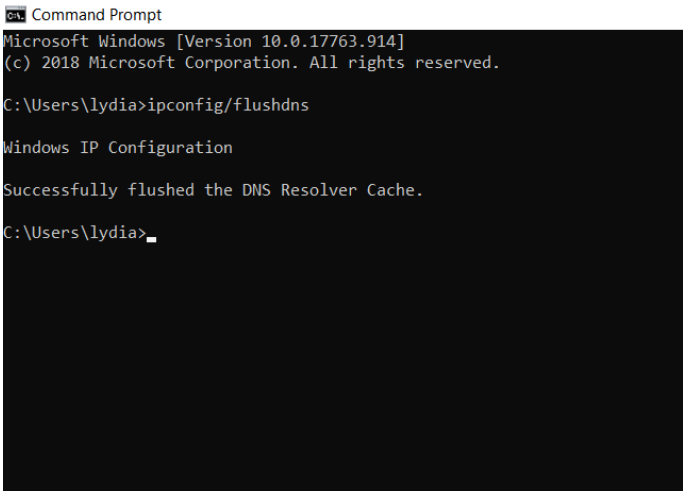
Λυδία Αθανασίου p3170003

ΕΡΓΑΣΙΑ ΔΙΚΤΥΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

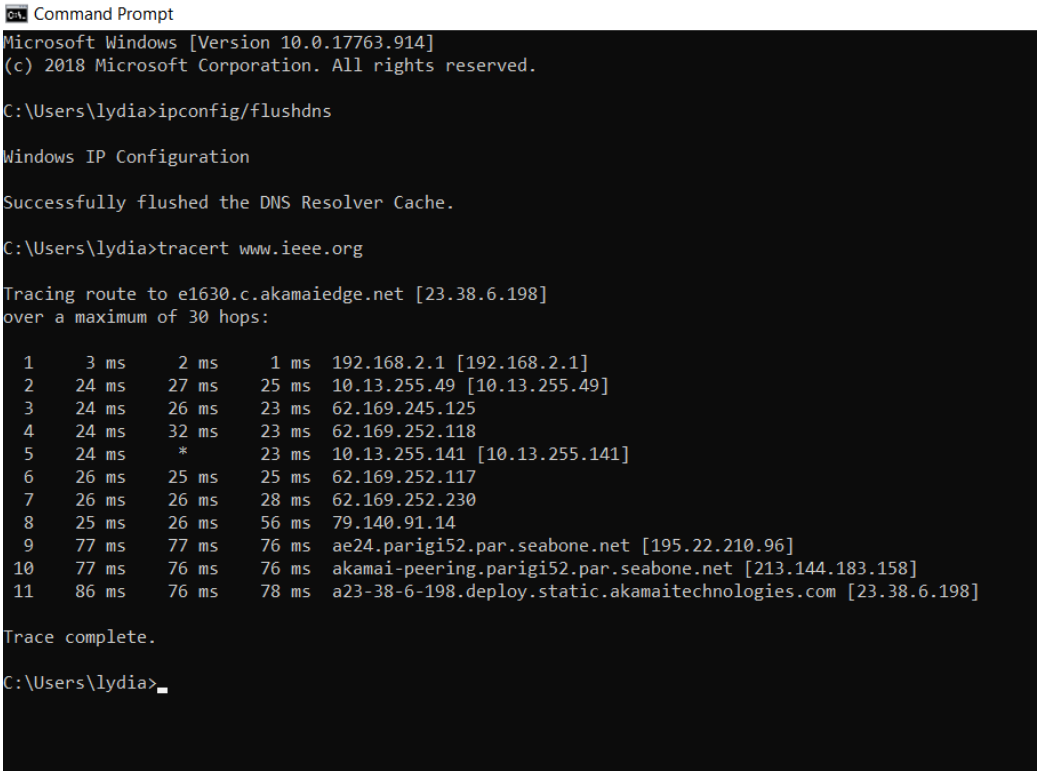
Α' ΜΕΡΟΣ

Εισαγωγικά:

3) Αποτέλεσμα εντολής ipconfig /flushdns στο command prompt έτσι ώστε να καθαριστεί η προσωρινή μνήμη DNS του υπολογιστή και στη συνέχεια να χρειάζεται επικοινωνία με DNS Server.



5) Αποτέλεσμα εντολής tracert www.ieee.org στο command prompt



Γενικές Ερωτήσεις:

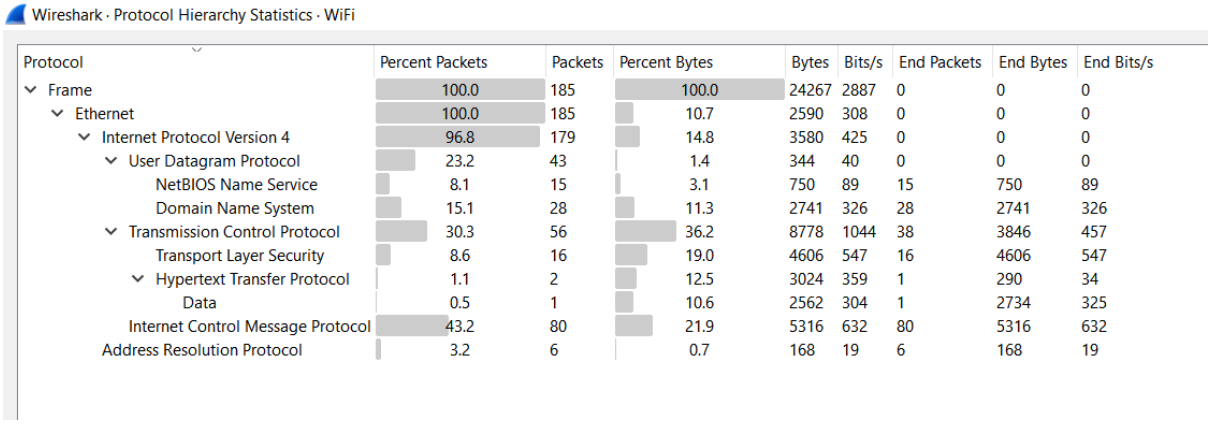
1) Η χρονική διάρκεια της ανίχνευσής ήταν 67.244231 msec (time τελευταίου πακέτου).

2) Πίνακας με τα διαφορετικά πρωτόκολλα που χρησιμοποίησε ο υπολογιστής στη χρονική διάρκεια της ανίχνευσης, διαχωρισμένα σύμφωνα με τα επίπεδα στα οποία ανήκουν.

Πακέτο	Επίπεδο που ανήκει
TCP	Transfer layer
ICMP	Internet layer
ARP	Network access layer
DNS	Application Layer
HTTP	
Hypertext transfer protocol HTTP	
NBNS	
TLSv1.2	

3) Εξετάστε ποιο πρωτόκολλο επιπέδου μεταφοράς χρησιμοποιούν τα πρωτόκολλα του επιπέδου εφαρμογής που έχετε εντοπίσει.
   - Το πρωτόκολλο επιπέδου εφαρμογής DNS χρησιμοποιεί το πρωτόκολλο επιπέδου μεταφοράς: UDP
   - Το πρωτόκολλο επιπέδου εφαρμογής HTTP χρησιμοποιεί το πρωτόκολλο επιπέδου μεταφοράς: ICMP
   - Το πρωτόκολλο επιπέδου εφαρμογής Hypertext transfer protocol HTTP χρησιμοποιεί το πρωτόκολλο επιπέδου μεταφοράς: UDP
   - Το πρωτόκολλο επιπέδου εφαρμογής NBNS χρησιμοποιεί το πρωτόκολλο επιπέδου μεταφοράς: UDP
   - Το πρωτόκολλο επιπέδου εφαρμογής TLS χρησιμοποιεί το πρωτόκολλο επιπέδου μεταφοράς: TCP

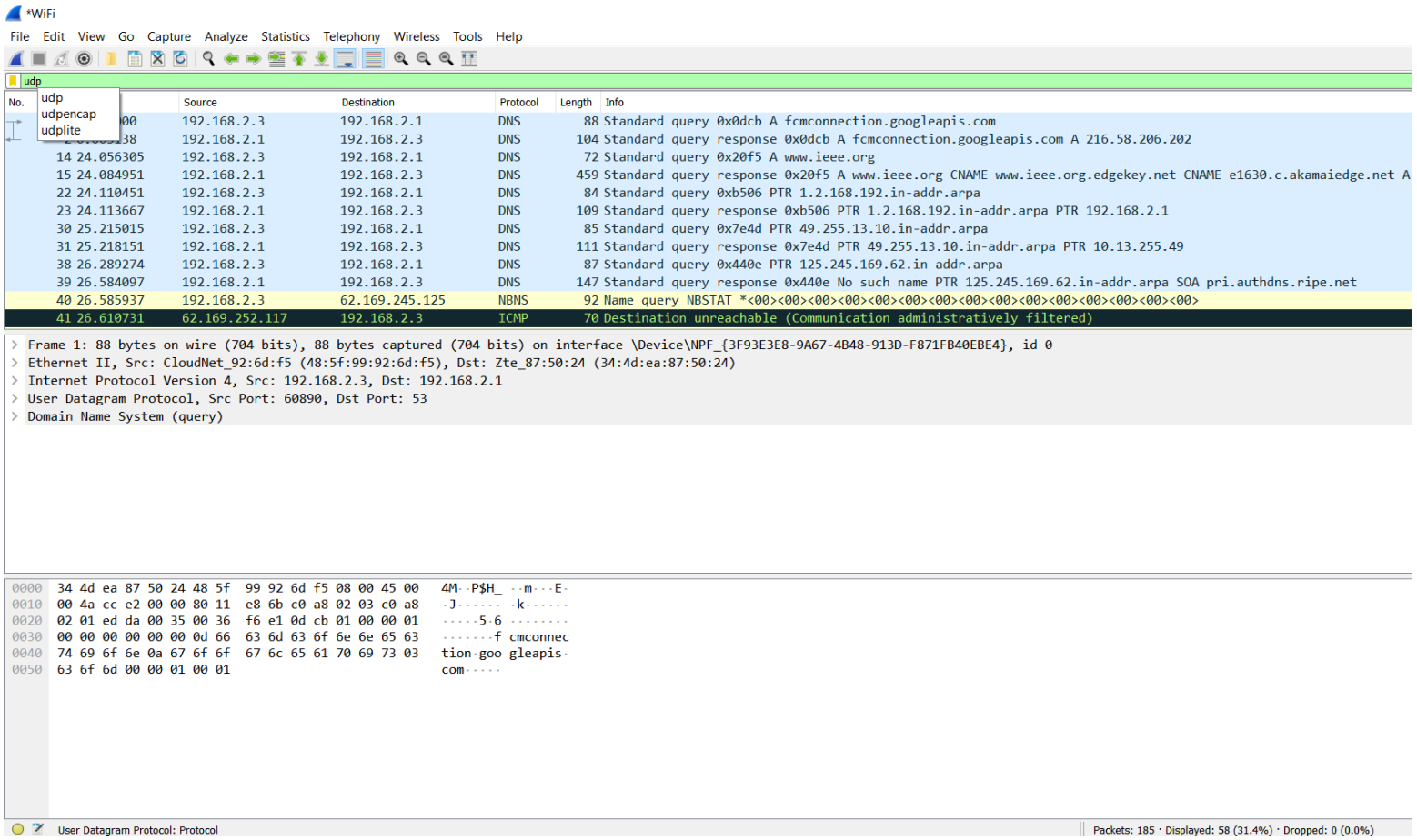
Με βοήθησε να τα εντοπίσω το παράθυρο του wireshark: statistics>protocol Hierarchy statistics



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	185	100.0	24267	2887	0	0	0
Ethernet	100.0	185	10.7	2590	308	0	0	0
Internet Protocol Version 4	96.8	179	14.8	3580	425	0	0	0
User Datagram Protocol	23.2	43	1.4	344	40	0	0	0
NetBIOS Name Service	8.1	15	3.1	750	89	15	750	89
Domain Name System	15.1	28	11.3	2741	326	28	2741	326
Transmission Control Protocol	30.3	56	36.2	8778	1044	38	3846	457
Transport Layer Security	8.6	16	19.0	4606	547	16	4606	547
Hypertext Transfer Protocol	1.1	2	12.5	3024	359	1	290	34
Data	0.5	1	10.6	2562	304	1	2734	325
Internet Control Message Protocol	43.2	80	21.9	5316	632	80	5316	632
Address Resolution Protocol	3.2	6	0.7	168	19	6	168	19

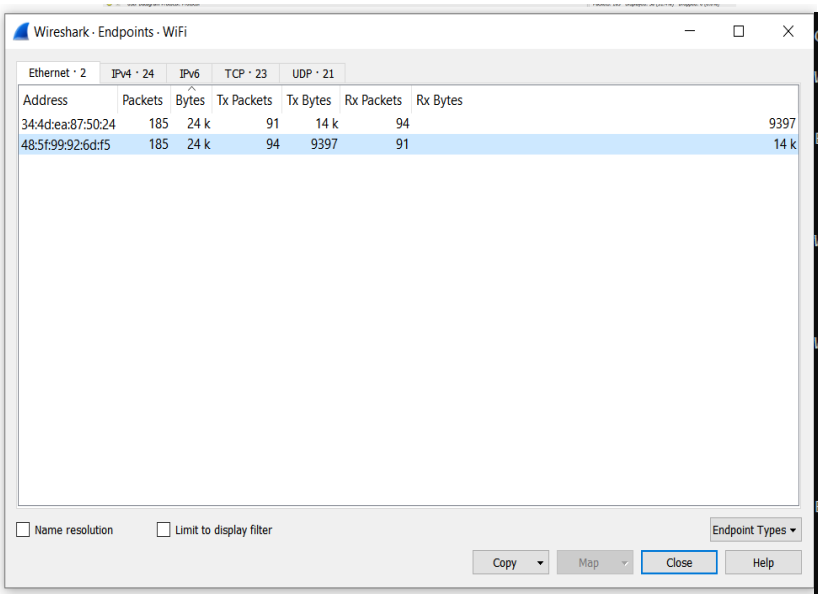
4) Πόσα πακέτα TCP και πόσα πακέτα UDP στάλθηκαν;

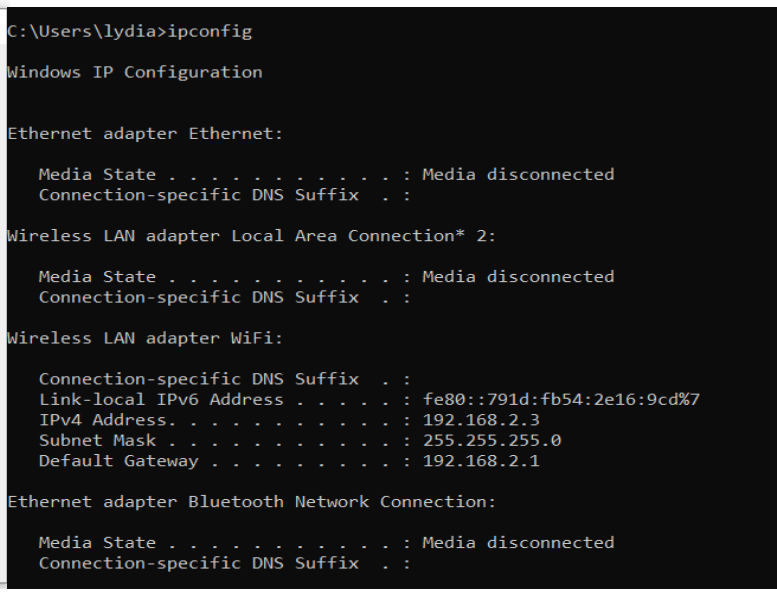
Εφαρμόζοντας στο wireshark τα κατάλληλα φίλτρα και βλέποντας κάτω δεξιά το display/packets βλέπουμε ότι τα UDP πακέτα που στάλθηκαν είναι 58 ενώ τα TCP πακέτα που στάλθηκαν είναι 56. Παρακάτω φαίνεται ένα παράδειγμα με το φίλτρο udp και το displayed εμφανίζει 58.



5) Πόσα και ποια είναι τα διαφορετικά endpoints (η σχετική πληροφορία βρίσκεται στο μενού Statistics) με τα οποία υπάρχει επικοινωνία σε επίπεδο Ethernet; Μπορείτε να βρείτε σε ποιες συσκευές αντιστοιχούν;

Τα endpoints με τα οποία υπάρχει επικοινωνία σε επίπεδο ethernet είναι 2 και φαίνονται στο παρακάτω screen. Τα endpoints αυτά αντιστοιχούν στις ακόλουθες συσκευές: τον υπολογιστή μου και το Wi-Fi (τρέχουμε στο command prompt την εντολή ipconfig).

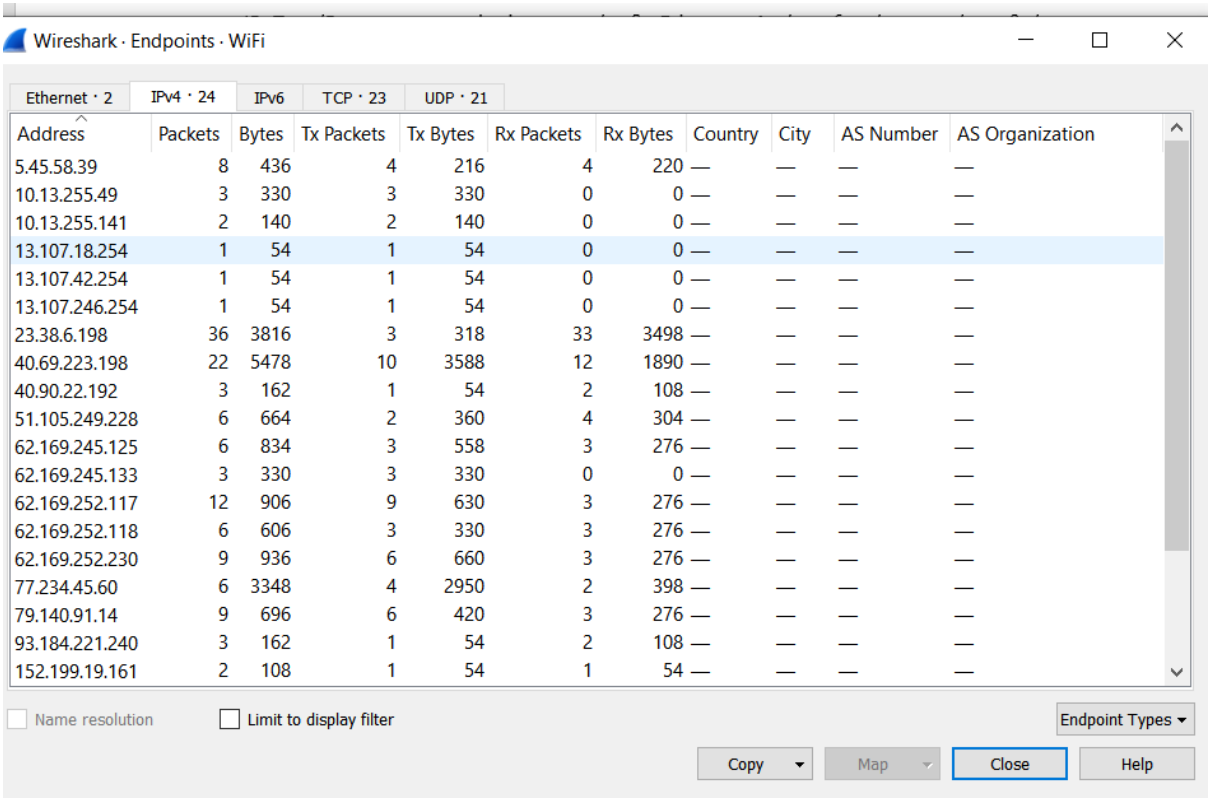




6) Πόσα και ποια είναι τα διαφορετικά endpoints με τα οποία υπάρχει επικοινωνία σε επίπεδο IP; Ταυτίζονται με τα endpoints σε επίπεδο Ethernet; Αν όχι, εξηγείστε γιατί συμβαίνει αυτό.

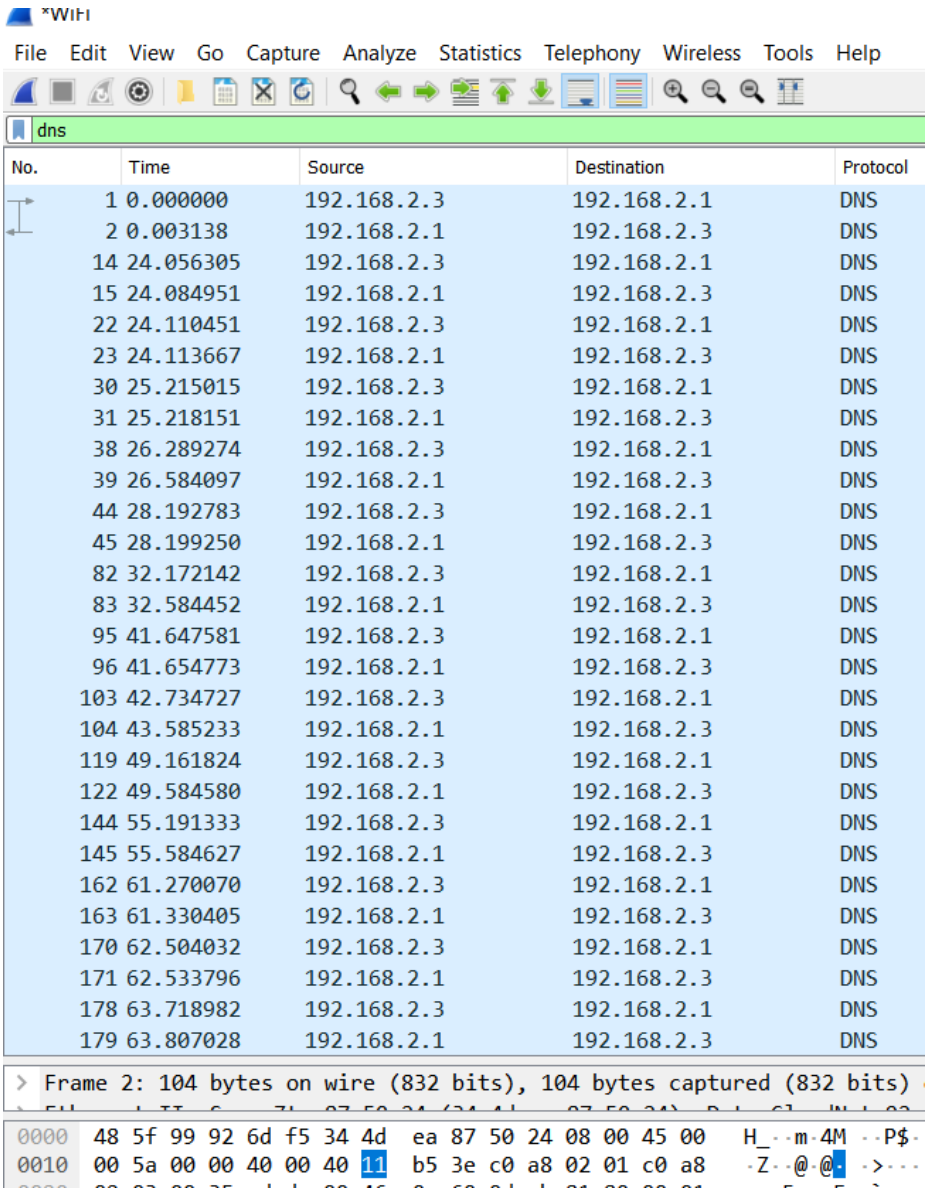
Τα endpoints με τα οποία υπάρχει επικοινωνία σε επίπεδο IP είναι 24 και φαίνονται στο παρακάτω screen. Τα endpoints αυτά δεν ταυτίζονται με τα endpoints σε επίπεδο ethernet. Αυτό συμβαίνει διότι τα endpoints

ethernet είναι φυσικές διευθύνσεις που συνδέονται με κάρτα ασύρματης διασύνδεσης, κάρα διασύνδεσης ethernet ή ειδική διεύθυνση MAC για broadcast(η οποία προορίζεται να ληφθεί από όλους). Τα endpoints IP είναι λογικές διευθύνσεις, στο επίπεδο δικτύου, που χρησιμοποιούνται από συσκευές που έχουν διευθύνσεις IP σε κάθε τμήμα (επίσης αποκαλούμενες VLAN) του δικτύου. Θα χρησιμοποιήσετε τα στατιστικά στοιχεία του τελικού σημείου Ethernet αν θέλουμε να δούμε τι συμβαίνει στην κάρτα διασύνδεσης (κάρτα ethernet ή wifi) ή στους δρομολογητές που είναι ο επόμενος host σε εμάς ενώ το τελικό σημείο IP, εάν θέλουμε να δούμε όλα τα δεδομένα που αναφέρονται σε μια συγκεκριμένη διεύθυνση IP με την οποία επικοινωνούμε (οποιαδήποτε συσκευή στο τοπικό δίκτυο ή στο διαδίκτυο). Άρα πρόκειται για τελείως διαφορετικά πράγματα γι' αυτό τα endpoints τους δεν ταυτίζονται.



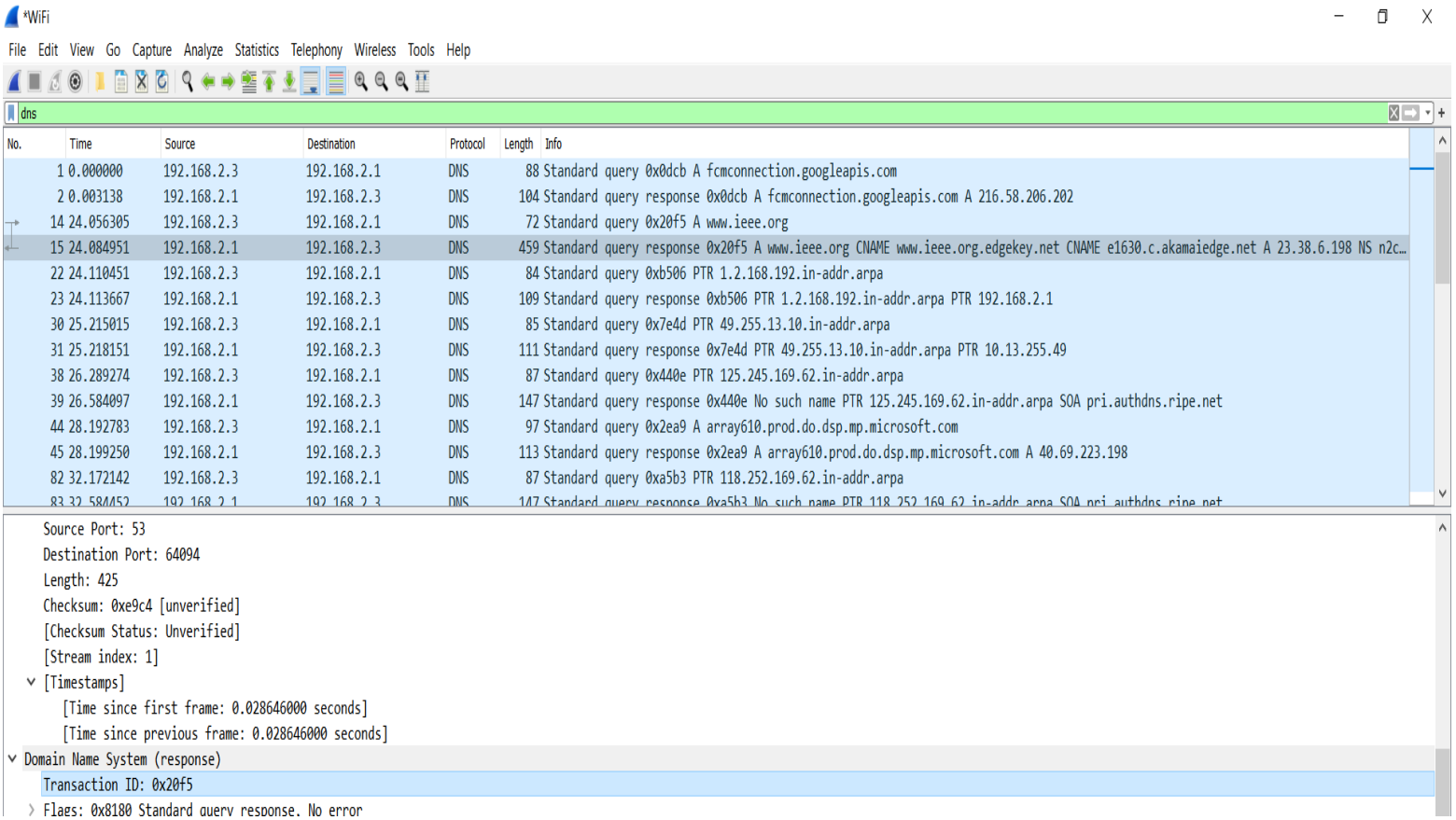
Ερωτήσεις σχετικά με το DNS:

7) Εξετάστε τις θύρες (ports) προέλευσης (source) και προορισμού (destination) που χρησιμοποιήθηκαν για την ερώτηση από τον υπολογιστή σας προς τον DNS server και για την απάντηση του DNS server.



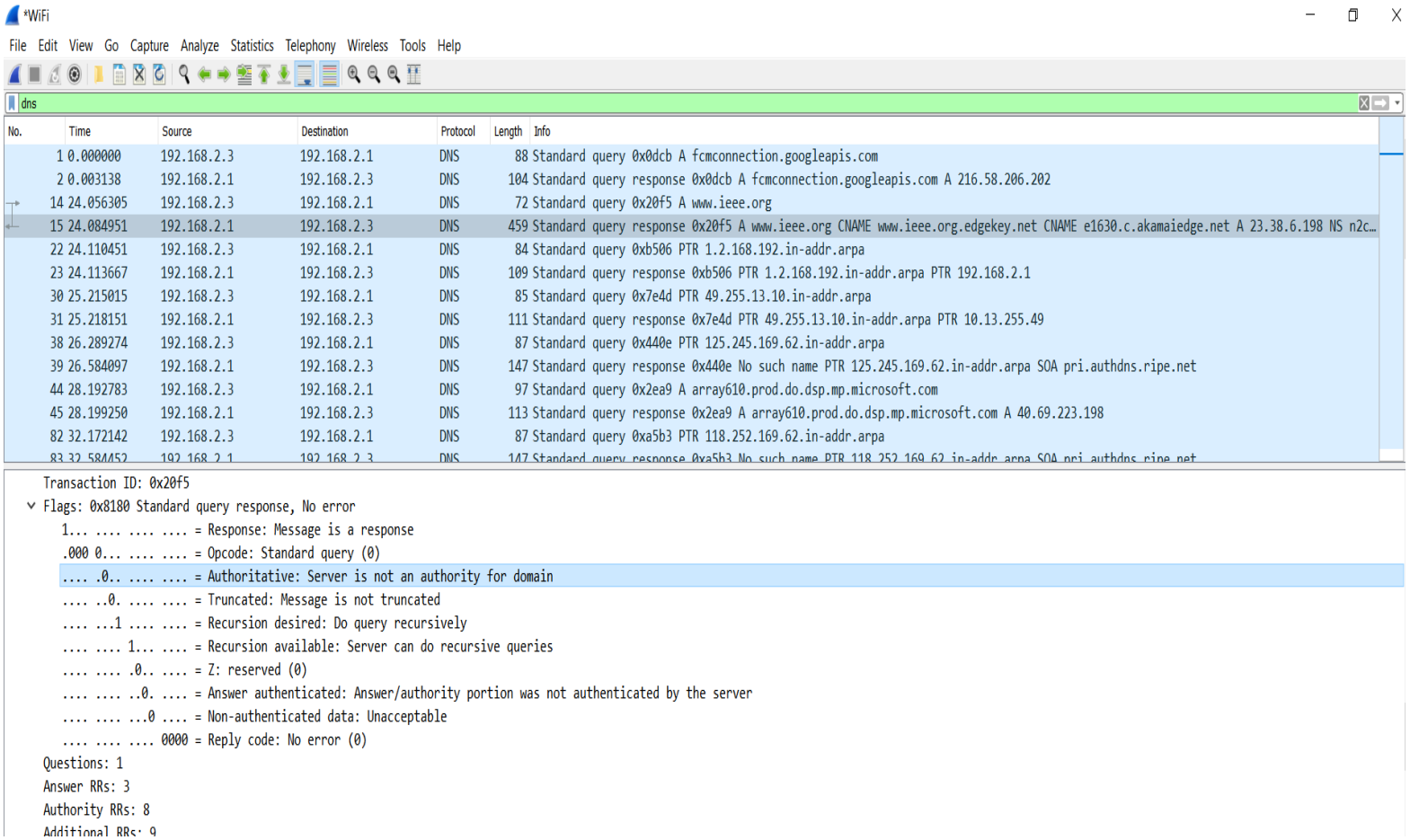
8) Πώς διακρίνετε αν ένα πακέτο περιέχει αίτημα προς τον DNS server ή απάντηση σε ερώτημα που έχετε κάνει; Πώς συνδέονται το πακέτο μιας απάντησης με το πακέτο της ερώτησης;

Το πακέτο μια απάντησης με το πακέτο της ερώτησης συνδέονται με το transaction ID . Οι αιτήσεις έχουν το ίδιο Id Με τις αντίστοιχες απαντήσεις τους. (Όταν περνάς το ποντίκι πάνω στο αίτημα δείχνει ένα εξερχόμενο και ένα εισερχόμενο βελάκι στα αριστερά).



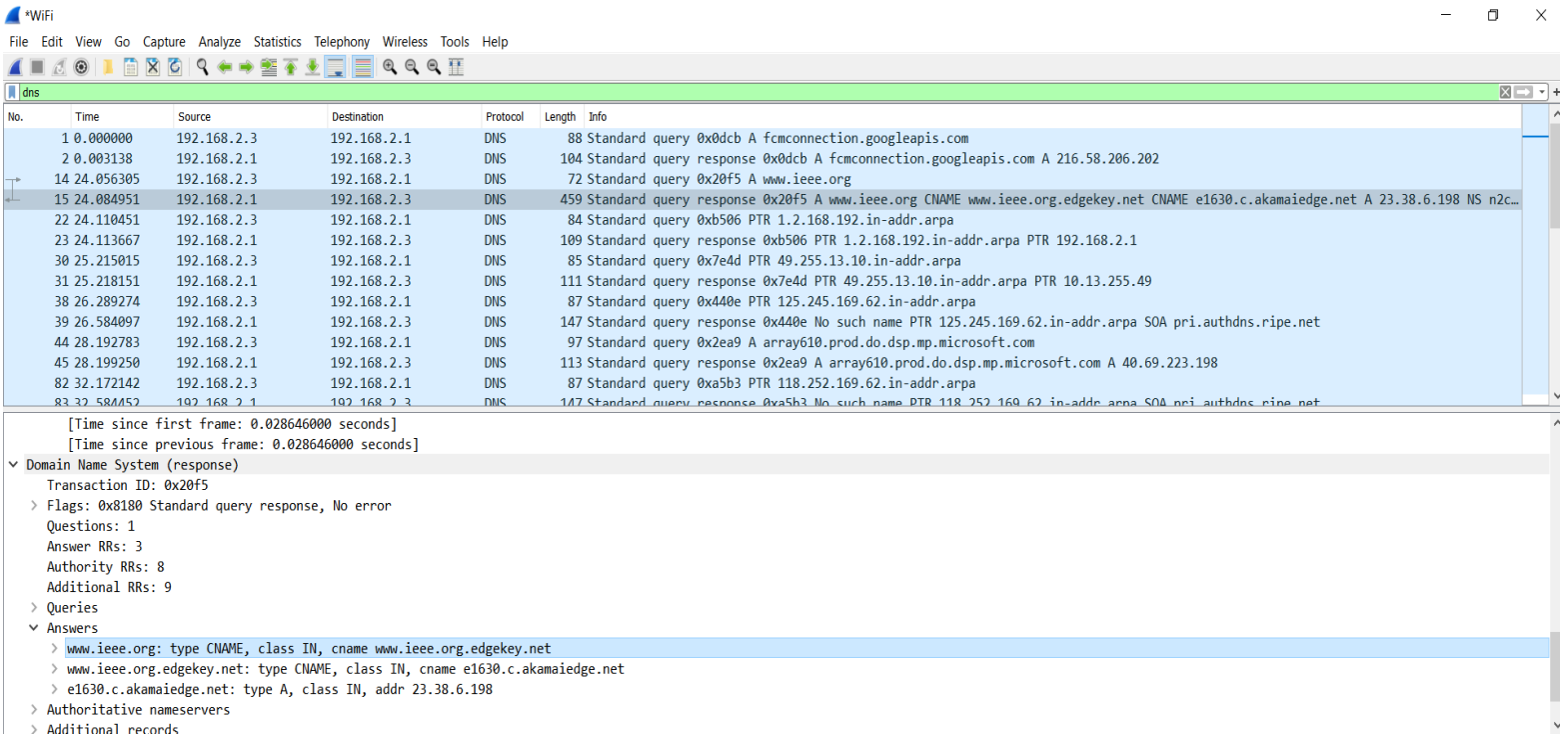
9) Υπάρχει κάποια σημαία (flag) που να προσδιορίζει αν ο name server που μας απαντάει για το www.ieee.org είναι authoritative για το συγκεκριμένο domain; Είναι ο name server που μας έχει απαντήσει authoritative για το συγκεκριμένο domain;

Υπάρχει σημαία flag που προσδιορίζει αν ο name server είναι authoritative στο συγκεκριμένο domain και μάλιστα στο παράδειγμά μας ο server που μας έχει απαντήσει δεν είναι (server is not an authoritative for domain).

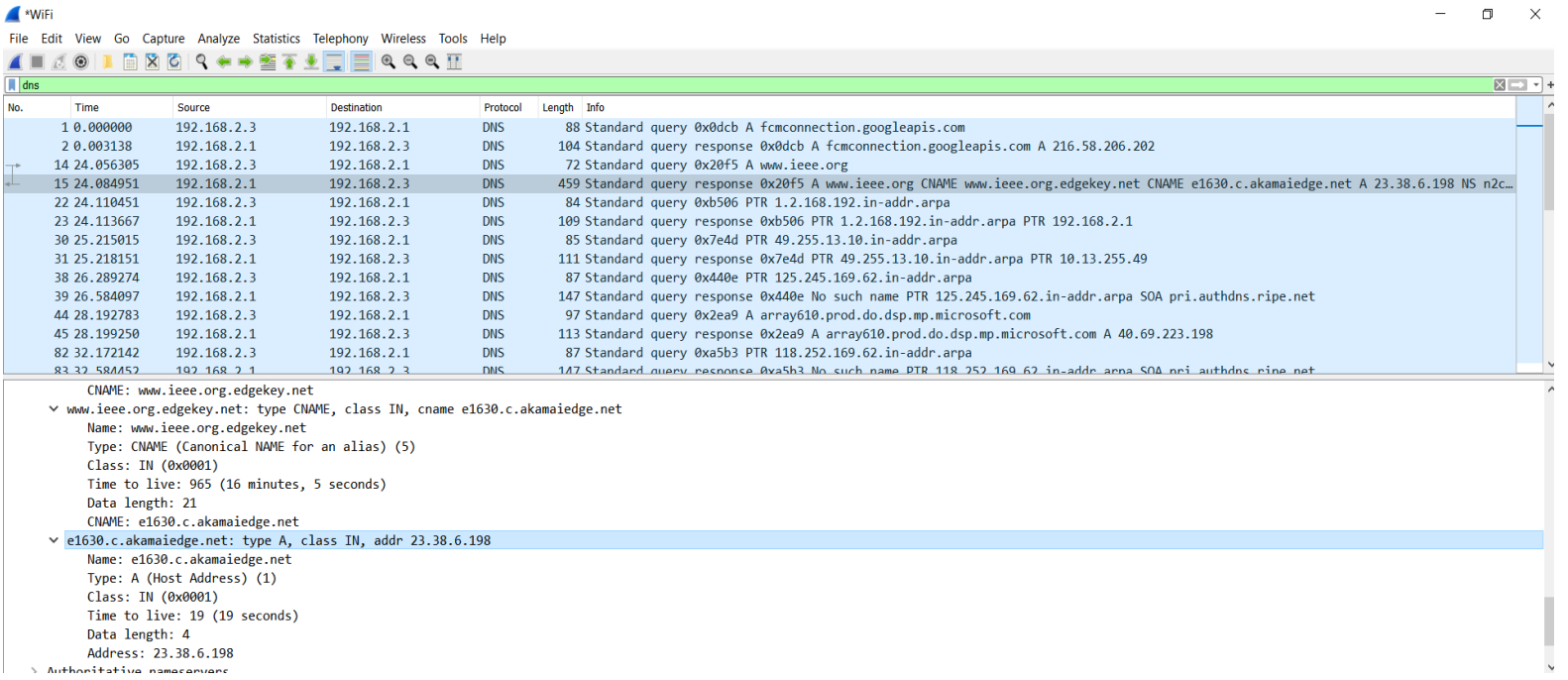


10) Ένα domain name είναι η διεύθυνση όπου οι internet users μπορούν να έχουν πρόσβαση στον ιστότοπό μας. Ένα domain name χρησιμοποιείται για την εύρεση και αναγνώριση υπολογιστών στο Διαδίκτυο. Οι υπολογιστές χρησιμοποιούν διευθύνσεις IP, οι οποίες είναι μια σειρά αριθμών. Ωστόσο, είναι δύσκολο για τους ανθρώπους να θυμούνται τις σειρές αριθμών. Εξαιτίας αυτού, τα ονόματα τομέα αναπτύχθηκαν και χρησιμοποιήθηκαν για τον εντοπισμό οντοτήτων στο Διαδίκτυο αντί για τη χρήση διευθύνσεων IP.

Ένα canonical name είναι το σωστά δηλωμένο όνομα κεντρικού υπολογιστή ενός διακομιστή υπολογιστή ή δικτύου. Ένα CNAME καθορίζει ένα ψευδώνυμο για μια κανονική εγγραφή ονόματος κεντρικού υπολογιστή σε μια βάση δεδομένων του συστήματος ονομάτων τομέα (DNS). Κατά τον προγραμματισμό, ο όρος "canonical" σημαίνει "σύμφωνα με τους κανόνες". Το DNS είναι η τυπική μέθοδος καθορισμού των τοποθεσιών των τοποθεσιών στο Διαδίκτυο, ιδιαίτερα στις τοποθεσίες Web. Άρα το όνομα www.ieee.org είναι canonical name.



11) Ποια είναι η IP διεύθυνση που αντιστοιχεί στον www.ieee.org; Ποια είναι η IP διεύθυνση του δικού σας υπολογιστή;
Η IP διεύθυνση που αντιστοιχεί στον www.ieee.org είναι η 23.98.6.198
Η IP διεύθυνση που αντιστοιχεί στον δικό μου υπολογιστή είναι η 192.168.2.3



Select Command Prompt

```
Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : B0-0C-D1-F1-50-E6
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : CA-5F-99-92-6D-F5
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter WiFi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek RTL8821CE 802.11ac PCIe Adapter
   Physical Address. . . . . . . . . : 48-5F-99-92-6D-F5
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::791d:fb54:2e16:9cd%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.2.3(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 08 January 2020 12:51:24
   Lease Expires . . . . . . . . . . : 10 January 2020 12:18:49
   Default Gateway . . . . . . . . . : 192.168.2.1
   DHCP Server . . . . . . . . . . . : 192.168.2.1
   DHCPv6 IAID . . . . . . . . . . . : 105406361
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-14-61-75-B0-0C-D1-F1-50-E6
   DNS Servers . . . . . . . . . . . : 192.168.2.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : 48-5F-99-92-6D-F6
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

Ερωτήσεις σχετικά με το ICMP:

12) Πως θα δείτε μόνο τα πακέτα που αφορούν την επικοινωνία με βάση το πρωτόκολλο ICMP;

Θα βάλω στα φίλτρα το φίλτρο ICMP

μερος A.pcapng

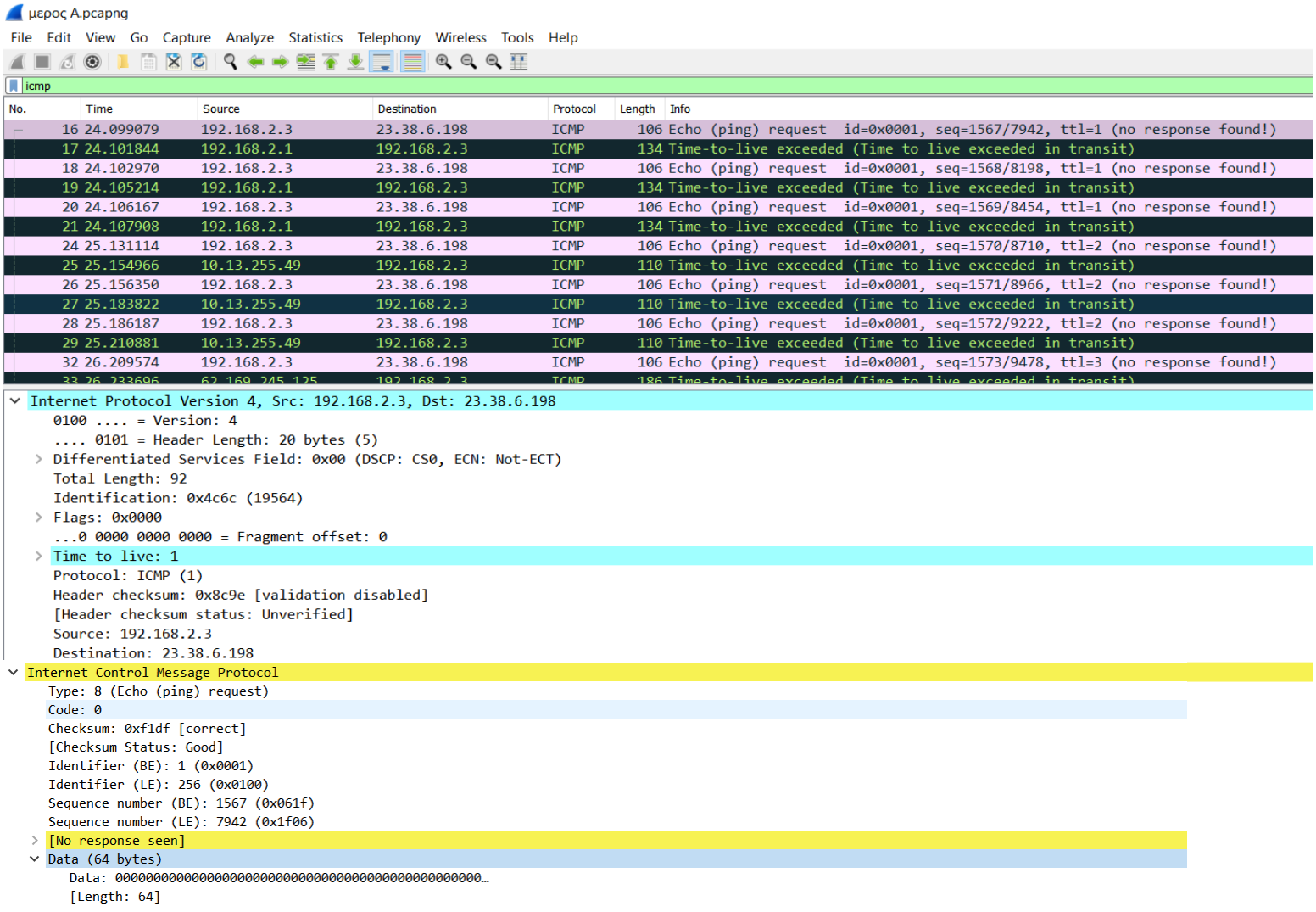
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

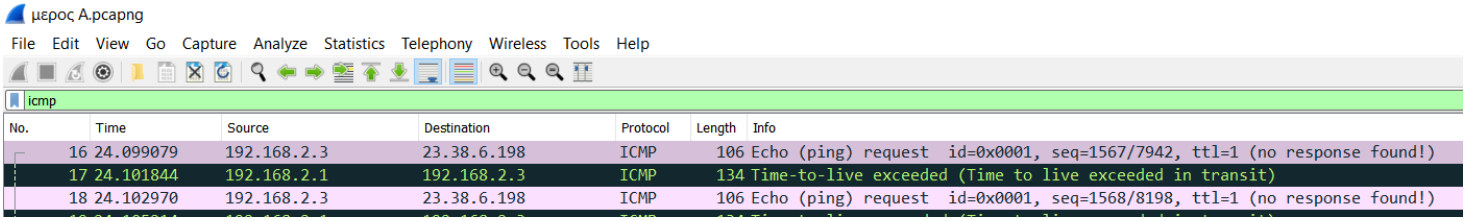
No.	Time	Source	Destination	Protocol	Length	Info
16	24.099079	192.168.2.3	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=1567/7942, ttl=1 (no response found!)
17	24.101844	192.168.2.1	192.168.2.3	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
18	24.102970	192.168.2.3	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=1568/8198, ttl=1 (no response found!)
19	24.105214	192.168.2.1	192.168.2.3	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
20	24.106167	192.168.2.3	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=1569/8454, ttl=1 (no response found!)
21	24.107908	192.168.2.1	192.168.2.3	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
24	25.131114	192.168.2.3	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=1570/8710, ttl=2 (no response found!)
25	25.154966	10.13.255.49	192.168.2.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
26	25.156350	192.168.2.3	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=1571/8966, ttl=2 (no response found!)
27	25.183822	10.13.255.49	192.168.2.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
28	25.186187	192.168.2.3	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=1572/9222, ttl=2 (no response found!)
29	25.210881	10.13.255.49	192.168.2.3	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
32	26.209574	192.168.2.3	23.38.6.198	ICMP	106	Echo (ping) request id=0x0001, seq=1573/9478, ttl=3 (no response found!)
33	26.233696	62.169.245.125	192.168.2.3	ICMP	186	Time-to-live exceeded (Time to live exceeded in transit)

```
> Frame 24: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{3F93E3E8-9A67-4B48-913D-F871FB40EBE4}, id 0
> Ethernet II, Src: CloudNet_92:6d:f5 (48:5f:99:92:6d:f5), Dst: Zte_87:50:24 (34:4d:ea:87:50:24)
> Internet Protocol Version 4, Src: 192.168.2.3, Dst: 23.38.6.198
> Internet Control Message Protocol
```

13) Εξετάστε το IP πακέτο που μεταφέρει το πρώτο ICMP Echo Request.
   a) Η IP διεύθυνση του destination = 23.38.6198
   b) Το time-to-live του πακέτου είναι = 1
   c) Πόσο είναι το μέγεθος (length) των δεδομένων που μεταφέρει =64 Bytes



14) Εξετάστε το IP πακέτο που μεταφέρει το πρώτο ICMP Time Exceeded. Ποια είναι η IP διεύθυνση του destination; Ποια είναι η IP διεύθυνση του Source;
IP διεύθυνση του destination: 192.168.2.3
IP διεύθυνση του Source: 192.168.2.1



15) Αναφέρατε όλες τις source IP διευθύνσεις των πακέτων που μεταφέρουν ICMP Time Exceeded μηνύματα. Υπάρχει αντιστοιχία με αυτές που φαίνονται κατά την εκτέλεση της εντολής tracert στο command prompt παράθυρο;

Υπάρχει αντιστοιχία των source ID διευθύνσεων των πακέτων που μεταφέρουν ICMP Time Exceeded μηνύματα με αυτές που φαίνονται κατά την εκτέλεση της εντολής tracert στο command prompt. Και συγκεκριμένα παρατηρώ πως το command prompt περιέχει τις ίδιες διευθύνσεις με το source IP απλά στο wireshark εμφανίζονται διπλότυπα ενώ στο tracert είναι μοναδικές οι διευθύνσεις.

μερος A.pcapng

File Edit View Go Capture Analyze Statistic

icmp.type == 11

No.	Time	Source
17	24.101844	192.168.2.1
19	24.105214	192.168.2.1
21	24.107908	192.168.2.1
25	25.154966	10.13.255.49
27	25.183822	10.13.255.49
29	25.210881	10.13.255.49
33	26.233696	62.169.245.125
35	26.261200	62.169.245.125
37	26.285860	62.169.245.125
77	32.110685	62.169.252.118
79	32.144377	62.169.252.118
81	32.169147	62.169.252.118
91	38.096455	10.13.255.141

μερος A.pcapng

File Edit View Go Capture Analyze Statistic

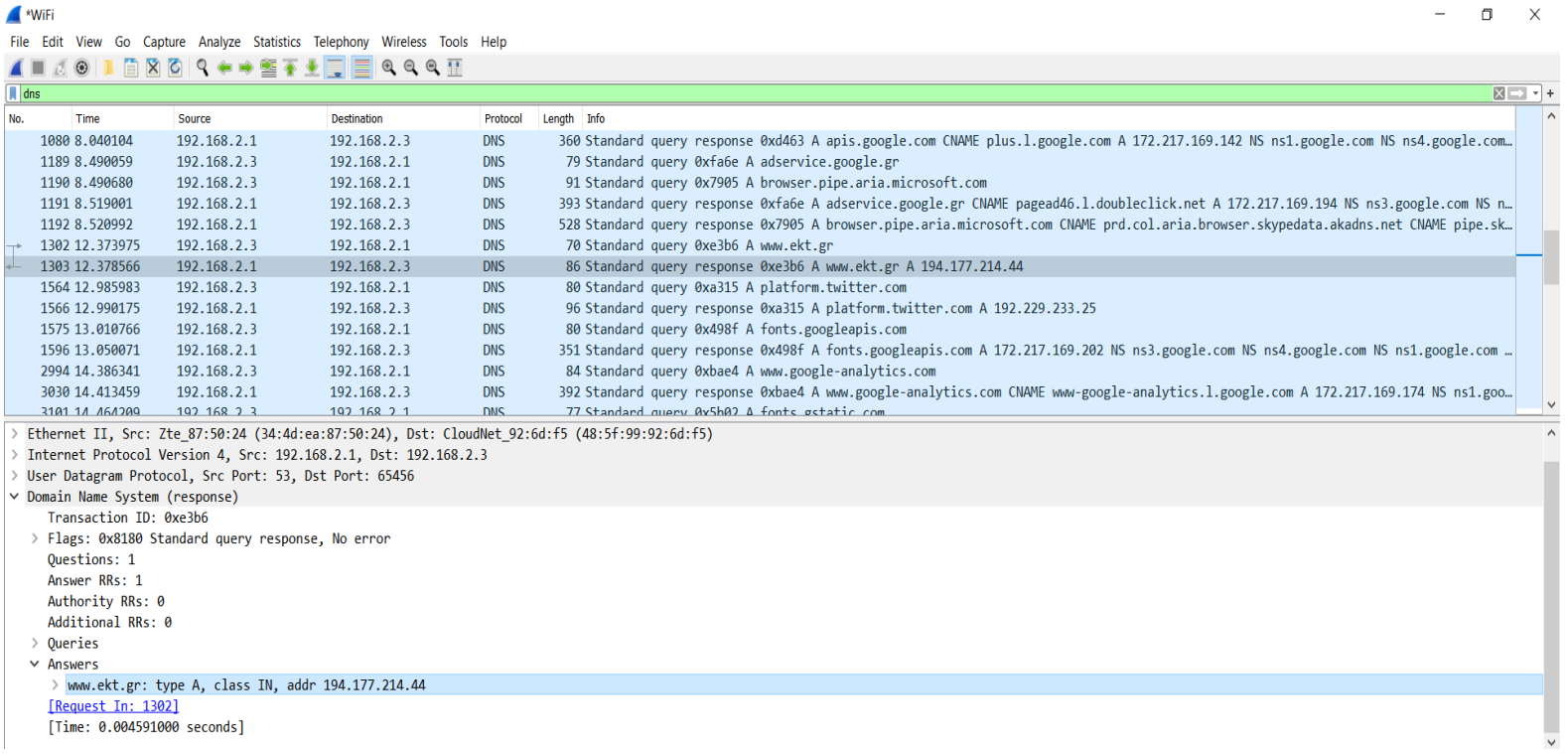
icmp.type == 11

No.	Time	Source
91	38.096455	10.13.255.141
94	41.644483	10.13.255.141
98	42.678323	62.169.252.117
100	42.705015	62.169.252.117
102	42.731653	62.169.252.117
114	49.101945	62.169.252.230
116	49.129256	62.169.252.230
118	49.158787	62.169.252.230
139	55.103394	79.140.91.14
141	55.130715	79.140.91.14
143	55.188146	79.140.91.14
157	61.109951	195.22.210.96
159	61.188327	195.22.210.96

159	61.188327	195.22.210.96
161	61.266502	195.22.210.96
165	62.344607	213.144.183.158
167	62.422132	213.144.183.158
169	62.500229	213.144.183.158

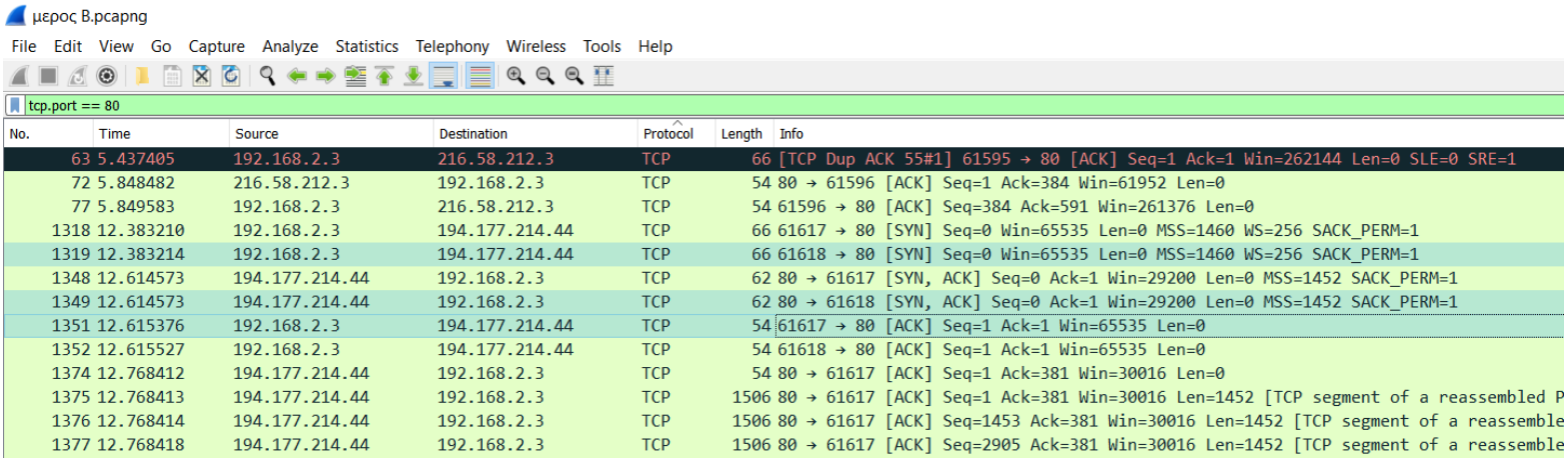
Β’ ΜΕΡΟΣ

1) Η IP διεύθυνση που αντιστοιχεί στον www.ekt.gr είναι η 194.177.214.44



2) Τα τρία πρώτα TCP segments που ανταλλάσσονται μεταξύ του υπολογιστή σας και του συστήματος που φιλοξενεί το www.ekt.gr υλοποιούν την εγκαθίδρυση της σύνδεσης με τη χειραψία 3 βημάτων. Δώστε ένα screenshot από το Wireshark που να περιέχει τα segments αυτά. Εξηγήστε τη διαδικασία χειραψίας τριών βημάτων με βάση την πληροφορία που περιέχεται στα TCP segments αυτά.

Εφαρμόζω το φίλτρο tcp.port == 80



Η σειρά εμφάνισης των πακέτων που ανταλλάσσονται μεταξύ του υπολογιστή μου και του συστήματος που φιλοξενεί το www.ekt.gr και υλοποιούν την εγκαθίδρυση της σύνδεσης με τη χειραψία 3 βημάτων πρέπει να εμφανίζονται με συγκεκριμένη σειρά όπως στο screen. Πρώτα εμφανίζεται το [SYN] έπειτα το [SYN,ACK] και τέλος το [ACK].
Για να δημιουργηθεί μία σύνδεση TCP από έναν υπολογιστή (πελάτη) σε έναν άλλο (διακομιστής) θα πρέπει να ακολουθηθούν τα βήματα που καθορίζονται στο πρωτόκολλο TCP. Συγκεκριμένα θα πρέπει οι δύο υπολογιστές να εμπλακούν σε μία διαδικασία που ονομάζεται τριμερής χειραψία, η οποία περιληπτικά έχει ως εξής:

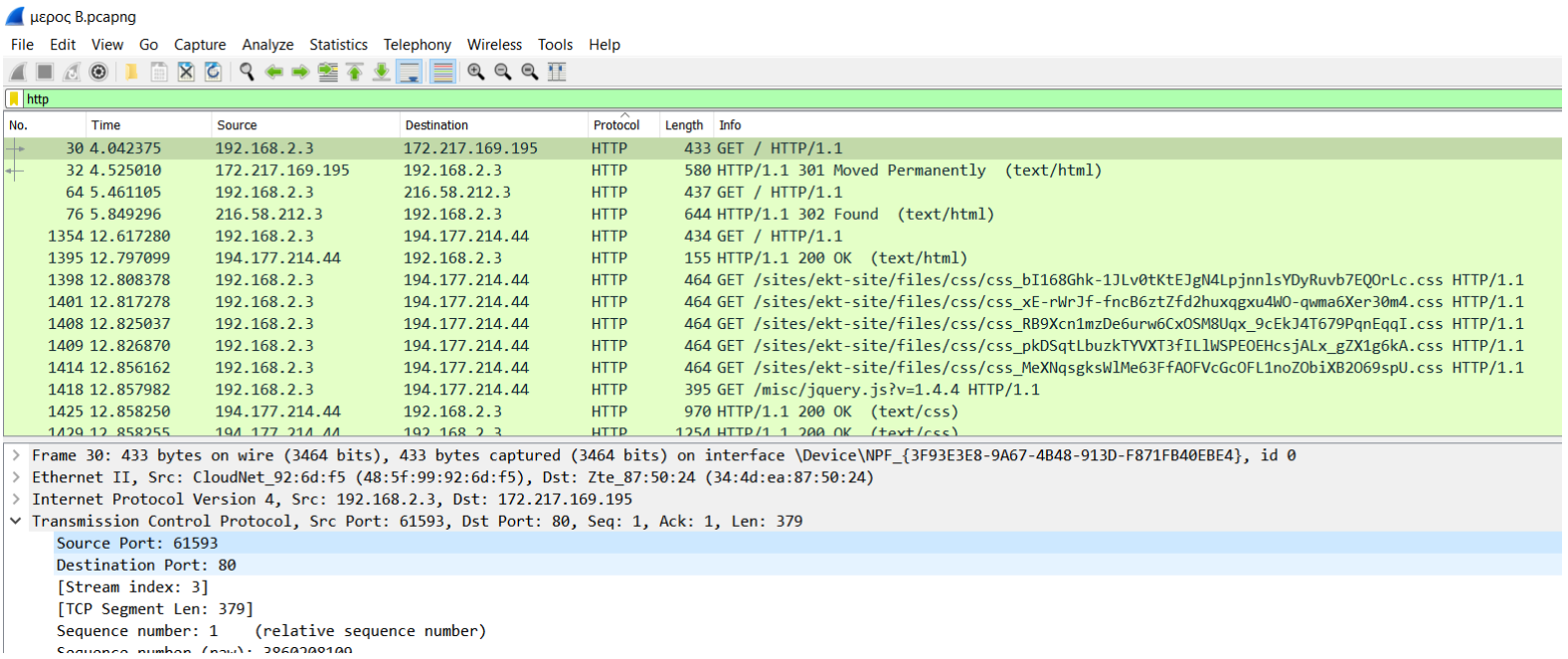
1. Ο πελάτης (client) ζητά την δημιουργία μίας σύνδεσης στέλνοντας έναν πακέτο TCP SYN στον διακομιστή (server). Το όνομα του πακέτου προέρχεται από την λέξη *syncronize* που σημαίνει συγχρονισμός.
2. Ο διακομιστής απαντά στην αίτηση του πελάτη στέλνοντάς του ένα πακέτο TCP SYN-ACK, από την αγγλική λέξη *acknowledge* που σημαίνει αναγνώριση, αποδοχή.
3. Ο πελάτης απαντά με ένα πακέτο TCP ACK δηλώνοντας ότι αποδέχεται και αυτός την σύνδεση.

Μετά το πέρας αυτών των τριών βημάτων, η σύνδεση TCP έχει εγκαθιδρυθεί και μπορούν να αποσταλούν δεδομένα προς και από τους δύο υπολογιστές

Η διαδικασία της χειραψίας τριών βημάτων πρέπει να έχει τα εξής χαρακτηριστικά :
Acknowledge number [ACK] = Sequence number [SYN, ACK]
Acknowledge number [SYN, ACK] = Sequence number [SYN]

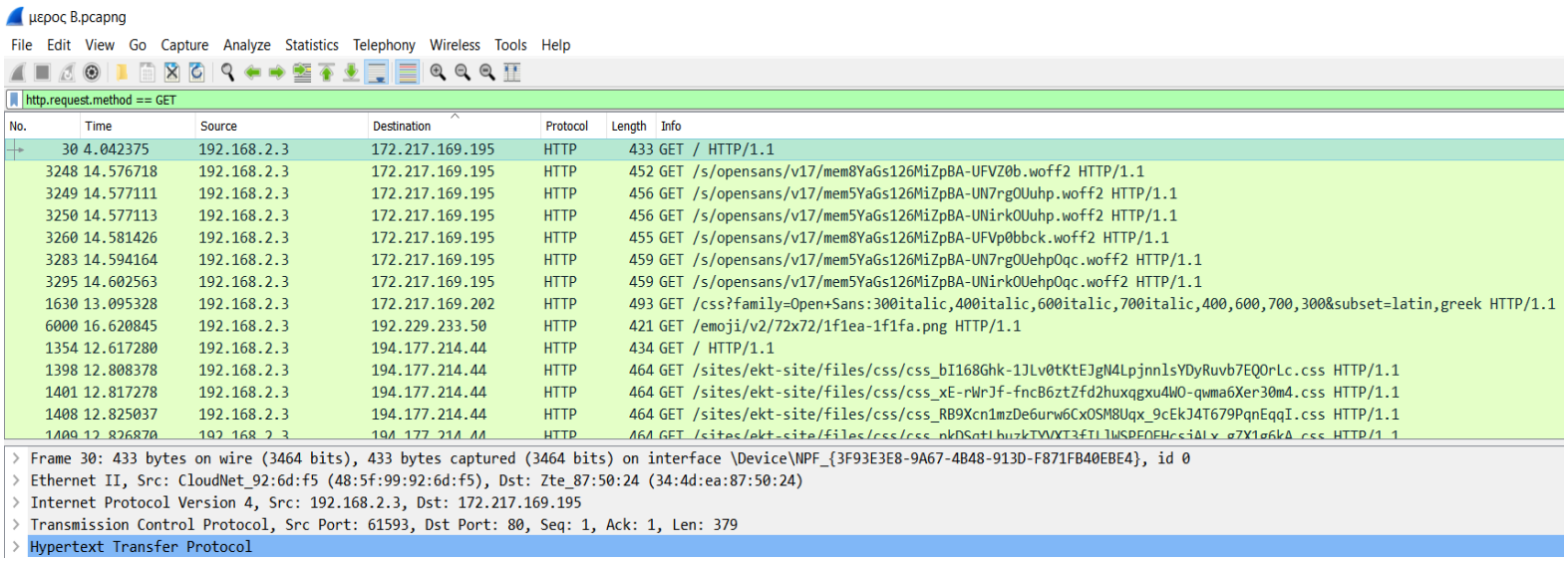
3) Εξετάστε τις θύρες (ports) προέλευσης (source) και προορισμού (destination) που χρησιμοποιήθηκαν από το HTTP πρωτόκολλο. Συνολικά έχω 230 πακέτα με φίλτρο http. Παρατηρώ πως κατά την επικοινωνία οι source ports γίνονται destination ports και το αντίθετο.
Ενδεικτικά:

Source ports	Destination ports
61593	80
80	61593
61596	80
80	61596
61617	80
80	61617
…	…



4) Τα πακέτα που περιείχαν HTTP GET αίτημα που έστειλε ο browser μου είναι: 100
Προς ποιες IP διευθύνσεις στάλθηκαν τα μηνύματα αυτά;
Παρατηρώ ότι οι IP destination διευθύνσεις επαναλαμβάνονται και συνολικά έχω 5 μοναδικές(Για διευκόλυνση ταξινομώ τα πακέτα στο wireshark με βάσει τις στήλες που μου εμφανίζει ανά πακέτο)..

- 172.217.169.195
- 172.217.169.202
- 192.229.233.50
- 194.177.214.44
- 216.28.212.3



Φαίνεται και στο screen πως η διεύθυνση 172.217.169.195 για παράδειγμα πως επαναλαμβάνεται πολλές φορές.
Οι μοναδικές distinct destination addresses είναι οι παραπάνω.

5) Ο browser μου τρέχει την έκδοση HTTP 1.1
Ο server Τρέχει την έκδοση 1.1