

| | | |
|---|----------------------------------|-------------------------|
| Όνοματεπώνυμο: Άγγελος Μητροκώτσας | | Ομάδα:6 |
| Όνομα PC/ΛΣ: DESKTOP-91G20CF/ Windows 10 Pro 20H2 | | Ημερομηνία:25/ 10/ 2021 |
| Διεύθυνση IP: 192.168.1.12 | Διεύθυνση MAC: F8-63-3F-59-24-C8 | |

Εργαστηριακή Άσκηση 2

Ενθυλάκωση και Επικεφαλίδες

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

1

1.1 Το φίλτρο επιτρέπει την απεικόνιση πρωτοκόλλων μόνο τύπου IP και AVR.

1.2 Destination, Source και Type.

1.3 Όχι δεν υπάρχει.

1.4 6 bytes

Wireshark packet capture analysis showing a TCP ACK packet (No. 230) from 192.168.1.12 to 147.102.40.15. The packet details pane shows the following structure:

- Ethernet II, Src: IntelCor_59:24:c8 (f8:63:3f:59:24:c8), Dst: Sercomm_f7:d3:40 (38:02:de:f7:d3:40)
- Internet Protocol Version 4, Src: 192.168.1.12, Dst: 147.102.40.15
- Hypertext Transfer Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII, including the HTTP status line: 200 OK (text/html).

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp or ip

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|---------------|---------------|----------|--------|--|
| 243 | 0.051971 | 192.168.1.12 | 78.46.103.41 | TCP | 54 | 55649 → 443 [ACK] Seq=98 Ack=5181 Win=515 Len=0 |
| 241 | 0.049071 | 192.168.1.12 | 78.46.103.41 | TCP | 54 | 55649 → 443 [ACK] Seq=98 Ack=5115 Win=516 Len=0 |
| 239 | 0.047799 | 192.168.1.12 | 78.46.103.41 | TCP | 54 | 55649 → 443 [ACK] Seq=98 Ack=5046 Win=510 Len=0 |
| 237 | 0.051034 | 192.168.1.12 | 78.46.103.41 | TCP | 54 | 55649 → 443 [ACK] Seq=98 Ack=4980 Win=510 Len=0 |
| 235 | 0.055757 | 192.168.1.12 | 147.102.40.15 | TCP | 54 | 56011 → 80 [ACK] Seq=558 Ack=234 Win=131072 Len=0 |
| 233 | 0.007356 | 147.102.40.15 | 192.168.1.12 | TCP | 60 | 80 → 56011 [ACK] Seq=1 Ack=558 Win=65344 Len=0 |
| 232 | 0.010874 | 192.168.1.12 | 78.46.103.41 | TCP | 54 | 55649 → 443 [ACK] Seq=98 Ack=4888 Win=511 Len=0 |
| 230 | 0.000178 | 192.168.1.12 | 147.102.40.15 | TCP | 590 | 56011 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=536 [TCP s |

> Frame 230: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface \Device\NPF_{11981F20-5231-4861-ABD2-DD8A4A}

> Ethernet II, Src: IntelCor_59:24:c8 (f8:63:3f:59:24:c8), Dst: Sercomm_f7:d3:40 (38:02:de:f7:d3:40)

> Destination: Sercomm_f7:d3:40 (38:02:de:f7:d3:40)

> Source: IntelCor_59:24:c8 (f8:63:3f:59:24:c8)

Type: IPv4 (0x0800)

```

0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 08 00 45 00 8...@.c ?Y$.E.
0010 02 40 a5 2e 40 00 80 06 d6 5f c0 a8 01 0c 93 66 .@..@..._.....f
0020 28 0f da cb 00 50 4e 69 ed ba 29 15 89 38 50 10 (...PNI...)..8P
0030 02 00 b7 d9 00 00 47 45 54 20 2f 6c 61 62 32 2f .....GE T /lab2/
0040 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a HTTP/1.1..Host:
0050 20 65 64 75 2d 64 79 2e 63 6e 2e 6e 74 75 61 2e edu-dy. cn.ntua.
0060 67 72 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 gr..Conn ection:
0070 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67 72 keep-ali ve..Upgr
0080 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 ade-Inse cure-Req
0090 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 72 2d 41 uests: 1 ..User-A

```

Source Hardware Address (eth.src), 6 byte(s)

Packets: 311 · Displayed: 307 (98.7%) · Dropped: 0 (0.0%) Profile: Default

1.5 14 bytes

*Wi-Fi (ether host f8-63-3f-59-24-c8)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp or ip

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|---------------|---------------|----------|--------|--|
| 243 | 0.051971 | 192.168.1.12 | 78.46.103.41 | TCP | 54 | 55649 → 443 [ACK] Seq=98 Ack=5181 Win=515 Len=0 |
| 241 | 0.049071 | 192.168.1.12 | 78.46.103.41 | TCP | 54 | 55649 → 443 [ACK] Seq=98 Ack=5115 Win=516 Len=0 |
| 239 | 0.047799 | 192.168.1.12 | 78.46.103.41 | TCP | 54 | 55649 → 443 [ACK] Seq=98 Ack=5046 Win=510 Len=0 |
| 237 | 0.051034 | 192.168.1.12 | 78.46.103.41 | TCP | 54 | 55649 → 443 [ACK] Seq=98 Ack=4980 Win=510 Len=0 |
| 235 | 0.055757 | 192.168.1.12 | 147.102.40.15 | TCP | 54 | 56011 → 80 [ACK] Seq=558 Ack=234 Win=131072 Len=0 |
| 233 | 0.007356 | 147.102.40.15 | 192.168.1.12 | TCP | 60 | 80 → 56011 [ACK] Seq=1 Ack=558 Win=65344 Len=0 |
| 232 | 0.010874 | 192.168.1.12 | 78.46.103.41 | TCP | 54 | 55649 → 443 [ACK] Seq=98 Ack=4888 Win=511 Len=0 |
| 230 | 0.000178 | 192.168.1.12 | 147.102.40.15 | TCP | 590 | 56011 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=536 [TCP s |

> Frame 230: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface \Device\NPF_{11981F20-5231-4861-ABD2-DD8A4A}

> Ethernet II, Src: IntelCor_59:24:c8 (f8:63:3f:59:24:c8), Dst: Sercomm_f7:d3:40 (38:02:de:f7:d3:40)

> Destination: Sercomm_f7:d3:40 (38:02:de:f7:d3:40)

> Source: IntelCor_59:24:c8 (f8:63:3f:59:24:c8)

Type: IPv4 (0x0800)

```

0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 08 00 45 00 8...@.c ?Y$.E.
0010 02 40 a5 2e 40 00 80 06 d6 5f c0 a8 01 0c 93 66 .@..@..._.....f
0020 28 0f da cb 00 50 4e 69 ed ba 29 15 89 38 50 10 (...PNI...)..8P
0030 02 00 b7 d9 00 00 47 45 54 20 2f 6c 61 62 32 2f .....GE T /lab2/
0040 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a HTTP/1.1..Host:
0050 20 65 64 75 2d 64 79 2e 63 6e 2e 6e 74 75 61 2e edu-dy. cn.ntua.
0060 67 72 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 gr..Conn ection:
0070 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67 72 keep-ali ve..Upgr
0080 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 ade-Inse cure-Req
0090 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 72 2d 41 uests: 1 ..User-A

```

Πληκτρολογήστε εδώ για αναζήτηση

15°C 1:40 πμ 25/10/2021

1.6 To Type.

Wireshark capture showing TCP connections. The packet list shows several ACKs. The packet details pane shows the IP header for packet 100, highlighting the source IP 192.168.1.12 and the destination IP 78.46.103.41. The packet bytes pane shows the raw data of the packet.

1.7 Τα τελευταία 2 byte (φαίνεται στο στιγμιότυπο οθόνης στο 1.5)

1.8 0800 {IPv4(0x0800)}

1.9 0x0806

Wireshark capture showing an ARP request and response. The packet list shows an ARP request from 192.168.1.12 to 192.168.1.1. The packet details pane shows the ARP header for packet 177, highlighting the source IP 192.168.1.12 and the destination IP 192.168.1.1. The packet bytes pane shows the raw data of the packet.

2

2.1 Το φίλτρο επιτρέπει την απεικόνιση πρωτοκολλών μόνο τύπου ICMP

2.2 4 bytes (όπως πριν)

Wireshark packet capture showing ICMP Echo (ping) requests and replies. The packet list shows several ping requests and replies. The packet details pane shows the Ethernet II and Internet Protocol Version 4 headers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|--------------|--------------|----------|--------|---|
| 279 | 0.000000 | 192.168.1.12 | 1.1.1.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=128/32768, ttl=128 (repl |
| 281 | 0.012735 | 1.1.1.1 | 192.168.1.12 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=128/32768, ttl=59 (reque |
| 306 | 1.004636 | 192.168.1.12 | 1.1.1.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=129/33024, ttl=128 (repl |
| 307 | 0.023952 | 1.1.1.1 | 192.168.1.12 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=129/33024, ttl=59 (reque |
| 322 | 0.982241 | 192.168.1.12 | 1.1.1.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=130/33280, ttl=128 (repl |
| 324 | 0.013366 | 1.1.1.1 | 192.168.1.12 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=130/33280, ttl=59 (reque |
| 346 | 1.001671 | 192.168.1.12 | 1.1.1.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=131/33536, ttl=128 (repl |
| 347 | 0.012525 | 1.1.1.1 | 192.168.1.12 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=131/33536, ttl=59 (reque |

Ethernet II, Src: IntelCor_59:24:c8 (f8:63:3f:59:24:c8), Dst: Sercomm_f7:d3:40 (38:02:de:f7:d3:40)

Internet Protocol Version 4, Src: 192.168.1.12, Dst: 1.1.1.1

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 08 00 45 00 8....@.c ?Y\$...E

0010 00 3c e9 03 00 00 80 01 8e 07 c0 a8 01 0c 01 01 .<.....

0020 01 01 08 00 4c db 00 01 00 80 61 62 63 64 65 66L... ..abcdef

0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv

0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

Ethernet (eth), 14 byte(s) | Packets: 404 · Displayed: 8 (2.0%) · Dropped: 0 (0.0%) | Profile: Default

2.3 Version, Header Length

Wireshark packet capture showing ICMP Echo (ping) requests and replies. The packet list shows several ping requests and replies. The packet details pane shows the Ethernet II and Internet Protocol Version 4 headers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|--------------|--------------|----------|--------|---|
| 279 | 0.000000 | 192.168.1.12 | 1.1.1.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=128/32768, ttl=128 |
| 281 | 0.012735 | 1.1.1.1 | 192.168.1.12 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=128/32768, ttl=59 |
| 306 | 1.004636 | 192.168.1.12 | 1.1.1.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=129/33024, ttl=128 |
| 307 | 0.023952 | 1.1.1.1 | 192.168.1.12 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=129/33024, ttl=59 |
| 322 | 0.982241 | 192.168.1.12 | 1.1.1.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=130/33280, ttl=128 |
| 324 | 0.013366 | 1.1.1.1 | 192.168.1.12 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=130/33280, ttl=59 |
| 346 | 1.001671 | 192.168.1.12 | 1.1.1.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=131/33536, ttl=128 |
| 347 | 0.012525 | 1.1.1.1 | 192.168.1.12 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=131/33536, ttl=59 |

Ethernet II, Src: IntelCor_59:24:c8 (f8:63:3f:59:24:c8), Dst: Sercomm_f7:d3:40 (38:02:de:f7:d3:40)

Internet Protocol Version 4, Src: 192.168.1.12, Dst: 1.1.1.1

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 08 00 45 00 8....@.c ?Y\$...E

0010 00 3c e9 03 00 00 80 01 8e 07 c0 a8 01 0c 01 01 .<.....

0020 01 01 08 00 4c db 00 01 00 80 61 62 63 64 65 66L... ..abcdef

0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv

0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

Πληκτρολογήστε εδώ για αναζήτηση

15°C 2:44 πμ 25/10/2021

2.4 0b0100 και 0b0101 για το Version και Header Length αντιστοιχα.

2.5 20 bytes

Wireshark packet capture showing ICMP Echo (ping) requests and replies. The packet list shows 8 packets (279-347). The packet details pane shows Ethernet II and Internet Protocol Version 4. The packet bytes pane shows the raw data in hexadecimal and ASCII.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|--------------|--------------|----------|--------|--|
| 279 | 0.000000 | 192.168.1.12 | 1.1.1.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=128/32768, ttl=128 (reply expected) |
| 281 | 0.012735 | 1.1.1.1 | 192.168.1.12 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=128/32768, ttl=59 (request received) |
| 306 | 1.004636 | 192.168.1.12 | 1.1.1.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=129/33024, ttl=128 (reply expected) |
| 307 | 0.023952 | 1.1.1.1 | 192.168.1.12 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=129/33024, ttl=59 (request received) |
| 322 | 0.982241 | 192.168.1.12 | 1.1.1.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=130/33280, ttl=128 (reply expected) |
| 324 | 0.013366 | 1.1.1.1 | 192.168.1.12 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=130/33280, ttl=59 (request received) |
| 346 | 1.001671 | 192.168.1.12 | 1.1.1.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=131/33536, ttl=128 (reply expected) |
| 347 | 0.012525 | 1.1.1.1 | 192.168.1.12 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=131/33536, ttl=59 (request received) |

Internet Protocol Version 4 (ip), 20 byte(s) | Packets: 404 · Displayed: 8 (2.0%) · Dropped: 0 (0.0%) | Profile: Default

2.6 Η τιμή του αντίστοιχου πεδίου της επικεφαλίδας IPv4 είναι 5, αν το πολ/με επι 4 είναι το συνολικό μήκος της επικεφαλίδας (ή τα μετράμε και με το ματι)

2.7 74 bytes ή 592bits

Wireshark packet capture showing ICMP Echo (ping) requests and replies. The packet list shows 8 packets (279-347). The packet details pane shows Ethernet II and Internet Protocol Version 4. The packet bytes pane shows the raw data in hexadecimal and ASCII.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|--------------|--------------|----------|--------|--|
| 279 | 0.000000 | 192.168.1.12 | 1.1.1.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=128/32768, ttl=128 (reply expected) |
| 281 | 0.012735 | 1.1.1.1 | 192.168.1.12 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=128/32768, ttl=59 (request received) |
| 306 | 1.004636 | 192.168.1.12 | 1.1.1.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=129/33024, ttl=128 (reply expected) |
| 307 | 0.023952 | 1.1.1.1 | 192.168.1.12 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=129/33024, ttl=59 (request received) |
| 322 | 0.982241 | 192.168.1.12 | 1.1.1.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=130/33280, ttl=128 (reply expected) |
| 324 | 0.013366 | 1.1.1.1 | 192.168.1.12 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=130/33280, ttl=59 (request received) |
| 346 | 1.001671 | 192.168.1.12 | 1.1.1.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=131/33536, ttl=128 (reply expected) |
| 347 | 0.012525 | 1.1.1.1 | 192.168.1.12 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=131/33536, ttl=59 (request received) |

Frame 279: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{11981F20-5231-4861-ABD2-DD8A4A767C} (ethernet) | 0 bytes captured on the interface (0 bits) | 0 bytes filtered (0 bits) | 0 bytes dropped (0 bits) | 0 bytes captured on the interface (0 bits) | 0 bytes filtered (0 bits) | 0 bytes dropped (0 bits) | 0 bytes captured on the interface (0 bits) | 0 bytes filtered (0 bits) | 0 bytes dropped (0 bits)

Internet Protocol Version 4 (ip), 20 byte(s) | Packets: 404 · Displayed: 8 (2.0%) · Dropped: 0 (0.0%) | Profile: Default

2.8 Ναι υπάρχει, αυτό με την ονομασία «Length», και συμφωνεί, καθώς γραφεί 74

2.9 54bytes

2.10 $74 - 20 = 54$ bytes (συνολικό μήκος – μήκος επικεφαλίδας)

2.11 Το πεδίο με ονομασία “Protocol”

2.12 Στο 10^ο byte της επικεφαλίδας

2.13 0x01

*Wi-Fi (ether host F8-63-3F-59-24-C8)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|--------------|--------------|----------|--------|---|
| 279 | 0.000000 | 192.168.1.12 | 1.1.1.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=128/32768, ttl=128 |
| 281 | 0.012735 | 1.1.1.1 | 192.168.1.12 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=128/32768, ttl=59 |
| 306 | 1.004636 | 192.168.1.12 | 1.1.1.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=129/33024, ttl=128 |
| 307 | 0.023952 | 1.1.1.1 | 192.168.1.12 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=129/33024, ttl=59 |
| 322 | 0.982241 | 192.168.1.12 | 1.1.1.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=130/33280, ttl=128 |
| 324 | 0.013366 | 1.1.1.1 | 192.168.1.12 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=130/33280, ttl=59 |
| 346 | 1.001671 | 192.168.1.12 | 1.1.1.1 | ICMP | 74 | Echo (ping) request id=0x0001, seq=131/33536, ttl=128 |
| 347 | 0.012525 | 1.1.1.1 | 192.168.1.12 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=131/33536, ttl=59 |

> Flags: 0x00
 Fragment Offset: 0
 Time to Live: 128
 Protocol: ICMP (1)
 Header Checksum: 0x8e07 [validation disabled]

```

0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 08 00 45 00 8 . . . @ . c ? Y $ . . . E .
0010 00 3c e9 03 00 00 80 01 8e 07 c0 a8 01 0c 01 01 - < . . . . .
0020 01 01 08 00 4c db 00 01 00 80 61 62 63 64 65 66 . . . L . . . a b c d e f
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 g h i j k l m n o p q r s t u v
0040 77 61 62 63 64 65 66 67 68 69 w a b c d e f g h i

```

Πληκτρολογήστε εδώ για αναζήτηση

15°C 3:11 πμ 25/10/2021

3

3.1 Κρατάει μόνο το σύνολο των πακέτων που είναι πρωτόκολλου UDP και εκείνα που στην επικεφαλίδα έχουν TCP type.

3.2 UDP, TCP, DNS, TLSv1.2, HTTP

3.3 Για το UDP: 17 ή 0x11

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-----------------|-----------------|----------|--------|----------------------|
| 40 | 0.198677 | 192.168.1.12 | 142.250.185.206 | UDP | 1388 | 63091 → 443 Len=1346 |
| 41 | 0.000640 | 192.168.1.12 | 142.250.185.206 | UDP | 212 | 63091 → 443 Len=170 |
| 44 | 0.035974 | 142.250.185.206 | 192.168.1.12 | UDP | 69 | 443 → 63091 Len=27 |
| 45 | 0.026658 | 142.250.185.206 | 192.168.1.12 | UDP | 67 | 443 → 63091 Len=25 |
| 46 | 0.000338 | 192.168.1.12 | 142.250.185.206 | UDP | 75 | 63091 → 443 Len=33 |
| 47 | 0.019842 | 142.250.185.206 | 192.168.1.12 | UDP | 618 | 443 → 63091 Len=576 |
| 48 | 0.000000 | 142.250.185.206 | 192.168.1.12 | UDP | 76 | 443 → 63091 Len=34 |
| 49 | 0.000000 | 142.250.185.206 | 192.168.1.12 | UDP | 177 | 443 → 63091 Len=135 |

> Flags: 0x40, Don't fragment
Fragment Offset: 0
Time to Live: 128
Protocol: UDP (17)
Header Checksum: 0x5c13 [validation disabled]

0010 05 5e 8e fe 40 00 80 11 5c 13 c0 a8 01 0c 8e fa .^..@.. \.....
0020 b9 ce f6 73 01 bb 05 4a 5a 27 57 40 a1 ec 59 56 ...s...J Z'W@..YV
0030 74 bd ea 80 04 25 ea 0c 1c 97 15 57 90 be ad 3f t...%...W...?
0040 f6 ea 65 6f fe 30 bf 2f 68 dc 35 0f 3b 76 d5 66 ..eo-0/ h-5;v-f
0050 da 3e 27 6e a4 b9 91 41 8e 85 c5 84 24 9f dd 36 ->'n...A...\$-6
0060 97 e8 6c 2d 2c 26 3c 80 22 d4 69 e3 a2 51 1a 86 ..l-,&< "i Q..
0070 2f 55 84 2c 7f 37 22 56 93 9b d2 a9 42 8e d4 02 /U,7"VB..
0080 96 14 e4 19 f9 6b a9 79 1d 88 98 d2 85 96 da 2ck-y
0090 74 d7 83 8d d2 0b 2c 87 8e ca db d2 6a b3 8b 24 t.....-....j...\$
00a0 b4 31 3c d8 c4 2b 30 67 9e 2d 30 31 03 bb 69 2c -1<...+0g --01-i,

Protocol (ip.proto), 1 byte(s) | Packets: 65 · Displayed: 65 (100.0%) | Profile: Default

Για το TCP: 6 ή 0x06

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-----------------|-----------------|----------|--------|--|
| 16 | 1.006835 | 192.168.1.12 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 2 | 0.301714 | 192.168.1.12 | 142.250.185.174 | TCP | 55 | 54466 → 443 [ACK] Seq=1 Ack=1 Win=509 Len=1 [TCP segme |
| 3 | 0.132837 | 142.250.185.174 | 192.168.1.12 | TCP | 66 | 443 → 54466 [ACK] Seq=1 Ack=2 Win=444 Len=0 SLE=1 SRE= |
| 4 | 0.000000 | 142.250.185.99 | 192.168.1.12 | TCP | 54 | 80 → 54453 [FIN, ACK] Seq=1 Ack=1 Win=262 Len=0 |
| 7 | 0.000172 | 192.168.1.12 | 142.250.185.99 | TCP | 54 | 54453 → 80 [ACK] Seq=1 Ack=2 Win=511 Len=0 |
| 8 | 0.000613 | 192.168.1.12 | 142.250.185.77 | TCP | 54 | 54455 → 443 [FIN, ACK] Seq=1 Ack=74 Win=513 Len=0 |
| 9 | 0.000533 | 192.168.1.12 | 216.58.212.131 | TCP | 54 | 54454 → 443 [FIN, ACK] Seq=1 Ack=74 Win=509 Len=0 |
| 10 | 0.044787 | 142.250.185.77 | 192.168.1.12 | TCP | 54 | 443 → 54455 [FIN, ACK] Seq=74 Ack=2 Win=283 Len=0 |

> Flags: 0x40, Don't fragment
Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0xfa26 [validation disabled]

0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 08 00 45 00 8...@-c ?Y\$...E-
0010 00 29 f6 4a 40 00 80 06 fa 26 c0 a8 01 0c 8e fa .)J@...&.....
0020 b9 ae d4 c2 01 bb b9 08 4c da a4 be 41 26 50 10 L...A&P-
0030 01 fd e1 33 00 00 003...

Protocol (ip.proto), 1 byte(s) | Packets: 65 · Displayed: 65 (100.0%) | Profile: Default

3.4 Src Port και Dst port

3.5 8 bytes.

The image shows a Wireshark packet capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. A display filter bar shows 'Apply a display filter ... <Ctrl-/>'. The packet list pane shows several packets, with packet 40 selected. The packet details pane shows the selected packet's structure: Ethernet II (Type: IPv4), Internet Protocol Version 4, and a selected 8-byte field in the payload. The packet bytes pane shows the raw data in hexadecimal and ASCII.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-----------------|-----------------|----------|--------|----------------------|
| 58 | 6.675622 | 13.69.244.117 | 192.168.1.12 | TLSv1.2 | 353 | Application Data |
| 60 | 0.074200 | 192.168.1.12 | 13.69.244.117 | TLSv1.2 | 226 | Application Data |
| 40 | 0.198677 | 192.168.1.12 | 142.250.185.206 | UDP | 1388 | 63091 → 443 Len=1346 |
| 41 | 0.000640 | 192.168.1.12 | 142.250.185.206 | UDP | 212 | 63091 → 443 Len=170 |
| 44 | 0.035974 | 142.250.185.206 | 192.168.1.12 | UDP | 69 | 443 → 63091 Len=27 |
| 45 | 0.026658 | 142.250.185.206 | 192.168.1.12 | UDP | 67 | 443 → 63091 Len=25 |
| 46 | 0.000338 | 192.168.1.12 | 142.250.185.206 | UDP | 75 | 63091 → 443 Len=33 |
| 47 | 0.019842 | 142.250.185.206 | 192.168.1.12 | UDP | 618 | 443 → 63091 Len=576 |
| 48 | 0.000000 | 142.250.185.206 | 192.168.1.12 | UDP | 76 | 443 → 63091 Len=34 |

Address: IntelCor_59:24:c8 (f8:63:3f:59:24:c8)
0. = LG bit: Globally unique address (factory default)
0. = IG bit: Individual address (unicast)
 Type: IPv4 (0x0800)
 Internet Protocol Version 4, Src: 192.168.1.12, Dst: 142.250.185.206

0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 08 00 45 00 8...@.c ?Y\$.E.
 0010 05 5e 8e fe 40 00 80 11 5c 13 c0 a8 01 0c 8e fa ^...@... \.....
 0020 b9 ce f6 73 01 bb 05 4a 5a 27 57 40 a1 ec 59 56 ...s...J Z'W@..YV
 0030 74 bd ea 80 04 25 ea 0c 1c 97 15 57 90 be ad 3f t...%...W...?
 0040 f6 ea 65 6f fe 30 bf 2f 68 dc 35 0f 3b 76 d5 66 ..eo.0./ h.5;v.f
 0050 da 3e 27 6e a4 b9 91 41 8e 85 c5 84 24 9f dd 36 ->'n...A\$.6
 0060 97 e8 6c 2d 2c 26 3c 80 22 d4 69 e3 a2 51 1a 86 ..l-,&< ".i.Q..
 0070 2f 55 84 2c 7f 37 22 56 93 9b d2 a9 42 8e d4 02 /U.,.7"V ...B...

Type (eth.type), 2 byte(s) | Packets: 65 · Displayed: 65 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

3.6 Ναι, υπάρχει (φαίνεται στο παραπάνω στιγμιότυπο οθόνης).

3.7 Το βρίσκουμε στο 13^ο byte της επικεφαλίδας

3.8 Αντίστοιχο πεδίο δεν υπάρχει. Το συνολικό μήκος προκύπτει από άθροισμα των IPv4 Header Length και TCP Header Length

3.9 Το Destination Port.

3.10 SSDP, ICMPv6, ARP

4

4.1 Το UDP.

4.2 Το TCP.

4.3 Το καθορίζει το 1^ο bit του flag (σημειας) και έχει τιμή 0 όταν είναι query και 1 όταν είναι response.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http or dns

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|------------------------|------------------------|----------|--------|--|
| 21 | 0.000000 | fe80::7dce:53ff:b0e... | fe80::1 | DNS | 97 | Standard query 0x6b49 A edu-dy.cn.ntua.gr |
| 25 | 0.010024 | fe80::1 | fe80::7dce:53ff:b0e... | DNS | 148 | Standard query response 0x6b49 A edu-dy.cn.ntua.gr CNAME edu |
| 33 | 0.015033 | 192.168.1.12 | 147.102.40.15 | HTTP | 56 | GET /lab2/ HTTP/1.1 |
| 35 | 0.012061 | 147.102.40.15 | 192.168.1.12 | HTTP | 287 | HTTP/1.1 304 Not Modified |

Domain Name System (query)
Transaction ID: 0x6b49
Flags: 0x0100 Standard query
0... .. = Response: Message is a query
.000 0... .. = Opcode: Standard query (0)

```

0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 86 dd 60 01 8...@.c ?Y$...
0010 6a 4d 00 2b 11 ff fe 80 00 00 00 00 00 7d ce jM.+...
0020 53 ff b0 ed 7b 06 fe 80 00 00 00 00 00 00 00 S...{...
0030 00 00 00 00 00 01 da c7 00 35 00 2b 05 85 6b 49 .....5...kI
0040 01 00 00 01 00 00 00 00 00 00 06 65 64 75 2d 64 ..edu-d
0050 79 02 63 6e 04 6e 74 75 61 02 67 72 00 00 01 00 y.cn.ntu a.gr...
0060 01

```

Is the message a response? (dns.flags.response), 2 byte(s) | Packets: 65 · Displayed: 4 (6.2%) | Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http or dns

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|------------------------|------------------------|----------|--------|--|
| 21 | 0.000000 | fe80::7dce:53ff:b0e... | fe80::1 | DNS | 97 | Standard query 0x6b49 A edu-dy.cn.ntua.gr |
| 25 | 0.010024 | fe80::1 | fe80::7dce:53ff:b0e... | DNS | 148 | Standard query response 0x6b49 A edu-dy.cn.ntua.gr CNAME edu |
| 33 | 0.015033 | 192.168.1.12 | 147.102.40.15 | HTTP | 56 | GET /lab2/ HTTP/1.1 |
| 35 | 0.012061 | 147.102.40.15 | 192.168.1.12 | HTTP | 287 | HTTP/1.1 304 Not Modified |

Domain Name System (response)
Transaction ID: 0x6b49
Flags: 0x8180 Standard query response, No error
1... .. = Response: Message is a response
.000 0... .. = Opcode: Standard query (0)

```

0010 00 00 00 5e 11 ff fe 80 00 00 00 00 00 00 00 ...^...
0020 00 00 00 00 00 01 fe 80 00 00 00 00 00 7d ce .....}..
0030 53 ff b0 ed 7b 06 00 35 da c7 00 5e 6e 75 6b 49 S...{..5 ...^nukI
0040 81 80 00 01 00 02 00 00 00 00 06 65 64 75 2d 64 ..edu-d
0050 79 02 63 6e 04 6e 74 75 61 02 67 72 00 00 01 00 y.cn.ntu a.gr...
0060 01 c0 0c 00 05 00 01 00 00 03 bb 00 17 06 65 64 .....ed
0070 75 2d 64 79 02 63 6e 03 65 63 65 04 6e 74 75 61 u-dy.cn. ece ntua
0080 02 47 52 00 c0 2f 00 01 00 01 00 00 03 bb 00 04 .GR../.
0090 93 66 28 0f .f(

```

Is the message a response? (dns.flags.response), 2 byte(s) | Packets: 65 · Displayed: 4 (6.2%) | Profile: Default

4.4 56007

4.5 53

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http or dns

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|------------------------|------------------------|----------|--------|--|
| 21 | 0.000000 | fe80::7dce:53ff:b0e... | fe80::1 | DNS | 97 | Standard query 0x6b49 A edu-dy.cn.ntua.gr |
| 25 | 0.010024 | fe80::1 | fe80::7dce:53ff:b0e... | DNS | 148 | Standard query response 0x6b49 A edu-dy.cn.ntua.gr CNAME edu |
| 33 | 0.015033 | 192.168.1.12 | 147.102.40.15 | HTTP | 56 | GET /lab2/ HTTP/1.1 |
| 35 | 0.012061 | 147.102.40.15 | 192.168.1.12 | HTTP | 287 | HTTP/1.1 304 Not Modified |

User Datagram Protocol, Src Port: 56007, Dst Port: 53

Source Port: 56007
Destination Port: 53
Length: 43
Checksum: 0x0585 [unverified]

```

0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 86 dd 60 01 8....@.c ?Y$...
0010 6a 4d 00 2b 11 ff fe 80 00 00 00 00 00 7d ce jM.+...
0020 53 ff b0 ed 7b 06 fe 80 00 00 00 00 00 00 00 S...{...
0030 00 00 00 00 00 01 da c7 00 35 00 2b 05 85 6b 49 .....5...kI
0040 01 00 00 01 00 00 00 00 00 00 65 64 75 2d 64 .....edu-d
0050 79 02 63 6e 04 6e 74 75 61 02 67 72 00 00 01 00 y.cn.ntu a.gr...
0060 01
  
```

User Datagram Protocol (udp), 8 byte(s) | Packets: 65 · Displayed: 4 (6.2%) | Profile: Default

4.6 53

4.7 56007

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http or dns

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|------------------------|------------------------|----------|--------|--|
| 21 | 0.000000 | fe80::7dce:53ff:b0e... | fe80::1 | DNS | 97 | Standard query 0x6b49 A edu-dy.cn.ntua.gr |
| 25 | 0.010024 | fe80::1 | fe80::7dce:53ff:b0e... | DNS | 148 | Standard query response 0x6b49 A edu-dy.cn.ntua.gr CNAME edu |
| 33 | 0.015033 | 192.168.1.12 | 147.102.40.15 | HTTP | 56 | GET /lab2/ HTTP/1.1 |
| 35 | 0.012061 | 147.102.40.15 | 192.168.1.12 | HTTP | 287 | HTTP/1.1 304 Not Modified |

User Datagram Protocol, Src Port: 56007, Dst Port: 53

Source Port: 56007
Destination Port: 53
Length: 43
Checksum: 0x0585 [unverified]

```

0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 86 dd 60 01 8....@.c ?Y$...
0010 6a 4d 00 2b 11 ff fe 80 00 00 00 00 00 7d ce jM.+...
0020 53 ff b0 ed 7b 06 fe 80 00 00 00 00 00 00 00 S...{...
0030 00 00 00 00 00 01 da c7 00 35 00 2b 05 85 6b 49 .....5...kI
0040 01 00 00 01 00 00 00 00 00 00 65 64 75 2d 64 .....edu-d
0050 79 02 63 6e 04 6e 74 75 61 02 67 72 00 00 01 00 y.cn.ntu a.gr...
0060 01
  
```

User Datagram Protocol (udp), 8 byte(s) | Packets: 65 · Displayed: 4 (6.2%) | Profile: Default

4.8 Είναι οι ίδιες.

4.9 Η θύρα 53

4.10 Η θύρα 80 (Destination)

4.11 Η 54654 (Source)

The screenshot shows a Wireshark capture of network traffic. The packet list pane displays the following packets:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|------------------------|------------------------|----------|--------|---|
| 21 | 0.000000 | fe80::7dce:53ff:b0e... | fe80::1 | DNS | 97 | Standard query 0x6b49 A edu-dy.cn.ntua.gr |
| 25 | 0.010024 | fe80::1 | fe80::7dce:53ff:b0e... | DNS | 148 | Standard query response 0x6b49 A edu-dy.cn.ntua.gr CNAME ed |
| 33 | 0.015033 | 192.168.1.12 | 147.102.40.15 | HTTP | 56 | GET /lab2/ HTTP/1.1 |
| 35 | 0.012061 | 147.102.40.15 | 192.168.1.12 | HTTP | 287 | HTTP/1.1 304 Not Modified |

The packet details pane for packet 33 shows:

- Internet Protocol Version 4, Src: 192.168.1.12, Dst: 147.102.40.15
- Transmission Control Protocol, Src Port: 54654, Dst Port: 80, Seq: 537, Ack: 1, Len: 2
- Source Port: 54654
- Destination Port: 80
- Stream index: 71

The packet bytes pane shows the raw data of the HTTP GET request.

4.12 Η θύρα 80 (Source)

4.13 Η 54654 (Destination)

The screenshot shows a Wireshark capture of network traffic. The packet list pane displays the following packets:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|------------------------|------------------------|----------|--------|---|
| 21 | 0.000000 | fe80::7dce:53ff:b0e... | fe80::1 | DNS | 97 | Standard query 0x6b49 A edu-dy.cn.ntua.gr |
| 25 | 0.010024 | fe80::1 | fe80::7dce:53ff:b0e... | DNS | 148 | Standard query response 0x6b49 A edu-dy.cn.ntua.gr CNAME ed |
| 33 | 0.015033 | 192.168.1.12 | 147.102.40.15 | HTTP | 56 | GET /lab2/ HTTP/1.1 |
| 35 | 0.012061 | 147.102.40.15 | 192.168.1.12 | HTTP | 287 | HTTP/1.1 304 Not Modified |

The packet details pane for packet 35 shows:

- Internet Protocol Version 4, Src: 147.102.40.15, Dst: 192.168.1.12
- Transmission Control Protocol, Src Port: 80, Dst Port: 54654, Seq: 1, Ack: 539, Len: 233
- Source Port: 80
- Destination Port: 54654
- Stream index: 71

The packet bytes pane shows the raw data of the HTTP 304 Not Modified response.

4.14 Η θύρα 80

4.15 Είναι οι ίδες θύρες

4.16 GET /lab2/ HTTP/1.1

4.17 HTTP/1.1 304 Not Modified

The image shows a Wireshark packet capture window. The main pane displays the details of a selected packet, which is an HTTP 304 Not Modified response. The request headers are shown in red text, and the response headers are in blue text. The status bar at the bottom indicates '2 client pkt(s), 1 server pkt(s), 1 turn(s)'. The packet list pane shows 'Entire conversation (771 bytes)'. The packet details pane shows 'Show data as ASCII'. The packet bytes pane shows 'Stream 7'. The packet list pane shows 'Find:'. The packet details pane shows 'Find Next'. The packet bytes pane shows '15°C'.

```
GET /lab2/ HTTP/1.1
Host: edu-dy.cn.ntua.gr
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: el,en;q=0.9,fr;q=0.8
If-None-Match: "18afa1-92-5cedc86f6c700"
If-Modified-Since: Thu, 21 Oct 2021 13:03:56 GMT

HTTP/1.1 304 Not Modified
Date: Sat, 23 Oct 2021 17:57:29 GMT
Server: Apache/2.2.22 (FreeBSD) mod_ssl/2.2.22 OpenSSL/0.9.8zh-freebsd DAV/2
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
ETag: "18afa1-92-5cedc86f6c700"
```

2 client pkt(s), 1 server pkt(s), 1 turn(s).

Entire conversation (771 bytes) Show data as ASCII Stream 7

Find: Find Next

15°C

4.18 Με την εντολή `ipconfig /flushdns` καθαρίζουμε την DNS cache. Την 1η φορά που επισκεπτόμαστε μια ιστοσελίδα να μην χρειάζεται η διαδικασία να γίνουν DNS queries πριν τη λήψη του πακέτου GET, αλλά θα χρειαστεί μόνο μία φορά και τις υπόλοιπες φορές δεν θα χρειαστεί γιατί το αποτέλεσμα θα υπάρχει αποθηκευμένο στη μνήμη cache. Η εντολή χρειαζόταν για να δούμε αυτή τη μοναδική φορά που θα συμβεί, τι περιέχουν τα πακέτα, τι ερωτήσεις κάνουν και σε ποιες διευθύνσεις και θύρες κάνουν ερωτήσεις κλπ