

Όνοματεπώνυμο: Άγγελος Μητροκώτσας		Ομάδα:6
Όνομα PC/ΛΣ: DESKTOP-91G20CF/ Windows 10 Pro 20H2	Ημερομηνία: 31 /10/ 2021	
Διεύθυνση IP: 192.168.1.12	Διεύθυνση MAC: F8-63-3F-59-24-C8	

Εργαστηριακή Άσκηση 3

Επικοινωνία στο τοπικό δίκτυο (πλαίσιο Ethernet και πρωτόκολλο ARP)

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

Άσκηση 1

1.1 Η εντολή arp -a

1.2 Με την εντολή arp -d *

1.3 Με την εντολή ipconfig /all,

IPv4 Address. : 192.168.1.12(Preferred)

DNS Servers : fe80::1%3

192.168.1.1

192.168.1.1

```
C:\Windows\system32>ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-91G20CF
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : home

Wireless LAN adapter Τοπική σύνδεση* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : F8-63-3F-59-24-C9
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Τοπική σύνδεση* 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address. . . . . : FA-63-3F-59-24-C8
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : home
Description . . . . . : Intel(R) Dual Band Wireless-AC 8265
Physical Address. . . . . : F8-63-3F-59-24-C8
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Temporary IPv6 Address. . . . . : 2a02:587:2103:db95:bd93:2779:92af:f3a4(Preferred)
Temporary IPv6 Address. . . . . : 2a02:587:2103:db95:fd28:957f:56f7:3fbb(Preferred)
Link-local IPv6 Address . . . . . : fe80::c161:5c8:9f00:b45b%3(Preferred)
IPv4 Address. . . . . : 192.168.1.12(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Σάββατο, 30 Οκτωβρίου 2021 3:49:12 μμ
Lease Expires . . . . . : Δευτέρα, 1 Νοεμβρίου 2021 1:06:48 μμ
Default Gateway . . . . . : fe80::1%3
                          192.168.1.1
```

```

DNS Suffix Search List. . . . . : home

Wireless LAN adapter Τοπική σύνδεση* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . : 
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : F8-63-3F-59-24-C9
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Τοπική σύνδεση* 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . : 
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address. . . . . : FA-63-3F-59-24-C8
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . . : home
Description . . . . . : Intel(R) Dual Band Wireless-AC 8265
Physical Address. . . . . : F8-63-3F-59-24-C8
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Temporary IPv6 Address. . . . . : 2a02:587:2103:db95:bd93:2779:92af:f3a4(Preferred)
Temporary IPv6 Address. . . . . : 2a02:587:2103:db95:fd28:957f:56f7:3fbb(Preferred)
Link-local IPv6 Address . . . . . : fe80::c161:5c8:9f00:b45b%3(Preferred)
IPv4 Address. . . . . : 192.168.1.12(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Σάββατο, 30 Οκτωβρίου 2021 3:49:12 μμ
Lease Expires . . . . . : Δευτέρα, 1 Νοεμβρίου 2021 1:06:48 μμ
Default Gateway . . . . . : fe80::1%3
                          192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 66609983
DHCPv6 Client DUID. . . . . : 00-01-00-01-27-47-6E-E2-F8-63-3F-59-24-C8
DNS Servers . . . . . : fe80::1%3
                          192.168.1.1
                          192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled

C:\Windows\system32>

```

1.4

```

C:\Windows\system32>arp -a

Interface: 192.168.1.12 --- 0x3
Internet Address      Physical Address      Type
192.168.1.1           38-02-de-f7-d3-40     dynamic
192.168.1.255         ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Windows\system32>

```

1.5 Τα DNS resolves εκτελούνται από την προκαθορισμένη πύλη. Υπάρχει η διεύθυνση της προκαθορισμένης πύλης (default gateway) και όχι του DNS εξυπηρετητή (όπως φαίνεται στο αποτέλεσμα της `ipconfig /all` πανω, ταντιζονται οι 2 διευθύνσεις).

1.6 `C:\Windows\system32>arp -d *`

`C:\Windows\system32>ping 192.168.1.1`

Pinging 192.168.1.1 with 32 bytes of data:

```
Reply from 192.168.1.1: bytes=32 time=4ms TTL=64
Reply from 192.168.1.1: bytes=32 time=4ms TTL=64
Reply from 192.168.1.1: bytes=32 time=6ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
```

Ping statistics for 192.168.1.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 2ms, Maximum = 6ms, Average = 4ms

1.7 C:\Windows\system32>arp -a

Interface: 192.168.1.12 --- 0x3

Internet Address	Physical Address	Type
192.168.1.1	38-02-de-f7-d3-40	dynamic
224.0.0.22	01-00-5e-00-00-16	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

Παρατηρώ ότι υπάρχουν λιγότερες διευθύνσεις στον πίνακα

1.8

C:\Windows\system32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Windows\system32>arp -d *

C:\Windows\system32>arp -a

Interface: 192.168.1.12 --- 0x3

Internet Address	Physical Address	Type
192.168.1.1	38-02-de-f7-d3-40	dynamic
224.0.0.22	01-00-5e-00-00-16	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

1.9 Όχι, είναι σε διαφορετικό υποδίκτυο

Άσκηση 2

2.1 Το πεδία Source, Destination και Type

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip or ipv6 or arp

No.	Time	Source	Destination	Protocol	Length	Info
557	0.008854	Sercomm_f7:d3:40	Broadcast	ARP	42	Who has 192.168.1.6? Tell 192.168.1.1
689	0.001861	Sercomm_f7:d3:40	Broadcast	ARP	42	Who has 192.168.1.8? Tell 192.168.1.1
745	0.000368	Sercomm_f7:d3:40	Broadcast	ARP	42	Who has 192.168.1.9? Tell 192.168.1.1
1435	0.011241	Sercomm_f7:d3:40	Broadcast	ARP	42	Who has 192.168.1.12? Tell 192.168.1.1
1436	0.000025	IntelCor_59:24:c8	Sercomm_f7:d3:40	ARP	42	192.168.1.12 is at f8:63:3f:59:24:c8
1359	0.014252	fe80::c161:5c8:9f00...	fe80::1	DNS	97	Standard query 0xda96 AAAA edu-dy.cn.ntua.gr
1363	0.012764	192.168.1.12	192.168.1.1	DNS	77	Standard query 0xda96 AAAA edu-dy.cn.ntua.gr
1375	0.008140	192.168.1.1	192.168.1.12	DNS	176	Standard query response 0xda96 Refused AAAA eDu-Dy.cn.

Ethernet II, Src: Sercomm_f7:d3:40 (38:02:de:f7:d3:40), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

- Destination: Broadcast (ff:ff:ff:ff:ff:ff)
- Source: Sercomm_f7:d3:40 (38:02:de:f7:d3:40)
- Type: ARP (0x0806)
- Address Resolution Protocol (request)

```

0000  ff ff ff ff ff ff 38 02 de f7 d3 40 08 06 00 01  .....8.  ...@...
0010  08 00 06 04 00 01 38 02 de f7 d3 40 c0 a8 01 01  .....8.  ...@...
0020  00 00 00 00 00 00 c0 a8 01 09  .....
  
```

Ethernet (eth), 14 byte(s) | Packets: 1750 · Displayed: 1750 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

80 00 20 7A 3F 3E
Destination MAC Address

80 00 20 20 3A AE
Source MAC Address

08 00
EtherType

IP, ARP, etc.
Payload

00 20 20 3A
CRC Checksum

MAC Header
(14 bytes)

Data
(46 - 1500 bytes)

Ethernet Type II Frame
(64 to 1518 bytes)

2.2 Το προοίμιο δεν καταγραφεται από το wireshark γιατί δεν είναι μέρος του πλαισίου ethernet. (Τα πρώτα 56 bit του προοιμίου είναι εναλλαγές του 1 και του 0 για να επιτευχθεί συγχρονισμός. Χρησιμοποιούν ώστε τα ηλεκτρονικά στοιχεία να προλάβουν να ανιχνεύσουν την ύπαρξη σήματος και να αρχίσουν να διαβάζουν προτού αρχίσει η μετάδοση του πλαισίου. Τα επόμενα 8 bit είναι και υποδεικνύουν την αρχή του πλαισίου)

2.3 Το wireshark δεν μπορεί να καταγραφει πακέτα τύπου CRC. Γι' αυτό ευθύνεται το λειτουργικό μας σύστημα καθώς και οι βιβλιοθήκες που χρησιμοποιεί η εφαρμογή, οι οποίες χρειάζονται μετατροπές για να το πετύχουν

2.4 0x0800

2.5 0x0806

2.6 0x86dd

2.7 f8:63:3f:59:24:c8

2.8 38:02:de:f7:d3:40

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip or ipv6 or arp

No.	Time	Source	Destination	Protocol	Length	Info
1398	0.006188	192.168.1.1	192.168.1.12	DNS	176	Standard query response 0xda96 Refused AAAA Edu-Dy.CN.
1406	0.000479	192.168.1.12	147.102.40.15	HTTP	499	GET /lab3 HTTP/1.1
1409	0.015767	147.102.40.15	192.168.1.12	HTTP	69	[TCP Previous segment not captured] Continuation
1414	0.004682	192.168.1.12	147.102.40.15	HTTP	500	GET /lab3/ HTTP/1.1
1416	0.005974	147.102.40.15	192.168.1.12	HTTP	536	HTTP/1.1 200 OK (text/html)
1425	0.002582	192.168.1.12	147.102.40.15	HTTP	446	GET /favicon.ico HTTP/1.1
1431	0.000000	147.102.40.15	192.168.1.12	HTTP	281	HTTP/1.1 200 OK (image/x-icon)
343	0.005156	fe80::1	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::1 (rtr, ovr) is at 38:02:

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)

Internet Protocol Version 4, Src: 192.168.1.12, Dst: 147.102.40.15

Offset	Time	Source	Destination	Protocol	Length	Info
0000	38 02 de f7 d3 40 f8 63	3f 59 24 c8 08 00 45 00	8...	@.c ?Y\$...E.		
0010	01 e5 e2 69 40 00 80 06	99 7f c0 a8 01 0c 93 66	...	i@... ..f		
0020	28 0f cd 20 00 50 11 73	b8 ab 0c 56 49 b1 50 18	(..	.P.s ...VI.P.		
0030	02 00 4b 8f 00 00 47 45	54 20 2f 6c 61 62 33 20	..K...	GE T /lab3		
0040	48 54 54 50 2f 31 2e 31	0d 0a 48 6f 73 74 3a 20	HTTP/1.1	..Host:		
0050	65 64 75 2d 64 79 2e 63	6e 2e 6e 74 75 61 2e 67	edu-dy.c	n.ntua.g		
0060	72 0d 0a 43 6f 6e 6e 65	63 74 69 6f 6e 3a 20 6b	r..Conne	ction: k		
0070	65 65 70 2d 61 6c 69 76	65 0d 0a 55 70 67 72 61	ee-p-aliv	e..Upgra		
0080	64 65 2d 49 6e 73 65 63	75 72 65 2d 52 65 71 75	de-Insec	ure-Requ		
0090	65 73 74 73 3a 20 31 0d	0a 55 73 65 72 2d 41 67	ests: 1.	..User-Ag		

Ethernet (eth), 14 byte(s) | Packets: 1750 · Displayed: 1750 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

2.9 Όχι

2.10 Η διεύθυνση αυτού του ιστότοπου είναι σε διαφορετικό δίκτυο από το τοπικό μου δίκτυο. Η παραπάνω MAC διεύθυνση ανήκει στην προκαθορισμένη πύλη (default gateway), γιατί μέσω αυτής στέλνονται τα πακέτα και γίνεται η επικοινωνία.

2.11 499 bytes

Wireshark · Packet 1406 · Wi-Fi

Arrival Time: Oct 31, 2021 15:21:16.566717000 Χειμερινή ώρα GTB

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1635686476.566717000 seconds

[Time delta from previous captured frame: 0.000479000 seconds]

[Time delta from previous displayed frame: 0.000479000 seconds]

[Time since reference or first frame: 12.428359000 seconds]

Frame Number: 1406

Frame Length: 499 bytes (3992 bits)

Capture Length: 499 bytes (3992 bits)

[Frame is marked: False]

Offset	Time	Source	Destination	Protocol	Length	Info
0000	38 02 de f7 d3 40 f8 63	3f 59 24 c8 08 00 45 00	8...	@.c ?Y\$...E.		
0010	01 e5 e2 69 40 00 80 06	99 7f c0 a8 01 0c 93 66	...	i@... ..f		
0020	28 0f cd 20 00 50 11 73	b8 ab 0c 56 49 b1 50 18	(..	.P.s ...VI.P.		
0030	02 00 4b 8f 00 00 47 45	54 20 2f 6c 61 62 33 20	..K...	GE T /lab3		
0040	48 54 54 50 2f 31 2e 31	0d 0a 48 6f 73 74 3a 20	HTTP/1.1	..Host:		
0050	65 64 75 2d 64 79 2e 63	6e 2e 6e 74 75 61 2e 67	edu-dy.c	n.ntua.g		
0060	72 0d 0a 43 6f 6e 6e 65	63 74 69 6f 6e 3a 20 6b	r..Conne	ction: k		
0070	65 65 70 2d 61 6c 69 76	65 0d 0a 55 70 67 72 61	ee-p-aliv	e..Upgra		
0080	64 65 2d 49 6e 73 65 63	75 72 65 2d 52 65 71 75	de-Insec	ure-Requ		
0090	65 73 74 73 3a 20 31 0d	0a 55 73 65 72 2d 41 67	ests: 1.	..User-Ag		
00a0	65 6e 74 3a 20 4d 6f 7a	69 6c 6c 61 2f 35 2e 30	ent: Moz	illa/5.0		
00b0	20 28 57 69 6e 64 6f 77	73 20 4e 54 20 31 30 2e	(Window	s NT 10.		
00c0	30 3b 20 57 69 6e 36 34	3b 20 78 36 34 29 20 41	0; Win64	; x64) A		
00d0	70 70 6c 65 57 65 62 4b	69 74 2f 35 33 37 2e 33	ppleWebK	it/537.3		

Close Help

Πληκτρολογήστε εδώ για αναζήτηση

19°C 4:35 μμ 31/10/2021

2.12 499 – TCP payload = 44bytes

Wireshark - Packet 1406 - Wi-Fi

[Window size scaling factor: 256]
Checksum: 0x4b8f [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> [SEQ/ACK analysis]
> [Timestamps]
TCP payload (445 bytes)
> Hypertext Transfer Protocol
> TRANSUM RTE Data

```

0030  02 00 4b 8f 00 00 47 45 54 20 2f 6c 61 62 33 20  ..K...GET /lab3
0040  48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20  HTTP/1.1 ..Host:
0050  65 64 75 2d 64 79 2e 63 6e 2e 6e 74 75 61 2e 67  edu-dy.c n.ntua.g
0060  72 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b  r...Conne ction: k
0070  65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67 72 61  eep-aliv e...Upgra
0080  64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75  de-Insec ure-Requ
0090  65 73 74 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67  ests: 1. .User-Ag
00a0  65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30  ent: Moz illa/5.0
00b0  20 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e  (window s NT 10.
00c0  30 3b 20 57 69 6e 36 34 3b 20 78 36 34 29 20 41  0; Win64 ; x64) A
00d0  70 70 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 33  ppleWebK it/537.3
00e0  36 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 47  6 (KHTML , like G
00f0  65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f 39 35 2e  ecko) Ch rome/95.
0100  30 2e 34 36 33 38 2e 36 39 20 53 61 66 61 72 69  0.4638.6 9 Safari

```

Close Help

Πληκτρολογήστε εδώ για αναζήτηση

19°C 4:35 μμ 31/10/2021

2.13 38:02:de:f7:d3:40

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip or ipv6 or arp

No.	Time	Source	Destination	Protocol	Length	Info
1398	0.006188	192.168.1.1	192.168.1.12	DNS	176	Standard query response 0xda96 Refused AAAA Edu-Dy.CN.
1406	0.000479	192.168.1.12	147.102.40.15	HTTP	499	GET /lab3 HTTP/1.1
1409	0.015767	147.102.40.15	192.168.1.12	HTTP	69	[TCP Previous segment not captured] Continuation
1414	0.004682	192.168.1.12	147.102.40.15	HTTP	500	GET /lab3/ HTTP/1.1
1416	0.005974	147.102.40.15	192.168.1.12	HTTP	536	HTTP/1.1 200 OK (text/html)
1425	0.002582	192.168.1.12	147.102.40.15	HTTP	446	GET /favicon.ico HTTP/1.1
1431	0.000000	147.102.40.15	192.168.1.12	HTTP	281	HTTP/1.1 200 OK (image/x-icon)
343	0.005156	fe80::1	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::1 (rtr, ovr) is at 38:02:

> Frame 1416: 536 bytes on wire (4288 bits), 536 bytes captured (4288 bits) on interface \Device\NPF_{11981F20-5231-4861-ABD2-DD8A4} Ethernet II, Src: Sercomm_f7:d3:40 (38:02:de:f7:d3:40), Dst: IntelCor_59:24:c8 (f8:63:3f:59:24:c8)
> Destination: IntelCor_59:24:c8 (f8:63:3f:59:24:c8)
> Source: Sercomm_f7:d3:40 (38:02:de:f7:d3:40)
Type: IPv4 (0x0800)

```

0000  f8 63 3f 59 24 c8 38 02 de f7 d3 40 08 00 45 00  .c?Y$.8. ...@..E.
0010  02 0a 1d f3 40 00 3a 06 a3 d1 93 66 28 0f c0 a8  ....@.:...f(...
0020  01 0c 00 50 cd 20 0c 56 4b d8 11 73 bc 26 50 18  ...P. .V K...s&P.
0030  04 06 3e 3c 00 00 48 54 54 50 2f 31 2e 31 20 32  ...><...HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 53 61 74  00 OK...D ate: Sat
0050  2c 20 33 30 20 4f 63 74 20 32 30 32 31 20 31 38  , 30 Oct 2021 18
0060  3a 30 30 3a 35 37 20 47 4d 54 0d 0a 53 65 72 76  :00:57 G MT...Serv
0070  65 72 3a 20 41 70 61 63 68 65 2f 32 2e 32 2e 32  er: Apac he/2.2.2
0080  32 20 28 46 72 65 65 42 53 44 29 20 6d 6f 64 5f  2 (FreeB SD) mod
0090  73 73 6c 2f 32 2e 32 2e 32 32 20 4f 70 65 6e 53  ssl/2.2. 22 OpenS

```

Frame (frame), 536 byte(s) | Packets: 1750 · Displayed: 1750 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

2.14 Όχι

2.15 Στο router του δικτύου στο οποίο βρίσκομαι.

2.16 f8:63:3f:59:24:c8

2.17 Ανήκει στον δικό μου υπολογιστή

2.18 536 bytes

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip or ipv6 or arp

No.	Time	Source	Destination	Protocol	Length	Info
1398	0.006188	192.168.1.1	192.168.1.12	DNS	176	Standard query response 0xda96 Refused AAAA Edu-Dy.CN.
1406	0.000479	192.168.1.12	147.102.40.15	HTTP	499	GET /lab3 HTTP/1.1
1409	0.015767	147.102.40.15	192.168.1.12	HTTP	69	[TCP Previous segment not captured] Continuation
1414	0.004682	192.168.1.12	147.102.40.15	HTTP	500	GET /lab3/ HTTP/1.1
1416	0.005974	147.102.40.15	192.168.1.12	HTTP	536	HTTP/1.1 200 OK (text/html)
1425	0.002582	192.168.1.12	147.102.40.15	HTTP	446	GET /favicon.ico HTTP/1.1
1431	0.000000	147.102.40.15	192.168.1.12	HTTP	281	HTTP/1.1 200 OK (image/x-icon)
343	0.005156	fe80::1	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::1 (rtr, ovr) is at 38:02:

Frame Length: 536 bytes (4288 bits)
 Capture Length: 536 bytes (4288 bits)
 [Frame is marked: False]
 [Frame is ignored: False]
 [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]

```

0000 f8 63 3f 59 24 c8 38 02 de f7 d3 40 08 00 45 00  c?Y$ 8  ...@..E.
0010 02 0a 1d f3 40 00 3a 06 a3 d1 93 66 28 0f c0 a8  ....@.:  ...f(...
0020 01 0c 00 50 cd 20 0c 56 4b d8 11 73 bc 26 50 18  ...P..V K...s &P.
0030 04 06 3e 3c 00 00 48 54 54 50 2f 31 2e 31 20 32  ..><..HT TP/1.1 2
0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 53 61 74  00 OK..D ate: Sat
0050 2c 20 33 30 20 4f 63 74 20 32 30 32 31 20 31 38  , 30 Oct 2021 18
0060 3a 30 30 3a 35 37 20 47 4d 54 0d 0a 53 65 72 76  :00:57 G MT..Serv
0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 32 2e 32  er: Apac he/2.2.2
0080 32 20 28 46 72 65 65 42 53 44 29 20 6d 6f 64 5f  2 (FreeB SD) mod_
0090 73 73 6c 2f 32 2e 32 2e 32 32 20 4f 70 65 6e 53  ssl/2.2. 22 OpenS

```

Frame length on the wire (frame.len) || Packets: 1750 · Displayed: 1750 (100.0%) · Dropped: 0 (0.0%) || Profile: Default

2.19

536 – 482 = 54bytes

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip or ipv6 or arp

No.	Time	Source	Destination	Protocol	Length	Info
1398	0.006188	192.168.1.1	192.168.1.12	DNS	176	Standard query response 0xda96 Refused AAAA Edu-Dy.CN.
1406	0.000479	192.168.1.12	147.102.40.15	HTTP	499	GET /lab3 HTTP/1.1
1409	0.015767	147.102.40.15	192.168.1.12	HTTP	69	[TCP Previous segment not captured] Continuation
1414	0.004682	192.168.1.12	147.102.40.15	HTTP	500	GET /lab3/ HTTP/1.1
1416	0.005974	147.102.40.15	192.168.1.12	HTTP	536	HTTP/1.1 200 OK (text/html)
1425	0.002582	192.168.1.12	147.102.40.15	HTTP	446	GET /favicon.ico HTTP/1.1
1431	0.000000	147.102.40.15	192.168.1.12	HTTP	281	HTTP/1.1 200 OK (image/x-icon)
343	0.005156	fe80::1	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::1 (rtr, ovr) is at 38:02:

Urgent Pointer: 0
 > [SEQ/ACK analysis]
 > [Timestamps]
 TCP payload (482 bytes)
 Hypertext Transfer Protocol

```

0030 04 06 3e 3c 00 00 48 54 54 50 2f 31 2e 31 20 32  ..><..HT TP/1.1 2
0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 53 61 74  00 OK..D ate: Sat
0050 2c 20 33 30 20 4f 63 74 20 32 30 32 31 20 31 38  , 30 Oct 2021 18
0060 3a 30 30 3a 35 37 20 47 4d 54 0d 0a 53 65 72 76  :00:57 G MT..Serv
0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 32 2e 32  er: Apac he/2.2.2
0080 32 20 28 46 72 65 65 42 53 44 29 20 6d 6f 64 5f  2 (FreeB SD) mod_
0090 73 73 6c 2f 32 2e 32 2e 32 32 20 4f 70 65 6e 53  ssl/2.2. 22 OpenS
00a0 53 4c 2f 30 2e 39 2e 38 7a 68 2d 66 72 65 65 62  SL/0.9.8 zh-freeb
00b0 73 64 20 44 41 56 2f 32 0d 0a 4c 61 73 74 2d 4d  sd DAV/2 ..Last-M
00c0 6f 64 69 66 69 65 64 3a 20 54 68 75 2c 20 32 31  odified: Thu, 21

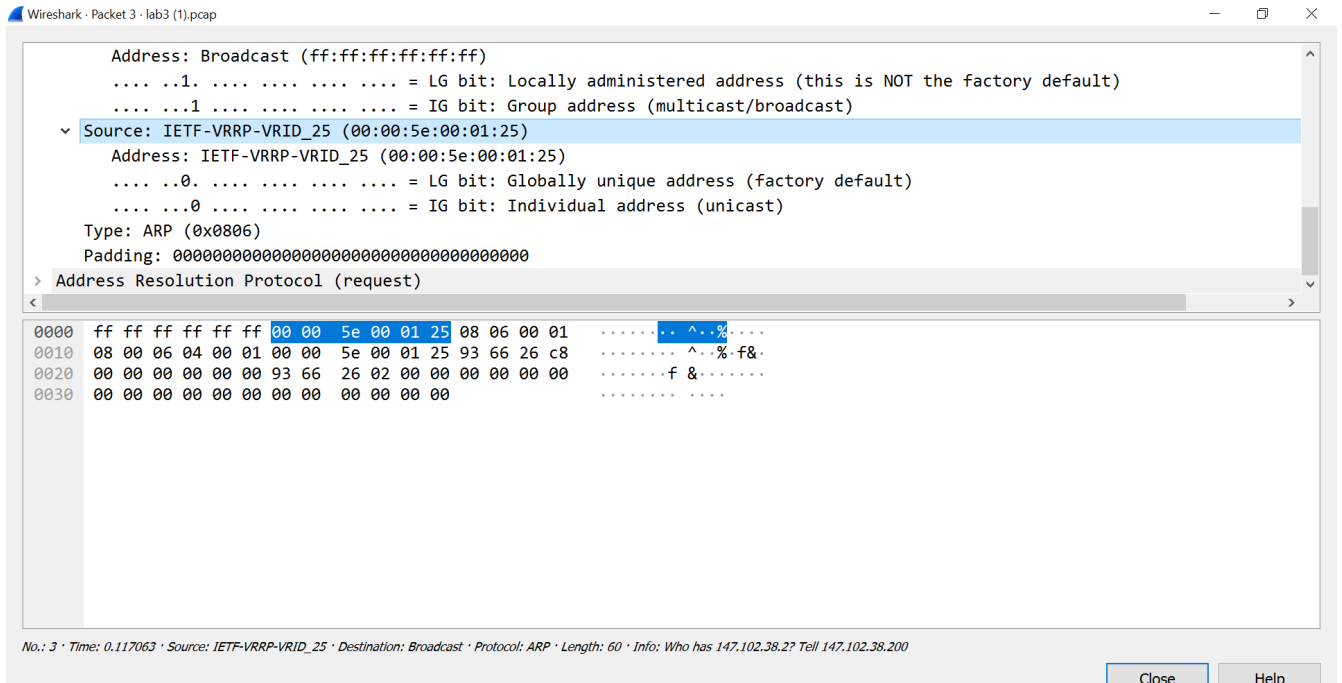
```

The TCP payload of this packet (tcp.payload), 482 byte(s) || Packets: 1750 · Displayed: 1750 (100.0%) · Dropped: 0 (0.0%) || Profile: Default

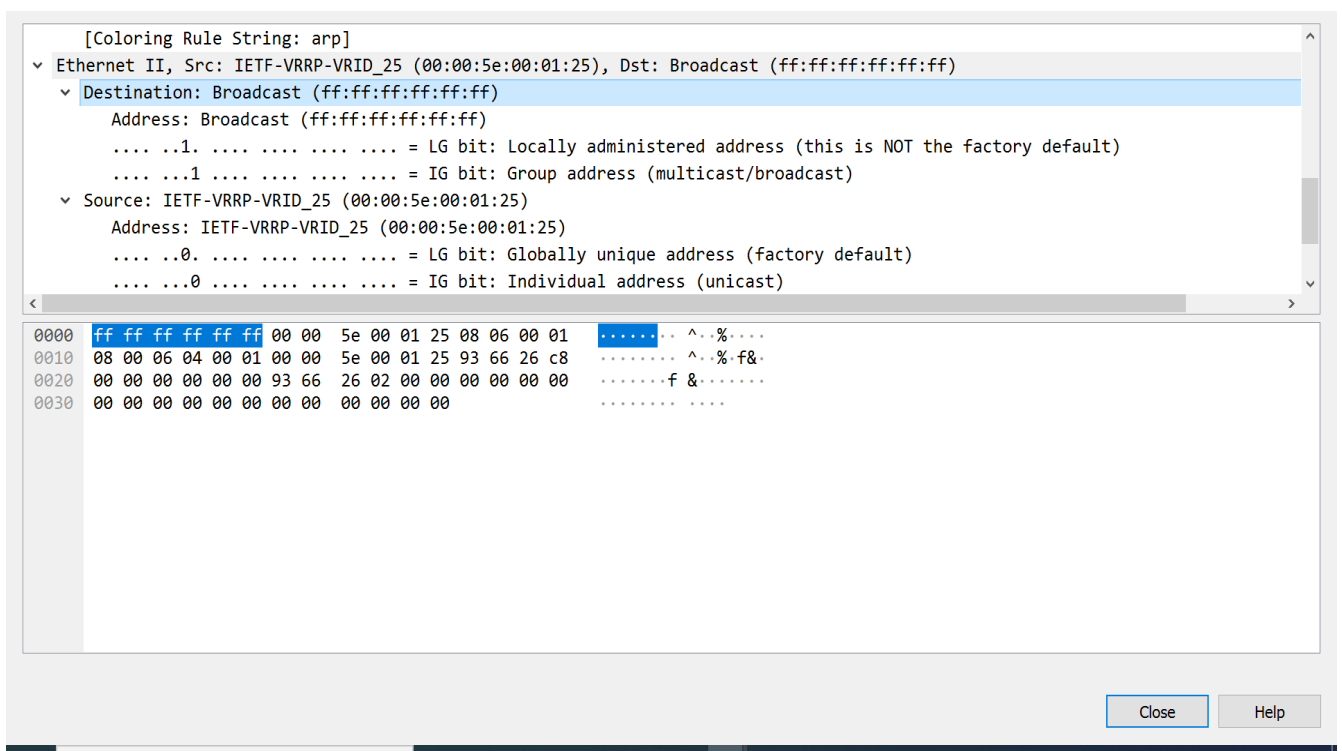
Άσκηση 3

(χρησιμοποίησα το αρχείο που κατέβασα)

3.1 Το 2^ο byte είναι 0 άρα καταγράψαμε μοναδικές διευθύνσεις MAC πηγής και το 2^ο LSB είναι 0 άρα καταγράψαμε ατομικές διευθύνσεις MAC πηγής.



3.2 Το 2^ο byte είναι 1 άρα καταγράψαμε τοπικές διευθύνσεις MAC προορισμού (κάποιες) και το 2^ο LSB είναι 1 άρα καταγράψαμε ομαδικές διευθύνσεις MAC προορισμού.



Πρόκειται βασικά για broadcasting, καθώς οι διευθύνσεις MAC προορισμού αποτελούνται μόνο από 1 (το γράφει κίτρινος)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	147.102.50.222	239.255.255.250	IPv4	850	Fragmented IP protocol (proto=UDP 17, off=1480, ID=000)
2	0.122047	147.102.50.222	239.255.255.250	IPv4	850	Fragmented IP protocol (proto=UDP 17, off=1480, ID=000)
3	0.117063	IETF-VRRP-VRID_25	Broadcast	ARP	60	Who has 147.102.38.2? Tell 147.102.38.200
4	0.010907	147.102.38.87	147.102.38.255	NBNS	92	Name query NB ST-001<00>
5	0.241809	IETF-VRRP-VRID_25	Broadcast	ARP	60	Who has 147.102.38.18? Tell 147.102.38.200
6	0.260970	IETF-VRRP-VRID_25	Broadcast	ARP	60	Who has 147.102.38.76? Tell 147.102.38.200
7	0.050182	147.102.38.200	224.0.0.18	VRRP	60	Announcement (v2)
8	0.166241	Dell_26:40:51	Broadcast	ARP	60	Who has 147.102.38.13? Tell 147.102.38.103

Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Address: Broadcast (ff:ff:ff:ff:ff:ff)
.... ..1. = LG bit: Locally administered address (this is NOT the factory default)
.... ..1. = IG bit: Group address (multicast/broadcast)
Source: IETF-VRRP-VRID 25 (00:00:5e:00:01:25)

```

0000  ff ff ff ff ff ff 00 00 5e 00 01 25 08 06 00 01  ..^... ^..%...
0010  08 00 06 04 00 01 00 00 5e 00 01 25 93 66 26 c8  ..^... ^..%f&
0020  00 00 00 00 00 00 93 66 26 02 00 00 00 00 00 00  ..f &.....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....

```

Destination Hardware Address (eth.dst), 6 byte(s) | Packets: 74 · Displayed: 74 (100.0%) | Profile: Default

(Υπάρχει και μοναδική και ομαδική διεύθυνση MAC προορισμού σε κάποια πλαίσια:

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
3	0.117063	IETF-VRRP-VRID_25	Broadcast	ARP	60	Who has 147.102.38.2? Tell 147.102.38.200
4	0.010907	147.102.38.87	147.102.38.255	NBNS	92	Name query NB ST-001<00>
5	0.241809	IETF-VRRP-VRID_25	Broadcast	ARP	60	Who has 147.102.38.18? Tell 147.102.38.200
6	0.260970	IETF-VRRP-VRID_25	Broadcast	ARP	60	Who has 147.102.38.76? Tell 147.102.38.200
7	0.050182	147.102.38.200	224.0.0.18	VRRP	60	Announcement (v2)
8	0.166241	Dell_26:40:51	Broadcast	ARP	60	Who has 147.102.38.13? Tell 147.102.38.103
9	0.101990	147.102.38.200	224.0.0.5	OSPF	110	Hello Packet
10	0.045712	IETF-VRRP-VRID_25	Broadcast	ARP	60	Who has 147.102.38.206? Tell 147.102.38.200

Destination: IPv4mcast_12 (01:00:5e:00:00:12)
Address: IPv4mcast_12 (01:00:5e:00:00:12)
.... ..0. = LG bit: Globally unique address (factory default)
.... ..1. = IG bit: Group address (multicast/broadcast)
Source: IETF-VRRP-VRID 25 (00:00:5e:00:01:25)

```

0000  01 00 5e 00 00 12 00 00 5e 00 01 25 08 00 45 c0  ..^... ^..%..E
0010  00 28 d0 8a 00 00 ff 70 4f da 93 66 26 c8 e0 00  ..(....p O..f&
0020  00 12 21 25 ff 01 00 01 25 a9 93 66 26 c8 00 00  ..!%... %..f&
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....

```

Destination Hardware Address (eth.dst), 6 byte(s) | Packets: 74 · Displayed: 74 (100.0%) | Profile: Default

)

3.3 Εμφανίζεται στο LSB του 1^{ου} byte (1^ο απ'τα αριστερά)

3.4 Προορισμού: ff:ff:ff:ff:ff:ff, Πηγής: 00:00:5e:00:01:25

3.5 Παραμένουν πλαίσια με πρωτόκολλο STP:

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

llc

No.	Time	Source	Protocol	Length	Destination	Info
11	0.000000	Cisco_1b:ef:97	STP	60	Spanning-tree-(for-...	RST. Root = 12288/38/7c:ad:4f:42:cc:e0 Cost = 102 Port = 0
27	2.000112	Cisco_1b:ef:97	STP	60	Spanning-tree-(for-...	RST. Root = 12288/38/7c:ad:4f:42:cc:e0 Cost = 102 Port = 0
39	2.002554	Cisco_1b:ef:97	STP	60	Spanning-tree-(for-...	RST. Root = 12288/38/7c:ad:4f:42:cc:e0 Cost = 102 Port = 0
56	2.000152	Cisco_1b:ef:97	STP	60	Spanning-tree-(for-...	RST. Root = 12288/38/7c:ad:4f:42:cc:e0 Cost = 102 Port = 0
71	2.000117	Cisco_1b:ef:97	STP	60	Spanning-tree-(for-...	RST. Root = 12288/38/7c:ad:4f:42:cc:e0 Cost = 102 Port = 0

Logical-Link Control: Protocol | Packets: 74 · Displayed: 5 (6.8%) | Profile: Default

3.6 Δηλώνει το μήκος των δεδομένων (είναι το πεδίο length)

IEEE 802.3 Ethernet

- Destination: Spanning-tree-(for-bridges)_00 (01:80:c2:00:00:00)
 - Address: Spanning-tree-(for-bridges)_00 (01:80:c2:00:00:00)
 -0. = LG bit: Globally unique address (factory default)
 -1. = IG bit: Group address (multicast/broadcast)
- Source: Cisco_1b:ef:97 (cc:7f:76:1b:ef:97)
 - Address: Cisco_1b:ef:97 (cc:7f:76:1b:ef:97)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)

Length: 39

```

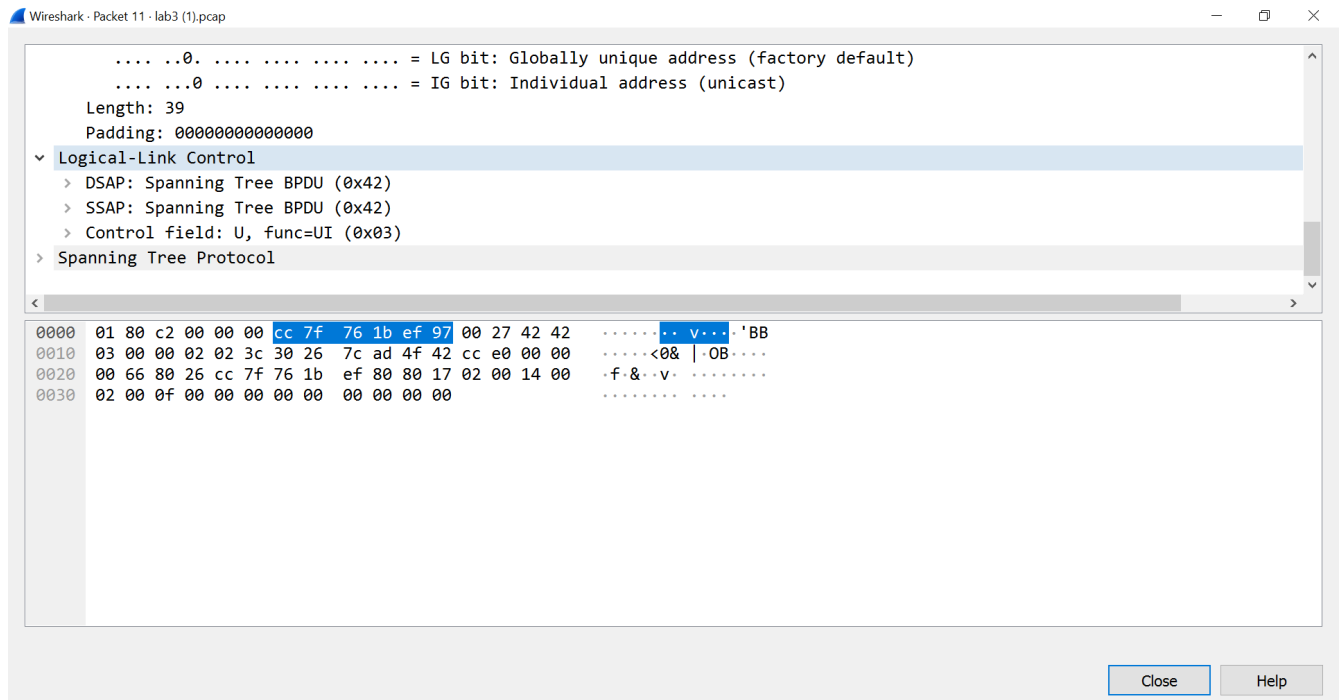
0000  01 80 c2 00 00 00 cc 7f 76 1b ef 97 00 27 42 42  ..... v....'BB
0010  03 00 00 02 02 3c 30 26 7c ad 4f 42 cc e0 00 00  ....<0& |·OB...
0020  00 66 80 26 cc 7f 76 1b ef 80 80 17 02 00 14 00  ·f·&··v· .....
0030  02 00 0f 00 00 00 00 00 00 00 00 00  .....
  
```

No.: 11 · Time: 0.000000 · Source: Cisco_1b:ef:97 · Protocol: STP · Length: 60 · Destination: Spanning-tree-(for-bridges)_00 · Info: RST. Root = 12288/38/7c:ad:4f:42:cc:e0 Cost = 102 Port = 0x8017

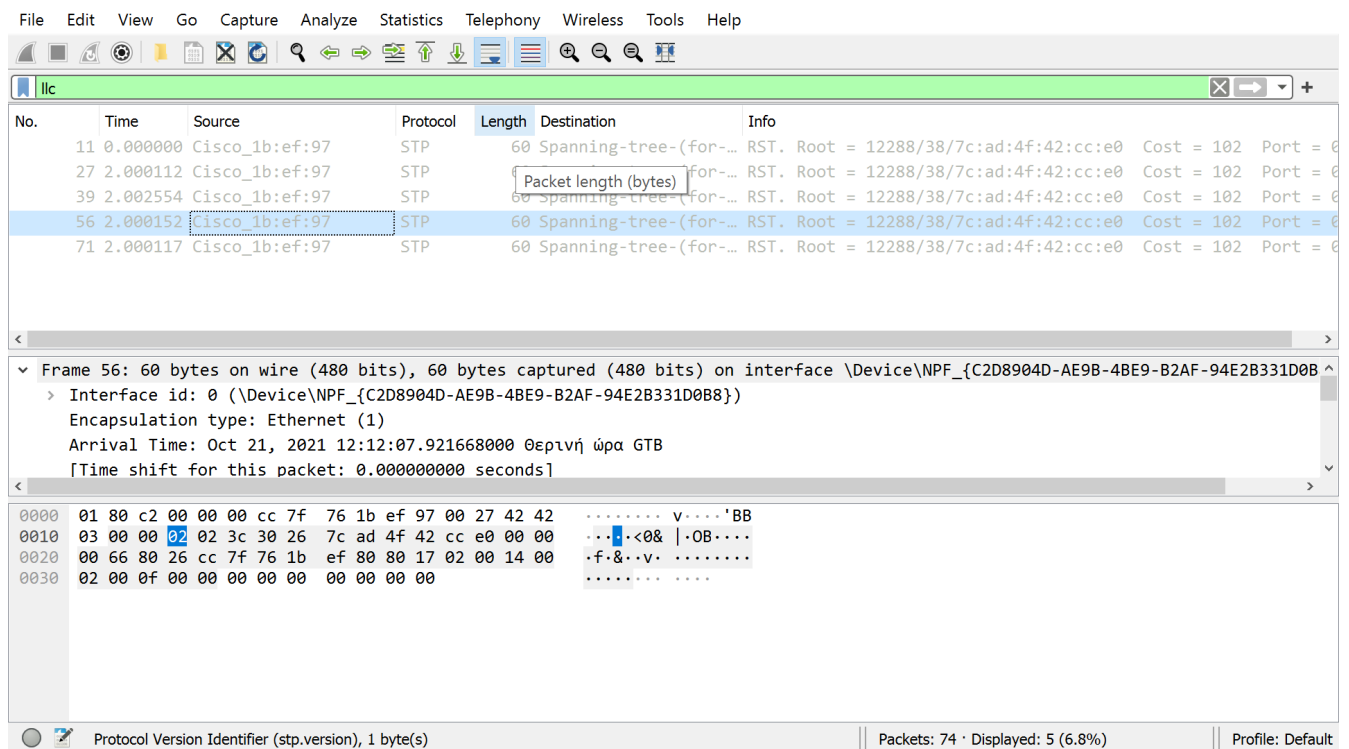
Close Help

3.7 Το πεδίο Type έχει τιμή ≤ 1500 για τα πλαίσια Ethernet IEEE802.3 ενώ για τα πλαίσια Ethernet II έχει την τιμή 1536.

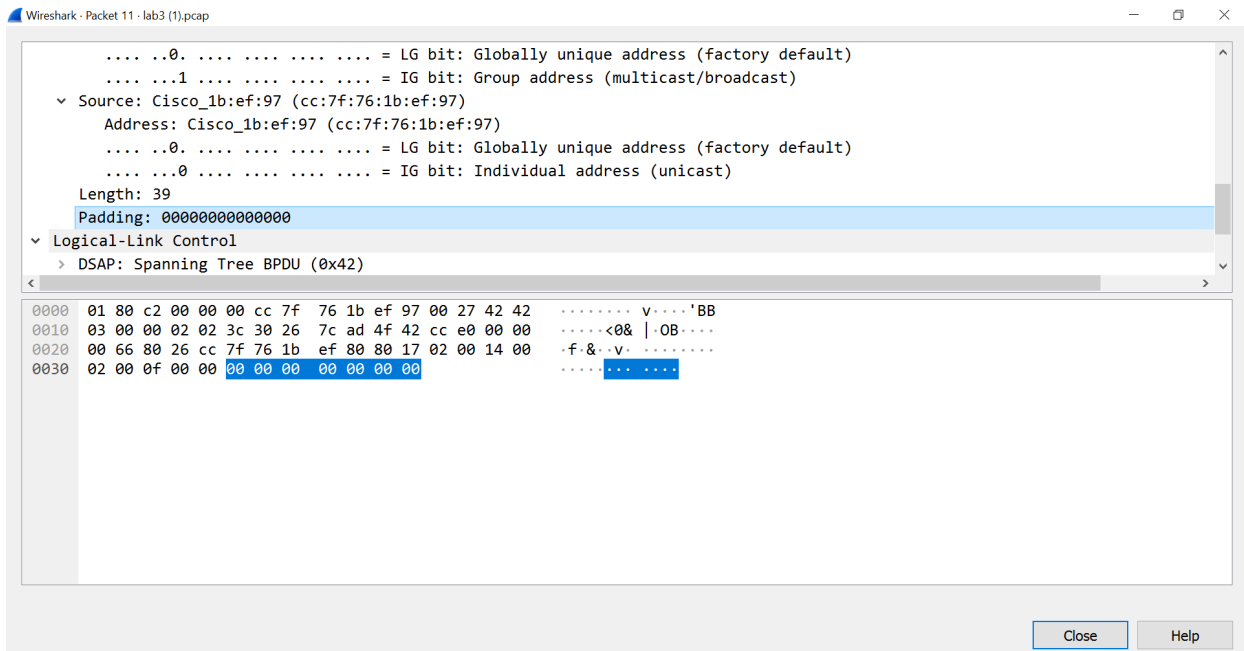
3.8 Μέγεθος: 3 byte. Περιέχει τα πεδία DSAP, SSAP, Control field



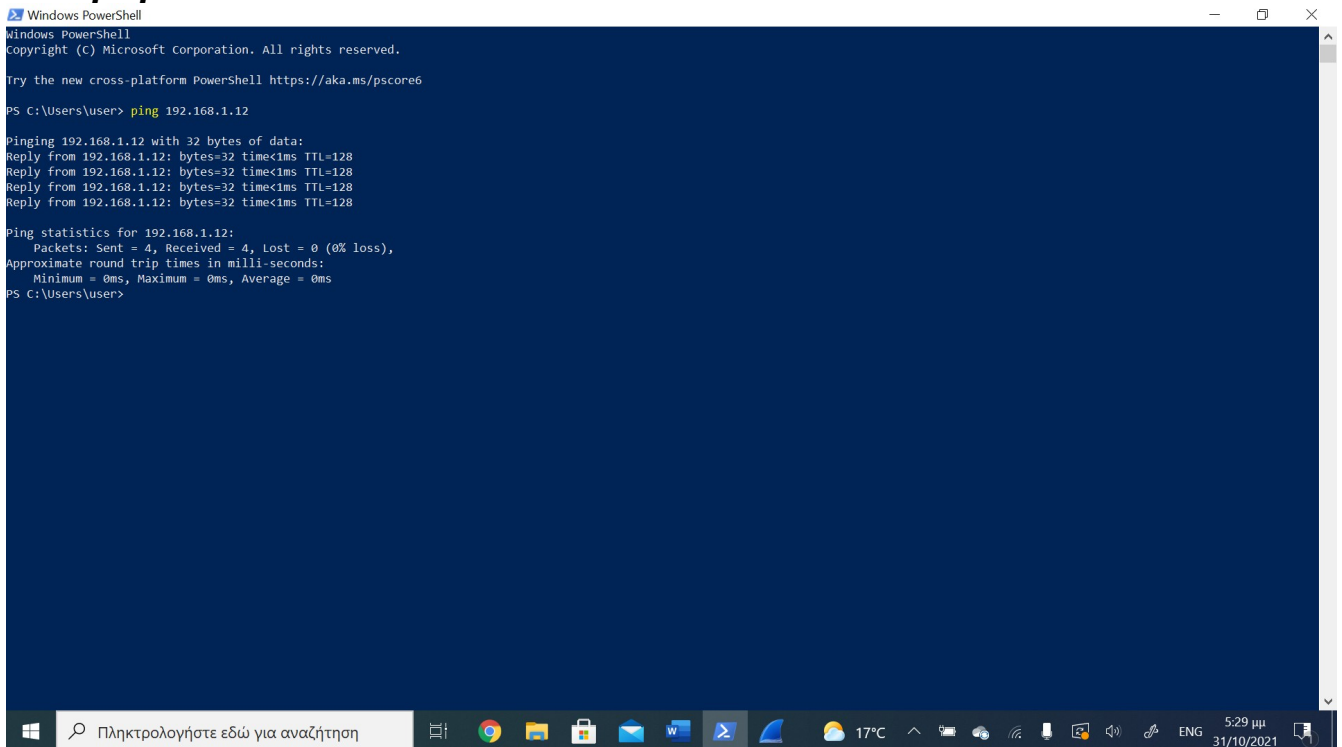
3.9 Μεταφέρουν δεδομένα πρωτοκόλλου STP και όλα έχουν μέγεθος 60 bytes



3.10 7 bytes



Άσκηση 4



4.1 Απεικονίζει όλα τα πλαίσια που έχουν destination ή source την MAC address που έβαλα στο φίλτρο.

4.2 Απεικονίζει μόνο τα πακέτα με πρωτόκολλο ARP που έχουν destination ή source την MAC address που έβαλα στο φίλτρο

4.3 Δύο

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

eth.addr == F8-63-3F-59-24-C8 and arp

No.	Time	Source	Destination	Protocol	Length	Info
504	0.000000	IntelCor_59:24:c8	Sercomm_f7:d3:40	ARP	42	Who has 192.168.1.1? Tell 192.168.1.12
505	0.003931	Sercomm_f7:d3:40	IntelCor_59:24:c8	ARP	42	192.168.1.1 is at 38:02:de:f7:d3:40

> Frame 504: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{11981F20-5231-4861-ABD2-DD8A4A767CB9}

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

> Address Resolution Protocol (request)

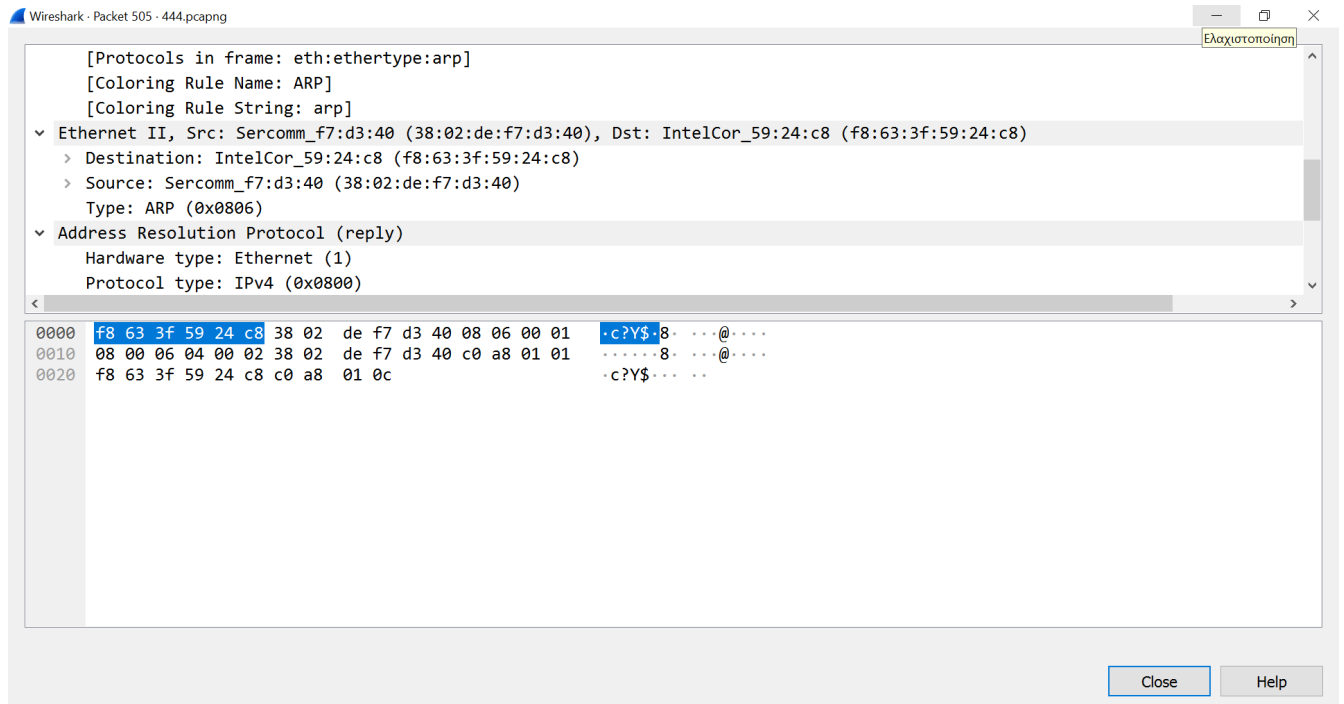
```

0000  38 02 de f7 d3 40 f8 63  3f 59 24 c8 08 06 00 01  8...@.c ?Y$.....
0010  08 00 06 04 00 01 f8 63  3f 59 24 c8 c0 a8 01 0c  .....c ?Y$.....
0020  38 02 de f7 d3 40 c0 a8  01 01                      8...@.. ..

```

Address Resolution Protocol: Protocol || Packets: 718 · Displayed: 2 (0.3%) · Dropped: 0 (0.0%) || Profile: Default

4.4



4.5

Hardware Type: Ethernet(1) :3 bytes

Hardware Size: 6 : 1 byte

Protocol Type: 2 bytes

Protocol Size: 4 : 1 byte

Opcode: request(1) : 2 bytes

Sender MAC Address: 6 bytes

Target MAC Address: 6 bytes

Sender IP Address: 4 bytes

Target IP Address: 4 bytes

Wireshark · Packet 504 · Wi-Fi

▼ Address Resolution Protocol (request)

- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: request (1)
- Sender MAC address: IntelCor_59:24:c8 (f8:63:3f:59:24:c8)
- Sender IP address: 192.168.1.12
- Target MAC address: Sercomm_f7:d3:40 (38:02:de:f7:d3:40)
- Target IP address: 192.168.1.1

0000	38 02 de f7 d3 40 f8 63 3f 59 24 c8 08 06 00 01	8...@.c ?Y\$.....
0010	08 00 06 04 00 01 f8 63 3f 59 24 c8 c0 a8 01 0cc ?Y\$.....
0020	38 02 de f7 d3 40 c0 a8 01 01	8...@. . .

No.: 504 · Time: 0.000000 · Source: IntelCor_59:24:c8 · Destination: Sercomm_f7:d3:40 · Protocol: ARP · Length: 42 · Info: Who has 192.168.1.1? Tell 192.168.1.12

Close Help

4.6 Τιμή: 0001 . Υποδεικνύει ότι η μεταφορά του πλαισίου γίνεται μέσω Ethernet.

444.pcapng

Wireshark · Packet 505 · 444.pcapng

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

- Destination: IntelCor_59:24:c8 (f8:63:3f:59:24:c8)
- Source: Sercomm_f7:d3:40 (38:02:de:f7:d3:40)
- Type: ARP (0x0806)

▼ Address Resolution Protocol (reply)

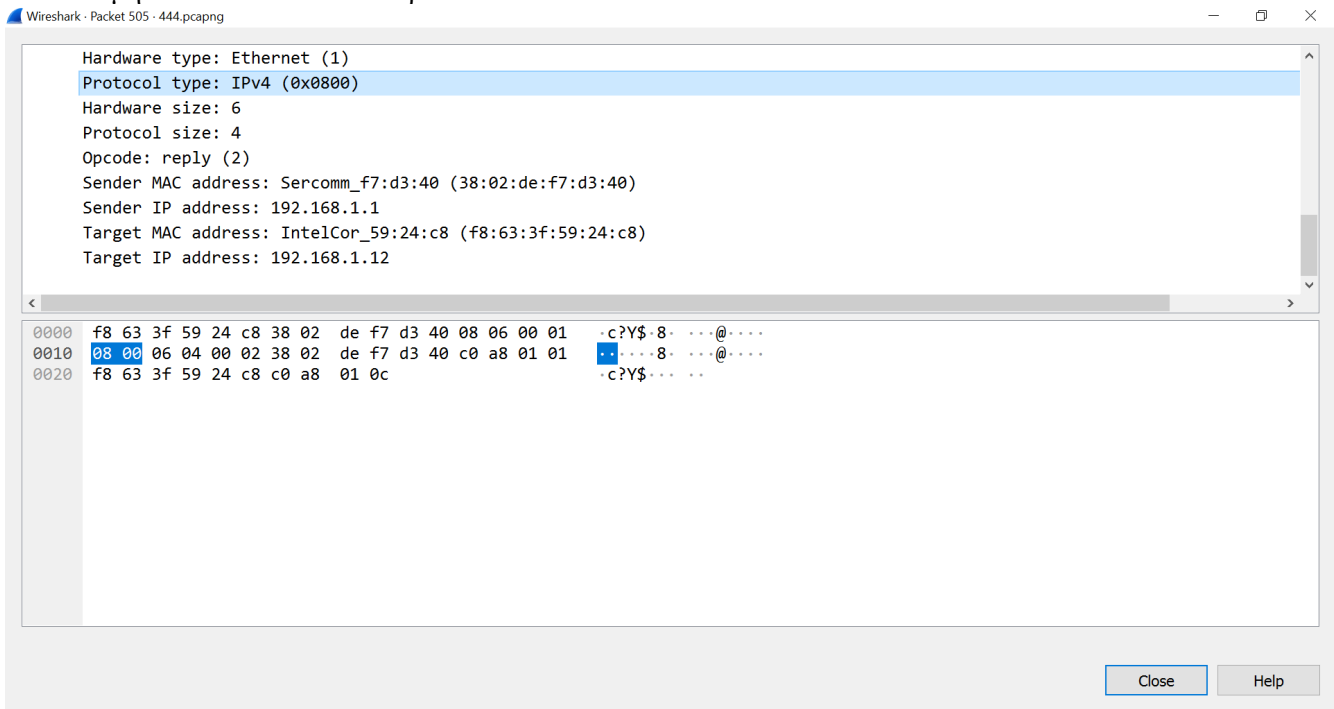
- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: reply (2)

0000	f8 63 3f 59 24 c8 38 02 de f7 d3 40 08 06 00 01	.c?Y\$.8. ...@. . .
0010	08 00 06 04 00 02 38 02 de f7 d3 40 c0 a8 01 018. ...@. . .
0020	f8 63 3f 59 24 c8 c0 a8 01 0c	.c?Y\$. . . .

No.: 505 · Time: 0.003931 · Source: Sercomm_f7:d3:40 · Destination: IntelCor_59:24:c8 · Protocol: ARP · Length: 42 · Info: 192.168.1.1 is at 38:02:de:f7:d3:40

Close Help

4.7 Τιμή: 0800. Υποδεικνύει: πρωτόκολλο IPv4.

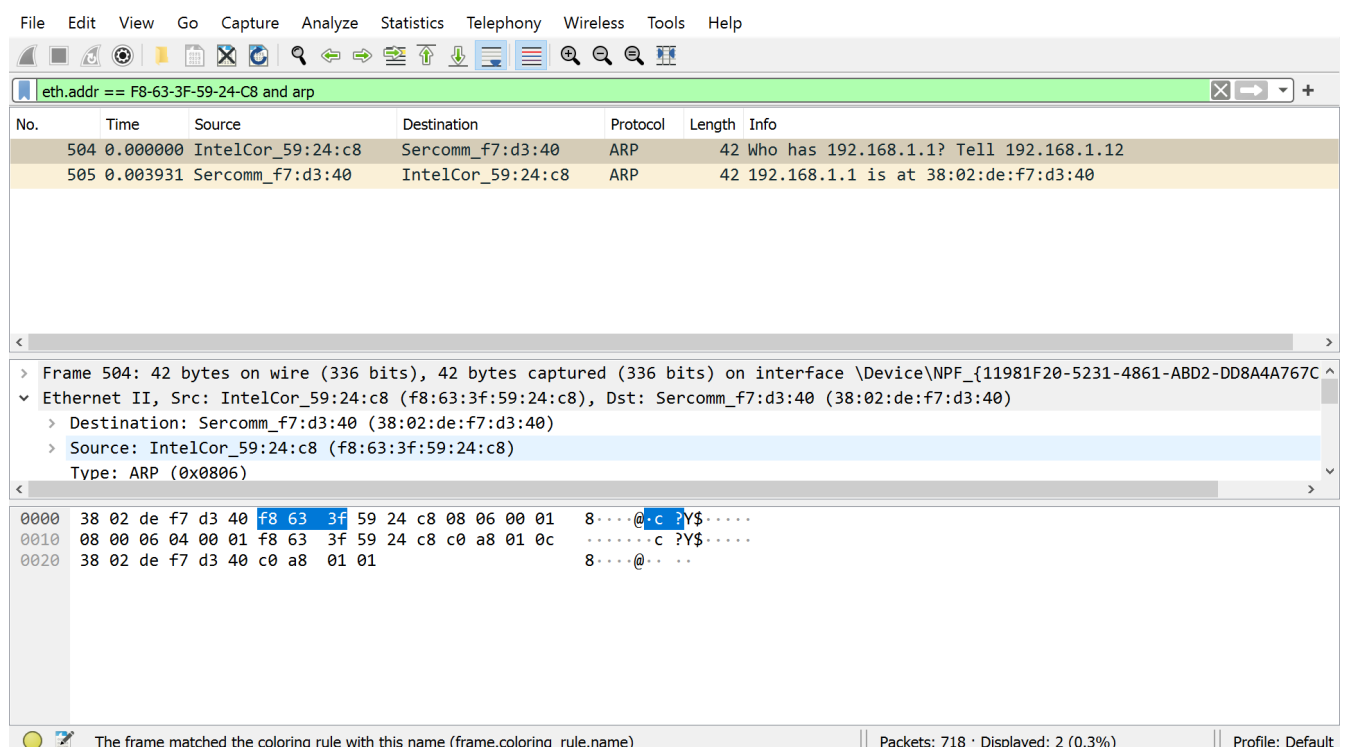


4.8 Έχουν ίδιο μήκος (2 bytes) και η τιμή του Protocol Type (η 16δική) αντιστοιχεί σε κάποιο EtherType

4.9 Δηλώνει το μέγεθος της διεύθυνσης του πρωτόκολλου IPv4, το οποίο είναι 4 bytes

4.10 Δηλώνει το μέγεθος της διεύθυνσης MAC, το οποίο είναι 6 bytes.

4.11 Ανήκει στον υπολογιστή μου



4.12 38:02:de:f8:09:a0 (κανονικά δεν την γνωρίζουμε ως τότε, και αυτός είναι εξάλλου και ο λόγος που στέλνουμε το ARP request)

4.13 Μέγεθος ARP: 28 bytes, Μέγεθος Ethernet: 42 bytes επειδή έχει ενθυλακώσει το ARP

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

eth.addr == F8-63-3F-59-24-C8 and arp

No.	Time	Source	Destination	Protocol	Length	Info
504	0.000000	IntelCor_59:24:c8	Sercomm_f7:d3:40	ARP	42	Who has 192.168.1.1? Tell 192.168.1.12
505	0.003931	Sercomm_f7:d3:40	IntelCor_59:24:c8	ARP	42	192.168.1.1 is at 38:02:de:f7:d3:40

> Frame 504: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{11981F20-5231-4861-ABD2-DD8A4A767C}

▼ 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: ARP (0x0806)

```
0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 08 06 00 01 8...@.c ?Y$...
0010 08 00 06 04 00 01 f8 63 3f 59 24 c8 c0 a8 01 0c .....c ?Y$.....
0020 38 02 de f7 d3 40 c0 a8 01 01 8...@... ..
```

OneDrive
Το στιγμιότυπο οθόνης αποθηκεύτηκε
Το στιγμιότυπο οθόνης προστέθηκε στο OneDrive.

Ethernet (eth), 14 byte(s) | Packets: 718 · Displayed: 2 (0.3%) | Profile: Default

444.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

eth.addr == F8-63-3F-59-24-C8 and arp

No.	Time	Source	Destination	Protocol	Length	Info
504	0.000000	IntelCor_59:24:c8	Sercomm_f7:d3:40	ARP	42	Who has 192.168.1.1? Tell 192.168.1.12
505	0.003931	Sercomm_f7:d3:40	IntelCor_59:24:c8	ARP	42	192.168.1.1 is at 38:02:de:f7:d3:40

▼ Address Resolution Protocol (request)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

```
0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 08 06 00 01 8...@.c ?Y$...
0010 08 00 06 04 00 01 f8 63 3f 59 24 c8 c0 a8 01 0c .....c ?Y$.....
0020 38 02 de f7 d3 40 c0 a8 01 01 8...@... ..
```

4.14 20 bytes

eth.addr == F8-63-3F-59-24-C8 and arp

No.	Time	Source	Destination	Protocol	Length	Info
504	0.000000	IntelCor_59:24:c8	Sercomm_f7:d3:40	ARP	42	Who has 192.168.1.1? Tell 192.168.1.12
505	0.003931	Sercomm_f7:d3:40	IntelCor_59:24:c8	ARP	42	192.168.1.1 is at 38:02:de:f7:d3:40

Opcode: request (1)
Sender MAC address: IntelCor_59:24:c8 (f8:63:3f:59:24:c8)
Sender IP address: 192.168.1.12
Target MAC address: Sercomm_f7:d3:40 (38:02:de:f7:d3:40)
Target IP address: 192.168.1.1

```
0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 08 06 00 01 8...@.c ?Y$. ....
0010 08 00 06 04 00 01 f8 63 3f 59 24 c8 c0 a8 01 0c .....c ?Y$. ....
0020 38 02 de f7 d3 40 c0 a8 01 01 8...@. . .
```

Opcode (arp.opcode), 2 byte(s) | Packets: 718 · Displayed: 2 (0.3%) | Profile: Default

4.15 Είναι 0001 όπως φαίνεται και στο παραπάνω στιγμιότυπο οθόνης

4.16 Στο Sender MAC address

444.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

eth.addr == F8-63-3F-59-24-C8 and arp

No.	Time	Source	Destination	Protocol	Length	Info
504	0.000000	IntelCor_59:24:c8	Sercomm_f7:d3:40	ARP	42	Who has 192.168.1.1? Tell 192.168.1.12
505	0.003931	Sercomm_f7:d3:40	IntelCor_59:24:c8	ARP	42	192.168.1.1 is at 38:02:de:f7:d3:40

Opcode: request (1)
Sender MAC address: IntelCor_59:24:c8 (f8:63:3f:59:24:c8)
Sender IP address: 192.168.1.12
Target MAC address: Sercomm_f7:d3:40 (38:02:de:f7:d3:40)
Target IP address: 192.168.1.1

```
0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 08 06 00 01 8...@.c ?Y$. ....
0010 08 00 06 04 00 01 f8 63 3f 59 24 c8 c0 a8 01 0c .....c ?Y$. ....
0020 38 02 de f7 d3 40 c0 a8 01 01 8...@. . .
```

4.17 Στο Sender IP address

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

eth.addr == F8-63-3F-59-24-C8 and arp

No.	Time	Source	Destination	Protocol	Length	Info
504	0.000000	IntelCor_59:24:c8	Sercomm_f7:d3:40	ARP	42	Who has 192.168.1.1? Tell 192.168.1.12
505	0.003931	Sercomm_f7:d3:40	IntelCor_59:24:c8	ARP	42	192.168.1.1 is at 38:02:de:f7:d3:40

Opcode: request (1)
 Sender MAC address: IntelCor_59:24:c8 (f8:63:3f:59:24:c8)
 Sender IP address: 192.168.1.12
 Target MAC address: Sercomm_f7:d3:40 (38:02:de:f7:d3:40)
 Target IP address: 192.168.1.1

```

0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 08 06 00 01 8...@.c ?Y$. ....
0010 08 00 06 04 00 01 f8 63 3f 59 24 c8 c0 a8 01 0c .....c ?Y$. ....
0020 38 02 de f7 d3 40 c0 a8 01 01 8...@. . .
  
```

Sender IP address (arp.src.proto_ip_v4), 4 byte(s) | Packets: 718 · Displayed: 2 (0.3%) | Profile: Default

4.18 Στο πεδίο Target IP address (φαίνεται στα παραπάνω στιγμιότυπα οθόνης)

4.19 Είναι το πεδίο Target MAC address και η τιμή που θα έπρεπε να περιέχει είναι 00:00:00:00 καθώς δεν την ξέρουμε. (εδώ περιέχει την τιμή της ζητούμενης διεύθυνσης MAC σαν να την έχει ήδη βρει)

4.20 Η διεύθυνση MAC του αποστολέα είναι αυτή του router μου και η διεύθυνση MAC του παραλήπτη είναι του λαπτοπ μου.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

eth.addr == F8-63-3F-59-24-C8 and arp

No.	Time	Source	Destination	Protocol	Length	Info
504	0.000000	IntelCor_59:24:c8	Sercomm_f7:d3:40	ARP	42	Who has 192.168.1.1? Tell 192.168.1.12
505	0.003931	Sercomm_f7:d3:40	IntelCor_59:24:c8	ARP	42	192.168.1.1 is at 38:02:de:f7:d3:40

Sender MAC address: Sercomm_f7:d3:40 (38:02:de:f7:d3:40)
 Sender IP address: 192.168.1.1
 Target MAC address: IntelCor_59:24:c8 (f8:63:3f:59:24:c8)
 Target IP address: 192.168.1.12

```

0000 f8 63 3f 59 24 c8 38 02 de f7 d3 40 08 06 00 01 .c?Y$. 8. ...@. ....
0010 08 00 06 04 00 02 38 02 de f7 d3 40 c0 a8 01 01 .....8. ...@. ....
0020 f8 63 3f 59 24 c8 c0 a8 01 0c .c?Y$. . . .
  
```

Sender MAC address (arp.src.hw_mac), 6 byte(s) | Packets: 718 · Displayed: 2 (0.3%) | Profile: Default

4.21 Η τιμή είναι 0002

444.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

eth.addr == F8-63-3F-59-24-C8 and arp

No.	Time	Source	Destination	Protocol	Length	Info
504	0.000000	IntelCor_59:24:c8	Sercomm_f7:d3:40	ARP	42	Who has 192.168.1.1? Tell 192.168.1.12
505	0.003931	Sercomm_f7:d3:40	IntelCor_59:24:c8	ARP	42	192.168.1.1 is at 38:02:de:f7:d3:40

Protocol type: IPv4 (0x0800)
 Hardware size: 6
 Protocol size: 4
 Opcode: reply (2)
 Sender MAC address: Sercomm_f7:d3:40 (38:02:de:f7:d3:40)

```

0000 f8 63 3f 59 24 c8 38 02 de f7 d3 40 08 06 00 01  .c?Y$.8. ...@....
0010 08 00 06 04 00 02 38 02 de f7 d3 40 c0 a8 01 01  ....8. ....@....
0020 f8 63 3f 59 24 c8 c0 a8 01 0c                    .c?Y$... ..
  
```

4.22 Στο πεδίο Sender IP address

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

eth.addr == F8-63-3F-59-24-C8 and arp

No.	Time	Source	Destination	Protocol	Length	Info
504	0.000000	IntelCor_59:24:c8	Sercomm_f7:d3:40	ARP	42	Who has 192.168.1.1? Tell 192.168.1.12
505	0.003931	Sercomm_f7:d3:40	IntelCor_59:24:c8	ARP	42	192.168.1.1 is at 38:02:de:f7:d3:40

Sender MAC address: Sercomm_f7:d3:40 (38:02:de:f7:d3:40)
 Sender IP address: 192.168.1.1
 Target MAC address: IntelCor_59:24:c8 (f8:63:3f:59:24:c8)
 Target IP address: 192.168.1.12

```

0000 f8 63 3f 59 24 c8 38 02 de f7 d3 40 08 06 00 01  .c?Y$.8. ...@....
0010 08 00 06 04 00 02 38 02 de f7 d3 40 c0 a8 01 01  ....8. ....@....
0020 f8 63 3f 59 24 c8 c0 a8 01 0c                    .c?Y$... ..
  
```

Sender IP address (arp.src.proto_ipv4), 4 byte(s) | Packets: 718 · Displayed: 2 (0.3%) | Profile: Default

4.23 Sender MAC address

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

eth.addr == F8-63-3F-59-24-C8 and arp

No.	Time	Source	Destination	Protocol	Length	Info
504	0.000000	IntelCor_59:24:c8	Sercomm_f7:d3:40	ARP	42	Who has 192.168.1.1? Tell 192.168.1.12
505	0.003931	Sercomm_f7:d3:40	IntelCor_59:24:c8	ARP	42	192.168.1.1 is at 38:02:de:f7:d3:40

Sender MAC address: Sercomm_f7:d3:40 (38:02:de:f7:d3:40)
Sender IP address: 192.168.1.1
Target MAC address: IntelCor_59:24:c8 (f8:63:3f:59:24:c8)
Target IP address: 192.168.1.12

0000 f8 63 3f 59 24 c8 38 02 de f7 d3 40 08 06 00 01 .c?Y\$.8. ...@...
0010 08 00 06 04 00 02 38 02 de f7 d3 40 c0 a8 01 018. ...@...
0020 f8 63 3f 59 24 c8 c0 a8 01 0c .c?Y\$. . . .

Sender MAC address (arp.src.hw_mac), 6 byte(s) | Packets: 718 · Displayed: 2 (0.3%) | Profile: Default

4.24 Target IP address

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

eth.addr == F8-63-3F-59-24-C8 and arp

No.	Time	Source	Destination	Protocol	Length	Info
504	0.000000	IntelCor_59:24:c8	Sercomm_f7:d3:40	ARP	42	Who has 192.168.1.1? Tell 192.168.1.12
505	0.003931	Sercomm_f7:d3:40	IntelCor_59:24:c8	ARP	42	192.168.1.1 is at 38:02:de:f7:d3:40

Sender MAC address: Sercomm_f7:d3:40 (38:02:de:f7:d3:40)
Sender IP address: 192.168.1.1
Target MAC address: IntelCor_59:24:c8 (f8:63:3f:59:24:c8)
Target IP address: 192.168.1.12

0000 f8 63 3f 59 24 c8 38 02 de f7 d3 40 08 06 00 01 .c?Y\$.8. ...@...
0010 08 00 06 04 00 02 38 02 de f7 d3 40 c0 a8 01 018. ...@...
0020 f8 63 3f 59 24 c8 c0 a8 01 0c .c?Y\$. . . .

Target IP address (arp.dst.proto_ipv4), 4 byte(s) | Packets: 718 · Displayed: 2 (0.3%) | Profile: Default

4.25 Στο πεδίο Sender MAC address.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

eth.addr == F8-63-3F-59-24-C8 and arp

No.	Time	Source	Destination	Protocol	Length	Info
504	0.000000	IntelCor_59:24:c8	Sercomm_f7:d3:40	ARP	42	Who has 192.168.1.1? Tell 192.168.1.12
505	0.003931	Sercomm_f7:d3:40	IntelCor_59:24:c8	ARP	42	192.168.1.1 is at 38:02:de:f7:d3:40

Sender MAC address: Sercomm_f7:d3:40 (38:02:de:f7:d3:40)
 Sender IP address: 192.168.1.1
 Target MAC address: IntelCor_59:24:c8 (f8:63:3f:59:24:c8)
 Target IP address: 192.168.1.12

```

0000 f8 63 3f 59 24 c8 38 02 de f7 d3 40 08 06 00 01  .c?Y$.8. ...@...
0010 08 00 06 04 00 02 38 02 de f7 d3 40 c0 a8 01 01  ....8. ...@...
0020 f8 63 3f 59 24 c8 c0 a8 01 0c                    .c?Y$... ..
  
```

Sender MAC address (arp.src.hw_mac), 6 byte(s) | Packets: 718 · Displayed: 2 (0.3%) | Profile: Default

4.26 Μέγεθος ARP reply: 28 bytes, Μέγεθος Ethernet: 42 bytes, όπως πριν

444.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

eth.addr == F8-63-3F-59-24-C8 and arp

No.	Time	Source	Destination	Protocol	Length	Info
504	0.000000	IntelCor_59:24:c8	Sercomm_f7:d3:40	ARP	42	Who has 192.168.1.1? Tell 192.168.1.12
505	0.003931	Sercomm_f7:d3:40	IntelCor_59:24:c8	ARP	42	192.168.1.1 is at 38:02:de:f7:d3:40

> Source: Sercomm_f7:d3:40 (38:02:de:f7:d3:40)
 Type: ARP (0x0806)
 Address Resolution Protocol (reply)
 Hardware type: Ethernet (1)
 Protocol type: IPv4 (0x0800)

```

0000 f8 63 3f 59 24 c8 38 02 de f7 d3 40 08 06 00 01  .c?Y$.8. ...@...
0010 08 00 06 04 00 02 38 02 de f7 d3 40 c0 a8 01 01  ....8. ...@...
0020 f8 63 3f 59 24 c8 c0 a8 01 0c                    .c?Y$... ..
  
```


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

eth.addr == F8-63-3F-59-24-C8 and arp

No.	Time	Source	Destination	Protocol	Length	Info
504	0.000000	IntelCor_59:24:c8	Sercomm_f7:d3:40	ARP	42	Who has 192.168.1.1? Tell 192.168.1.12
505	0.003931	Sercomm_f7:d3:40	IntelCor_59:24:c8	ARP	42	192.168.1.1 is at 38:02:de:f7:d3:40

> Frame 505: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{11981F20-5231-4861-ABD2-DD8A4A767C}

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

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

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

Type: ARP (0x0806)

```

0000 f8 63 3f 59 24 c8 38 02 de f7 d3 40 08 06 00 01  .c?Y$.8. ...@...
0010 08 00 06 04 00 02 38 02 de f7 d3 40 c0 a8 01 01  ....8. ...@....
0020 f8 63 3f 59 24 c8 c0 a8 01 0c                   .c?Y$... ..
  
```

Ethernet (eth), 14 byte(s) | Packets: 718 · Displayed: 2 (0.3%) | Profile: Default

4.27 Ναι, αφού συνδέομαι από Wi-Fi (ασύρματα) δεν καταγραφεται (και ούτε βλέπω) το padding που φτάνει έως 64 bytes

4.28 (Θεωρητικά) Το wireshark θα καταγράφει τα πακέτα πριν φτάσουν στο στρώμα ζεύξης όπου και θα αποκτήσουν το απαραίτητο padding μέχρι τα 64 bytes που είναι το ελάχιστο μέγεθος για το πλαίσιο ethernet. Στην απάντηση όπου το padding έχει γίνει από τον αποστολέα θα είναι φαίνεται στο wireshark. Φυσικά εγώ βλέπω ίδια τα μεγέθη

4.29 Το πεδίο Opcode

4.30 Στο ARP request (θεωρητικά) το πεδίο Target MAC address έχει την τιμή 00:00:00:00:00:00 καθώς δεν το γνωρίζουμε (γι αυτό εξάλλου στέλνουμε το request). Στο reply αυτή η τιμή προφανώς θα αντικατασταθεί από την MAC address της συσκευής που ψάχναμε. Επίσης το request το στέλνουμε «ανοικτά» (broadcast) ενώ το reply στέλνεται προς συγκεκριμένο παραλήπτη.

4.31 Θα έχετε σε κίνδυνο τα δεδομένα όλων των χρηστών του δικτύου, καθώς θα έστελναν πλαίσια στον κακόβουλο υπολογιστή, και αυτός θα μπορεί να ελέγχει τη ροή επικοινωνίας και μπορεί να αποσπάσει ή να αλλάξει πληροφορίες που στέλνονται από κάποιον/ους φιλικό/ούς χρήστη/ες.