp Expression.

No.	Time	Source	Destination	Protocol	Length	Info
557	17.323962	195.251.234.170	195.134.99.74	FTP	68	Request: OPTS UTF8 ON
559	17.326332	195.134.99.74	195.251.234.170	FTP	80	Response: 200 Always in UTF8 mode.
702	20.579170	195.251.234.170	195.134.99.74	FTP	70	Request: USER anonymous
703	20.580755	195.134.99.74	195.251.234.170	FTP	88	Response: 331 Please specify the password.
...

> Frame 702: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0

> Ethernet II, Src: Giga-Byt_48:19:9f (fc:aa:14:48:19:9f), Dst: HewlettP_2a:82:00 (3c:4a:92:2a:82:00)

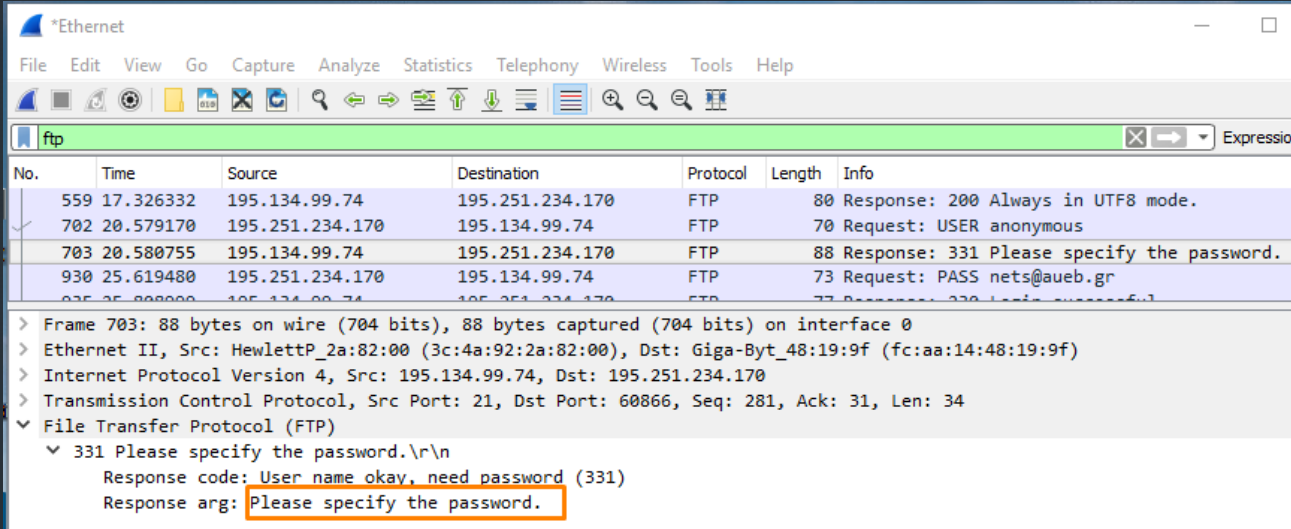
> Internet Protocol Version 4, Src: 195.251.234.170, Dst: 195.134.99.74

> Transmission Control Protocol, Src Port: 60866, Dst Port: 21, Seq: 15, Ack: 281, Len: 16

< File Transfer Protocol (FTP)

- USER anonymous\r\n
 - Request command: USER
 - Request arg: anonymous

FTP login: *password* (clear text)

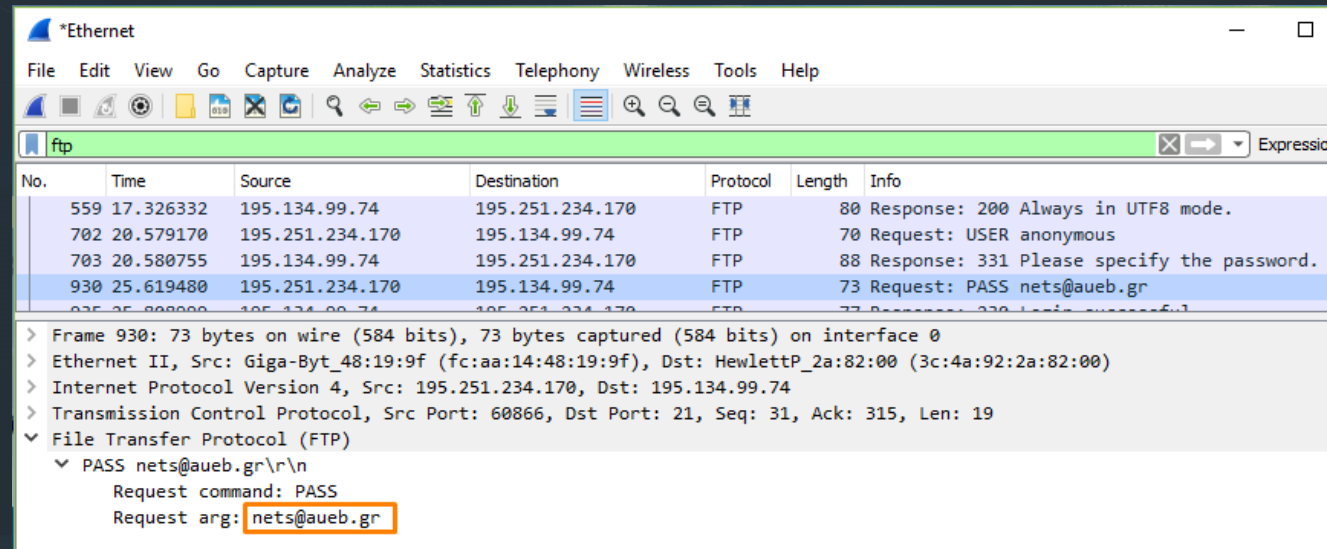


Wireshark capture showing FTP login response. The response code is 331 and the response argument is "Please specify the password." This indicates that the user's password was not accepted and they are prompted to re-enter it.

No.	Time	Source	Destination	Protocol	Length	Info
559	17.326332	195.134.99.74	195.251.234.170	FTP	80	Response: 200 Always in UTF8 mode.
702	20.579170	195.251.234.170	195.134.99.74	FTP	70	Request: USER anonymous
703	20.580755	195.134.99.74	195.251.234.170	FTP	88	Response: 331 Please specify the password.
930	25.619480	195.251.234.170	195.134.99.74	FTP	73	Request: PASS nets@aueb.gr

Frame 703: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0
 Ethernet II, Src: HewlettP_2a:82:00 (3c:4a:92:2a:82:00), Dst: Giga-Byt_48:19:9f (fc:aa:14:48:19:9f)
 Internet Protocol Version 4, Src: 195.134.99.74, Dst: 195.251.234.170
 Transmission Control Protocol, Src Port: 21, Dst Port: 60866, Seq: 281, Ack: 31, Len: 34
 File Transfer Protocol (FTP)
 331 Please specify the password.\r\n
 Response code: User name okay, need password (331)
 Response arg: Please specify the password.

Password is intercepted!!!



Wireshark capture showing FTP login request. The request command is PASS and the request argument is "nets@aueb.gr". This indicates that the user is sending their password in clear text.

No.	Time	Source	Destination	Protocol	Length	Info
559	17.326332	195.134.99.74	195.251.234.170	FTP	80	Response: 200 Always in UTF8 mode.
702	20.579170	195.251.234.170	195.134.99.74	FTP	70	Request: USER anonymous
703	20.580755	195.134.99.74	195.251.234.170	FTP	88	Response: 331 Please specify the password.
930	25.619480	195.251.234.170	195.134.99.74	FTP	73	Request: PASS nets@aueb.gr

Frame 930: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
 Ethernet II, Src: Giga-Byt_48:19:9f (fc:aa:14:48:19:9f), Dst: HewlettP_2a:82:00 (3c:4a:92:2a:82:00)
 Internet Protocol Version 4, Src: 195.251.234.170, Dst: 195.134.99.74
 Transmission Control Protocol, Src Port: 60866, Dst Port: 21, Seq: 31, Ack: 315, Len: 19
 File Transfer Protocol (FTP)
 PASS nets@aueb.gr\r\n
 Request command: PASS
 Request arg: nets@aueb.gr

Retrieve file commands



FTP Protocol

```

v File Transfer Protocol (FTP)
  v 200 PORT command successful. Consider using PASV.\r\n
    Response code: Command okay (200)
    Response arg: PORT command successful. Consider using PASV.
  
```

```

> Internet Protocol Version 4, Src: 195.251.234.170, Dst: 195.134.99.74
> Transmission Control Protocol, Src Port: 60866, Dst Port: 21, Seq: 96, Ack: 503, Len: 13
v File Transfer Protocol (FTP)
  v RETR README\r\n
    Request command: RETR
    Request arg: README
  
```

```

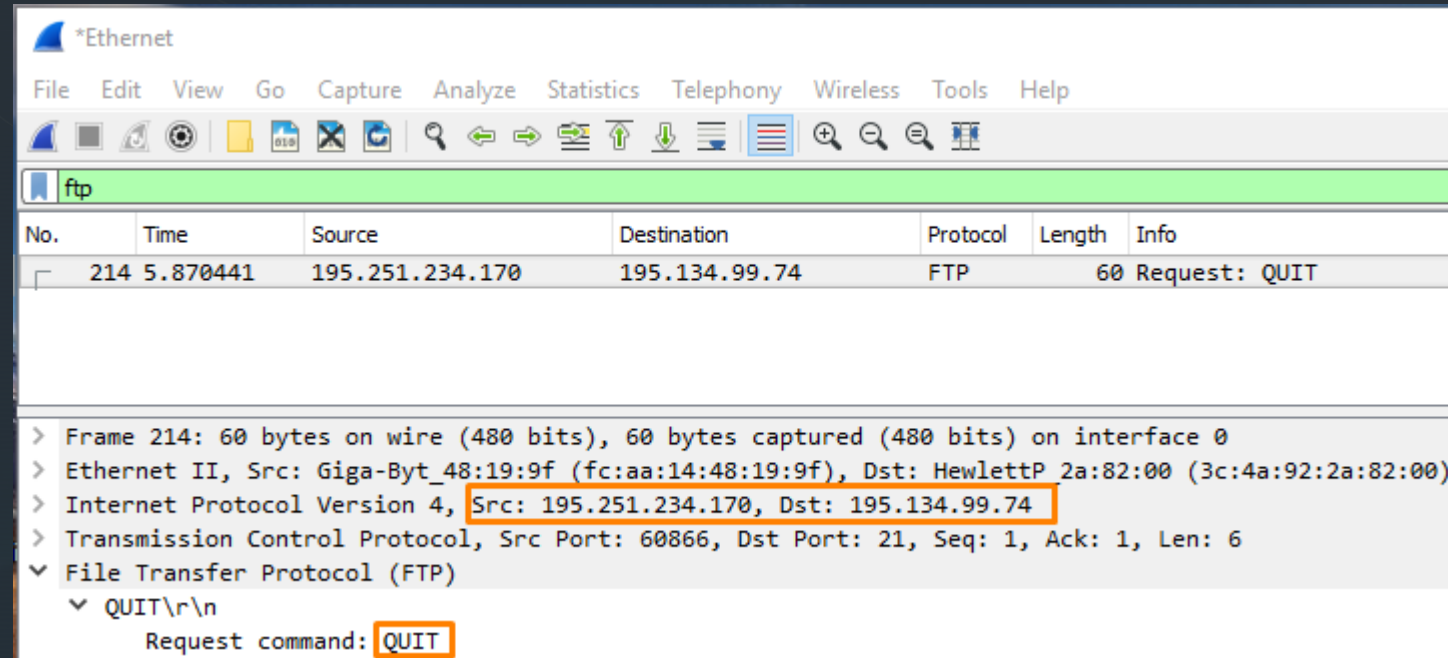
> Internet Protocol Version 4, Src: 195.134.99.74, Dst: 195.251.234.170
> Transmission Control Protocol, Src Port: 21, Dst Port: 60866, Seq: 503, Ack: 109, Len: 64
v File Transfer Protocol (FTP)
  v 150 Opening BINARY mode data connection for README (67 bytes).\r\n
    Response code: File status okay; about to open data connection (150)
    Response arg: Opening BINARY mode data connection for README (67 bytes).
  
```

```

> Internet Protocol Version 4, Src: 195.134.99.74, Dst: 195.251.234.170
> Transmission Control Protocol, Src Port: 21, Dst Port: 60866, Seq: 567, Ack: 109, Len: 24
v File Transfer Protocol (FTP)
  v 226 Transfer complete.\r\n
    Response code: Closing data connection (226)
    Response arg: Transfer complete.
  
```

Quit the session

```
ftp> close
421 timeout.
ftp> bye
```



The image shows a Wireshark packet capture window titled '*Ethernet'. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar with various icons. A packet list pane shows a single entry:

No.	Time	Source	Destination	Protocol	Length	Info
214	5.870441	195.251.234.170	195.134.99.74	FTP	60	Request: QUIT

The packet details pane below shows the following structure:

- > Frame 214: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
- > Ethernet II, Src: Giga-Byt_48:19:9f (fc:aa:14:48:19:9f), Dst: HewlettP 2a:82:00 (3c:4a:92:2a:82:00)
- > Internet Protocol Version 4, Src: 195.251.234.170, Dst: 195.134.99.74
- > Transmission Control Protocol, Src Port: 60866, Dst Port: 21, Seq: 1, Ack: 1, Len: 6
- ▼ File Transfer Protocol (FTP)
 - ▼ QUIT\r\n
 - Request command: QUIT



Το **traceroute** χρησιμοποιεί το πρωτόκολλο **ICMP** (Internet Control Message Protocol) για να ανακαλύψει τη διαδρομή που ακολουθεί ένα IP πακέτο από τον τοπικό host προς ένα απομακρυσμένο host:

στέλνει μικρά πακέτα με αρχικό TTL=1, και το αυξάνει κατά 1 με κάθε αποστολή πακέτου μέχρι να φτάσει στον τελικό προορισμό. Κάθε φορά που λήγει το TTL, ο κόμβος στον οποίο λήγει, στέλνει πίσω ICMP message (type 11 – TTL-exceeded)

→ μαθαίνουμε την ταυτότητα των ενδιάμεσων δρομολογητών

WireShark Traceroute Demo

Try it out!

- Ξεκινήστε το WireShark
- Ανοίξτε ένα παράθυρο με `command prompt`
- Επιλέξτε το interface για ανίχνευση
- Ξεκινήστε την ανίχνευση 
- Στο command prompt παράθυρο δώστε την εντολή:
`tracert www.acm.org` (windows) ή
`traceroute www.acm.org` (linux, Mac OS)
- Σταματήστε την ανίχνευση 

- Επιλέγουμε το πρώτο ICMP Echo Request μήνυμα

The screenshot shows the Wireshark interface with a packet capture of ICMP Echo requests. The first ICMP Echo request is highlighted in yellow. The packet details pane shows the following information:

```

Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: ActiontecEle_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysGroup_da:af:73 (00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 84
  Identification: 0x32d0 (13008)
  000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x2d2c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
  > Internet Control Message Protocol
  
```

▶ ποια είναι η IP διεύθυνση του υπολογιστή σας;

```
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 84
  Identification: 0x32d0 (13008)
  000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
  Protocol: ICMP (1)
  Header Checksum: 0x2d2c [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.102
  Destination Address: 128.59.23.100
```

μέσα στην επικεφαλίδα, ποιο ανώτερο πρωτόκολλο περιέχεται;

```
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 84
  Identification: 0x32d0 (13008)
  000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
  Protocol: ICMP (1)
  Header Checksum: 0x2d2c [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.102
  Destination Address: 128.59.23.100
```


ποιο το μέγεθος (σε bytes) της IP επικεφαλίδας;
ποιο το μέγεθος του IP payload;

```
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 84
  Identification: 0x32d0 (13008)
  000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0... .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
  Protocol: ICMP (1)
  Header Checksum: 0x2d2c [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.102
  Destination Address: 128.59.23.100
```

payload: 64

έχει γίνει fragmentation; πως το καταλαβαίνουμε;

```
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 84
  Identification: 0x32d0 (13008)
  000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
  Protocol: ICMP (1)
  Header Checksum: 0x2d2c [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.102
  Destination Address: 128.59.23.100
```

Παρατηρήστε την αλληλουχία των ICMP πακέτων που έχουν σταλεί από τον υπολογιστή σας

- ποια πεδία του IP datagram αλλάζουν από το ένα datagram στο άλλο;

tracertool με μέγεθος πακέτου 2000 bytes (για να αναγκάσουμε σε fragmentation)

```

132 32.0670... 192.168.1.102 199.2.53.206 TCP 62 1483 → 631 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
133 33.4517... 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3307) [Reassembled in #134]
134 33.4524... 192.168.1.102 128.59.23.100 ICMP 562 Echo (ping) request id=0x0300, seq=33795/900, ttl=1 (no response found!)
135 33.4705... 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
136 33.4778... 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3308) [Reassembled in #137]
137 33.4785... 192.168.1.102 128.59.23.100 ICMP 562 Echo (ping) request id=0x0300, seq=34051/901, ttl=2 (no response found!)
138 33.4976... 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3309) [Reassembled in #139]
139 33.4983... 192.168.1.102 128.59.23.100 ICMP 562 Echo (ping) request id=0x0300, seq=34307/902, ttl=3 (no response found!)
140 33.5280... 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=330a) [Reassembled in #141]
141 33.5290... 192.168.1.102 128.59.23.100 ICMP 562 Echo (ping) request id=0x0300, seq=34563/903, ttl=4 (no response found!)
142 33.5379... 24.218.0.153 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
143 33.5552... 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=330b) [Reassembled in #144]
144 33.5558... 192.168.1.102 128.59.23.100 ICMP 562 Echo (ping) request id=0x0300, seq=34819/904, ttl=5 (no response found!)
145 33.5780... 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=330c) [Reassembled in #146]
146 33.5787... 192.168.1.102 128.59.23.100 ICMP 562 Echo (ping) request id=0x0300, seq=35075/905, ttl=6 (no response found!)

```

```

Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x3307 (13063)
  < 001. .... = Flags: 0x1, More fragments
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..1. .... = More fragments: Set
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x076d [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
    [Reassembled IPv4 in frame: 134]

```

