# Μοντέλα και ανάλυση πακέτων

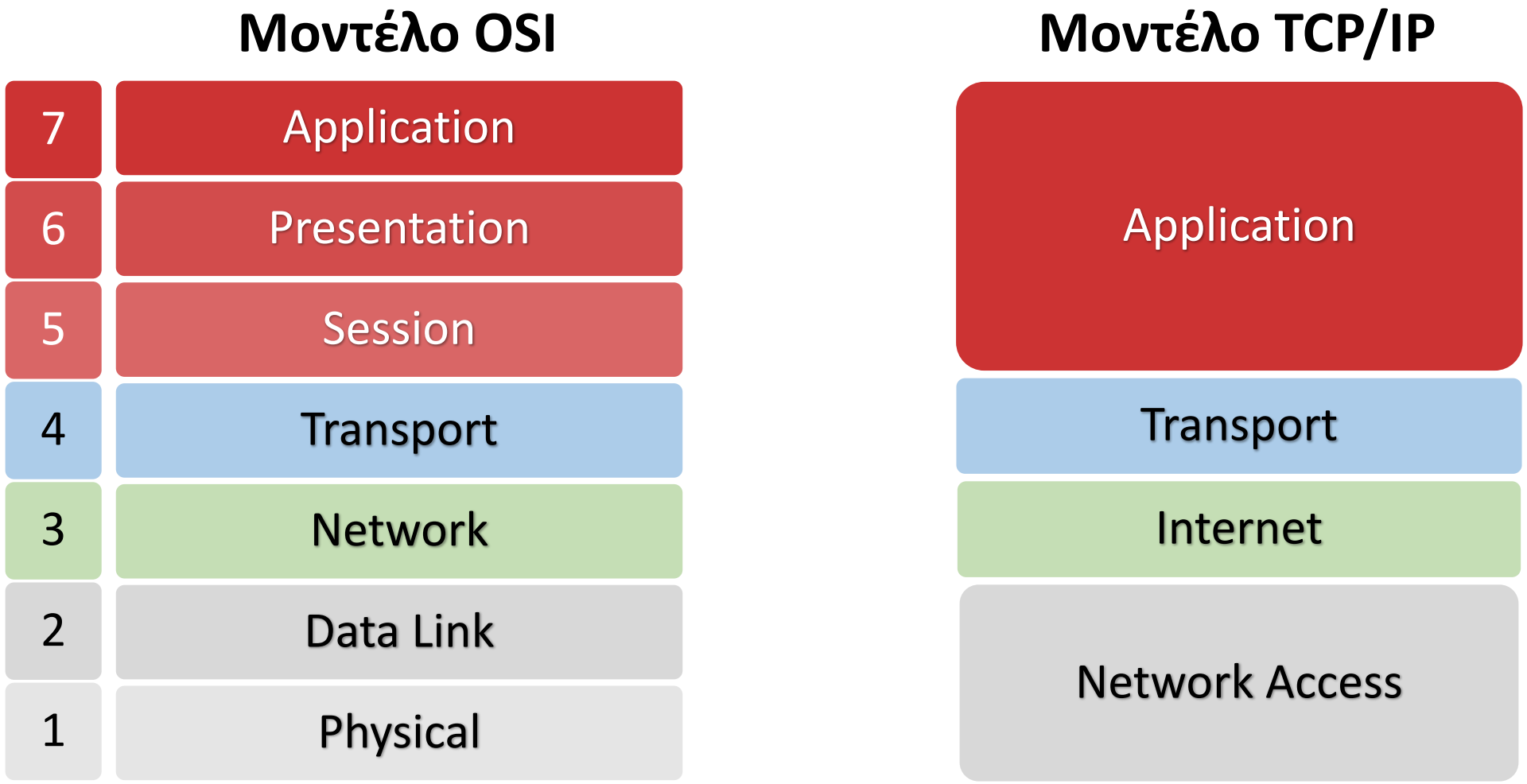
Εργαστήριο Δικτύων Υπολογιστών Ι

Καθ. Ι. Ξυδάς

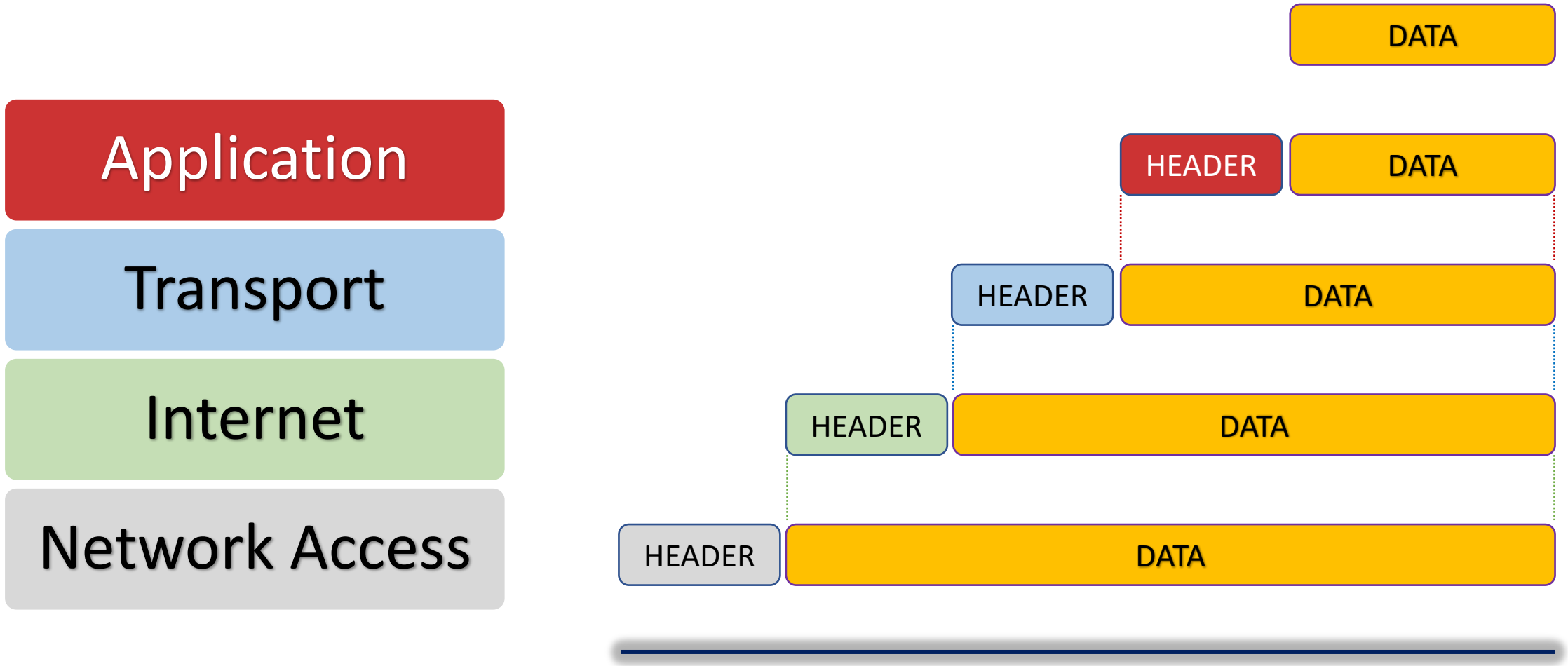
Ζ. Γαροφαλάκη, z.garofalaki@uniwa.gr

Δ. Καλλέργης, d.kallergis@uniwa.gr

# Μοντέλα OSI και TCP/IP



# Ενθυλάκωση (encapsulation)

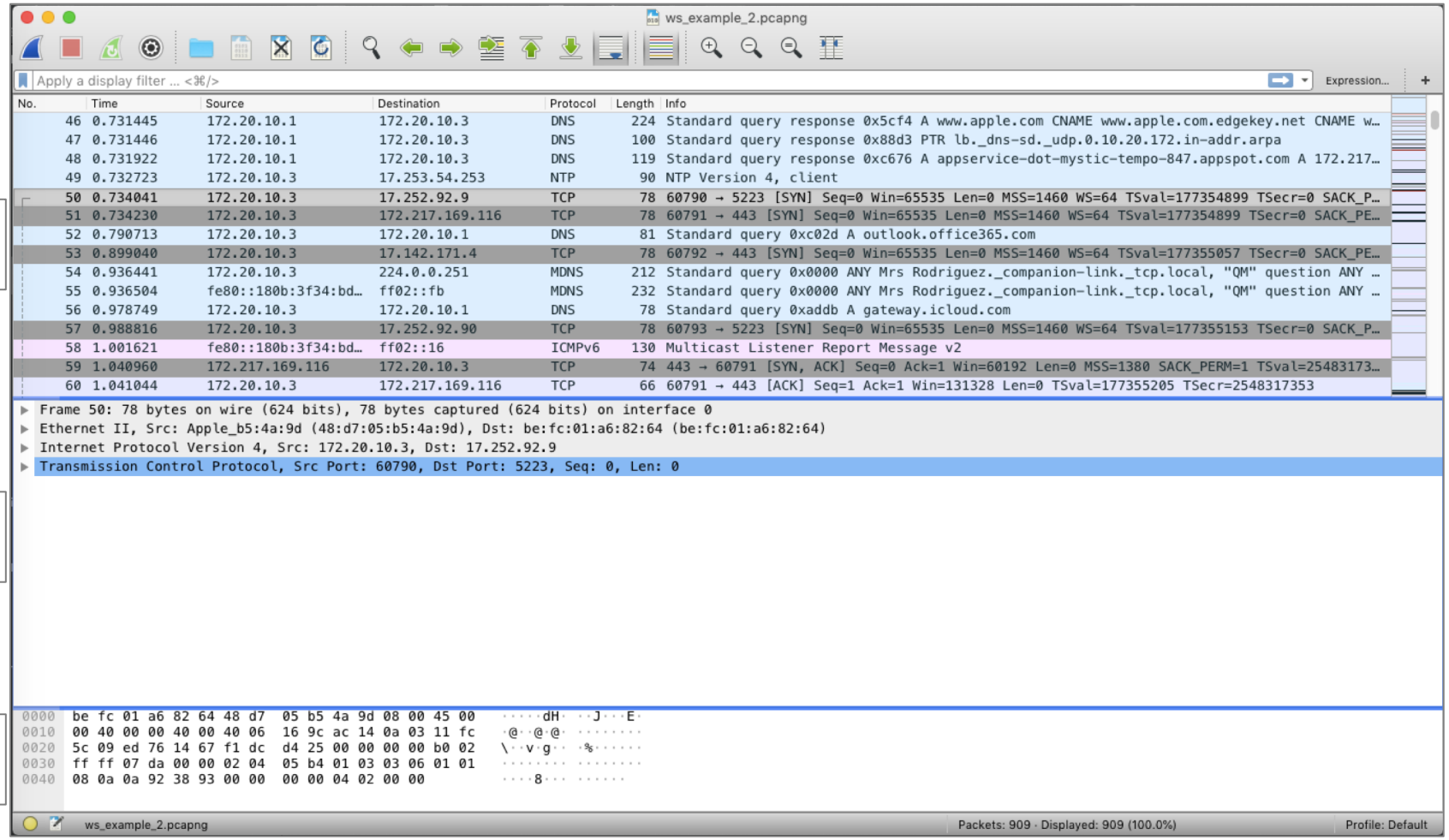


# Περιβάλλον Wireshark

**Packet-listing window**

**Packet-header details window**

**Packet-contents window**

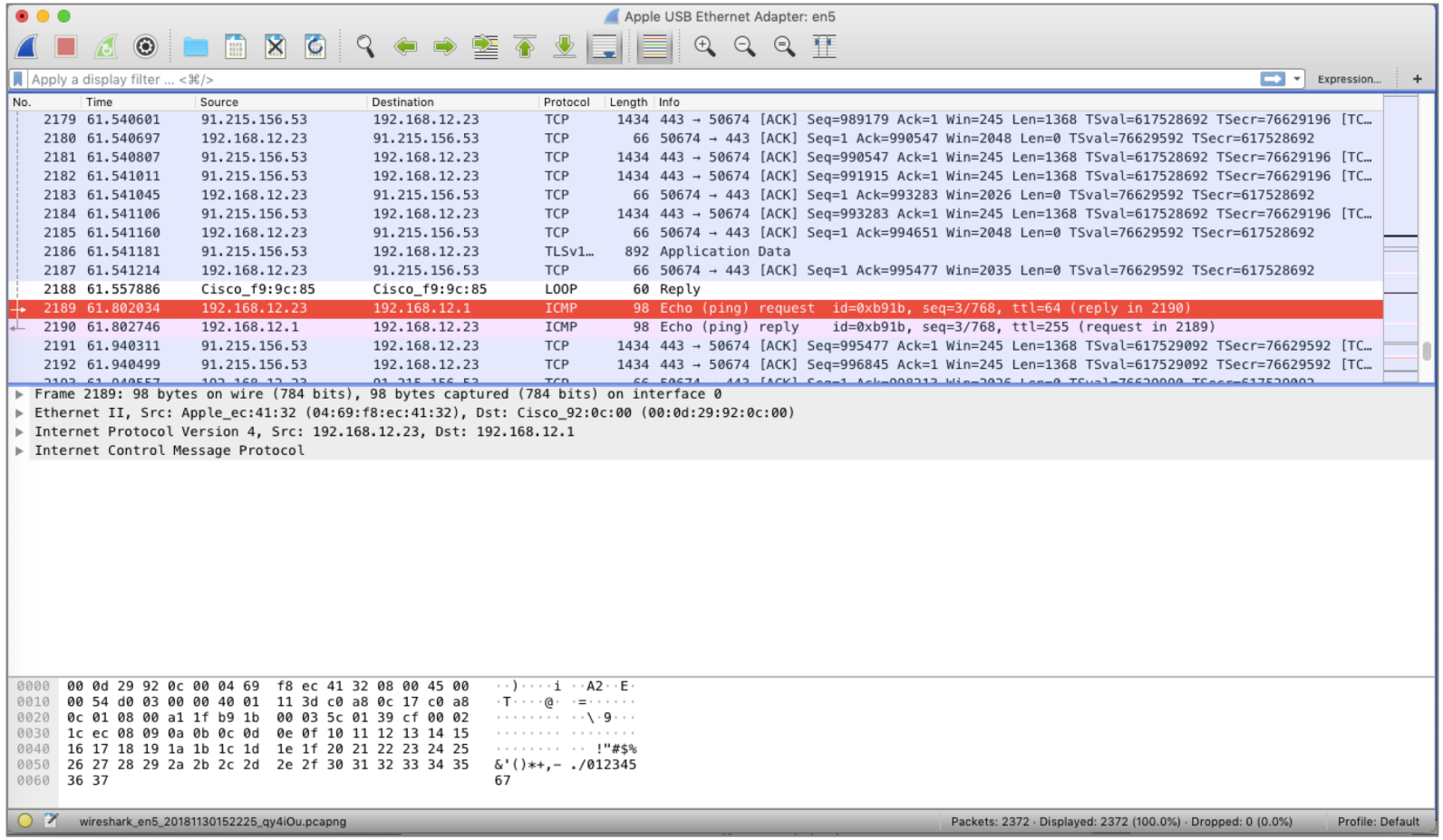


# Στοιχεία TCP/IP v.4

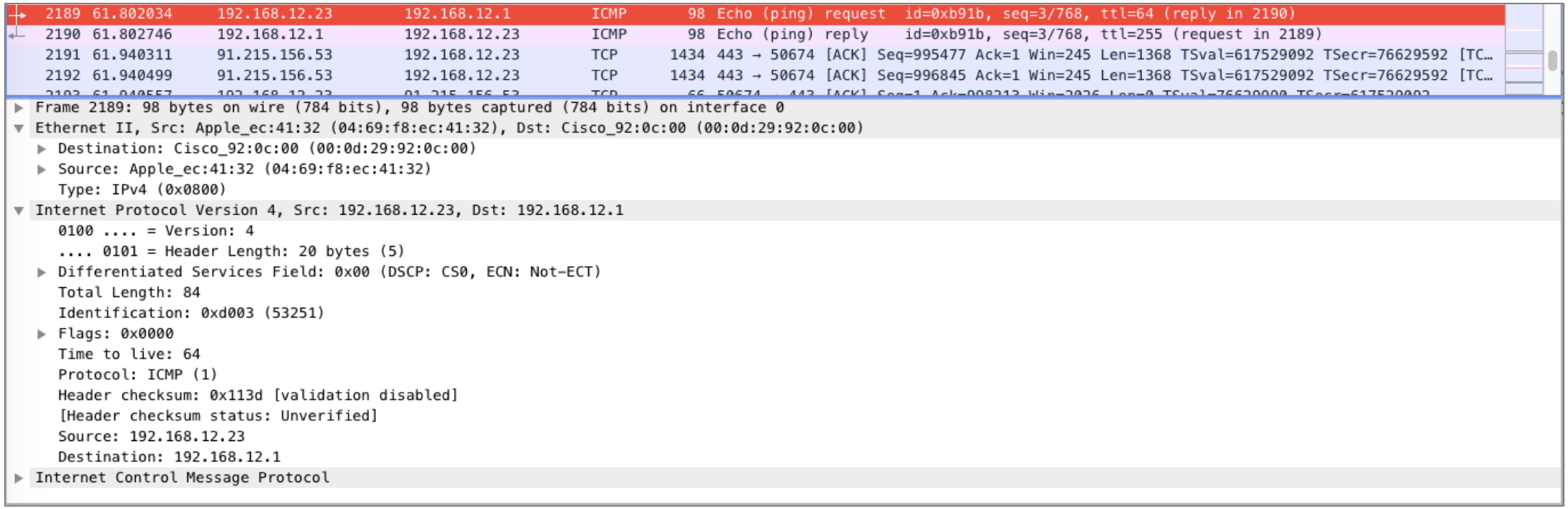
```
C:\>ipconfig -all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : myxp
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection 4:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter #2
        Physical Address. . . . . . . . . : 00-E0-4C-68-A5-3D
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        Autoconfiguration IP Address. . . : 192.168.88.20
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.88.1

C:\>
```

# ICMP

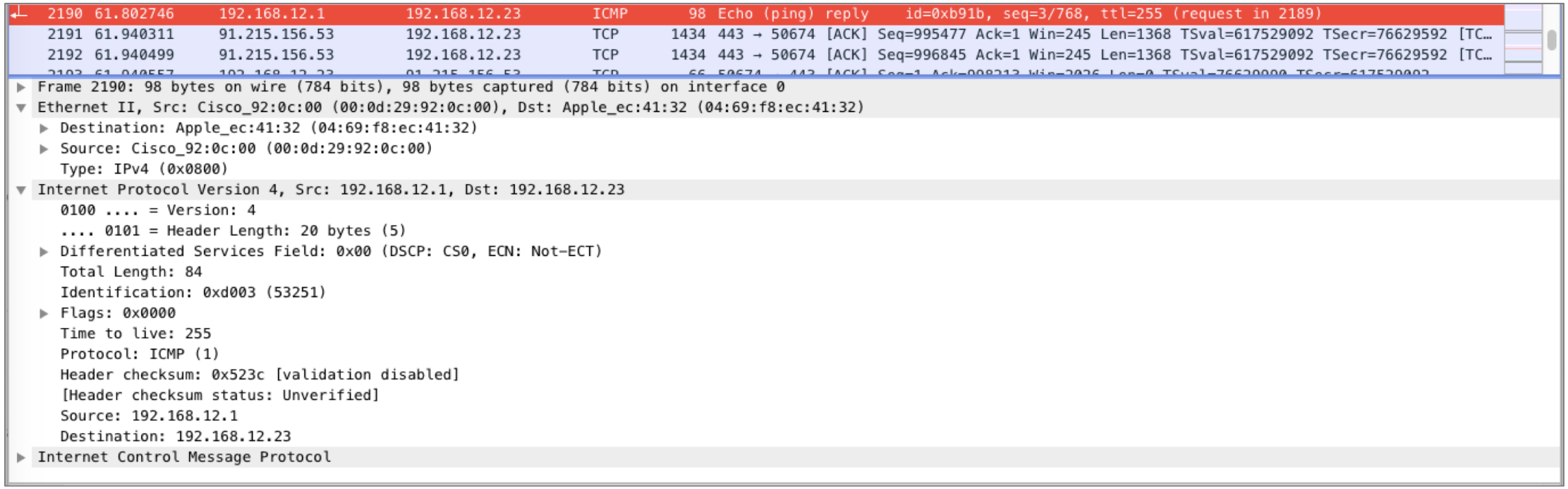
Ο Η/Υ με IP 192.168.12.23 επικοινωνεί (ping) με τον 192.168.12.1 (τοπικό δίκτυο)



# ICMP request

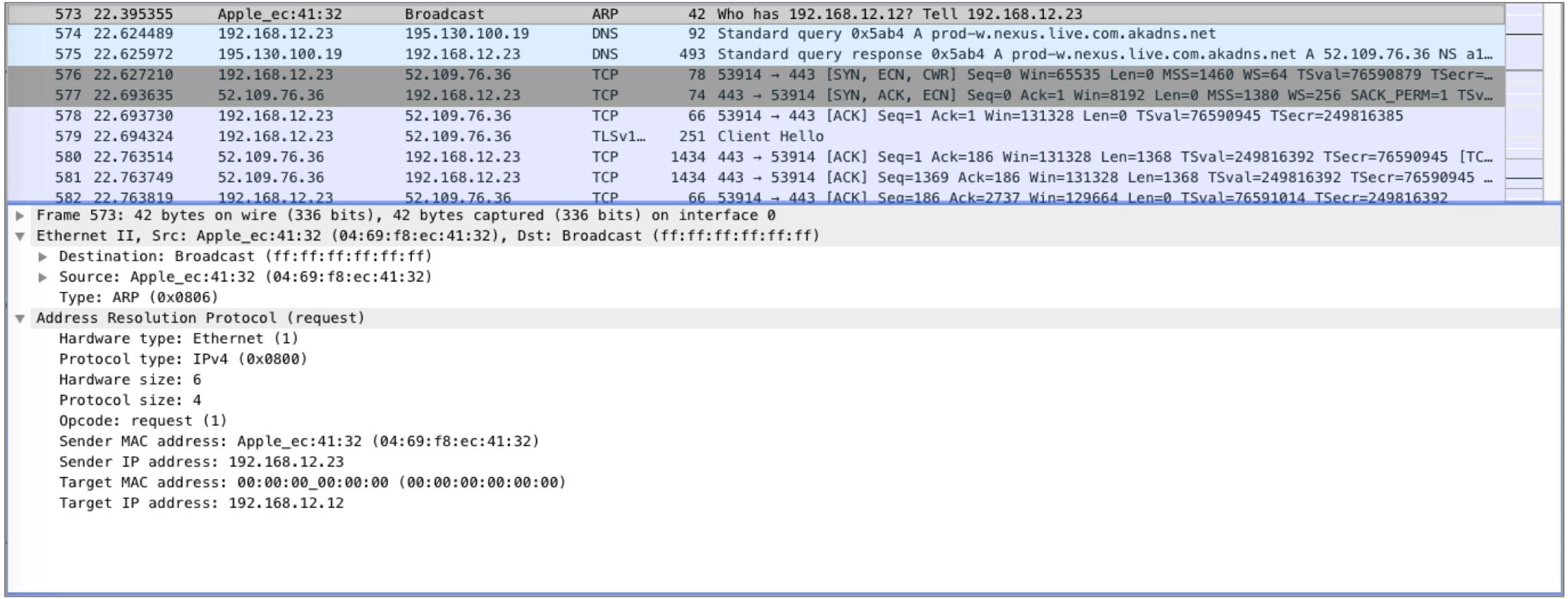


# ICMP reply


2190 61.802746 192.168.12.1 192.168.12.23 ICMP 98 Echo (ping) reply id=0xb91b, seq=3/768, ttl=255 (request in 2189)
2191 61.940311 91.215.156.53 192.168.12.23 TCP 1434 443 → 50674 [ACK] Seq=995477 Ack=1 Win=245 Len=1368 TSval=617529092 TSecr=76629592 [TC…
2192 61.940499 91.215.156.53 192.168.12.23 TCP 1434 443 → 50674 [ACK] Seq=996845 Ack=1 Win=245 Len=1368 TSval=617529092 TSecr=76629592 [TC…
Frame 2190: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: Cisco_92:0c:00 (00:0d:29:92:0c:00), Dst: Apple_ec:41:32 (04:69:f8:ec:41:32)
Destination: Apple_ec:41:32 (04:69:f8:ec:41:32)
Source: Cisco_92:0c:00 (00:0d:29:92:0c:00)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.12.1, Dst: 192.168.12.23
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84
Identification: 0xd003 (53251)
Flags: 0x0000
Time to live: 255
Protocol: ICMP (1)
Header checksum: 0x523c [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.12.1
Destination: 192.168.12.23
Internet Control Message Protocol

# ARP

Ο Η/Υ με IP 192.168.12.23 θέλει να επικοινωνήσει (ping) με τον 192.168.12.12



# Πίνακας ARP

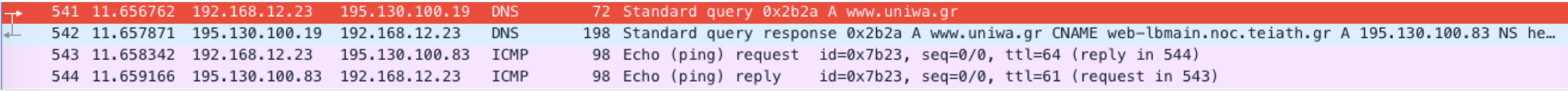
```
PC>arp -a
  Internet Address      Physical Address      Type
  192.168.88.1          0090.21b2.9701        dynamic
  192.168.88.3          000d.bd05.e174        dynamic
  192.168.88.4          0004.9a16.4b78        dynamic

PC>
```

- Πληροφορίες τοπικού δικτύου
- Type dynamic/static

Στην περίπτωση επικοινωνίας με IP **εκτός** του τοπικού δικτύου, τι συμβαίνει?

```
ping www.uniwa.gr
```

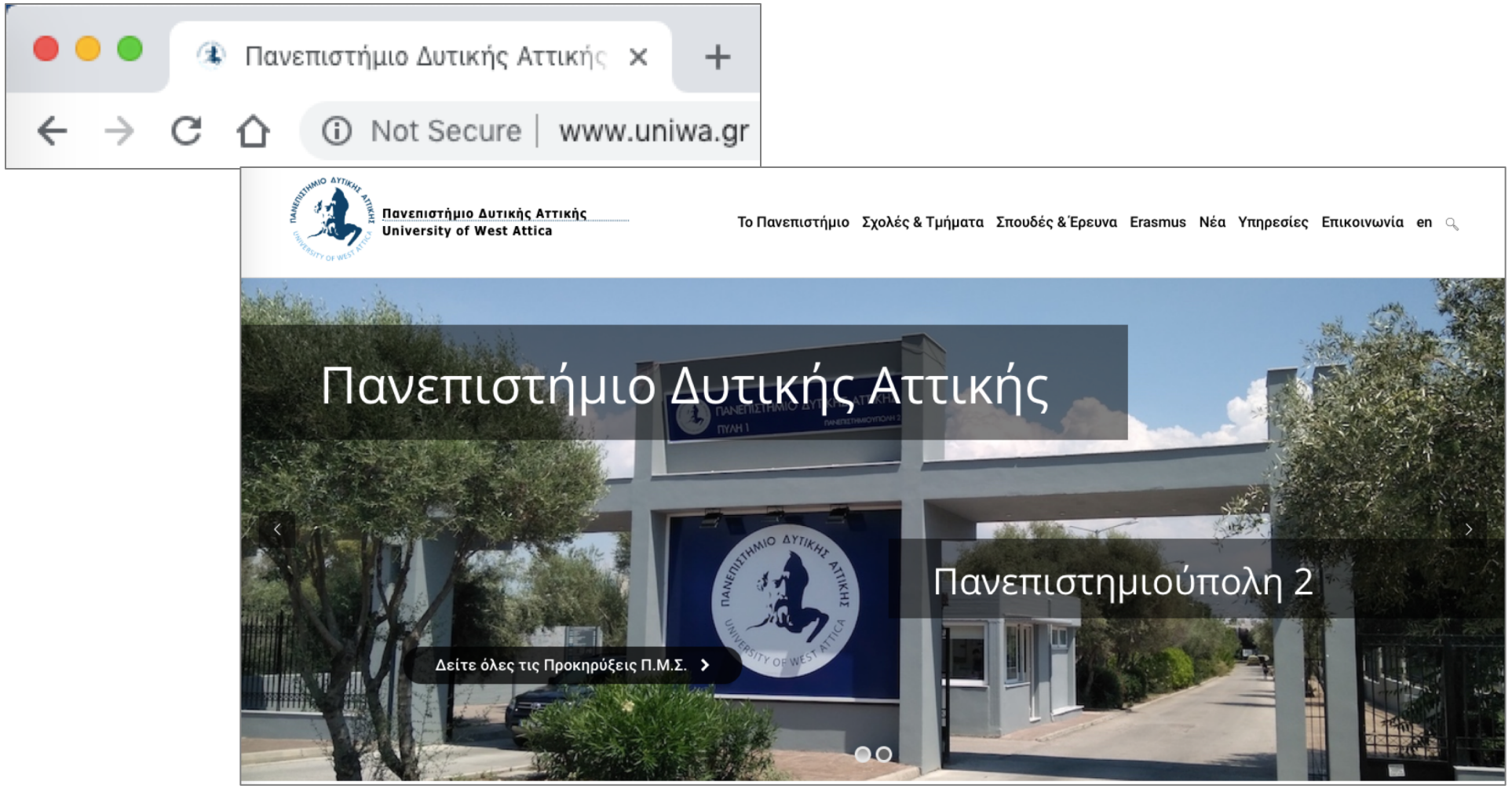
# DNS



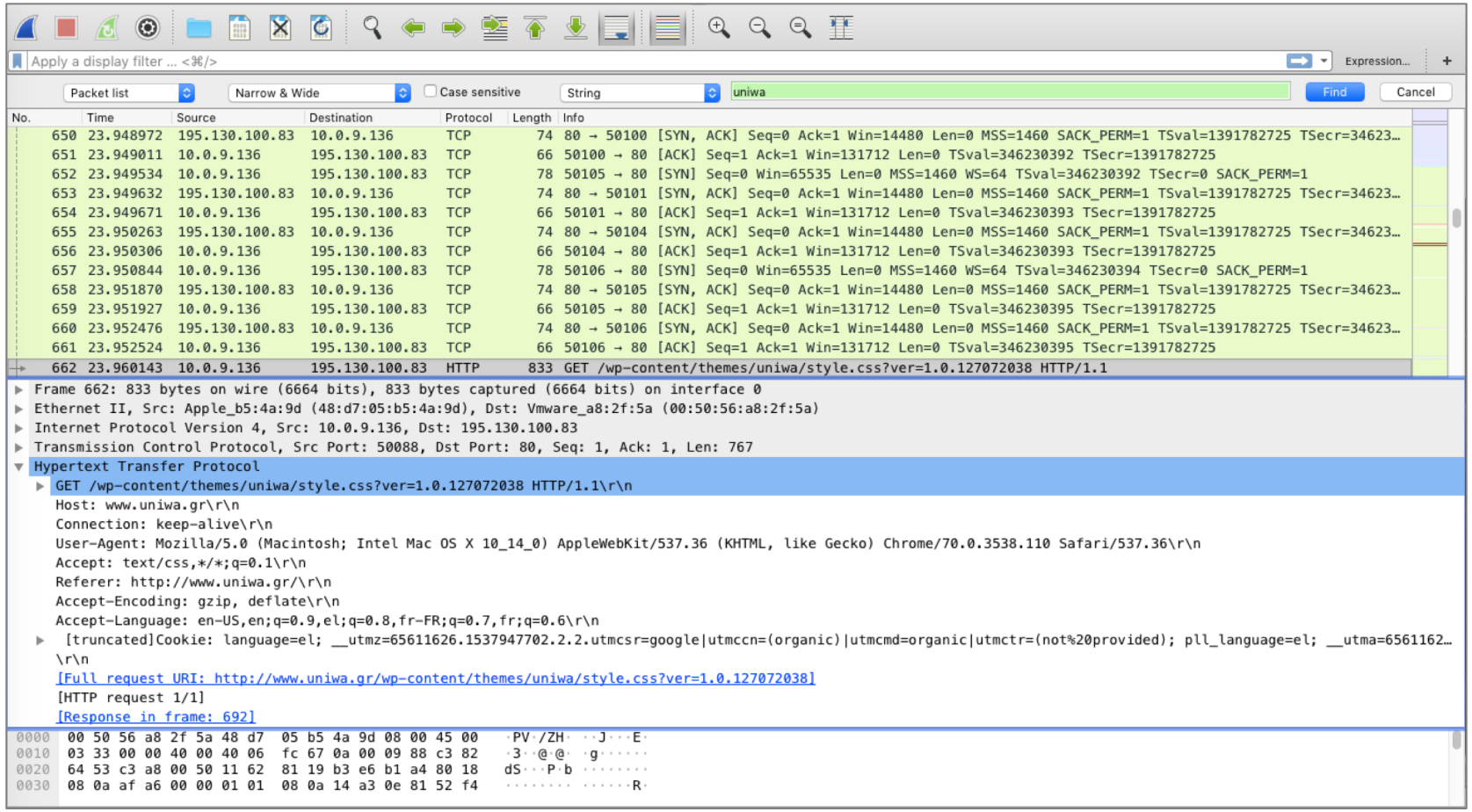
| | | | | | | |
|---|---|---|---|---|---|---|
| 541 | 11.656762 | 192.168.12.23 | 195.130.100.19 | DNS | 72 | Standard query 0x2b2a A www.uniwa.gr |
| 542 | 11.657871 | 195.130.100.19 | 192.168.12.23 | DNS | 198 | Standard query response 0x2b2a A www.uniwa.gr CNAME web-lbmain.noc.teiath.gr A 195.130.100.83 NS he… |
| 543 | 11.658342 | 192.168.12.23 | 195.130.100.83 | ICMP | 98 | Echo (ping) request id=0x7b23, seq=0/0, ttl=64 (reply in 544) |
| 544 | 11.659166 | 195.130.100.83 | 192.168.12.23 | ICMP | 98 | Echo (ping) reply id=0x7b23, seq=0/0, ttl=61 (request in 543) |

- Τι ερώτηση προηγείται της επικοινωνίας (ping) και γιατί;
- Ποιος απαντάει στην ερώτηση;
- Μπορούμε να εντοπίσουμε την πόρτα της υπηρεσίας DNS;
- Γιατί δεν προκύπτει ARP ερώτηση;
- Τι πληροφορίες εμπεριέχονται στην απάντηση;

# HTTP GET


Πανεπιστήμιο Δυτικής Αττικής
Not Secure | www.uniwa.gr
Πανεπιστήμιο Δυτικής Αττικής
University of West Attica
Το Πανεπιστήμιο Σχολές & Τμήματα Σπουδές & Έρευνα Erasmus Νέα Υπηρεσίες Επικοινωνία en
Πανεπιστήμιο Δυτικής Αττικής
Πανεπιστημιούπολη 2
Δείτε όλες τις Προκηρύξεις Π.Μ.Σ.

# HTTP GET


Apply a display filter ... <⌘/>
Expression...
Packet list
Narrow & Wide
Case sensitive
String
uniwa
Find
Cancel
No. Time Source Destination Protocol Length Info
650 23.948972 195.130.100.83 10.0.9.136 TCP 74 80 → 50100 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=1391782725 TSecr=34623…
651 23.949011 10.0.9.136 195.130.100.83 TCP 66 50100 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=346230392 TSecr=1391782725
652 23.949534 10.0.9.136 195.130.100.83 TCP 78 50105 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=346230392 TSecr=0 SACK_PERM=1
653 23.949632 195.130.100.83 10.0.9.136 TCP 74 80 → 50101 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=1391782725 TSecr=34623…
654 23.949671 10.0.9.136 195.130.100.83 TCP 66 50101 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=346230393 TSecr=1391782725
655 23.950263 195.130.100.83 10.0.9.136 TCP 74 80 → 50104 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=1391782725 TSecr=34623…
656 23.950306 10.0.9.136 195.130.100.83 TCP 66 50104 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=346230393 TSecr=1391782725
657 23.950844 10.0.9.136 195.130.100.83 TCP 78 50106 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=346230394 TSecr=0 SACK_PERM=1
658 23.951870 195.130.100.83 10.0.9.136 TCP 74 80 → 50105 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=1391782725 TSecr=34623…
659 23.951927 10.0.9.136 195.130.100.83 TCP 66 50105 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=346230395 TSecr=1391782725
660 23.952476 195.130.100.83 10.0.9.136 TCP 74 80 → 50106 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=1391782725 TSecr=34623…
661 23.952524 10.0.9.136 195.130.100.83 TCP 66 50106 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=346230395 TSecr=1391782725
662 23.960143 10.0.9.136 195.130.100.83 HTTP 833 GET /wp-content/themes/uniwa/style.css?ver=1.0.127072038 HTTP/1.1
Frame 662: 833 bytes on wire (6664 bits), 833 bytes captured (6664 bits) on interface 0
Ethernet II, Src: Apple_b5:4a:9d (48:d7:05:b5:4a:9d), Dst: Vmware_a8:2f:5a (00:50:56:a8:2f:5a)
Internet Protocol Version 4, Src: 10.0.9.136, Dst: 195.130.100.83
Transmission Control Protocol, Src Port: 50088, Dst Port: 80, Seq: 1, Ack: 1, Len: 767
Hypertext Transfer Protocol
GET /wp-content/themes/uniwa/style.css?ver=1.0.127072038 HTTP/1.1\r\n
Host: www.uniwa.gr\r\n
Connection: keep-alive\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.110 Safari/537.36\r\n
Accept: text/css,*/*;q=0.1\r\n
Referer: http://www.uniwa.gr/\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9,el;q=0.8,fr-FR;q=0.7,fr;q=0.6\r\n
[truncated]Cookie: language=el; __utmz=65611626.1537947702.2.2.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided); pll_language=el; __utma=6561162…
\r\n
[Full request URI: http://www.uniwa.gr/wp-content/themes/uniwa/style.css?ver=1.0.127072038]
[HTTP request 1/1]
[Response in frame: 692]
0000 00 50 56 a8 2f 5a 48 d7 05 b5 4a 9d 08 00 45 00 ·PV·/ZH· ··J···E·
0010 03 33 00 00 40 00 40 06 fc 67 0a 00 09 88 c3 82 ·3··@·@· ·g····
0020 64 53 c3 a8 00 50 11 62 81 19 b3 e6 b1 a4 80 18 dS···P·b ····
0030 08 0a af a6 00 00 01 01 08 0a 14 a3 0e 81 52 f4 ····· ·····R·