



Εργαστήριο Δικτύων Υπολογιστών

Wireshark by example

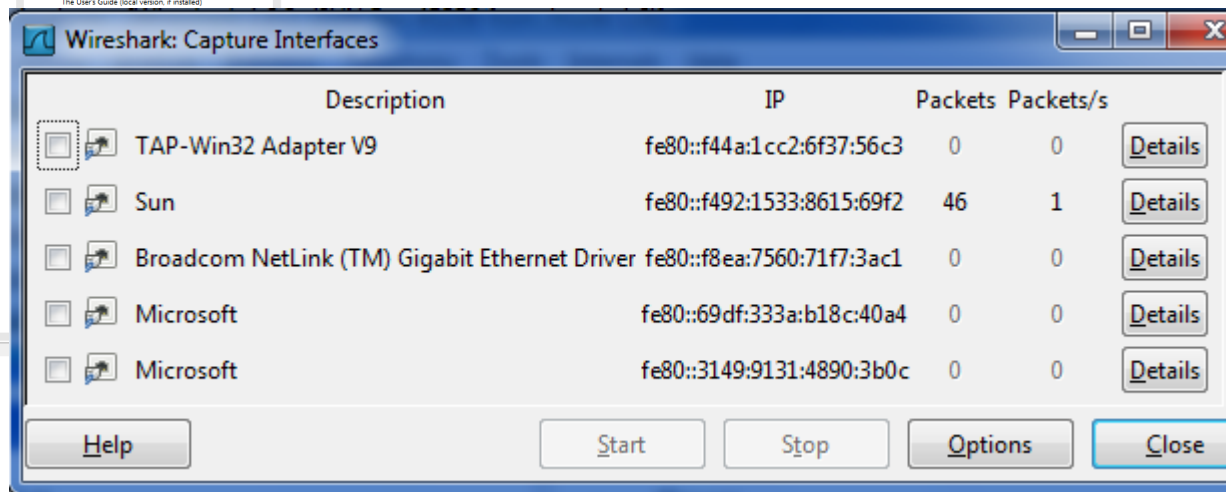
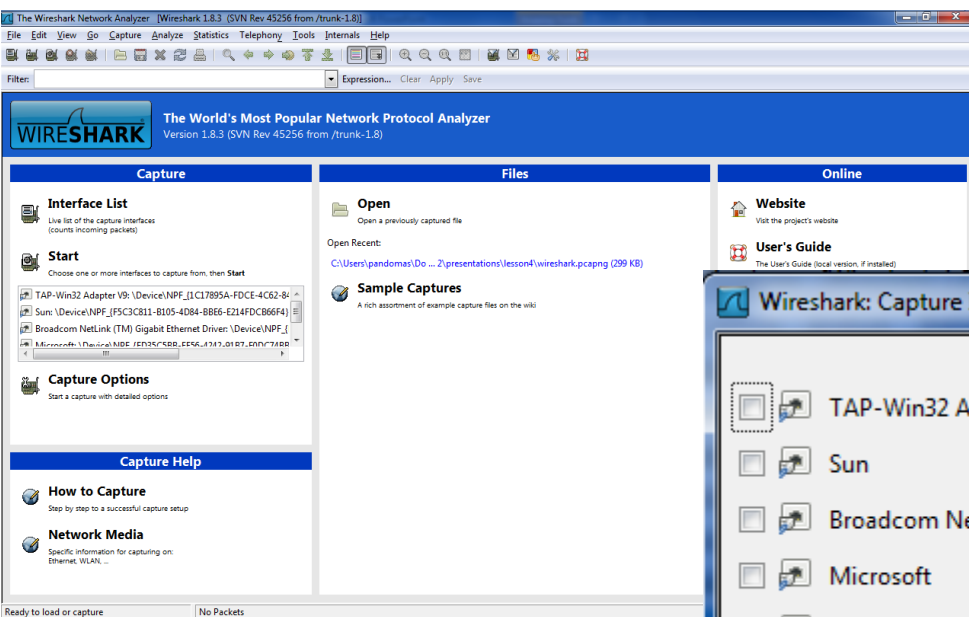
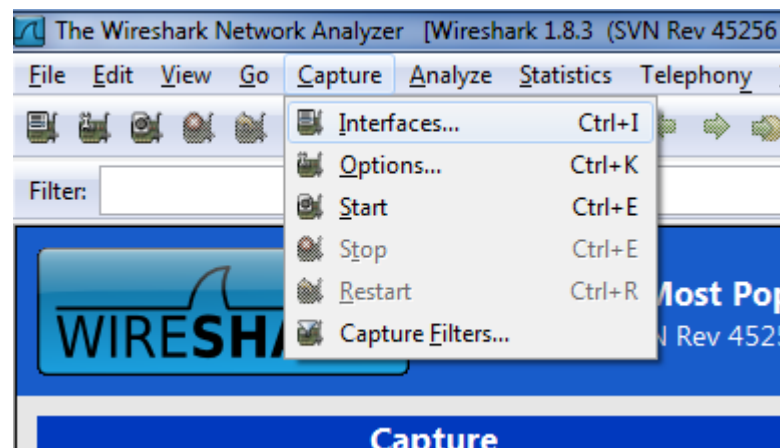
Wireshark

- Packet sniffer
- Network protocol analyzer
- Παλιότερα γνωστό με το όνομα Ethereal



Καταγραφή μίας HTTP συνόδου

- Καθαρισμός cache του φυλλομετρητή
- Άνοιγμα Wireshark
- Επιλογή διεπαφής καταγραφής



Καταγραφή μίας HTTP συνόδου

- Εκκίνηση καταγραφής
- Επίσκεψη στην σελίδα μέσω του φυλλομετρητή
- Κλείσιμο του φυλλομετρητή και διακοπή καταγραφής

Wireshark 1.8.3 [Wireshark 1.8.3 [SVN Rev 45256 from /trunk-1.8]]

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	150.140.158.11	239.255.255.250	SSDP	140	M-SEARCH * HTTP/1.1
2	0.07498200	150.140.139.106	239.255.255.250	SSDP	140	M-SEARCH * HTTP/1.1
3	0.74398800	150.140.139.229	150.140.139.242	TCP	74	46462 > 24800 [SYN] Seq=0 win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=734139206 TSecr=0 W
4	0.24409300	150.140.139.242	150.140.139.229	TCP	54	24800 > 46462 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
5	0.46219300	Cisco_82:a8:18	Spanning-tree-(for-STP	60	conf. root = 24576/243/00:d0:2b:9c:19:00 Cost = 16 Port = 0x8018	
6	0.59573000	150.140.139.238	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
7	1.04634000	150.140.187.40	239.255.255.250	SSDP	140	M-SEARCH * HTTP/1.1
8	1.31109200	150.140.139.229	150.140.139.242	TCP	74	46463 > 24800 [SYN] Seq=0 win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=734139473 TSecr=0 W
9	1.31117600	150.140.139.242	150.140.139.229	TCP	54	24800 > 46463 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
10	1.52646800	150.140.199.50	239.255.255.250	SSDP	393	NOTIFY * HTTP/1.1
11	1.63188100	150.140.199.50	239.255.255.250	SSDP	416	NOTIFY * HTTP/1.1
12	1.66912800	Cisco_82:a8:18	CDP/VTP/DTP/PagP/UD	60	dynamic Trunking Protocol	
13	1.66989000	Cisco_82:a8:18	CDP/VTP/DTP/PagP/UD	90	dynamic Trunking Protocol	
14	1.69401700	Cisco_82:a8:18	CDP/VTP/DTP/PagP/UD	389	device ID: sw0200Ab3 Port ID: FastEthernet0/24	
15	1.74249600	150.140.199.50	239.255.255.250	SSDP	465	NOTIFY * HTTP/1.1
16	1.85356600	150.140.199.50	239.255.255.250	SSDP	483	NOTIFY * HTTP/1.1
17	2.37888300	150.140.139.229	150.140.139.242	TCP	74	46464 > 24800 [SYN] Seq=0 win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=734139740 TSecr=0 W
18	2.37898300	150.140.139.242	150.140.139.229	TCP	54	24800 > 46464 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
19	2.46222400	Cisco_82:a8:18	Spanning-tree-(for-STP	60	conf. root = 24576/243/00:d0:2b:9c:19:00 Cost = 16 Port = 0x8018	
20	3.44112500	Vmware_41:c7:8f	Broadcast	ARP	60	who has 150.140.139.208? Tell 150.140.139.195
21	3.46428400	150.140.139.229	150.140.139.242	TCP	74	46465 > 24800 [SYN] Seq=0 win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=734140011 TSecr=0 W
22	3.46438700	150.140.139.242	150.140.139.229	TCP	54	24800 > 46465 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
23	3.59620100	150.140.139.238	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1

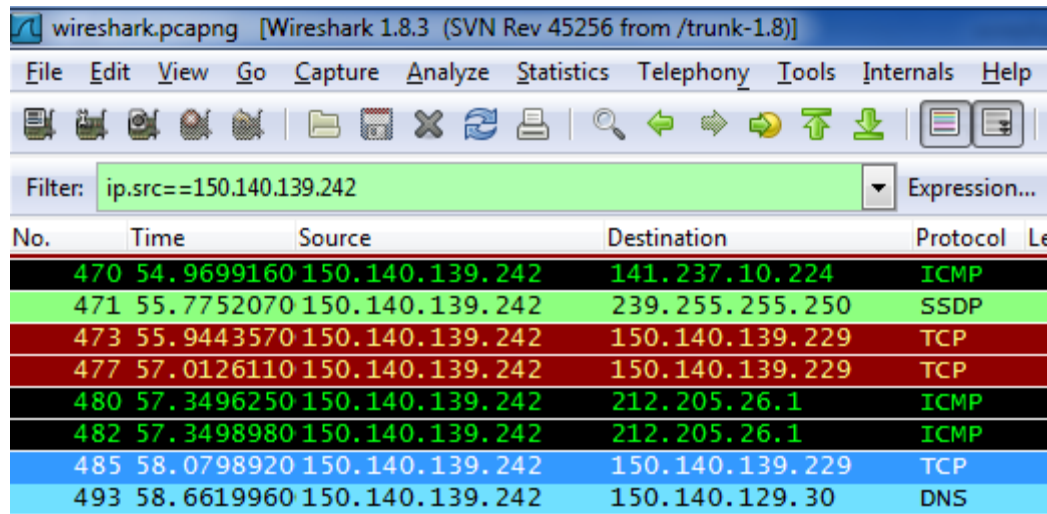
Frame 1: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Cisco_46:89:bf (00:1b:53:46:89:bf), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 150.140.158.11 (150.140.158.11), Dst: 239.255.255.250 (239.255.255.250)
User Datagram Protocol, Src Port: 50833 (50833), Dst Port: ssdp (1900)
Hypertext Transfer Protocol

```
0000 01 00 5e 7f ff fa 00 1b 53 46 89 bf 08 00 45 00 ..^.....SF....E.
0010 00 7e 2c 00 00 fd 11 6a 06 9d ff 9e 0b ef ff .....i...f....
0020 ff fa c6 91 07 6c 00 6a 40 b5 4d 2d 53 45 41 52 .....l...@M-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTTP/1.1..H
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239.255.255
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 53 54 3a 75 70 .250:190 0..STrup
0060 6e 70 3a 72 6f 6f 74 64 65 76 69 63 65 0d 0a 4d np:rootd evic..M
0070 41 4e 3a 22 73 73 64 70 3a 64 69 73 63 6f 76 65 AN:ssdp:discove
0080 72 22 0d 0a 4d 58 3a 33 0d 0a 0d 0a r".MX:3 .....
```

Packets: 788 Displayed: 788 Marked: 0 Load time: 0:00:374 Profile: Default

Ανάλυση Δεδομένων

- Επιλογή φίλτρου: `ip.src==150.140.xxx.xxx`



wireshark.pcapng [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]

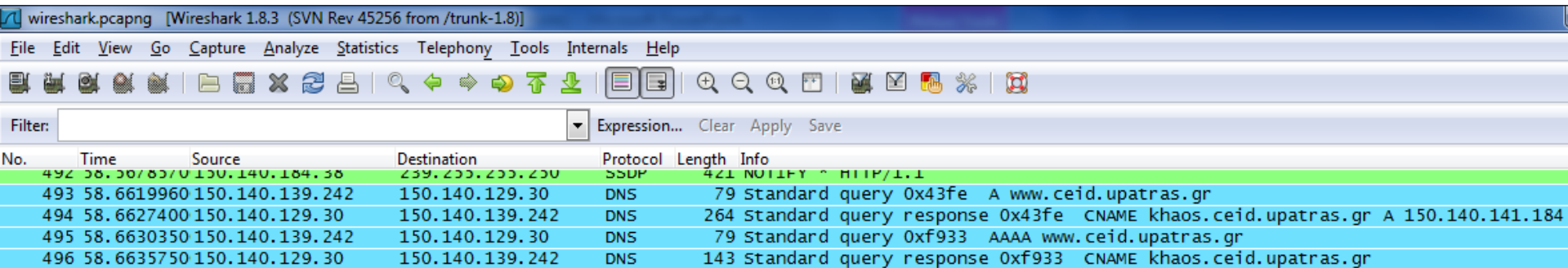
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `ip.src==150.140.139.242` Expression...

No.	Time	Source	Destination	Protocol	Length
470	54.9699160	150.140.139.242	141.237.10.224	ICMP	
471	55.7752070	150.140.139.242	239.255.255.250	SSDP	
473	55.9443570	150.140.139.242	150.140.139.229	TCP	
477	57.0126110	150.140.139.242	150.140.139.229	TCP	
480	57.3496250	150.140.139.242	212.205.26.1	ICMP	
482	57.3498980	150.140.139.242	212.205.26.1	ICMP	
485	58.0798920	150.140.139.242	150.140.139.229	TCP	
493	58.6619960	150.140.139.242	150.140.129.30	DNS	

Ανάλυση Δεδομένων

■ DNS αίτηση



The image shows a Wireshark capture of network traffic. The main pane displays a list of captured packets. Packet 493 is highlighted, showing a DNS standard query from 150.140.139.242 to 150.140.129.30 for the domain www.ceid.upatras.gr. Other packets include SSDP notifications and DNS responses for the same domain.

No.	Time	Source	Destination	Protocol	Length	Info
492	58.6619960	150.140.184.38	239.255.255.250	SSDP	421	NOTIFY - HTTP/1.1
493	58.6619960	150.140.139.242	150.140.129.30	DNS	79	Standard query 0x43fe A www.ceid.upatras.gr
494	58.6627400	150.140.129.30	150.140.139.242	DNS	264	Standard query response 0x43fe CNAME kaos.ceid.upatras.gr A 150.140.141.184
495	58.6630350	150.140.139.242	150.140.129.30	DNS	79	Standard query 0xf933 AAAA www.ceid.upatras.gr
496	58.6635750	150.140.129.30	150.140.139.242	DNS	143	Standard query response 0xf933 CNAME kaos.ceid.upatras.gr

- ⊕ Frame 493: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
- ⊕ Ethernet II, Src: Dell_6e:78:ac (00:21:70:6e:78:ac), Dst: Cisco_46:89:bf (00:1b:53:46:89:bf)
- ⊕ Internet Protocol Version 4, Src: 150.140.139.242 (150.140.139.242), Dst: 150.140.129.30 (150.140.129.30)
- ⊕ User Datagram Protocol, Src Port: 59779 (59779), Dst Port: domain (53)
- ⊕ Domain Name System (query)

Ανάλυση Δεδομένων

- Δημιουργία TCP σύνδεσης

The image shows a screenshot of the Wireshark network traffic analysis tool. The main display area shows a list of captured packets. Three packets are highlighted in green, representing a TCP SYN sequence:

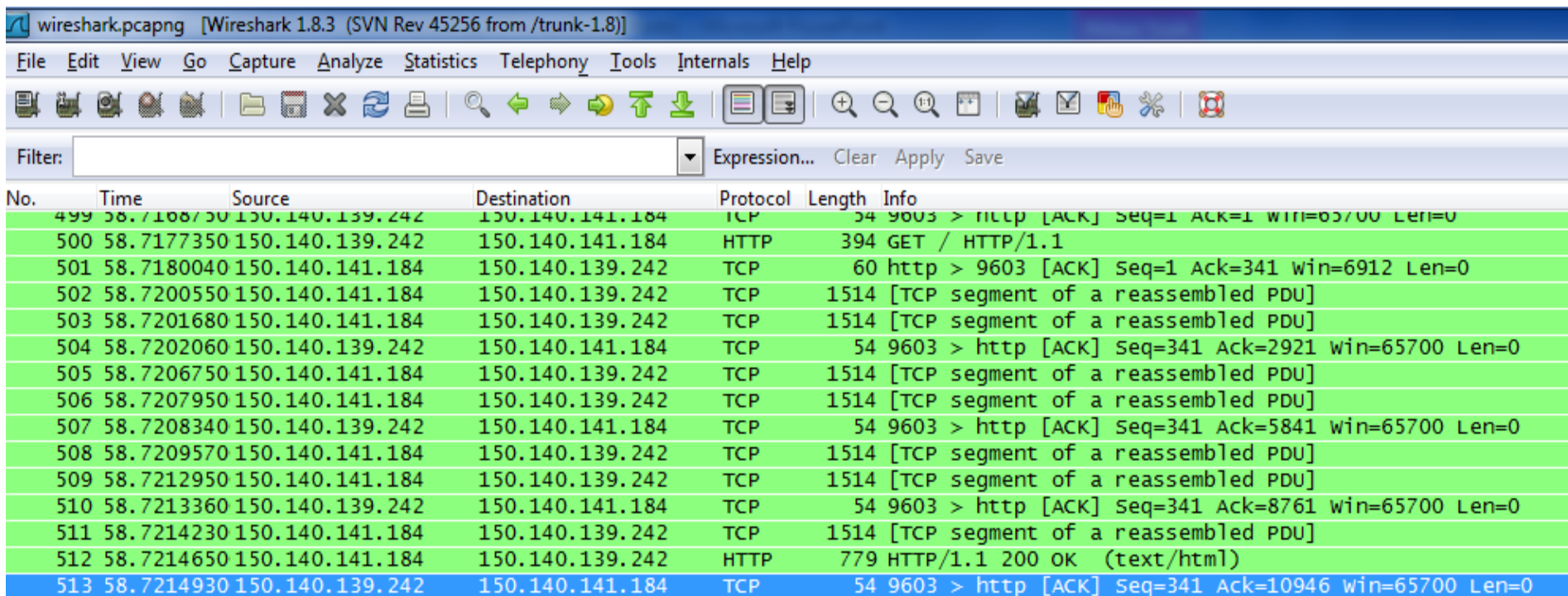
No.	Time	Source	Destination	Protocol	Length	Info
497	58.7165700	150.140.139.242	150.140.141.184	TCP	66	9603 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
498	58.7167950	150.140.141.184	150.140.139.242	TCP	66	http > 9603 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
499	58.7168750	150.140.139.242	150.140.141.184	TCP	54	9603 > http [ACK] Seq=1 Ack=1 win=65700 Len=0

Below the packet list, the details pane for the selected packet (Frame 497) is expanded, showing the following layers:

- Frame 497: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
- Ethernet II, Src: Dell_6e:78:ac (00:21:70:6e:78:ac), Dst: Cisco_46:89:bf (00:1b:53:46:89:bf)
- Internet Protocol version 4, Src: 150.140.139.242 (150.140.139.242), Dst: 150.140.141.184 (150.140.141.184)
- Transmission Control Protocol, Src Port: 9603 (9603), Dst Port: http (80), Seq: 0, Len: 0

Ανάλυση Δεδομένων

■ Μεταφορά δεδομένων

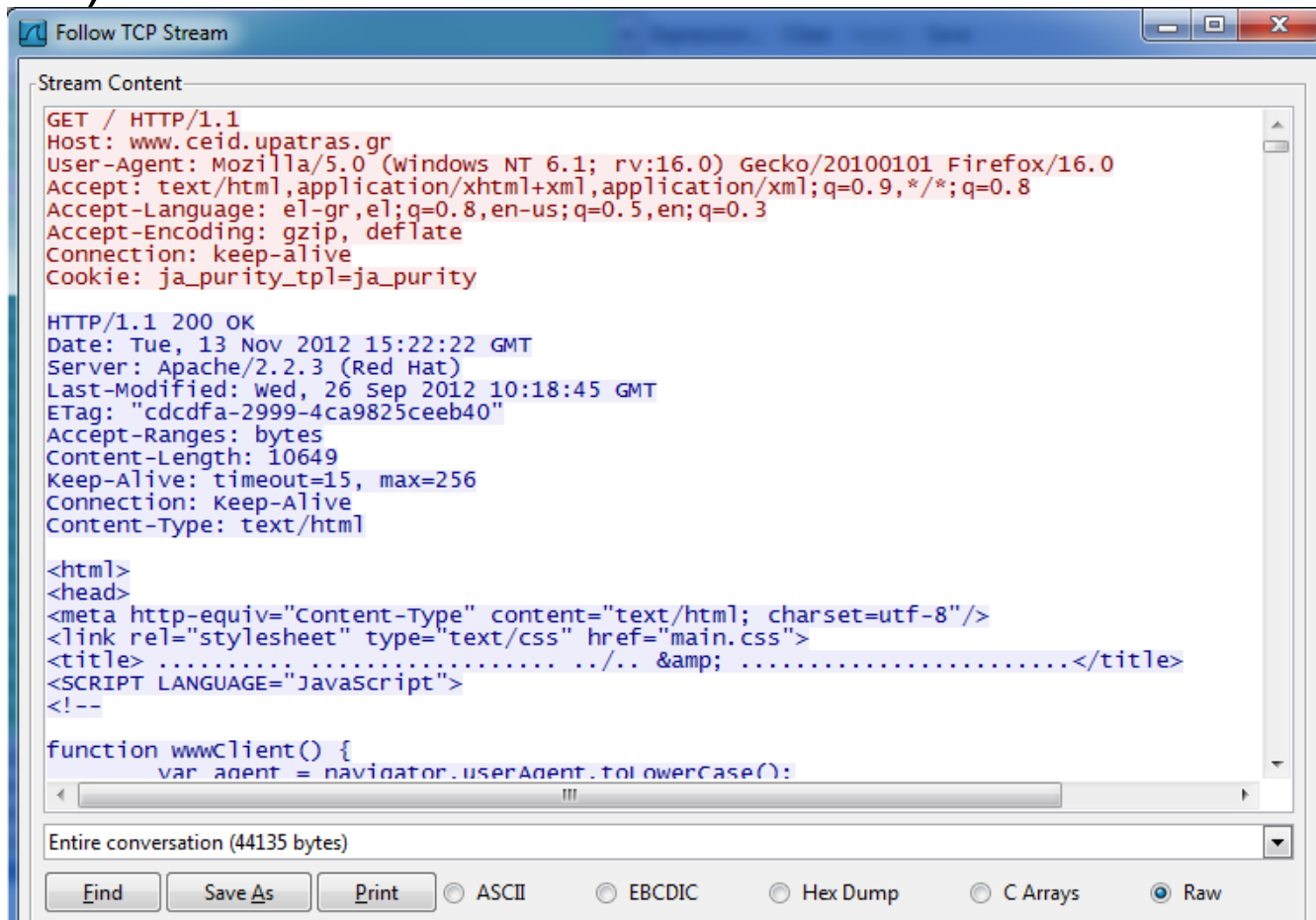


The image shows a Wireshark capture of network traffic. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, Help), a toolbar with various icons, and a filter field. The main display area shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The packets are highlighted in green, indicating they are selected. The traffic shows a sequence of TCP segments and an HTTP GET request.

No.	Time	Source	Destination	Protocol	Length	Info
499	58.7168750	150.140.139.242	150.140.141.184	TCP	54	9603 > nllp [ACK] Seq=1 Ack=1 win=65700 Len=0
500	58.7177350	150.140.139.242	150.140.141.184	HTTP	394	GET / HTTP/1.1
501	58.7180040	150.140.141.184	150.140.139.242	TCP	60	http > 9603 [ACK] Seq=1 Ack=341 win=6912 Len=0
502	58.7200550	150.140.141.184	150.140.139.242	TCP	1514	[TCP segment of a reassembled PDU]
503	58.7201680	150.140.141.184	150.140.139.242	TCP	1514	[TCP segment of a reassembled PDU]
504	58.7202060	150.140.139.242	150.140.141.184	TCP	54	9603 > http [ACK] Seq=341 Ack=2921 win=65700 Len=0
505	58.7206750	150.140.141.184	150.140.139.242	TCP	1514	[TCP segment of a reassembled PDU]
506	58.7207950	150.140.141.184	150.140.139.242	TCP	1514	[TCP segment of a reassembled PDU]
507	58.7208340	150.140.139.242	150.140.141.184	TCP	54	9603 > http [ACK] Seq=341 Ack=5841 win=65700 Len=0
508	58.7209570	150.140.141.184	150.140.139.242	TCP	1514	[TCP segment of a reassembled PDU]
509	58.7212950	150.140.141.184	150.140.139.242	TCP	1514	[TCP segment of a reassembled PDU]
510	58.7213360	150.140.139.242	150.140.141.184	TCP	54	9603 > http [ACK] Seq=341 Ack=8761 win=65700 Len=0
511	58.7214230	150.140.141.184	150.140.139.242	TCP	1514	[TCP segment of a reassembled PDU]
512	58.7214650	150.140.141.184	150.140.139.242	HTTP	779	HTTP/1.1 200 OK (text/html)
513	58.7214930	150.140.139.242	150.140.141.184	TCP	54	9603 > http [ACK] Seq=341 Ack=10946 win=65700 Len=0

Ανάλυση Δεδομένων

- Μεταφορά δεδομένων (δεξί κλικ και “Follow TCP stream”)



The screenshot shows a 'Follow TCP Stream' window with the following content:

```
Stream Content
GET / HTTP/1.1
Host: www.ceid.upatras.gr
User-Agent: Mozilla/5.0 (windows NT 6.1; rv:16.0) Gecko/20100101 Firefox/16.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: el-gr,el;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: ja_purity_tpl=ja_purity

HTTP/1.1 200 OK
Date: Tue, 13 Nov 2012 15:22:22 GMT
Server: Apache/2.2.3 (Red Hat)
Last-Modified: wed, 26 Sep 2012 10:18:45 GMT
ETag: "cdcdfa-2999-4ca9825ceeb40"
Accept-Ranges: bytes
Content-Length: 10649
Keep-Alive: timeout=15, max=256
Connection: Keep-Alive
Content-Type: text/html

<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
<link rel="stylesheet" type="text/css" href="main.css">
<title> ..... & .....</title>
<SCRIPT LANGUAGE="JavaScript">
<!--

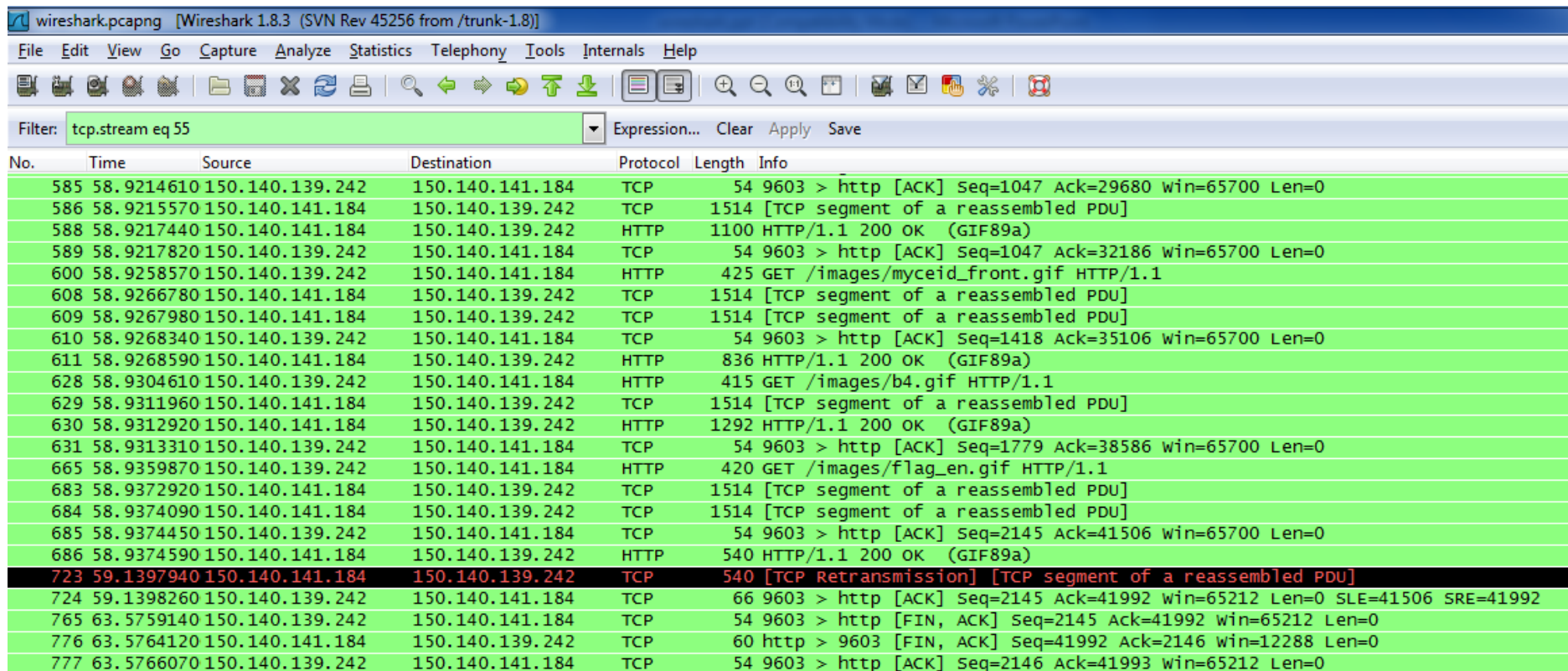
function wwwClient() {
    var agent = navigator.userAgent.toLowerCase();
```

Entire conversation (44135 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Ανάλυση Δεδομένων

- Ολοκλήρωση σύνδεσης
- Ενώ νέες συνδέσεις δημιουργούνται για την μεταφορά των υπόλοιπων δεδομένων



The image shows a Wireshark network traffic capture. The filter is set to 'tcp.stream eq 55'. The packet list shows a sequence of packets, with packet 723 highlighted in red, indicating a TCP retransmission. The retransmission is a TCP segment of a reassembled PDU, with sequence number 540, source IP 150.140.141.184, and destination IP 150.140.139.242. The surrounding packets are green, indicating they are not retransmissions.

No.	Time	Source	Destination	Protocol	Length	Info
585	58.9214610	150.140.139.242	150.140.141.184	TCP	54	9603 > http [ACK] Seq=1047 Ack=29680 win=65700 Len=0
586	58.9215570	150.140.141.184	150.140.139.242	TCP	1514	[TCP segment of a reassembled PDU]
588	58.9217440	150.140.141.184	150.140.139.242	HTTP	1100	HTTP/1.1 200 OK (GIF89a)
589	58.9217820	150.140.139.242	150.140.141.184	TCP	54	9603 > http [ACK] Seq=1047 Ack=32186 win=65700 Len=0
600	58.9258570	150.140.139.242	150.140.141.184	HTTP	425	GET /images/myceid_front.gif HTTP/1.1
608	58.9266780	150.140.141.184	150.140.139.242	TCP	1514	[TCP segment of a reassembled PDU]
609	58.9267980	150.140.141.184	150.140.139.242	TCP	1514	[TCP segment of a reassembled PDU]
610	58.9268340	150.140.139.242	150.140.141.184	TCP	54	9603 > http [ACK] Seq=1418 Ack=35106 win=65700 Len=0
611	58.9268590	150.140.141.184	150.140.139.242	HTTP	836	HTTP/1.1 200 OK (GIF89a)
628	58.9304610	150.140.139.242	150.140.141.184	HTTP	415	GET /images/b4.gif HTTP/1.1
629	58.9311960	150.140.141.184	150.140.139.242	TCP	1514	[TCP segment of a reassembled PDU]
630	58.9312920	150.140.141.184	150.140.139.242	HTTP	1292	HTTP/1.1 200 OK (GIF89a)
631	58.9313310	150.140.139.242	150.140.141.184	TCP	54	9603 > http [ACK] Seq=1779 Ack=38586 win=65700 Len=0
665	58.9359870	150.140.139.242	150.140.141.184	HTTP	420	GET /images/flag_en.gif HTTP/1.1
683	58.9372920	150.140.141.184	150.140.139.242	TCP	1514	[TCP segment of a reassembled PDU]
684	58.9374090	150.140.141.184	150.140.139.242	TCP	1514	[TCP segment of a reassembled PDU]
685	58.9374450	150.140.139.242	150.140.141.184	TCP	54	9603 > http [ACK] Seq=2145 Ack=41506 win=65700 Len=0
686	58.9374590	150.140.141.184	150.140.139.242	HTTP	540	HTTP/1.1 200 OK (GIF89a)
723	59.1397940	150.140.141.184	150.140.139.242	TCP	540	[TCP Retransmission] [TCP segment of a reassembled PDU]
724	59.1398260	150.140.139.242	150.140.141.184	TCP	66	9603 > http [ACK] Seq=2145 Ack=41992 win=65212 Len=0 SLE=41506 SRE=41992
765	63.5759140	150.140.139.242	150.140.141.184	TCP	54	9603 > http [FIN, ACK] Seq=2145 Ack=41992 win=65212 Len=0
776	63.5764120	150.140.141.184	150.140.139.242	TCP	60	http > 9603 [FIN, ACK] Seq=41992 Ack=2146 win=12288 Len=0
777	63.5766070	150.140.139.242	150.140.141.184	TCP	54	9603 > http [ACK] Seq=2146 Ack=41993 win=65212 Len=0