Δρ. Άννα Κεφάλα

WireShark
(a network protocol analyser)

WireShark

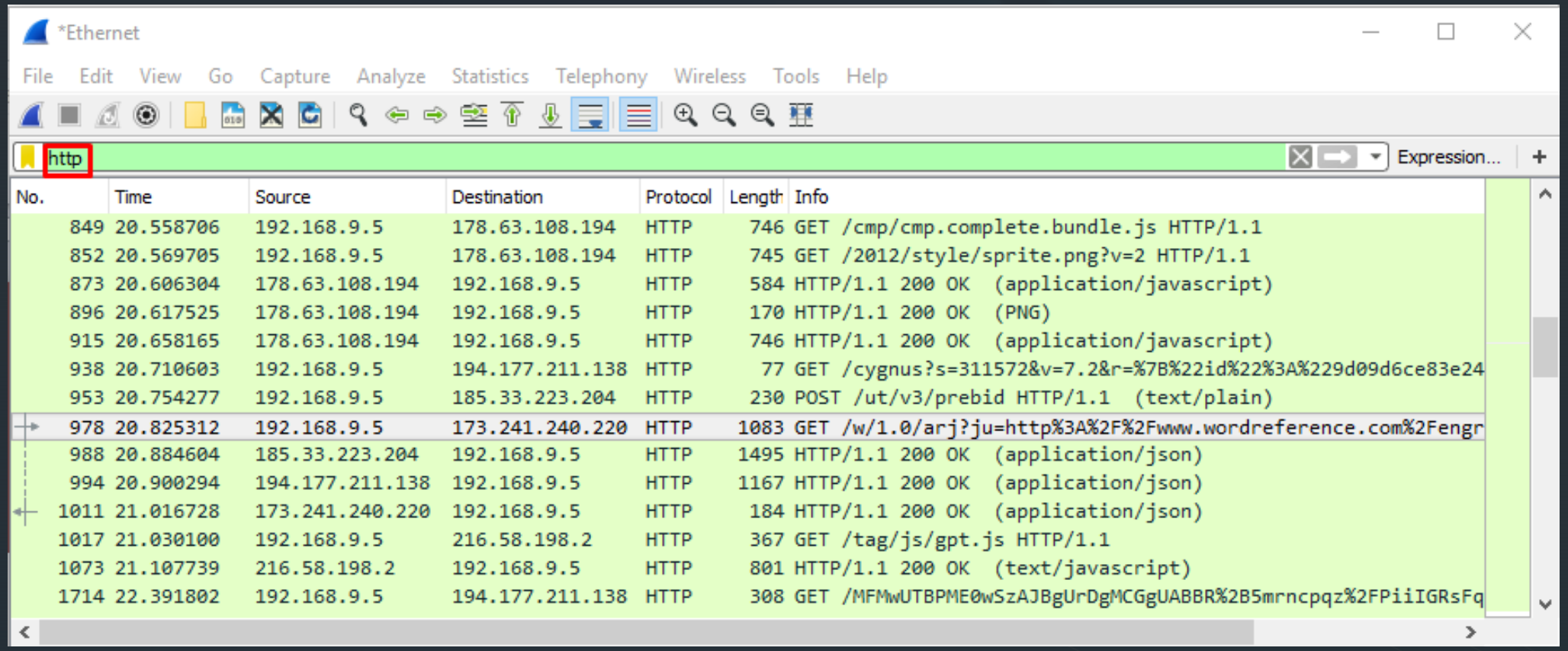
Web Browsing Demo

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…

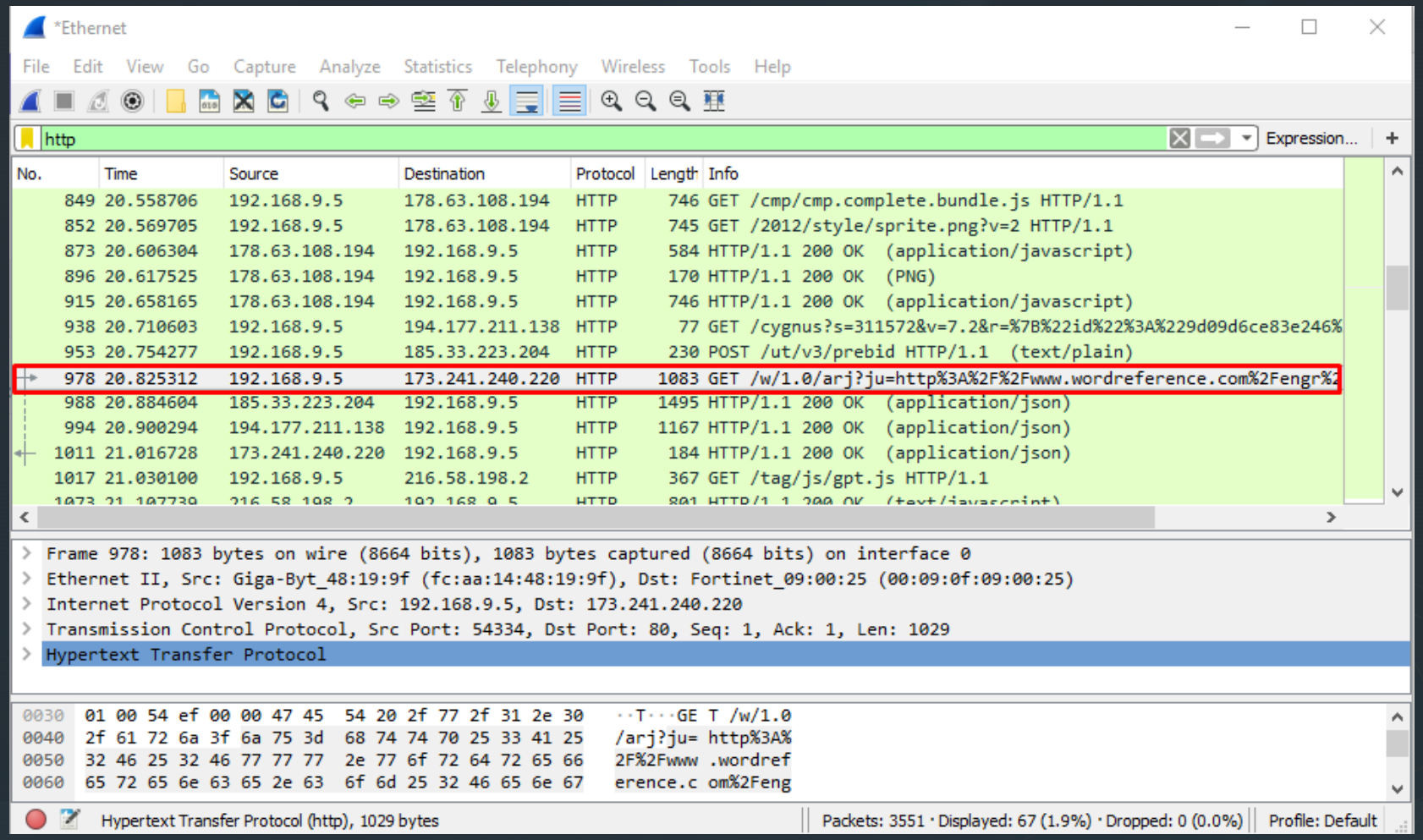
Filtering

Filter HTTP κίνηση



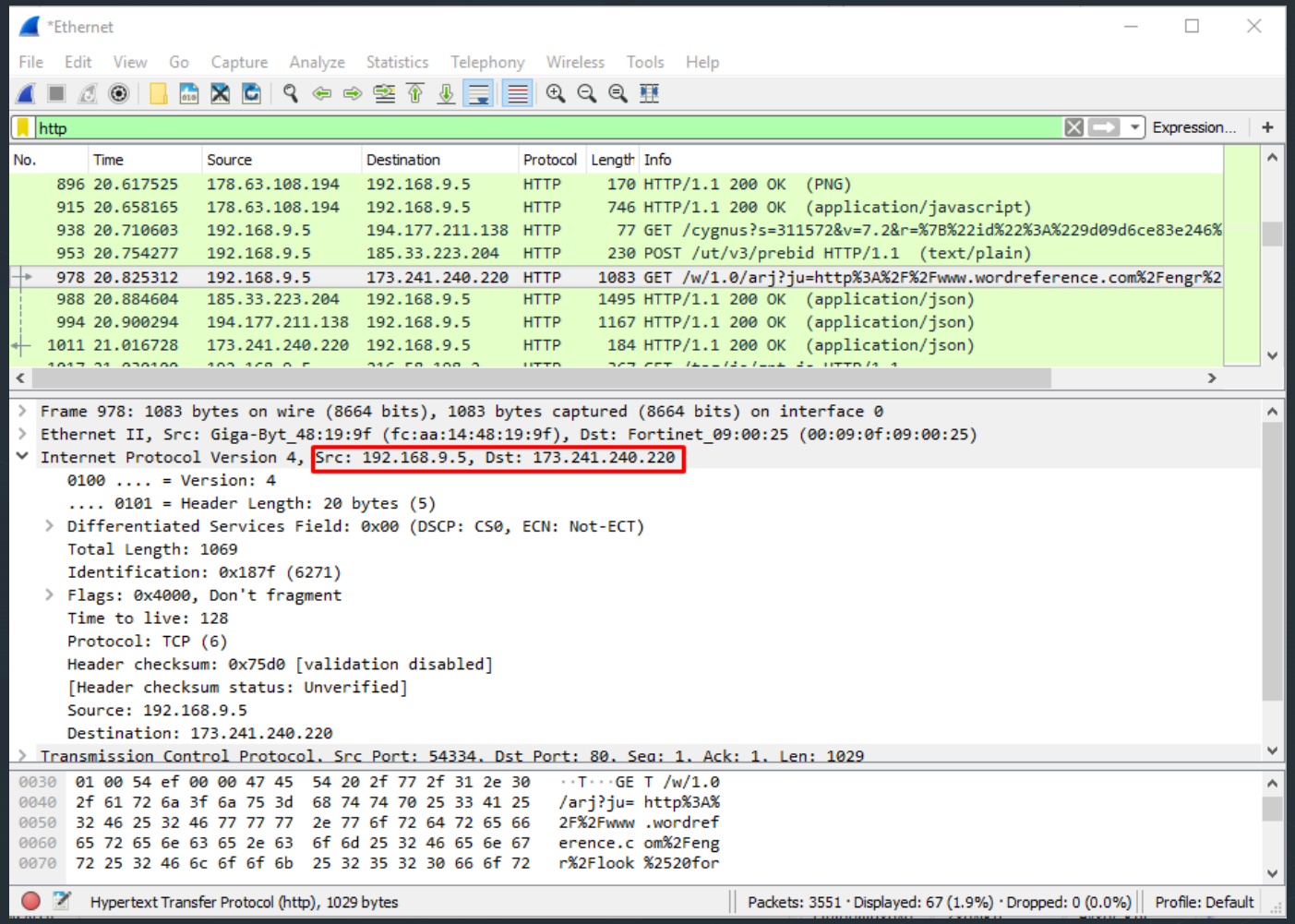
Analyzing

- Επιλέξτε ένα HTTP GET πακέτο



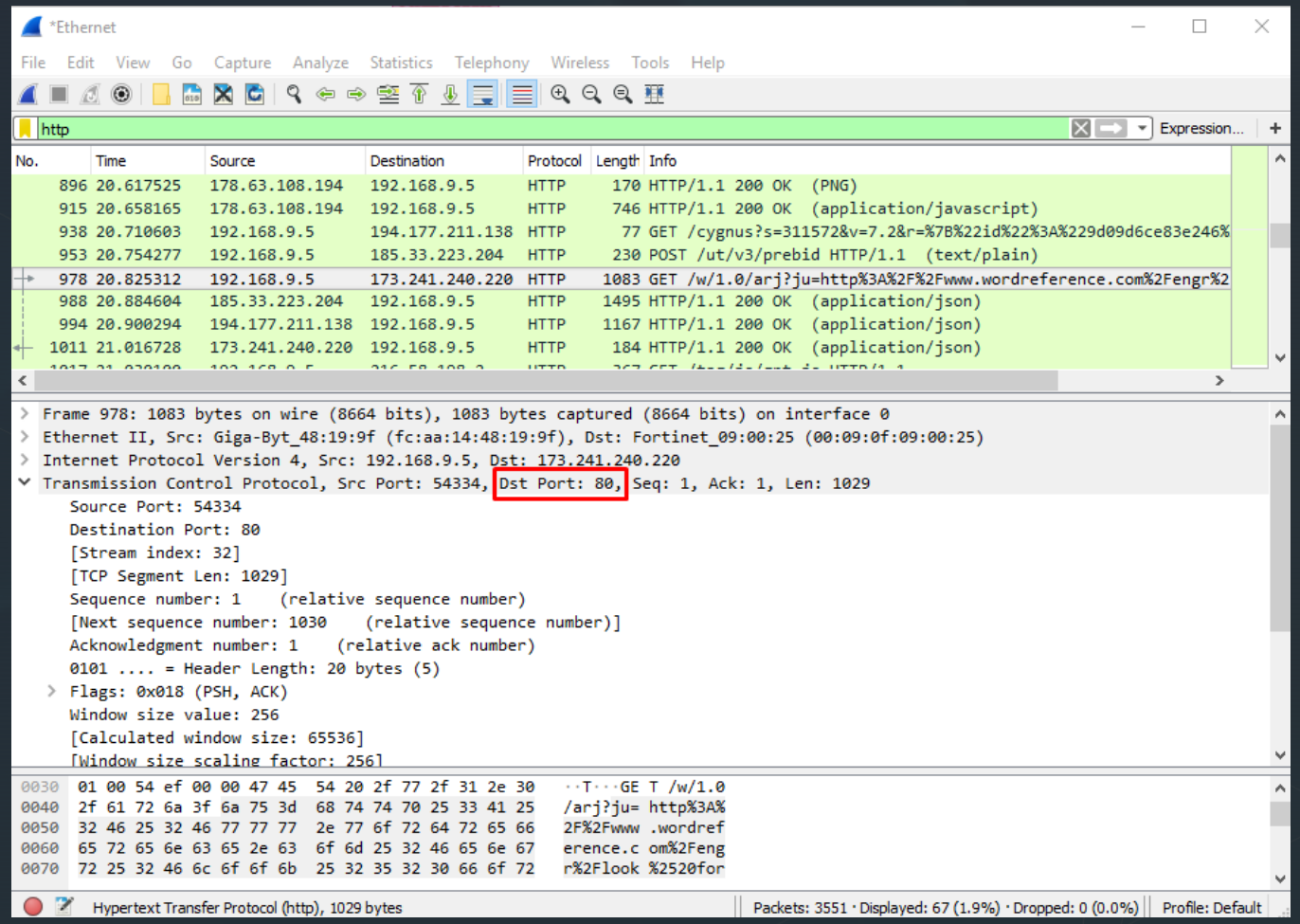
Analyzing IP

- Communicating peers



Analyzing Transportation Level

- TCP, well-known port for HTTP?



Analyzing HTTP GET message

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

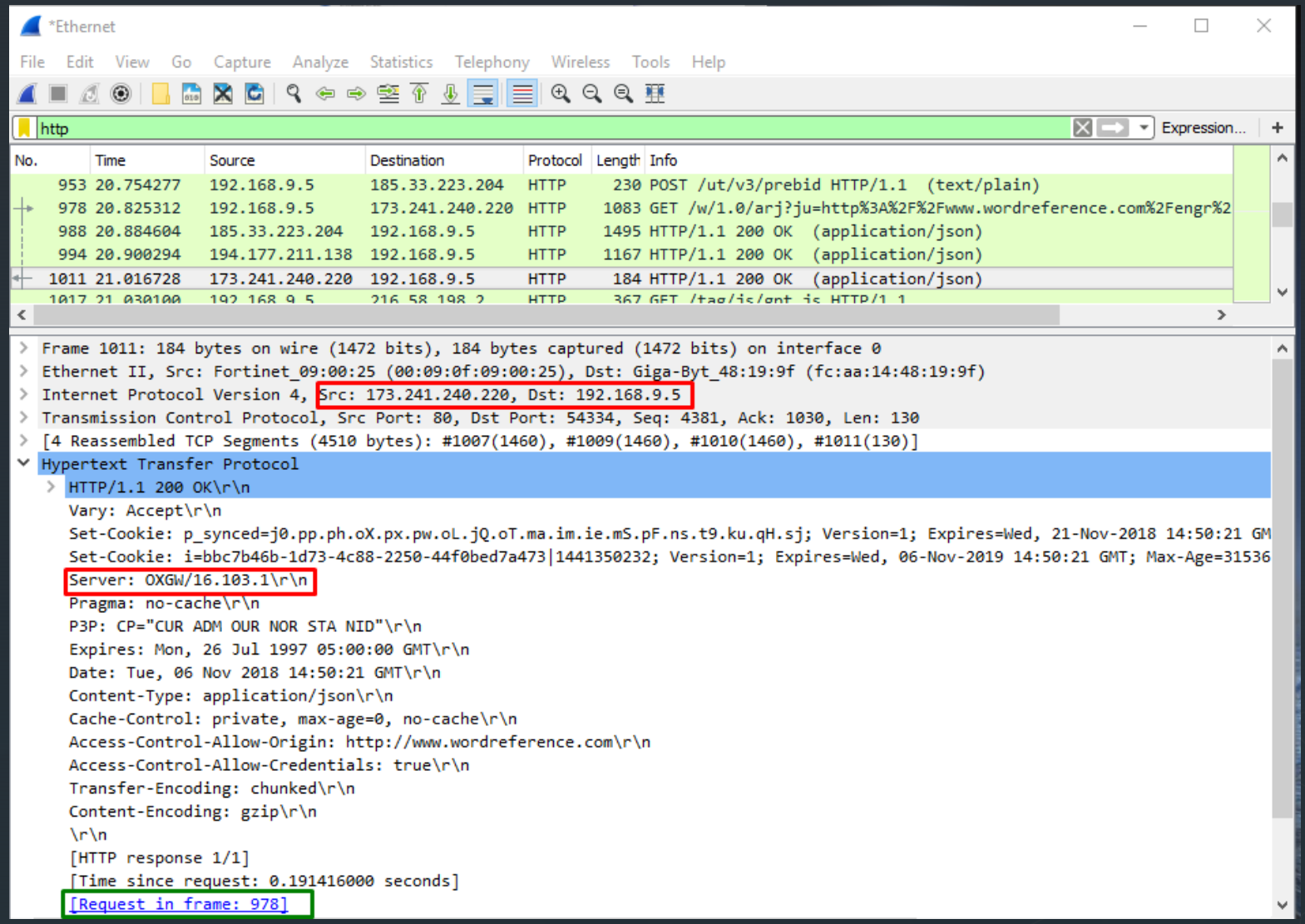
http

Expression...

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/js/gpt.js 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
v 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



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 (user: anonymous, pass: email address)

Command Prompt - ftp ftp.hellug.gr

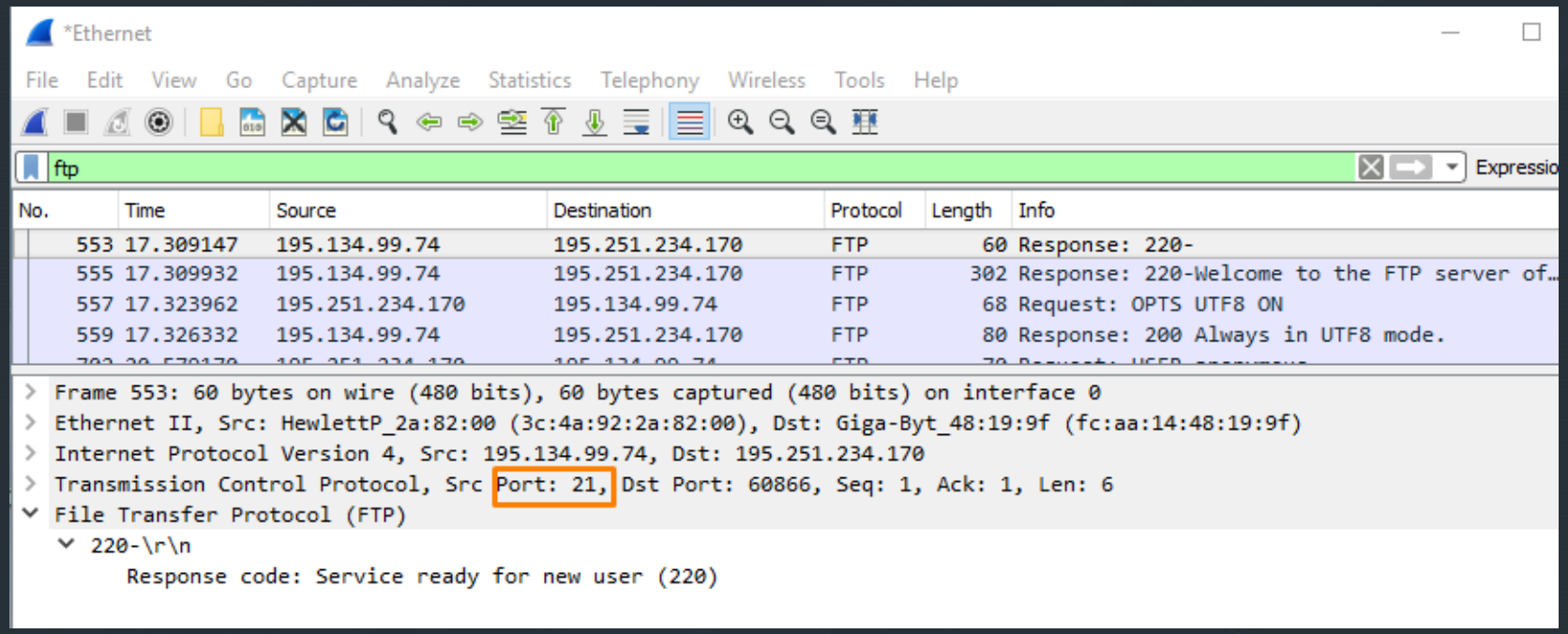
```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

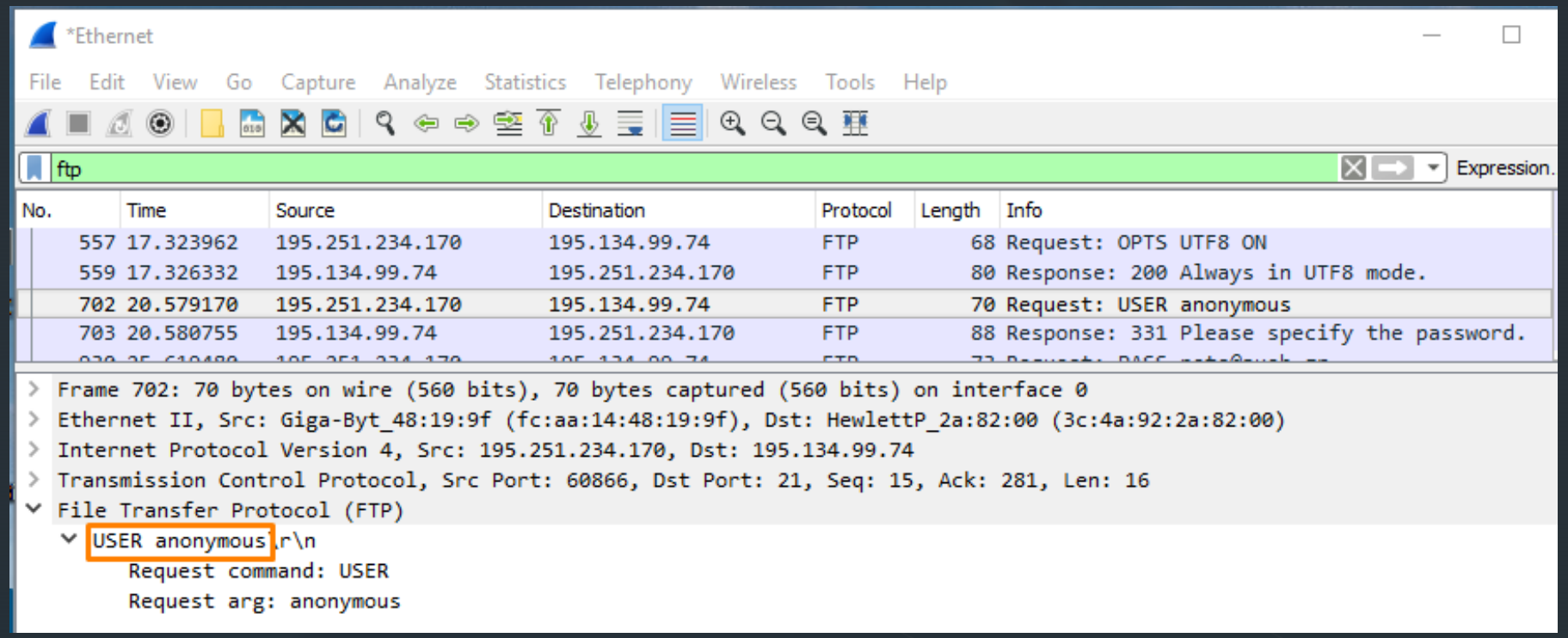
```
ftp>
ftp> cd pub/gnutls
250-More information on GnuTLS can be found at http://www.gnutls.org/
250-
250 Directory successfully changed.
ftp> get README
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for README (67 bytes).
226 Transfer complete.
ftp: 67 bytes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

Filter: ftp

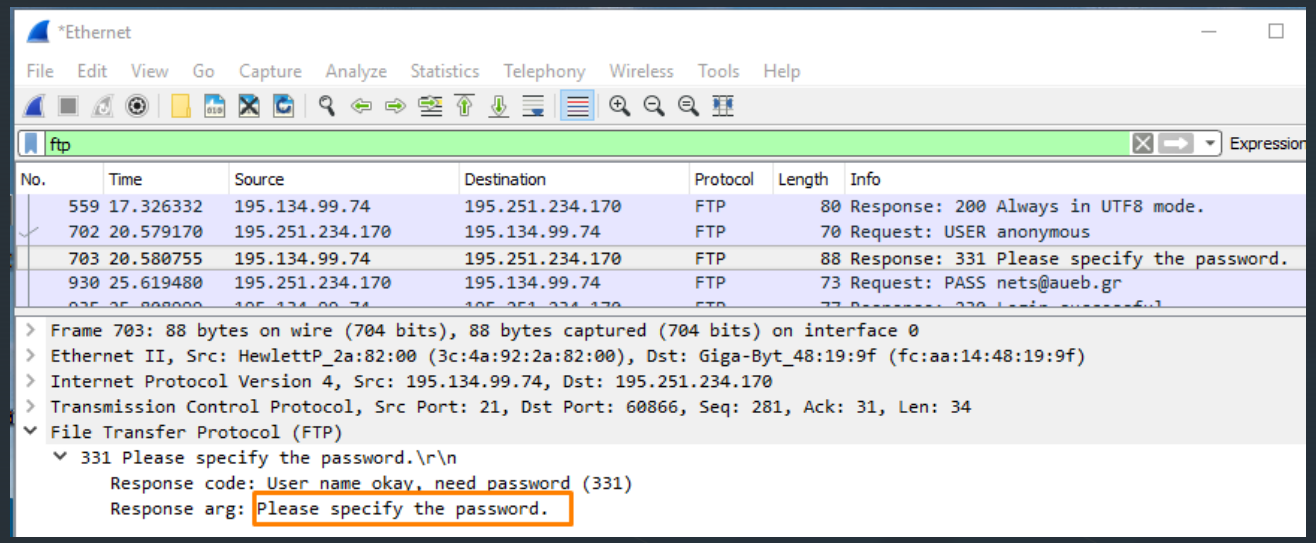


TCP port 21
(well known)

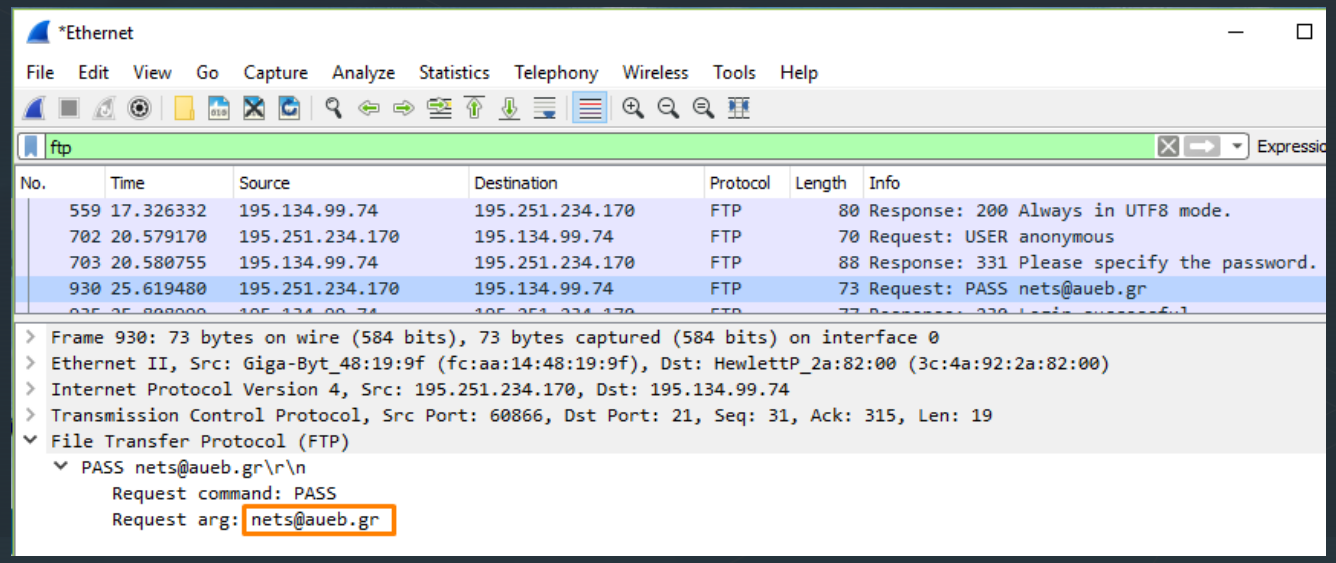
FTP login: *username*



FTP login: *password* (clear text)



Password is intercepted!!!



Retrieve file commands

FTP Protocol

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

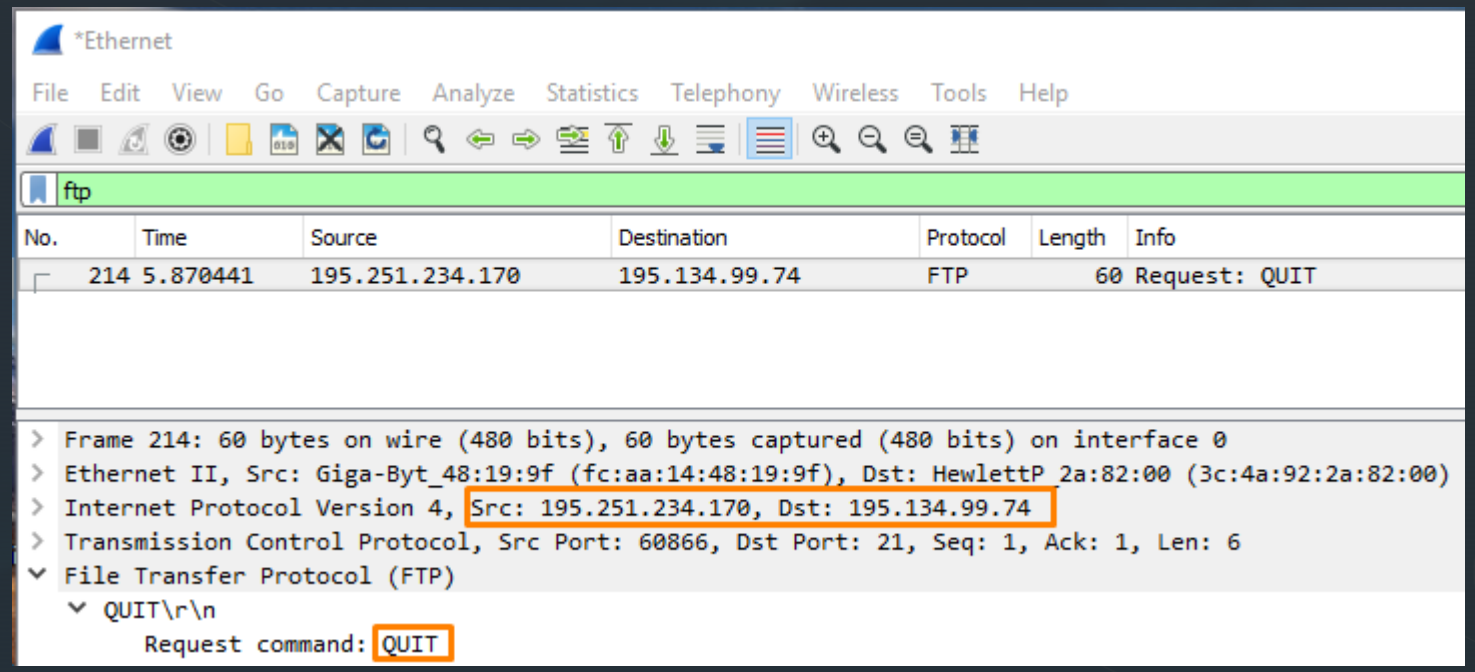
```
Internet Protocol Version 4, Src: 195.251.234.170, Dst: 195.134.99.74
Transmission Control Protocol, Src Port: 60866, Dst Port: 21, Seq: 96, Ack: 503, Len: 13
File Transfer Protocol (FTP)
  RETR README\r\n
      Request command: RETR
      Request arg: README
```

```
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
File Transfer Protocol (FTP)
  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
File Transfer Protocol (FTP)
  226 Transfer complete.\r\n
      Response code: Closing data connection (226)
      Response arg: Transfer complete.
```

Quit the session

```
ftp> close
421 Timeout.
ftp> bye
```



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

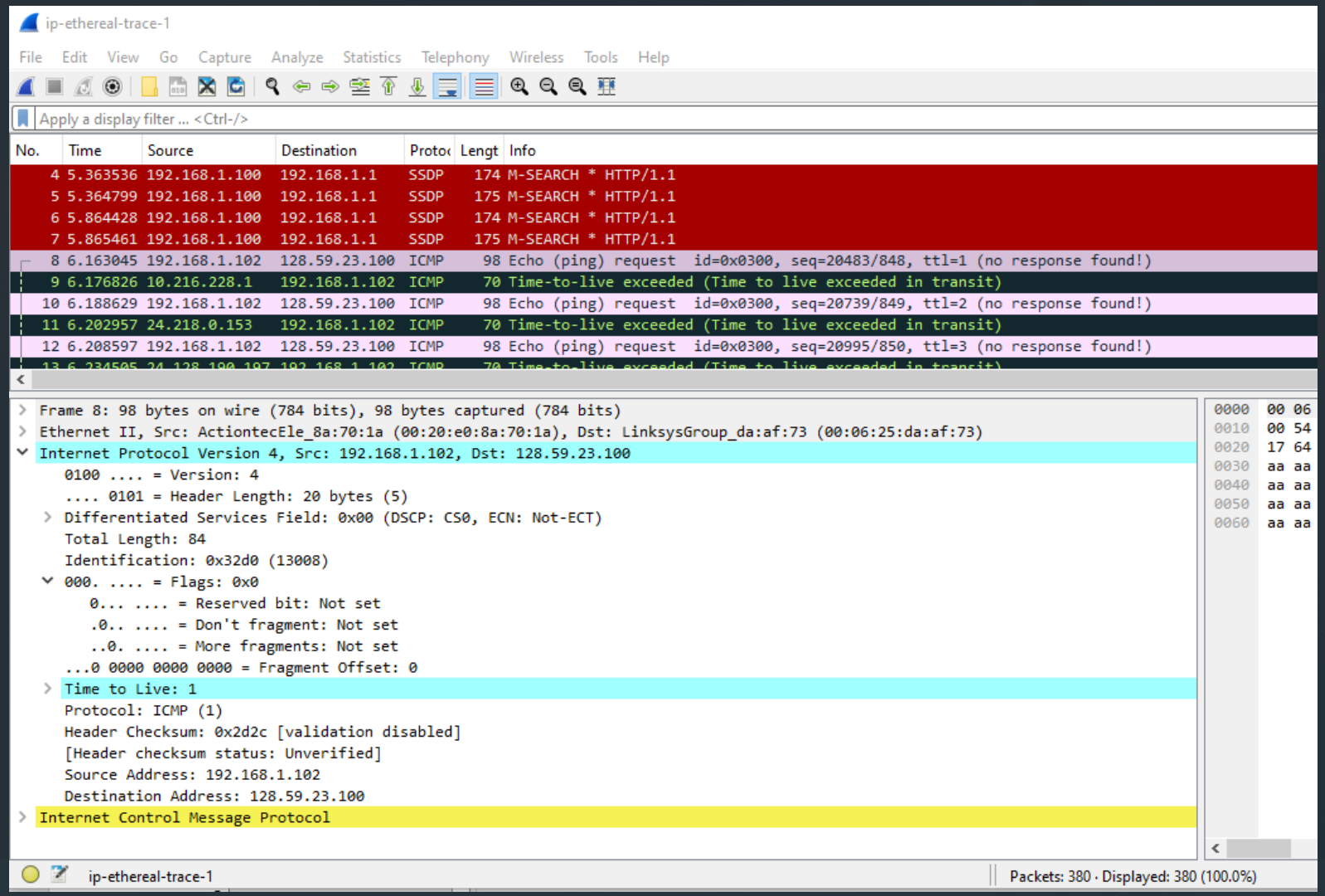
Traceroute Demo

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

IP protocol

- Επιλέγουμε το πρώτο ICMP Echo Request μήνυμα



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)
  v 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)
  v 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)
  v 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)
  v 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
```

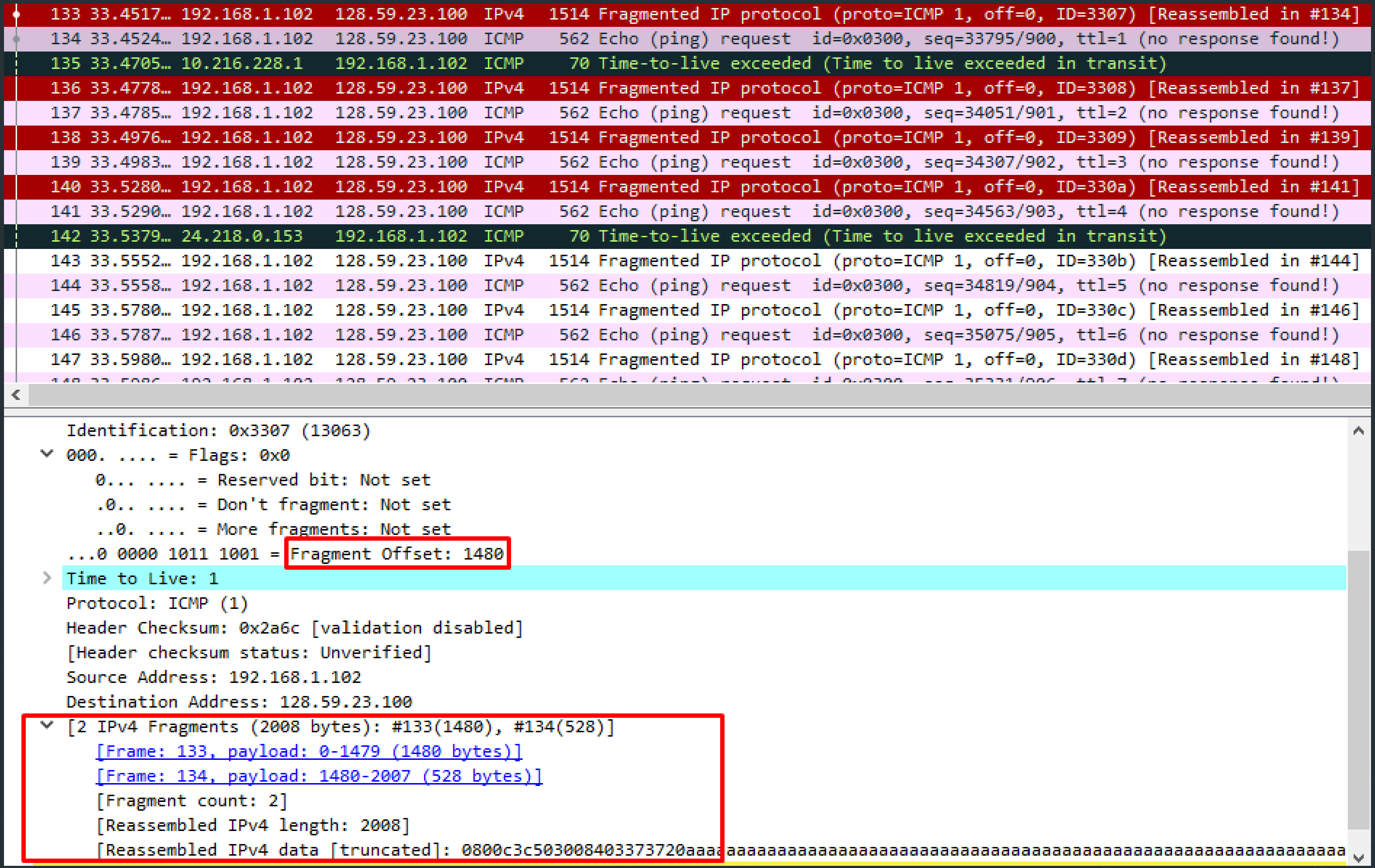
Παρατηρήστε την αλληλουχία των ICMP πακέτων που έχουν σταλεί από τον υπολογιστή σας

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

traceroute 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)
  v 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]
```



```
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!)
147 33.5980… 192.168.1.102  128.59.23.100  IPv4  1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=330d) [Reassembled in #148]
```

```
    Identification: 0x3307 (13063)
  ˅ 000. .... = Flags: 0x0
       0... .... = Reserved bit: Not set
       .0.. .... = Don't fragment: Not set
       ..0. .... = More fragments: Not set
    ...0 0000 1011 1001 = Fragment Offset: 1480
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x2a6c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
  ˅ [2 IPv4 Fragments (2008 bytes): #133(1480), #134(528)]
       [Frame: 133, payload: 0-1479 (1480 bytes)]
       [Frame: 134, payload: 1480-2007 (528 bytes)]
       [Fragment count: 2]
       [Reassembled IPv4 length: 2008]
       [Reassembled IPv4 data [truncated]: 0800c3c503008403373720aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```