

Μοντέλα και ανάλυση πακέτων

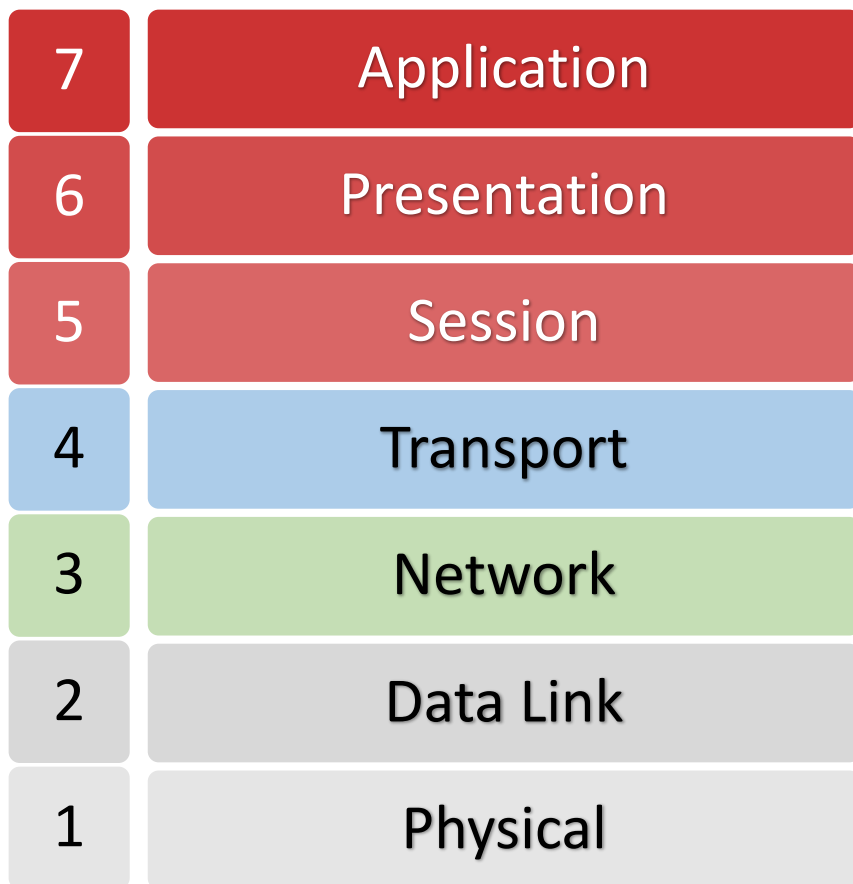
Εργαστήριο Δικτύων Υπολογιστών Ι
Καθ. Ι. Ξυδάς

Z. Γαροφαλάκη, z.garofalaki@uniwa.gr

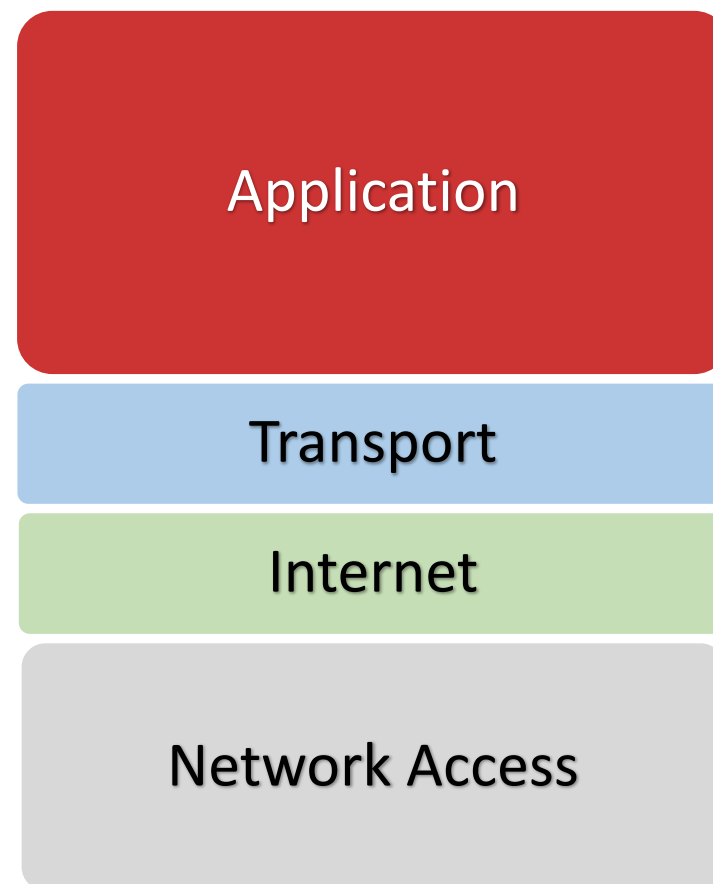
Δ. Καλλέργης, d.kallergis@uniwa.gr

Μοντέλα OSI και TCP/IP

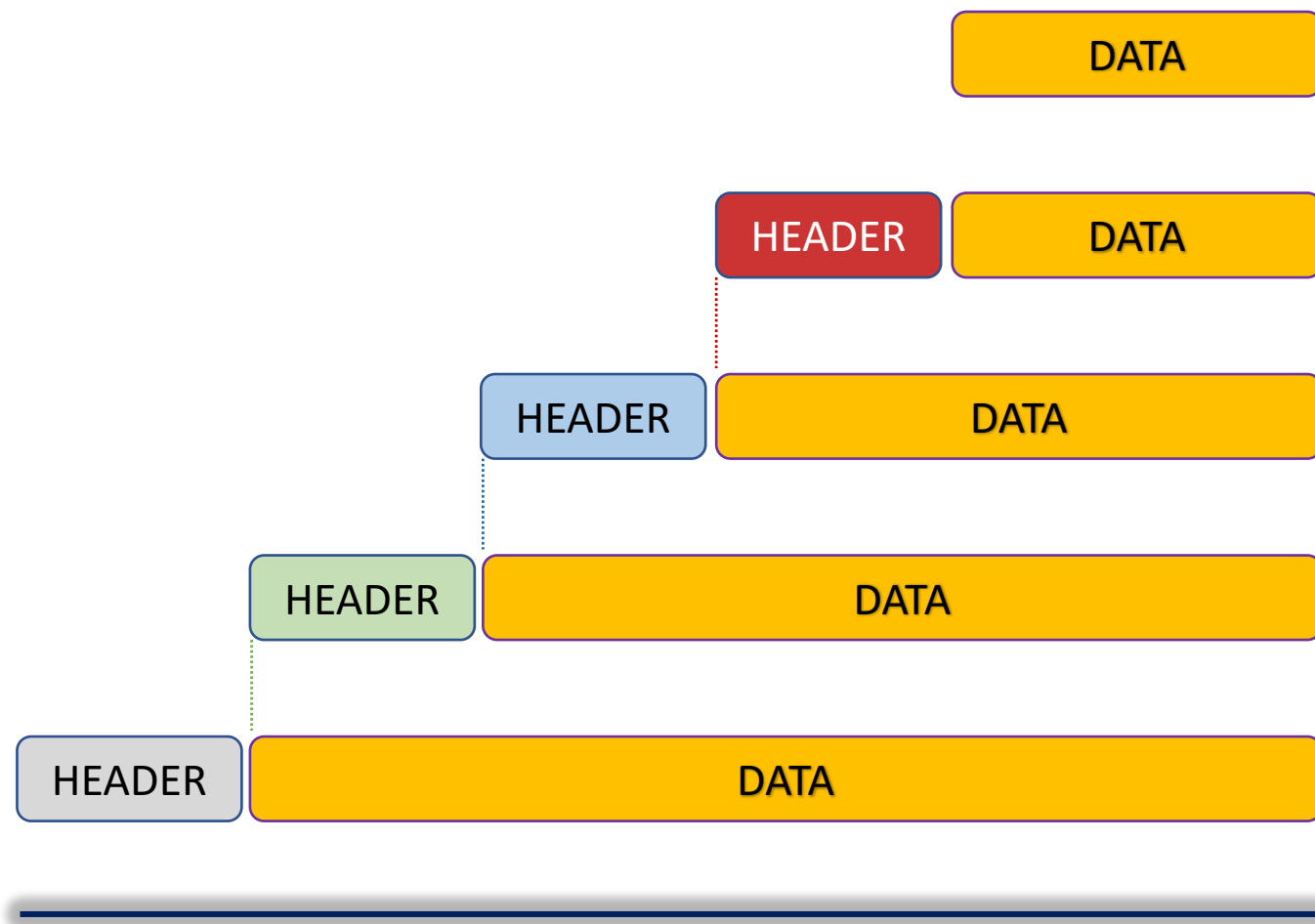
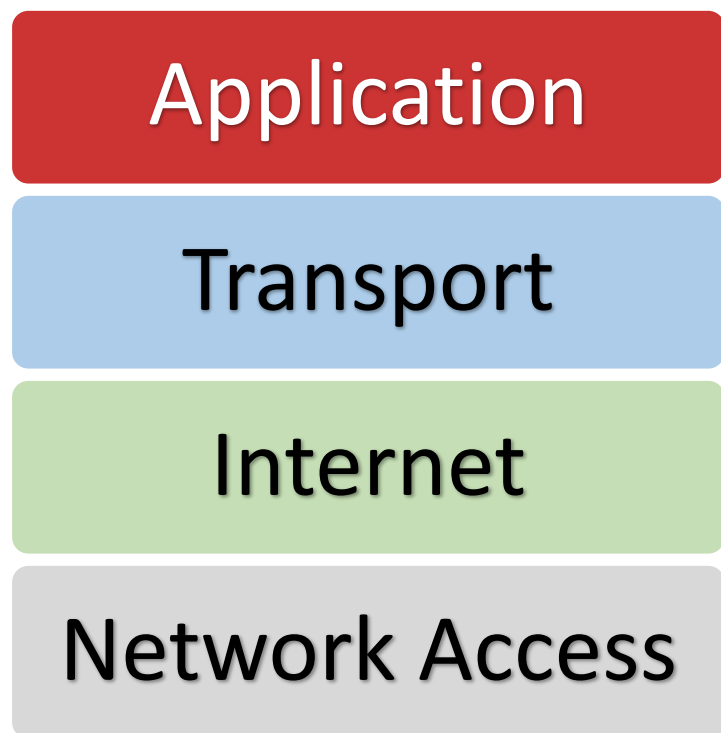
Μοντέλο OSI



Μοντέλο TCP/IP



Ενθυλάκωση (encapsulation)



Περιβάλλον Wireshark

Packet-listing window

The screenshot displays the Wireshark interface with the following components:

- Packet-listing window:** A table showing a list of captured packets. The columns are No., Time, Source, Destination, Protocol, Length, and Info. Packet 50 is highlighted.
- Packet-header details window:** A tree view showing the structure of the selected packet (No. 50). It includes Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol.
- Packet-contents window:** A hex dump of the packet data, showing hexadecimal values and their corresponding ASCII characters.

No.	Time	Source	Destination	Protocol	Length	Info
46	0.731445	172.20.10.1	172.20.10.3	DNS	224	Standard query response 0x5cf4 A www.apple.com CNAME www.apple.com.edgekey.net CNAME w...
47	0.731446	172.20.10.1	172.20.10.3	DNS	100	Standard query response 0x88d3 PTR lb._dns-sd._udp.0.10.20.172.in-addr.arpa
48	0.731922	172.20.10.1	172.20.10.3	DNS	119	Standard query response 0xc676 A appservice-dot-mystic-tempo-847.appspot.com A 172.217...
49	0.732723	172.20.10.3	17.253.54.253	NTP	90	NTP Version 4, client
50	0.734041	172.20.10.3	17.252.92.9	TCP	78	60790 → 5223 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=177354899 TSecr=0 SACK_P...
51	0.734230	172.20.10.3	172.217.169.116	TCP	78	60791 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=177354899 TSecr=0 SACK_PE...
52	0.790713	172.20.10.3	172.20.10.1	DNS	81	Standard query 0xc02d A outlook.office365.com
53	0.899040	172.20.10.3	17.142.171.4	TCP	78	60792 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=177355057 TSecr=0 SACK_PE...
54	0.936441	172.20.10.3	224.0.0.251	MDNS	212	Standard query 0x0000 ANY Mrs Rodriguez._companion-link._tcp.local, "QM" question ANY ...
55	0.936504	fe80::180b:3f34:bd...	ff02::fb	MDNS	232	Standard query 0x0000 ANY Mrs Rodriguez._companion-link._tcp.local, "QM" question ANY ...
56	0.978749	172.20.10.3	172.20.10.1	DNS	78	Standard query 0xaddb A gateway.icloud.com
57	0.988816	172.20.10.3	17.252.92.90	TCP	78	60793 → 5223 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=177355153 TSecr=0 SACK_P...
58	1.001621	fe80::180b:3f34:bd...	ff02::16	ICMPv6	130	Multicast Listener Report Message v2
59	1.040960	172.217.169.116	172.20.10.3	TCP	74	443 → 60791 [SYN, ACK] Seq=0 Ack=1 Win=60192 Len=0 MSS=1380 SACK_PERM=1 TSval=25483173...
60	1.041044	172.20.10.3	172.217.169.116	TCP	66	60791 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0 TSval=177355205 TSecr=2548317353

▶ Frame 50: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
▶ Ethernet II, Src: Apple_b5:4a:9d (48:d7:05:b5:4a:9d), Dst: be:fc:01:a6:82:64 (be:fc:01:a6:82:64)
▶ Internet Protocol Version 4, Src: 172.20.10.3, Dst: 17.252.92.9
▶ Transmission Control Protocol, Src Port: 60790, Dst Port: 5223, Seq: 0, Len: 0

```
0000  be fc 01 a6 82 64 48 d7 05 b5 4a 9d 08 00 45 00  ....dH...J...E...
0010  00 40 00 00 40 00 40 06 16 9c ac 14 0a 03 11 fc  @...@...
0020  5c 09 ed 76 14 67 f1 dc d4 25 00 00 00 00 b0 02  \..v.g...%.....
0030  ff ff 07 da 00 00 02 04 05 b4 01 03 03 06 01 01  .....8.....
0040  08 0a 0a 92 38 93 00 00 00 00 04 02 00 00
```

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)

The image shows a Wireshark network traffic capture window. The main pane displays a list of network packets. Packet 2189 is highlighted in red, representing an ICMP Echo (ping) request. The details pane below shows the structure of this packet: Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol. The hex dump at the bottom shows the raw bytes of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
2179	61.540601	91.215.156.53	192.168.12.23	TCP	1434	443 → 50674 [ACK] Seq=989179 Ack=1 Win=245 Len=1368 TSval=617528692 TSecr=76629196 [TC...
2180	61.540697	192.168.12.23	91.215.156.53	TCP	66	50674 → 443 [ACK] Seq=1 Ack=990547 Win=2048 Len=0 TSval=76629592 TSecr=617528692
2181	61.540807	91.215.156.53	192.168.12.23	TCP	1434	443 → 50674 [ACK] Seq=990547 Ack=1 Win=245 Len=1368 TSval=617528692 TSecr=76629196 [TC...
2182	61.541011	91.215.156.53	192.168.12.23	TCP	1434	443 → 50674 [ACK] Seq=991915 Ack=1 Win=245 Len=1368 TSval=617528692 TSecr=76629196 [TC...
2183	61.541045	192.168.12.23	91.215.156.53	TCP	66	50674 → 443 [ACK] Seq=1 Ack=993283 Win=2026 Len=0 TSval=76629592 TSecr=617528692
2184	61.541106	91.215.156.53	192.168.12.23	TCP	1434	443 → 50674 [ACK] Seq=993283 Ack=1 Win=245 Len=1368 TSval=617528692 TSecr=76629196 [TC...
2185	61.541160	192.168.12.23	91.215.156.53	TCP	66	50674 → 443 [ACK] Seq=1 Ack=994651 Win=2048 Len=0 TSval=76629592 TSecr=617528692
2186	61.541181	91.215.156.53	192.168.12.23	TLSv1...	892	Application Data
2187	61.541214	192.168.12.23	91.215.156.53	TCP	66	50674 → 443 [ACK] Seq=1 Ack=995477 Win=2035 Len=0 TSval=76629592 TSecr=617528692
2188	61.557886	Cisco_f9:9c:85	Cisco_f9:9c:85	LOOP	60	Reply
2189	61.802034	192.168.12.23	192.168.12.1	ICMP	98	Echo (ping) request id=0xb91b, seq=3/768, ttl=64 (reply in 2190)
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 2189: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▶ Ethernet II, Src: Apple_ec:41:32 (04:69:f8:ec:41:32), Dst: Cisco_92:0c:00 (00:0d:29:92:0c:00)
▶ Internet Protocol Version 4, Src: 192.168.12.23, Dst: 192.168.12.1
▶ Internet Control Message Protocol

```
0000 00 0d 29 92 0c 00 04 69 f8 ec 41 32 08 00 45 00  ..)....i..A2..E.  
0010 00 54 d0 03 00 00 40 01 11 3d c0 a8 0c 17 c0 a8  .T...@...:=.....  
0020 0c 01 08 00 a1 f b9 1b 00 03 5c 01 39 cf 00 02  .....9...  
0030 1c ec 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15  .....  
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  .....!#$%  
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,-./012345  
0060 36 37 67
```

ICMP request

No.	Time	Source	Destination	Protocol	Length	Info
2189	61.802034	192.168.12.23	192.168.12.1	ICMP	98	Echo (ping) request id=0xb91b, seq=3/768, ttl=64 (reply in 2190)
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...
2193	61.940557	192.168.12.23	91.215.156.53	TCP	66	50674 → 443 [ACK] Seq=1 Ack=998212 Win=2026 Len=0 TSval=76629000 TSecr=617529092

▶ Frame 2189: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0

▼ Ethernet II, Src: Apple_ec:41:32 (04:69:f8:ec:41:32), Dst: Cisco_92:0c:00 (00:0d:29:92:0c:00)

- ▶ Destination: Cisco_92:0c:00 (00:0d:29:92:0c:00)
- ▶ Source: Apple_ec:41:32 (04:69:f8:ec:41:32)
- Type: IPv4 (0x0800)

▼ Internet Protocol Version 4, Src: 192.168.12.23, Dst: 192.168.12.1

- 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: 64
- Protocol: ICMP (1)
- Header checksum: 0x113d [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.12.23
- Destination: 192.168.12.1

▶ Internet Control Message Protocol

ICMP reply

The image shows a Wireshark packet capture interface. The top pane displays a list of packets, with packet 2190 selected. The packet list pane shows:

No.	Time	Source	Destination	Protocol	Length	Info
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...
2193	61.940557	192.168.12.23	91.215.156.53	TCP	66	50674 → 443 [ACK] Seq=1 Ack=998313 Win=2026 Len=0 TSval=76630000 TSecr=617529092

The packet details pane for packet 2190 shows the following structure:

- 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

573	22.395355	Apple_ec:41:32	Broadcast	ARP	42	Who has 192.168.12.12? Tell 192.168.12.23
574	22.624489	192.168.12.23	195.130.100.19	DNS	92	Standard query 0x5ab4 A prod-w.nexus.live.com.akadns.net
575	22.625972	195.130.100.19	192.168.12.23	DNS	493	Standard query response 0x5ab4 A prod-w.nexus.live.com.akadns.net A 52.109.76.36 NS a1...
576	22.627210	192.168.12.23	52.109.76.36	TCP	78	53914 → 443 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=76590879 TSecr=...
577	22.693635	52.109.76.36	192.168.12.23	TCP	74	443 → 53914 [SYN, ACK, ECN] Seq=0 Ack=1 Win=8192 Len=0 MSS=1380 WS=256 SACK_PERM=1 TSv...
578	22.693730	192.168.12.23	52.109.76.36	TCP	66	53914 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0 TSval=76590945 TSecr=249816385
579	22.694324	192.168.12.23	52.109.76.36	TLSv1...	251	Client Hello
580	22.763514	52.109.76.36	192.168.12.23	TCP	1434	443 → 53914 [ACK] Seq=1 Ack=186 Win=131328 Len=1368 TSval=249816392 TSecr=76590945 [TC...
581	22.763749	52.109.76.36	192.168.12.23	TCP	1434	443 → 53914 [ACK] Seq=1369 Ack=186 Win=131328 Len=1368 TSval=249816392 TSecr=76590945 ...
582	22.763819	192.168.12.23	52.109.76.36	TCP	66	53914 → 443 [ACK] Seq=186 Ack=2737 Win=129664 Len=0 TSval=76591014 TSecr=249816392

▶ Frame 573: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

▼ Ethernet II, Src: Apple_ec:41:32 (04:69:f8:ec:41:32), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

- ▶ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
- ▶ Source: Apple_ec:41:32 (04:69:f8:ec:41:32)
Type: ARP (0x0806)

▼ Address Resolution Protocol (request)

- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: request (1)
- Sender MAC address: Apple_ec:41:32 (04:69:f8:ec:41:32)
- Sender IP address: 192.168.12.23
- Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
- Target IP address: 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?

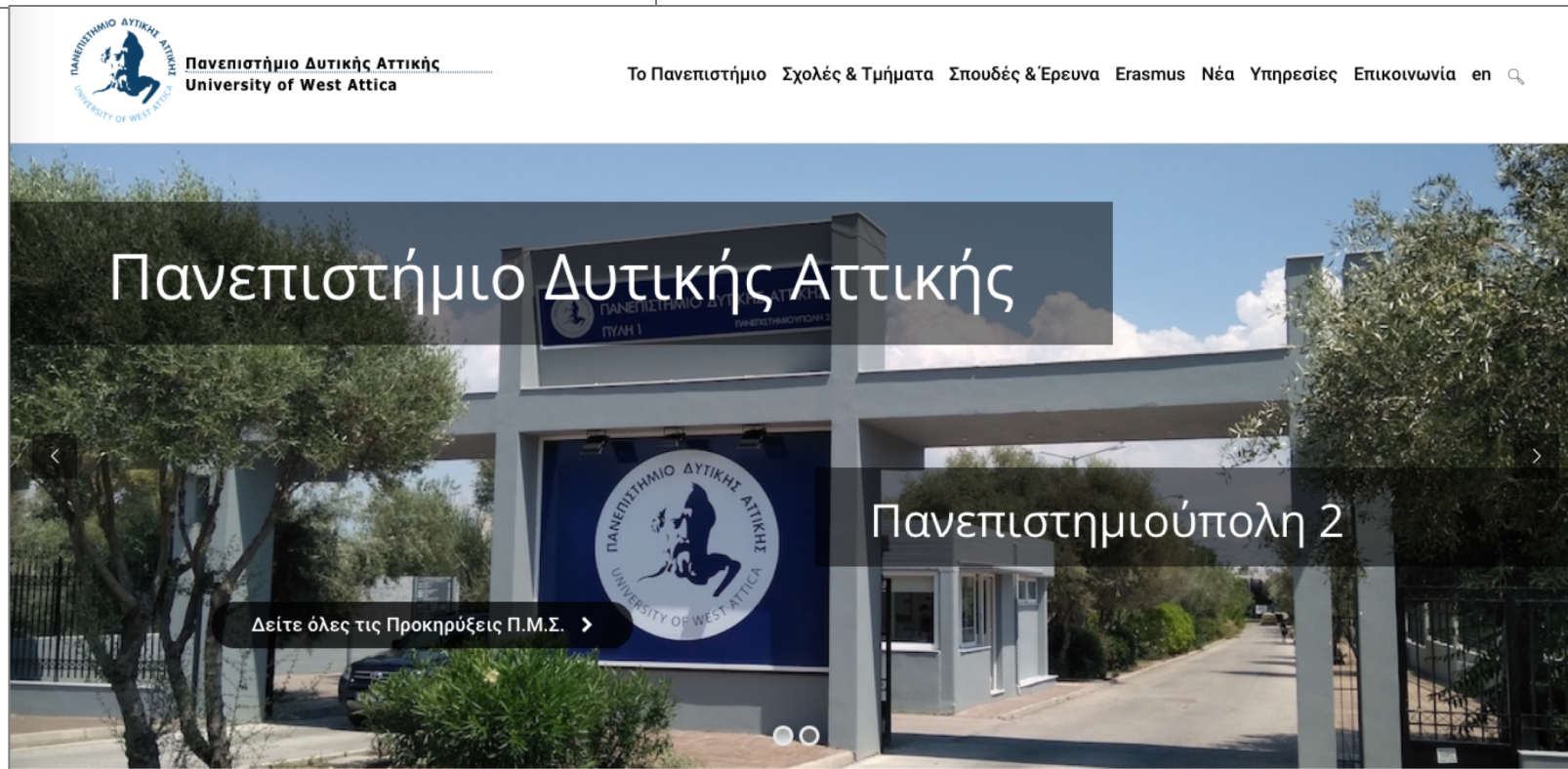
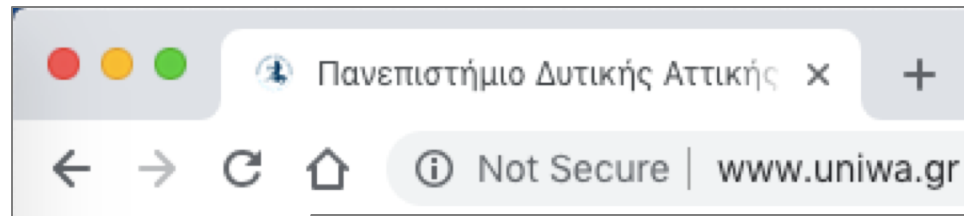
```
ping www.uniwa.gr
```

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



HTTP GET

The image shows a Wireshark packet capture window. The top toolbar includes various icons for file operations, search, and zooming. Below the toolbar, there's a search bar with the text 'uniwa' and a 'Find' button. The main area is a table of network packets. The selected packet (No. 662) is expanded to show its details. The details pane shows the following information:

- 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...
 - [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]

At the bottom of the window, there's a hex dump of the packet data:

```
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.....
```