

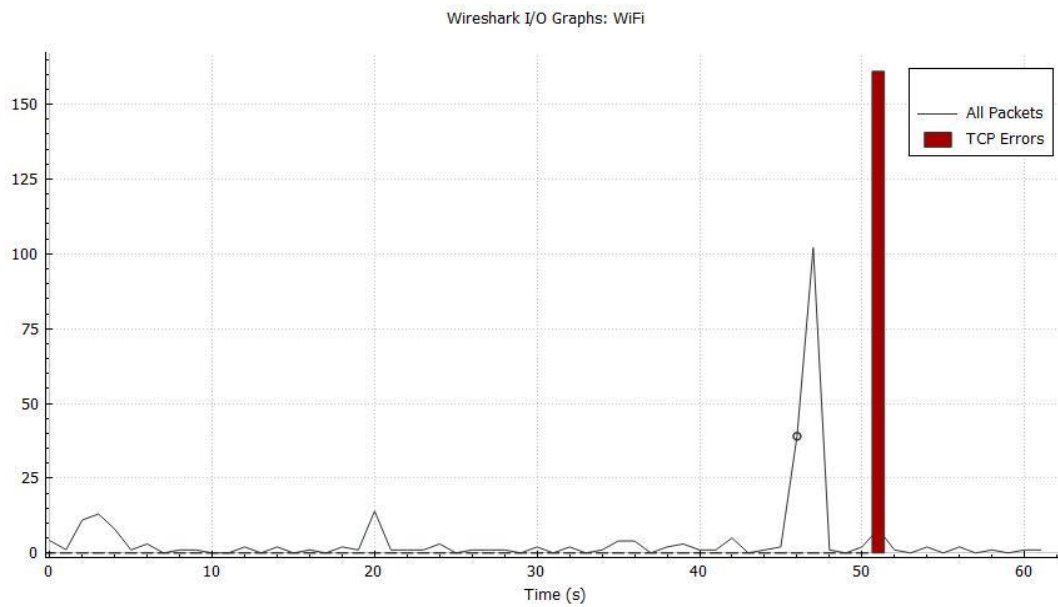
Εργασία εργαστηρίου 2 – Δίκτυα υπολογιστών

Όνομα: Ζήνα Γκούμα

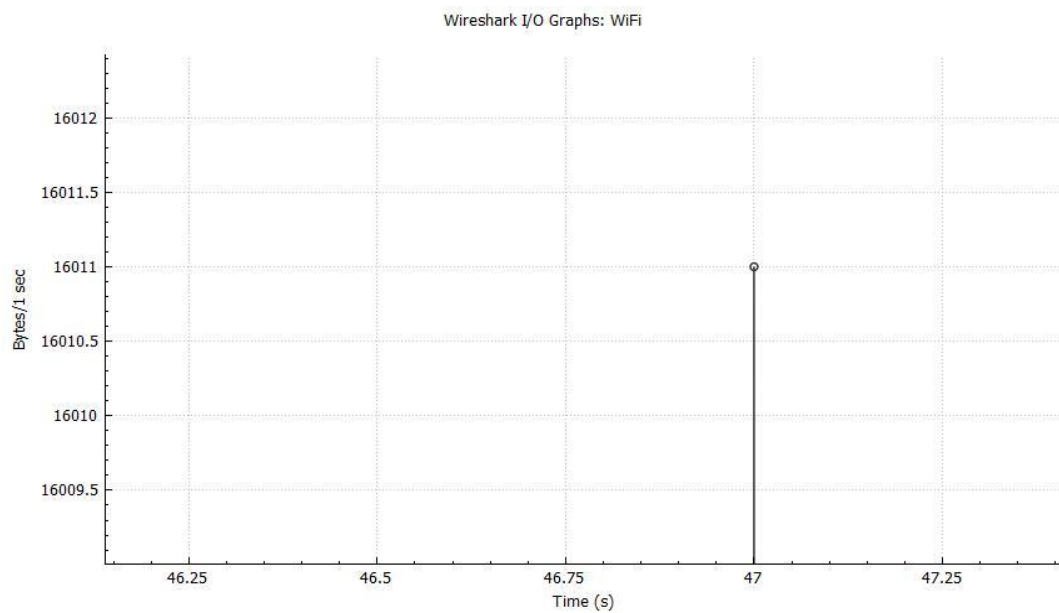
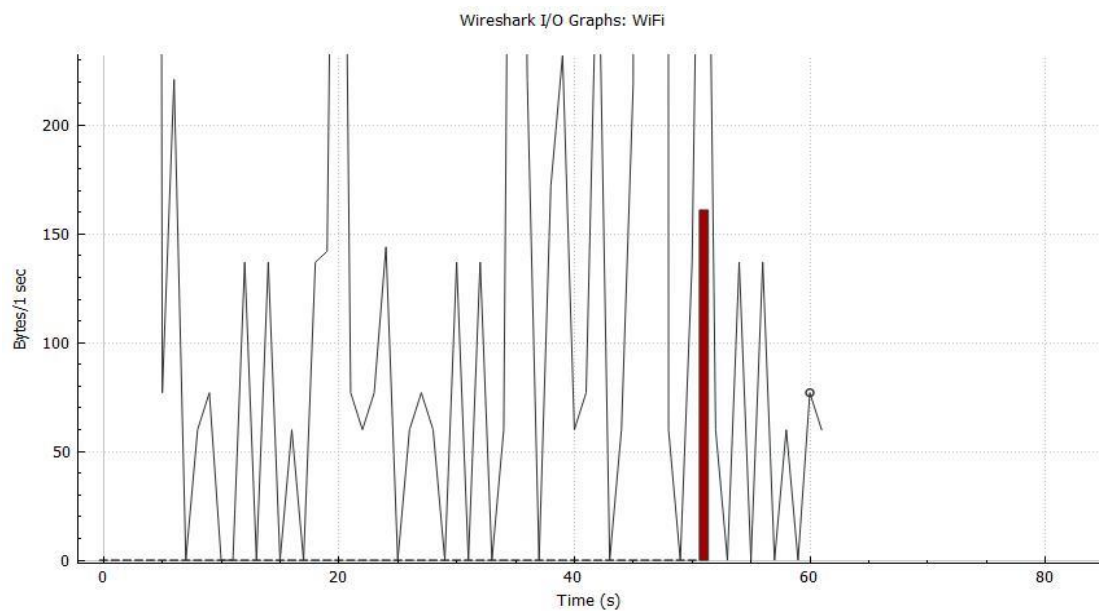
ΑΜ: Π20048

Δραστηριότητα 1^η

1.1) (α) Στο γράφημα packets/sec, η μέγιστη τιμή είναι 102 packets/sec.



(β) Στο γράφημα bytes/sec, η μέγιστη τιμή είναι 16.011 bytes/sec.

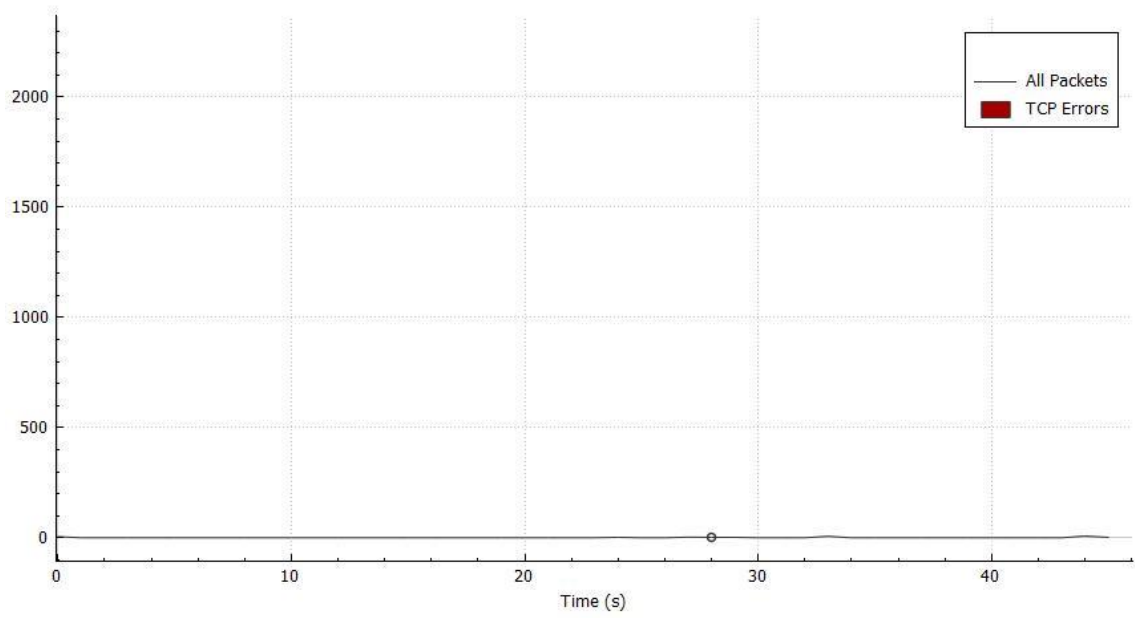


Δραστηριότητα 2^η

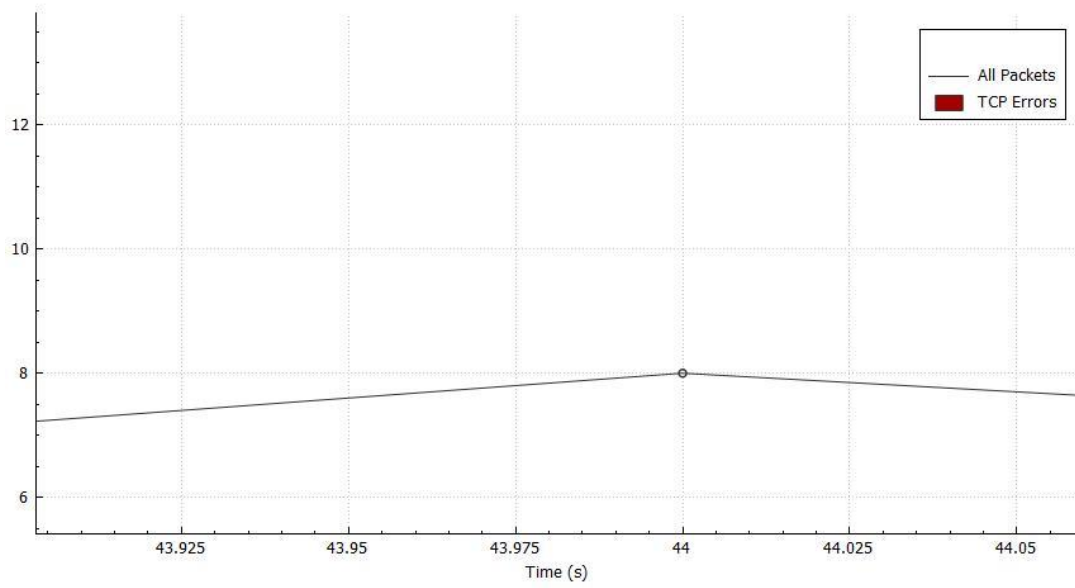
2.1) Η IP address είναι: IPv4 Address. : 192.168.1.5

(α) Η μέγιστη τιμή για packets/sec, είναι 8 packets/sec.

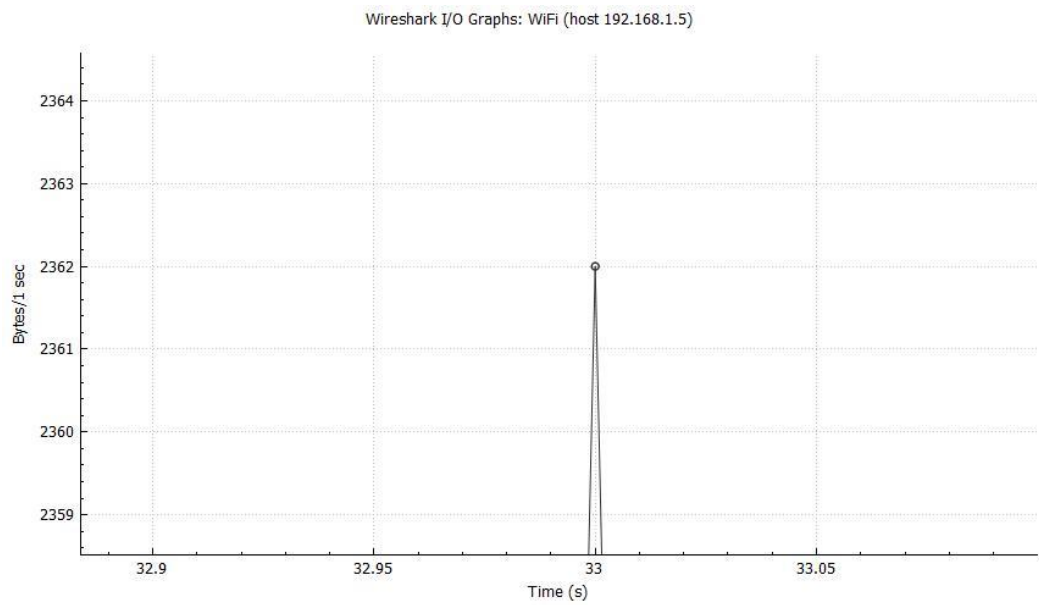
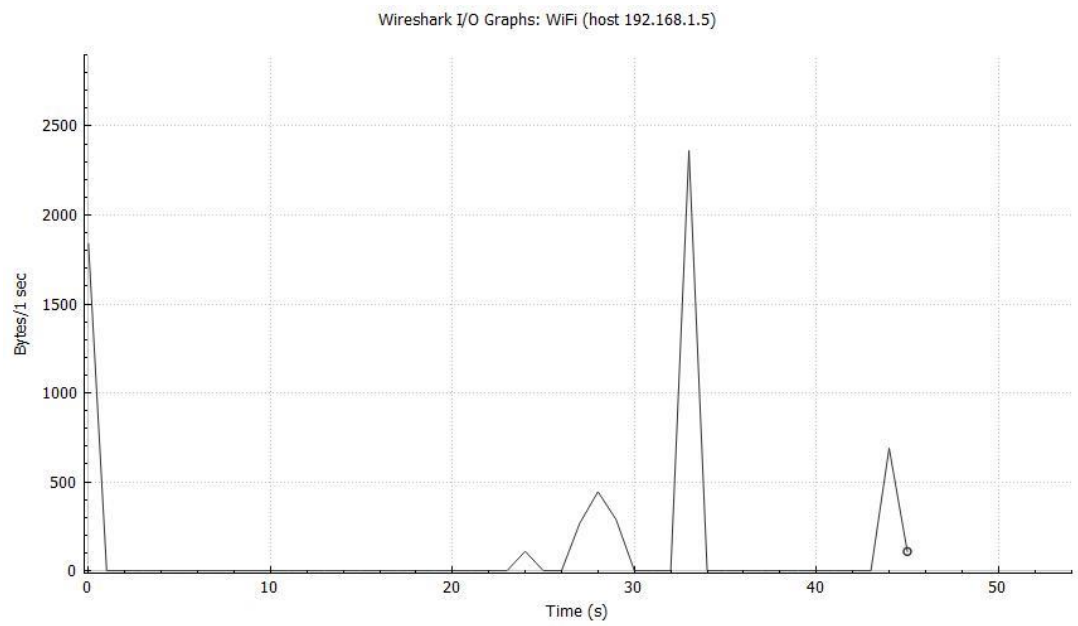
Wireshark I/O Graphs: WiFi (host 192.168.1.5)



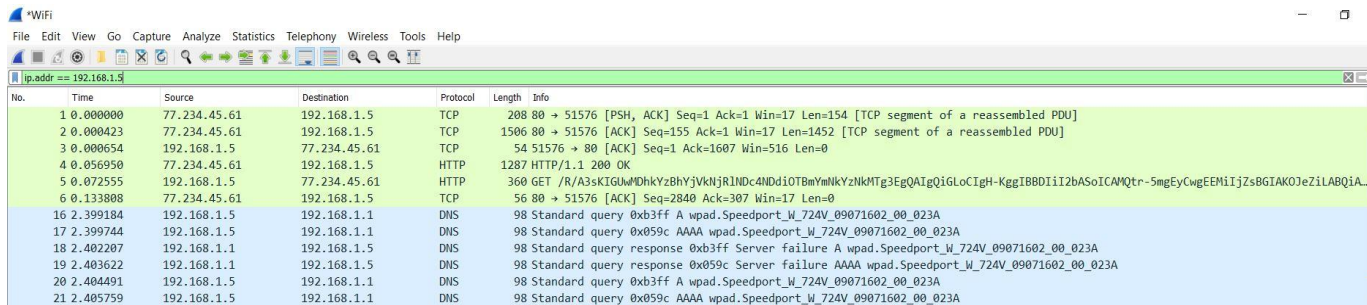
Wireshark I/O Graphs: WiFi (host 192.168.1.5)



(β) Η μέγιστη τιμή για bytes/sec, είναι 2362 byte/sec.



2.2) Παρατηρώ ότι από το σύνολο των ανάμεικτων πακέτων που έχουν συλληφθεί, εμφανίζονται μόνο αυτά στα οποία είτε ο πομπός είτε ο δέκτης ταυτίζονται με την δοθείσα IP.

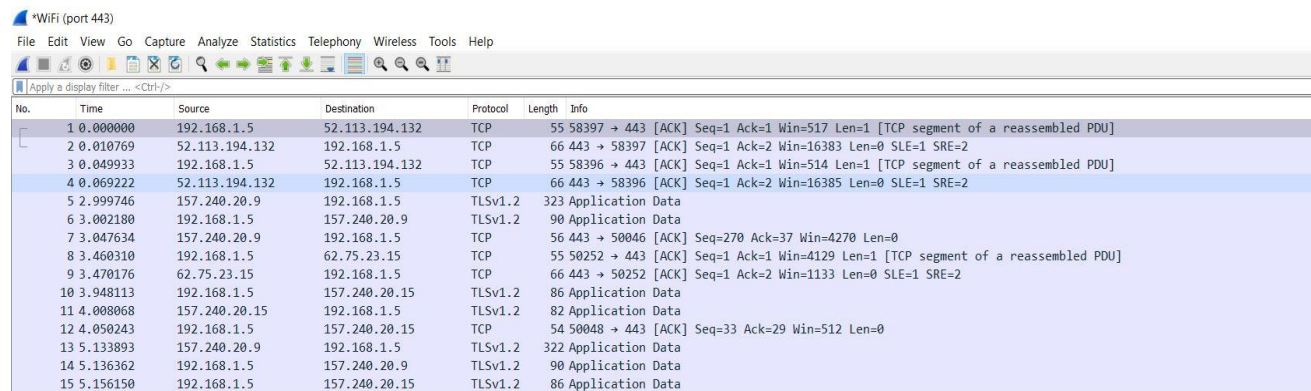


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	77.234.45.61	192.168.1.5	TCP	208	80 → 51576 [PSH, ACK] Seq=1 Ack=1 Win=17 Len=154 [TCP segment of a reassembled PDU]
2	0.000423	77.234.45.61	192.168.1.5	TCP	1506	80 → 51576 [ACK] Seq=155 Ack=1 Win=17 Len=1452 [TCP segment of a reassembled PDU]
3	0.000654	192.168.1.5	77.234.45.61	TCP	54	51576 → 80 [ACK] Seq=1 Ack=1607 Win=516 Len=0
4	0.056950	77.234.45.61	192.168.1.5	HTTP	1287	HTTP/1.1 200 OK
5	0.072555	192.168.1.5	77.234.45.61	HTTP	360	GET /R/A3sKIGUjMDhkYz8hYjVkJRlNDc4NDdiOTBmYmNkYzNkMTg3EgQAIgQigLoIgh-KggIBBDIIi2bASoICAMQtr-5mgEyCwgEEMiIjZs8GIAK0JeZiLABQIA...
6	0.133808	77.234.45.61	192.168.1.5	TCP	56	80 → 51576 [ACK] Seq=2840 Ack=307 Win=17 Len=0
16	2.399184	192.168.1.5	192.168.1.1	DNS	98	Standard query 0xb3ff A wpad.Speedport_W_724V_09071602_00_023A
17	2.399744	192.168.1.5	192.168.1.1	DNS	98	Standard query 0xb3ff AAAA wpad.Speedport_W_724V_09071602_00_023A
18	2.402207	192.168.1.1	192.168.1.5	DNS	98	Standard query response 0xb3ff Server failure A wpad.Speedport_W_724V_09071602_00_023A
19	2.403622	192.168.1.1	192.168.1.5	DNS	98	Standard query response 0xb3ff Server failure AAAA wpad.Speedport_W_724V_09071602_00_023A
20	2.404491	192.168.1.5	192.168.1.1	DNS	98	Standard query 0xb3ff A wpad.Speedport_W_724V_09071602_00_023A
21	2.405759	192.168.1.5	192.168.1.1	DNS	98	Standard query 0xb3ff AAAA wpad.Speedport_W_724V_09071602_00_023A

2.3) Η βασική διαφορά είναι ότι το capture filter καθορίζει απ' την αρχή τα χαρακτηριστικά των πακέτων που θα συλληφθούν, ενώ το display filter αφού πρώτα συλληφθούν όλα τα πακέτα θα προβάλλει τα πακέτα τα οποία πληρούν τα χαρακτηριστικά της εντολής. Μια άλλη διαφορά είναι ότι τα μέλη των εντολών στο capture filter ενώνονται με το κενό, όμως στο display filter θυμίζουν τις προγραμματιστικές εντολές, καθώς ενώνονται με τελεστές.

2.4) Εντολές capture filter

Με το capture filter **port 443**, θα συλληφθούν μόνο τα πακέτα στα οποία ο πομπός ή ο δέκτης είναι η θύρα 443.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.5	52.113.194.132	TCP	55	58397 → 443 [ACK] Seq=1 Ack=1 Win=517 Len=1 [TCP segment of a reassembled PDU]
2	0.010769	52.113.194.132	192.168.1.5	TCP	66	443 → 58397 [ACK] Seq=1 Ack=2 Win=16383 Len=0 SLE=1 SRE=2
3	0.049933	192.168.1.5	52.113.194.132	TCP	55	58396 → 443 [ACK] Seq=1 Ack=1 Win=514 Len=1 [TCP segment of a reassembled PDU]
4	0.069222	52.113.194.132	192.168.1.5	TCP	66	443 → 58396 [ACK] Seq=1 Ack=2 Win=16385 Len=0 SLE=1 SRE=2
5	2.999746	157.240.20.9	192.168.1.5	TLSv1.2	323	Application Data
6	3.002180	192.168.1.5	157.240.20.9	TLSv1.2	90	Application Data
7	3.047634	157.240.20.9	192.168.1.5	TCP	56	443 → 50046 [ACK] Seq=270 Ack=37 Win=4270 Len=0
8	3.460310	192.168.1.5	62.75.23.15	TCP	55	50252 → 443 [ACK] Seq=1 Ack=1 Win=4129 Len=1 [TCP segment of a reassembled PDU]
9	3.470176	62.75.23.15	192.168.1.5	TCP	66	443 → 50252 [ACK] Seq=1 Ack=2 Win=1133 Len=0 SLE=1 SRE=2
10	3.948113	192.168.1.5	157.240.20.15	TLSv1.2	86	Application Data
11	4.008068	157.240.20.15	192.168.1.5	TLSv1.2	82	Application Data
12	4.050243	192.168.1.5	157.240.20.15	TCP	54	50048 → 443 [ACK] Seq=33 Ack=29 Win=512 Len=0
13	5.133893	157.240.20.9	192.168.1.5	TLSv1.2	322	Application Data
14	5.136362	192.168.1.5	157.240.20.9	TLSv1.2	90	Application Data
15	5.156150	192.168.1.5	157.240.20.15	TLSv1.2	86	Application Data

Με το *src 192.168.1.5*, θα συλληφθούν μόνο τα πακέτα στα οποία ο πομπός ταυτίζεται με την συγκεκριμένη διεύθυνση IP.

*WiFi (src 192.168.1.5)

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	192.168.1.5	157.240.20.15	TLSv1.2	86	Application Data
2	0.000024	192.168.1.5	157.240.20.15	TLSv1.2	86	Application Data
3	0.108043	192.168.1.5	157.240.20.15	TCP	54	50048 → 443 [ACK] Seq=33 Ack=29 Win=515 Len=0
4	0.108043	192.168.1.5	157.240.20.15	TCP	54	50044 → 443 [ACK] Seq=33 Ack=29 Win=512 Len=0
5	2.506928	192.168.1.5	192.168.1.1	DNS	85	Standard query 0x62cc AAAA nexus.officeapps.live.com
6	2.526027	192.168.1.5	192.168.1.1	DNS	85	Standard query 0x62cc AAAA nexus.officeapps.live.com
7	2.540760	192.168.1.5	192.168.1.1	DNS	85	Standard query 0x62cc AAAA nexus.officeapps.live.com
8	2.558513	192.168.1.5	192.168.1.1	DNS	85	Standard query 0x62cc AAAA nexus.officeapps.live.com

Εντολές display filter

Με το *tcp*, από το σύνολο των συλληφθέντων πακέτων, θα εμφανιστούν μόνο τα πακέτα tcp.

*WiFi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
2	0.584215	192.168.1.5	5.62.48.208	TCP	55	49886 → 443 [ACK] Seq=1 Ack=1 Win=516 Len=1 [TCP segment of a reassembled PDU]
5	2.938544	192.168.1.5	52.114.74.224	TLSv1.2	111	Application Data
6	2.994182	52.114.74.224	192.168.1.5	TLSv1.2	100	Application Data
8	3.037818	192.168.1.5	52.114.74.224	TCP	54	62529 → 443 [ACK] Seq=58 Ack=47 Win=514 Len=0
19	4.278690	192.168.1.5	172.217.16.131	TCP	54	49294 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
20	4.279371	192.168.1.5	216.239.32.116	TCP	54	49293 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
21	4.280771	2a02:587:243e:da41::...	2a00:1450:4001:82a::...	TCP	86	55698 → 443 [SYN] Seq=0 Win=64440 Len=0 MSS=1432 WS=256 SACK_PERM=1
24	4.326317	2a00:1450:4001:82a::...	2a02:587:243e:da41::...	TCP	86	443 → 55698 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 SACK_PERM=1 WS=256
25	4.326613	2a02:587:243e:da41::...	2a00:1450:4001:82a::...	TCP	74	55698 → 443 [ACK] Seq=1 Ack=1 Win=65792 Len=0

Με το *tcp.port == 443 or dns*, εμφανίζονται μόνο τα πακέτα που έχουν την θύρα 443 ή είναι DNS.

*WiFi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 443 or dns

No.	Time	Source	Destination	Protocol	Length	Info
2	0.584215	192.168.1.5	5.62.48.208	TCP	55	49886 → 443 [ACK] Seq=1 Ack=1 Win=516 Len=1 [TCP segment of a reassembled PDU]
5	2.938544	192.168.1.5	52.114.74.224	TLSv1.2	111	Application Data
6	2.994182	52.114.74.224	192.168.1.5	TLSv1.2	100	Application Data
8	3.037818	192.168.1.5	52.114.74.224	TCP	54	62529 → 443 [ACK] Seq=58 Ack=47 Win=514 Len=0
9	4.162441	fe80::206b:624e:78f...	fe80::964a:cff:fe2e...	DNS	99	Standard query 0xafe2 A clients2.google.com
10	4.162946	fe80::206b:624e:78f...	fe80::964a:cff:fe2e...	DNS	99	Standard query 0xc54e AAAA clients2.google.com
11	4.174746	fe80::964a:cff:fe2e...	fe80::206b:624e:78f...	DNS	158	Standard query response 0xafe2 A clients2.google.com CNAME clients.l.google.com
12	4.178273	fe80::964a:cff:fe2e...	fe80::206b:624e:78f...	DNS	178	Standard query response 0xc54e AAAA clients2.google.com CNAME clients.l.google.com
19	4.278690	192.168.1.5	172.217.16.131	TCP	54	49294 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Δραστηριότητα 3^η

3.1)

Wireshark packet capture showing ICMPv6 traffic. The capture is filtered for 'Apply a display filter ... <Ctrl>+'. The packet list shows:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::964a:cff:fe2e::	ff02::1	ICMPv6	142	Router Advertisement
2	0.275596	2a02:587:243e:da41::	2a02:587:a00::d4cd::	TCP	75	60877 → 443 [ACK] Seq=1 Ack=1 Win=514 Len=1 [TCP segment of a reassembled PDU]
3	0.284196	2a02:587:a00::d4cd::	2a02:587:243e:da41::	TCP	74	443 → 60877 [RST] Seq=1 Win=0 Len=0
4	5.282688	fe80::964a:cff:fe2e::	2a02:587:243e:da41::	ICMPv6	86	Neighbor Solicitation for 2a02:587:243e:da41:988d:6200:25c2:4157 from 94:4a:0c:2e:79:e0
5	5.282881	2a02:587:243e:da41::	fe80::964a:cff:fe2e::	ICMPv6	86	Neighbor Advertisement 2a02:587:243e:da41:988d:6200:25c2:4157 (sol, ovr) is at 3c:a9:f4:19:c5
6	7.797292	2a02:587:243e:da41::	2603:1026:302:104::2	TCP	75	60883 → 443 [ACK] Seq=1 Ack=1 Win=514 Len=1 [TCP segment of a reassembled PDU]
7	7.831878	2603:1026:302:104::2	2a02:587:243e:da41::	TCP	86	443 → 60883 [ACK] Seq=1 Ack=2 Win=16381 Len=0 SLE=1 SRE=2
8	8.136228	192.168.1.5	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
9	9.148358	192.168.1.5	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

Frame 1: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface \Device\NPF_{D242DC68-0DC1-400B-A218-F0EC5B2CB6A5}, id 0
> Ethernet II, Src: Sercomm_2e:79:e0 (94:4a:0c:2e:79:e0), Dst: IPv6mcast_01 (33:33:00:00:00:01)
> Internet Protocol Version 6, Src: fe80::964a:cff:fe2e:79e0, Dst: ff02::1
> Internet Control Message Protocol v6

Handwritten notes in blue ink:

- Μέρος 1ο
- Μέρος 2ο
- Μέρος 3ο

1^ο μέρος: Εκεί εμφανίζονται τα πακέτα που κινούνται μέσα στο τοπικό δίκτυο, δηλαδή τα πακέτα που έχουν συλληφθεί.

2^ο μέρος: Είναι η στοίβα με τα πρωτόκολλα που χρησιμοποίησε το επιλεγμένο πακέτο για να φτάσει στον προορισμό του, ξεκινώντας απ' το φυσικό επίπεδο και προχωρώντας στα ανώτερα επίπεδα.

3^ο μέρος: Εκεί εμφανίζεται ένα επιλεγμένο πακέτο σε μορφή bit. Κάνοντας hover με το ποντίκι σ' ένα τμήμα bit, φαίνεται στο δεξί μέρος ποιες πληροφορίες αντιπροσωπεύει.

Δραστηριότητα 4^η

4.1) Η εντολή **ping** χρησιμοποιείται για τον έλεγχο σύνδεσης μεταξύ του συγκεκριμένου υπολογιστή μ' ένα άλλο host. Συγκεκριμένα, ο υπολογιστής μας στέλνει 4 πακέτα ICMP στον δέκτη (echo request) και αν αυτός απαντήσει (echo reply), σημαίνει πως υπάρχει σύνδεση πομπού – δέκτη. Χαρακτηριστικά των πακέτων ICMP είναι το μέγεθός του (28-2068 bytes), το Round Trip Time δηλαδή τον χρόνο που πέρασε μέχρι να ληφθεί η απάντηση και το time-to-live, το οποίο αναφέρεται στον αριθμό των 'hops' που έχει ένα πακέτο προτού απορριφθεί από έναν δρομολογητή. Ο μέγιστος αριθμός time-to-live που μπορεί να έχει ένα πακέτο είναι 255. Επιπλέον, η ping εμφανίζει κάποια στατιστικά, όπως τον αριθμό των πακέτων που στάλθηκαν, που ελήφθησαν και χάθηκαν αλλά και το μέγιστο, ελάχιστο και μέσο RTT.

4.2) Χρησιμοποιήθηκε το πρωτόκολλο ICMP και ανταλλάχθηκαν 4 ζεύγη μηνυμάτων echo request και echo reply.

4.3)

No.	Time	Source	Destination	Protocol	Length	Info
req	25 5.989904	192.168.1.5	195.251.229.4	ICMP	74	Echo (ping) request id=0x0001, seq=13/3328, ttl=128 (reply in 26)
rep	26 6.014411	195.251.229.4	192.168.1.5	ICMP	74	Echo (ping) reply id=0x0001, seq=13/3328, ttl=55 (request in 25)
	28 6.999232	192.168.1.5	195.251.229.4	ICMP	74	Echo (ping) request id=0x0001, seq=14/3584, ttl=128 (reply in 29)
	29 7.012566	195.251.229.4	192.168.1.5	ICMP	74	Echo (ping) reply id=0x0001, seq=14/3584, ttl=55 (request in 28)
	31 8.009304	192.168.1.5	195.251.229.4	ICMP	74	Echo (ping) request id=0x0001, seq=15/3840, ttl=128 (reply in 32)
	32 8.123719	195.251.229.4	192.168.1.5	ICMP	74	Echo (ping) reply id=0x0001, seq=15/3840, ttl=55 (request in 31)
	33 9.019348	192.168.1.5	195.251.229.4	ICMP	74	Echo (ping) request id=0x0001, seq=16/4096, ttl=128 (reply in 34)
	34 9.046659	195.251.229.4	192.168.1.5	ICMP	74	Echo (ping) reply id=0x0001, seq=16/4096, ttl=55 (request in 33)

Το πρώτο echo request μαζί με το αντίστοιχο echo reply είναι σημειωμένα στην εικόνα.

Περιγραφή στοίβας πρωτοκόλλων

Στο επίπεδο σύνδεσης δεδομένων, δηλαδή στο Ethernet, αναγράφεται η διεύθυνση MAC του αποστολέα και του παραλήπτη και τον τύπο πρωτοκόλλου που χρησιμοποιεί το Ethernet σε ανώτερο επίπεδο.

Στο επίπεδο δικτύου αναγράφεται η έκδοση IP που χρησιμοποιείται, το μέγεθος της επικεφαλίδας, ο τύπος υπηρεσίας που παρέχει, καθώς και το συνολικό μέγεθος του πακέτου και ο identifier. Επίσης, προβάλλονται το flags και το fragment offset, που αφορούν τον κατακερματισμό του πακέτου, η παράμετρος time-to-live, το πρωτόκολλο που χρησιμοποιεί το IP, το header checksum και το status του, αλλά και την διεύθυνση IP του αποστολέα και του παραλήπτη.

Στο επίπεδο ICMP φαίνονται ο τύπος και ο κωδικός του τύπου του μηνύματος, το checksum και το status του, καθώς και το identifier μαζί με το sequence number σε Big Endian και Little Endian μορφή. Τέλος, υπάρχει το τμήμα δεδομένων του πακέτου και το μέγεθος τους.

4.4) Κάθε πακέτο χρησιμοποιεί τα πρωτόκολλα Ethernet II, IPv4 και ICMP και έχει μέγεθος 74 byte. Επιπλέον, τα πακέτα echo request έχουν TTL 128, ενώ τα echo reply έχουν TTL 55.

Τα στοιχεία που περιέχονται στο πρωτόκολλο IPv4, είναι τα ακόλουθα:

```
▼ Internet Protocol Version 4, Src: 192.168.1.5, Dst: 195.251.229.4
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x69c3 (27075)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: ICMP (1)
    Header Checksum: 0x6650 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.5
    Destination Address: 195.251.229.4
```


Η αντιστοιχία σε bit πακέτου σε καθεμία απ' τις πληροφορίες είναι:

0100 = Version: 4

.... 0101 = Header Length: 20 bytes

0000	94	4a	0c	2e	79	e0	3c	a9	f4	19	c9	84	08	00	45	00	.J..y.<.....E.
0010	00	3c	69	c3	00	00	80	01	66	50	c0	a8	01	05	c3	fb	<i.....fP.....
0020	e5	04	08	00	44	25	00	01	09	36	61	62	63	64	65	66D%..-6abcdef
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

Differentiated Services Field: 0x00

0000	94	4a	0c	2e	79	e0	3c	a9	f4	19	c9	84	08	00	45	00	.J..y.<.....E.
0010	00	3c	69	c3	00	00	80	01	66	50	c0	a8	01	05	c3	fb	<i.....fP.....
0020	e5	04	08	00	44	25	00	01	09	36	61	62	63	64	65	66D%..-6abcdef
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

Total Length: 60

0000	94	4a	0c	2e	79	e0	3c	a9	f4	19	c9	84	08	00	45	00	.J..y.<.....E.
0010	00	3c	69	c3	00	00	80	01	66	50	c0	a8	01	05	c3	fb	<i.....fP.....
0020	e5	04	08	00	44	25	00	01	09	36	61	62	63	64	65	66D%..-6abcdef
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

Identification: 0x69c3

0000	94	4a	0c	2e	79	e0	3c	a9	f4	19	c9	84	08	00	45	00	.J..y.<.....E.
0010	00	3c	69	c3	00	00	80	01	66	50	c0	a8	01	05	c3	fb	<i.....fP.....
0020	e5	04	08	00	44	25	00	01	09	36	61	62	63	64	65	66D%..-6abcdef
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

Flags: 0x00

...0 0000 0000 0000 = Fragment Offset: 0

0000	94	4a	0c	2e	79	e0	3c	a9	f4	19	c9	84	08	00	45	00	.J..y.<.....E.
0010	00	3c	69	c3	00	00	80	01	66	50	c0	a8	01	05	c3	fb	<i.....fP.....
0020	e5	04	08	00	44	25	00	01	09	36	61	62	63	64	65	66D%..-6abcdef
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

Time to live: 128

0000	94	4a	0c	2e	79	e0	3c	a9	f4	19	c9	84	08	00	45	00	.J..y.<.....E.
0010	00	3c	69	c3	00	00	80	01	66	50	c0	a8	01	05	c3	fb	<i.....fP.....
0020	e5	04	08	00	44	25	00	01	09	36	61	62	63	64	65	66D%..-6abcdef
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

Protocol: ICMP

0000	94	4a	0c	2e	79	e0	3c	a9	f4	19	c9	84	08	00	45	00	.J..y.<.....E.
0010	00	3c	69	c3	00	00	80	01	66	50	c0	a8	01	05	c3	fb	<i.....fP.....
0020	e5	04	08	00	44	25	00	01	09	36	61	62	63	64	65	66D%..-6abcdef
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

Header Checksum: 0x6650

0000	94	4a	0c	2e	79	e0	3c	a9	f4	19	c9	84	08	00	45	00	.J..y.<.....E.
0010	00	3c	69	c3	00	00	80	01	66	50	c0	a8	01	05	c3	fb	<i.....fP.....
0020	e5	04	08	00	44	25	00	01	09	36	61	62	63	64	65	66D%..-6abcdef
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

Source Address: 192.168.1.5

0000	94 4a 0c 2e 79 e0 3c a9	f4 19 c9 84 08 00 45 00	-J..y.<E-
0010	00 3c 69 c3 00 00 80 01	66 50 c0 a8 01 05 c3 fb	-<i.fP.
0020	e5 04 08 00 44 25 00 01	09 36 61 62 63 64 65 66 D% . . . 6abcdef
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

Destination Address: 195.251.229.4

0000	94 4a 0c 2e 79 e0 3c a9	f4 19 c9 84 08 00 45 00	-J..y.<E-
0010	00 3c 69 c3 00 00 80 01	66 50 c0 a8 01 05 c3 fb	-<i.fP.
0020	e5 04 08 00 44 25 00 01	09 36 61 62 63 64 65 66 D% . . . 6abcdef
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

Επίσης, το τμήμα των Data που βλέπει το ICMP αποτελείται από 32 bytes.

0000	94 4a 0c 2e 79 e0 3c a9	f4 19 c9 84 08 00 45 00	-J..y.<E-
0010	00 3c 69 cb 00 00 80 01	66 48 c0 a8 01 05 c3 fb	-<i.fH.
0020	e5 04 08 00 44 1d 00 01	09 3e 61 62 63 64 65 66 D. . . . >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

4.5) Χρησιμοποιούμε την εντολή `ping -l 128`.

```
C:\WINDOWS\system32> ping -l 128
IP address must be specified.

C:\WINDOWS\system32> ping -l 128 www.unipi.gr

Pinging unipiweb.unipi.gr [195.251.229.4] with 128 bytes of data:
Reply from 195.251.229.4: bytes=128 time=16ms TTL=55
Reply from 195.251.229.4: bytes=128 time=14ms TTL=55
Reply from 195.251.229.4: bytes=128 time=16ms TTL=55
Reply from 195.251.229.4: bytes=128 time=13ms TTL=55

Ping statistics for 195.251.229.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 13ms, Maximum = 16ms, Average = 14ms

C:\WINDOWS\system32>
```

- a) Οι βασικές πληροφορίες είναι παρόμοιες με πριν, με την κύρια διαφορά ότι τα πακέτα τώρα έχουν μέγεθος 128 byte.

Τα στοιχεία που περιέχονται στο IPv4 είναι τα ακόλουθα:

```

Internet Protocol Version 4, Src: 192.168.1.5, Dst: 195.251.229.4
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 156
    Identification: 0x69c7 (27079)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: ICMP (1)
    Header Checksum: 0x65ec [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.5
    Destination Address: 195.251.229.4

```

Η αντιστοιχία σε bit πακέτου σε καθεμία απ' τις πληροφορίες είναι ακριβώς ίδια με την προηγούμενη περίπτωση.

- b) Τα Data πλέον αποτελούνται από 128 byte, ενώ πριν αποτελούνταν από 32.

0000	94 4a 0c 2e 79 e0 3c a9 f4 19 c9 84 08 00 45 00	-J..y.<.....E-
0010	00 9c 69 c7 00 00 80 01 65 ec c0 a8 01 05 c3 fb	..i.....e.....
0020	e5 04 08 00 f1 cc 00 01 09 3a 61 62 63 64 65 66: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 6a 6b 6c 6d 6e 6f	wabcdefgh hijklmno
0050	70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68	pqrstuvw abcdefgh
0060	69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61	ijklmnop qrstuvw
0070	62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71	bcdefghi jklmnopq
0080	72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 6a	rstuvwab cdefghij
0090	6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63	klmnopqr stuvwabc
00a0	64 65 66 67 68 69 6a 6b 6c 6d	defghijk lm

- c) Αυτά τα δεδομένα περιέχουν την Αγγλική αλφάβητο, διότι προκειμένου τα πακέτα να φτάσουν το μέγεθος που τους 'ζητήσαμε', γεμίζουν με πληροφορία που δεν έχει συγκεκριμένο νόημα.

Δραστηριότητα 5^η

5.1) Χρησιμοποιούνται τα πρωτόκολλα Ethernet, IP, UDP και DNS.

```
> Frame 3: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \Device\NPF_{D242DC68-0}
> Ethernet II, Src: IntelCor_19:c9:84 (3c:a9:f4:19:c9:84), Dst: Sercomm_2e:79:e0 (94:4a:0c:2e:79:e0)
> Internet Protocol Version 6, Src: fe80::206b:624e:78f2:cbdd, Dst: fe80::964a:cff:fe2e:79e0
> User Datagram Protocol, Src Port: 63327, Dst Port: 53
> Domain Name System (query)
```

5.2)

```
▼ Domain Name System (query)
  Transaction ID: 0x2c9e
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  > Queries
    [Response In: 5]
```

Στην επικεφαλίδα DNS περιέχεται το transaction ID του query, τα flags που είναι πληροφορίες σχετικά με τον τύπο του μηνύματος και τον τρόπο που μεταδίδεται αυτό, το πλήθος των ερωτήσεων, το πλήθος των απαντήσεων, των αυθεντικών απαντήσεων και των επιπλέον απαντήσεων.

```
▼ Queries
  ▼ apple.com: type A, class IN
    Name: apple.com
    [Name Length: 9]
    [Label Count: 2]
    Type: A (Host Address) (1)
    Class: IN (0x0001)
```

Επίσης, στο τμήμα των queries παρέχει πληροφορίες για το server με τον οποίο είμαστε σε επικοινωνία, όπως το όνομά του, τον τύπο του και την κλάση του.

Κάποια στοιχεία που είναι κοινά σε κάθε πακέτο είναι:

- α) Ο αποστολέας > Source: IntelCor_19:c9:84 (3c:a9:f4:19:c9:84)
- β) Ο παραλήπτης > Destination: Sercomm_2e:79:e0 (94:4a:0c:2e:79:e0)
- γ) Το μέγεθος του πακέτου Frame 20: 93 bytes on wire (744 bits)
- δ) (Η απάντηση στο 5.1)
- ε) Οι θύρες που εμπλέκονται Source Port: 60113
Destination Port: 53
- στ) Το ερώτημα υποβάλλεται με UDP request απ' τον πελάτη.
- ζ) Η απάντηση δίνεται μέσω UDP reply απ' τον εξυπηρετητή DNS.

5.3) Ethernet >> Επίπεδο Σύνδεσης Δεδομένων

IPv4 >> Επίπεδο Δικτύου

UDP >> Επίπεδο Μεταφοράς

DNS >> Επίπεδο Εφαρμογής

5.4) Μέγεθος: 503 bytes

IP αποστολέα: 192.168.1.5

IP παραλήπτη: 52.0.14.116

port αποστολέα: 60546

port παραλήπτη: 80

Το μήνυμα HTTP GET και η απόκριση του server είναι τα παρακάτω:

http						
Packet details Narrow & Wide Case sensitive String www.nasa.gov						
No.	Time	Source	Destination	Protocol	Length	Info
68	14.014755	192.168.1.5	52.0.14.116	HTTP	503	GET / HTTP/1.1
73	14.150150	52.0.14.116	192.168.1.5	HTTP	448	HTTP/1.1 301 Moved Permanently (text/html)

5.5)



```
Wireshark · Follow HTTP Stream (tcp.stream eq 11) · WiFi

GET / HTTP/1.1
Host: nasa.gov
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/100.0.4896.127 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: en-GB,en-US;q=0.9,en;q=0.8,el;q=0.7

HTTP/1.1 301 Moved Permanently
Server: nginx/1.14.0 (Ubuntu)
Date: Thu, 28 Apr 2022 16:04:45 GMT
Content-Type: text/html
Content-Length: 194
Connection: close
Location: https://www.nasa.gov/

<html>
<head><title>301 Moved Permanently</title></head>
<body bgcolor="white">
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx/1.14.0 (Ubuntu)</center>
</body>
</html>
```

5.6) (Η εικόνα στο 5.4)

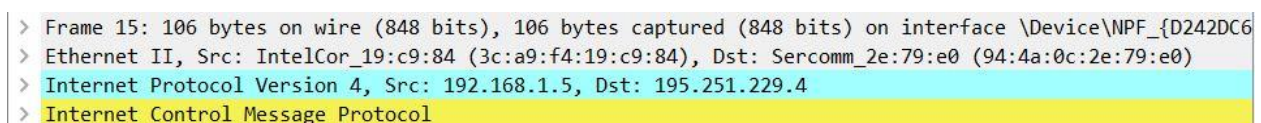
5.7) http && ip.src == 192.168.1.5

Δραστηριότητα 6^η

6.1) Η εντολή **tracert** είναι το εργαλείο ανίχνευσης διαδρομής που χρησιμοποιείται σε λειτουργικά συστήματα τύπου Unix. Καθορίζει την διαδρομή προς έναν προορισμό στέλνοντας σ' αυτόν πακέτα ICMP, στα οποία χρησιμοποιεί ποικίλες τιμές time-to-live (TTL).

Η εντολή **pathping** συνδυάζει την λειτουργικότητα της ping και της tracert και χρησιμοποιείται για την για τον εντοπισμό σημείων που παρουσιάζεται καθυστέρηση δικτύου και απώλεια δικτύου. Αναλυτικότερα, παρέχει λεπτομέρειες της διαδρομής μεταξύ δυο υπολογιστών και στατιστικά για κάθε κόμβο στην διαδρομή, με βάση δείγματα που λαμβάνονται σε μια χρονική περίοδο, ανάλογα με το πόσοι κόμβοι υπάρχουν ανάμεσα στο κεντρικό υπολογιστή αρχής και τέλους.

6.2) Χρησιμοποιούνται τα πρωτόκολλα Ethernet II, IPv4 και ICMP.



```
> Frame 15: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{D242DC6...}
> Ethernet II, Src: IntelCor_19:c9:84 (3c:a9:f4:19:c9:84), Dst: Sercomm_2e:79:e0 (94:4a:0c:2e:79:e0)
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 195.251.229.4
> Internet Control Message Protocol
```


Στο επίπεδο Ethernet αναφέρεται ότι η διεύθυνση MAC του αποστολέα είναι 3c:a9:f4:19:c9:84 και του παραλήπτη είναι 94:4a:0c:2e:79:e0, καθώς και ότι ο τύπος πρωτοκόλλου που χρησιμοποιεί το Ethernet σε ανώτερο επίπεδο είναι IPv4.

Στο επίπεδο IPv4 αναφέρεται ότι η έκδοση IP που χρησιμοποιείται είναι η 4, το μέγεθος της επικεφαλίδας είναι 20 byte, ο τύπος υπηρεσίας που παρέχει, καθώς και ότι ο identifier είναι 0x699a. Επίσης, προβάλλονται το flags και το fragment offset, που αφορούν τον κατακερματισμό του πακέτου, η παράμετρος time-to-live, το πρωτόκολλο που χρησιμοποιεί το IP, το header checksum και το status του, αλλά και το ότι η διεύθυνση IP του αποστολέα είναι 192.168.1.5 και του παραλήπτη 195.251.229.4

Στο επίπεδο ICMP φαίνεται ότι ο τύπος είναι 8 και ο κωδικός του τύπου του μηνύματος είναι 0, το checksum είναι το 0xeee6 και το status του είναι καλό, καθώς και το ότι ο identifier μαζί με το sequence number σε Big Endian και Little Endian μορφή. Τέλος, υπάρχει το τμήμα δεδομένων του πακέτου και το μέγεθος τους.

6.3) Χρησιμοποιούνται τα πρωτόκολλα Ethernet II, IPv4 και ICMP, τα οποία αναλύονται με τον ίδιο τρόπο όπως παραπάνω.

```
> Frame 2106: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{D242D
> Ethernet II, Src: IntelCor_19:c9:84 (3c:a9:f4:19:c9:84), Dst: Sercomm_2e:79:e0 (94:4a:0c:2e:79:e0)
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 184.30.18.203
> Internet Control Message Protocol
```

6.4) Με την εκτέλεση της tracerf, έχουμε:

icmp && ip.addr == 192.168.1.5						
No.	Time	Source	Destination	Protocol	Length	Info
24	5.030315	192.168.1.5	195.251.229.4	ICMP	106	Echo (ping) request id=0x0001, seq=2370/16905, ttl=1 (no response found!)
25	5.032163	192.168.1.1	192.168.1.5	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
26	5.034487	192.168.1.5	195.251.229.4	ICMP	106	Echo (ping) request id=0x0001, seq=2371/17161, ttl=1 (no response found!)
27	5.036030	192.168.1.1	192.168.1.5	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
28	5.038113	192.168.1.5	195.251.229.4	ICMP	106	Echo (ping) request id=0x0001, seq=2372/17417, ttl=1 (no response found!)
29	5.040057	192.168.1.1	192.168.1.5	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
72	10.560619	192.168.1.5	195.251.229.4	ICMP	106	Echo (ping) request id=0x0001, seq=2373/17673, ttl=2 (no response found!)
73	10.569629	10.106.108.100	192.168.1.5	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
74	10.571305	192.168.1.5	195.251.229.4	ICMP	106	Echo (ping) request id=0x0001, seq=2374/17929, ttl=2 (no response found!)
75	10.579540	10.106.108.100	192.168.1.5	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
76	10.580824	192.168.1.5	195.251.229.4	ICMP	106	Echo (ping) request id=0x0001, seq=2375/18185, ttl=2 (no response found!)
77	10.595742	10.106.108.100	192.168.1.5	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
93	16.131482	192.168.1.5	195.251.229.4	ICMP	106	Echo (ping) request id=0x0001, seq=2376/18441, ttl=3 (no response found!)
94	16.139592	79.128.250.18	192.168.1.5	ICMP	186	Time-to-live exceeded (Time to live exceeded in transit)
95	16.142110	192.168.1.5	195.251.229.4	ICMP	106	Echo (ping) request id=0x0001, seq=2377/18697, ttl=3 (no response found!)
96	16.150351	79.128.250.18	192.168.1.5	ICMP	186	Time-to-live exceeded (Time to live exceeded in transit)
97	16.152317	192.168.1.5	195.251.229.4	ICMP	106	Echo (ping) request id=0x0001, seq=2378/18953, ttl=3 (no response found!)
98	16.160338	79.128.250.18	192.168.1.5	ICMP	186	Time-to-live exceeded (Time to live exceeded in transit)
103	16.219304	79.128.35.205	192.168.1.5	ICMP	110	Destination unreachable (Communication administratively filtered)
108	17.721881	79.128.35.205	192.168.1.5	ICMP	110	Destination unreachable (Communication administratively filtered)
110	19.228093	79.128.35.205	192.168.1.5	ICMP	110	Destination unreachable (Communication administratively filtered)
121	21.725635	192.168.1.5	195.251.229.4	ICMP	106	Echo (ping) request id=0x0001, seq=2379/19209, ttl=4 (no response found!)
122	21.734047	79.128.248.242	192.168.1.5	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
123	21.736661	192.168.1.5	195.251.229.4	ICMP	106	Echo (ping) request id=0x0001, seq=2380/19465, ttl=4 (no response found!)
124	21.747454	79.128.248.242	192.168.1.5	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
125	21.749654	192.168.1.5	195.251.229.4	ICMP	106	Echo (ping) request id=0x0001, seq=2381/19721, ttl=4 (no response found!)

Ενώ με την εκτέλεση της pathping έχουμε:

icmp && ip.addr == 192.168.1.5						
No.	Time	Source	Destination	Protocol	Length	Info
19	2.422524	192.168.1.5	195.251.229.4	ICMP	106	Echo (ping) request id=0x0001, seq=2400/24585, ttl=1 (no response found!)
20	2.425002	192.168.1.1	192.168.1.5	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
23	2.440009	192.168.1.5	195.251.229.4	ICMP	106	Echo (ping) request id=0x0001, seq=2401/24841, ttl=2 (no response found!)
24	2.448387	10.106.108.100	192.168.1.5	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
45	6.960055	192.168.1.5	195.251.229.4	ICMP	106	Echo (ping) request id=0x0001, seq=2402/25097, ttl=3 (no response found!)
46	6.968775	79.128.250.18	192.168.1.5	ICMP	186	Time-to-live exceeded (Time to live exceeded in transit)
50	6.989681	79.128.35.205	192.168.1.5	ICMP	110	Destination unreachable (Communication administratively filtered)
55	8.486715	79.128.35.205	192.168.1.5	ICMP	110	Destination unreachable (Communication administratively filtered)
57	9.990588	79.128.35.205	192.168.1.5	ICMP	110	Destination unreachable (Communication administratively filtered)
60	11.488946	192.168.1.5	195.251.229.4	ICMP	106	Echo (ping) request id=0x0001, seq=2403/25353, ttl=4 (no response found!)
61	11.496793	79.128.248.242	192.168.1.5	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
64	11.511288	192.168.1.5	195.251.229.4	ICMP	106	Echo (ping) request id=0x0001, seq=2404/25609, ttl=5 (no response found!)
65	11.524662	79.128.35.201	192.168.1.5	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
69	11.556601	79.128.250.75	192.168.1.5	ICMP	110	Destination unreachable (Port unreachable)
72	13.052679	79.128.250.75	192.168.1.5	ICMP	110	Destination unreachable (Port unreachable)
74	14.555736	79.128.250.75	192.168.1.5	ICMP	110	Destination unreachable (Port unreachable)
84	16.055266	192.168.1.5	195.251.229.4	ICMP	106	Echo (ping) request id=0x0001, seq=2405/25865, ttl=6 (no response found!)
85	16.065005	79.128.250.76	192.168.1.5	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
89	16.087020	79.128.35.205	192.168.1.5	ICMP	110	Destination unreachable (Communication administratively filtered)
102	17.582357	79.128.35.205	192.168.1.5	ICMP	110	Destination unreachable (Communication administratively filtered)
104	19.086006	79.128.35.205	192.168.1.5	ICMP	110	Destination unreachable (Communication administratively filtered)
119	20.584276	192.168.1.5	195.251.229.4	ICMP	106	Echo (ping) request id=0x0001, seq=2406/26121, ttl=7 (no response found!)
120	20.593357	79.128.227.219	192.168.1.5	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
124	20.615110	79.128.35.205	192.168.1.5	ICMP	110	Destination unreachable (Communication administratively filtered)
132	22.110237	79.128.35.205	192.168.1.5	ICMP	110	Destination unreachable (Communication administratively filtered)
134	23.615092	79.128.35.205	192.168.1.5	ICMP	110	Destination unreachable (Communication administratively filtered)
135	25.113769	192.168.1.5	195.251.229.4	ICMP	106	Echo (ping) request id=0x0001, seq=2407/26377, ttl=8 (no response found!)
136	25.124532	176.126.38.1	192.168.1.5	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
139	25.143282	192.168.1.5	195.251.229.4	ICMP	106	Echo (ping) request id=0x0001, seq=2408/26633, ttl=9 (no response found!)
140	25.156457	62.217.96.87	192.168.1.5	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
143	25.172432	192.168.1.5	195.251.229.4	ICMP	106	Echo (ping) request id=0x0001, seq=2409/26889, ttl=10 (reply in 144)
144	25.185559	195.251.229.4	192.168.1.5	ICMP	106	Echo (ping) reply id=0x0001, seq=2409/26889, ttl=55 (request in 143)
147	25.203609	192.168.1.5	192.168.1.1	ICMP	106	Echo (ping) request id=0x0001, seq=2410/27145, ttl=10 (reply in 148)
148	25.205526	192.168.1.1	192.168.1.5	ICMP	106	Echo (ping) reply id=0x0001, seq=2410/27145, ttl=64 (request in 147)
149	25.457698	192.168.1.5	10.106.108.100	ICMP	106	Echo (ping) request id=0x0001, seq=2411/27401, ttl=10 (reply in 150)

Γίνεται αντιληπτό ότι υπάρχουν σημαντικές αλλαγές στην λειτουργία των δύο εντολών. Συγκεκριμένα, το πλήθος των πακέτων στην pathping είναι πολύ μεγαλύτερο και το TTL αυξάνει κάθε ένα πακέτο αντί για κάθε 3 που ισχύει για την tracer. Επιπρόσθετα, στην pathping αφού φτάσει το ring μέχρι τον τελικό προορισμό, η συσκευή μας θα ξανακάνει ring 100 φορές σε κάθε κόμβο που βρίσκεται στην διαδρομή μέχρι τον τελικό κόμβο, με σκοπό να προσδιορίσει τα σημεία που έχουν καθυστέρηση στο δίκτυο και να βγάλει τα σχετικά στατιστικά στοιχεία. Αυτός είναι από τους βασικούς λόγους που η pathping έχει μεγάλο αριθμό πακέτων.

Δραστηριότητα 7^η

7.1)

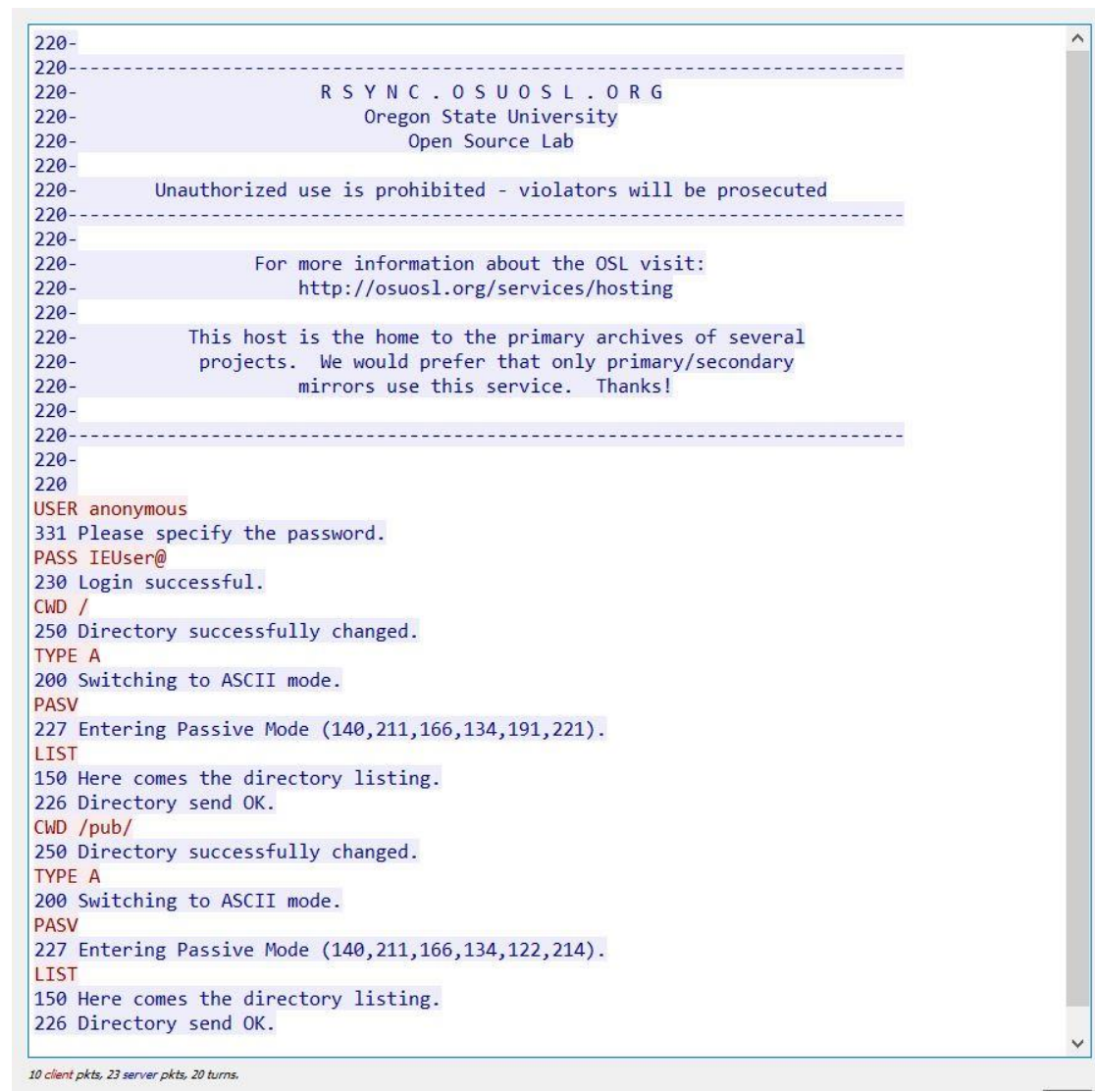
Χρησιμοποιούνται τα πρωτόκολλα Ethernet, IPv4, UDP και DHCP.

```
> Frame 685: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface \Device\NPF_{D242...}
> Ethernet II, Src: IntelCor_19:c9:84 (3c:a9:f4:19:c9:84), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Discover)
```

dhcp						
No.	Time	Source	Destination	Protocol	Length	Info
39	9.275305	192.168.1.5	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0x2422f14f
685	30.207608	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xb96307df
741	32.760042	192.168.1.1	192.168.1.5	DHCP	590	DHCP Offer - Transaction ID 0xb96307df
742	32.760960	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xb96307df
744	32.768597	192.168.1.1	192.168.1.5	DHCP	590	DHCP ACK - Transaction ID 0xb96307df

Με την εντολή *ipconfig /release*, στέλνεται στο router μας ένα πακέτο DHCP για να απελευθερώσει την τρέχων διεύθυνση IP. Στην συνέχεια, με την χρήση της *ipconfig /renew* ο υπολογιστής μας, που πλέον έχει IP 0.0.0.0, στέλνει στην broadcast IP του τοπικού δικτύου (255.255.255.255) ένα πακέτο DHCP discover το οποίο περιέχει πληροφορίες για την συσκευή, όπως το υλικό και την διεύθυνση MAC. Το broadcast αυτό το 'ακούει' και ο Gateway του δικτύου (δηλαδή το router), ο οποίος με ιδιότητα DHCP server στέλνει στην συσκευή ένα πακέτο DHCP Offer που 'προσφέρει' μια νέα διεύθυνση IP με την οποία ο υπολογιστής θα επανασυνδεθεί στο δίκτυο. Έτσι, ο υπολογιστής μας θα στείλει ένα πακέτο DHCP Request στο broadcast, πληροφορώντας ότι δέχεται να χρησιμοποιήσει την καινούργια IP. Τέλος, το router θα επικυρώσει την ανανέωση της IP, στέλνοντας ένα πακέτο DHCP ACK.

Δραστηριότητα 8^η



```
220-
220-----
220-                R S Y N C . O S U O S L . O R G
220-                Oregon State University
220-                Open Source Lab
220-
220-    Unauthorized use is prohibited - violators will be prosecuted
220-----
220-
220-    For more information about the OSL visit:
220-    http://osuosl.org/services/hosting
220-
220-    This host is the home to the primary archives of several
220-    projects. We would prefer that only primary/secondary
220-    mirrors use this service. Thanks!
220-----
220-
220-
USER anonymous
331 Please specify the password.
PASS IEUser@
230 Login successful.
CWD /
250 Directory successfully changed.
TYPE A
200 Switching to ASCII mode.
PASV
227 Entering Passive Mode (140,211,166,134,191,221).
LIST
150 Here comes the directory listing.
226 Directory send OK.
CWD /pub/
250 Directory successfully changed.
TYPE A
200 Switching to ASCII mode.
PASV
227 Entering Passive Mode (140,211,166,134,122,214).
LIST
150 Here comes the directory listing.
226 Directory send OK.
```

10 client pkts, 23 server pkts, 20 turns.

Από την παραπάνω εικόνα, φαίνεται ότι το password είναι το *IEUser@*.