ΣΤΟΙΧΕΙΑ: Διονυσία Ψυρρή,1080424,3ο έτος

Ανάλυση DNS πρωτοκόλλου:

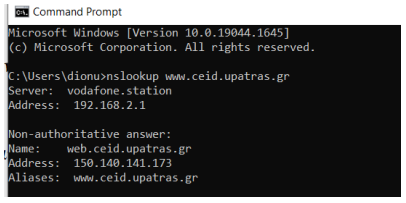
Εκτέλεση εντολών:

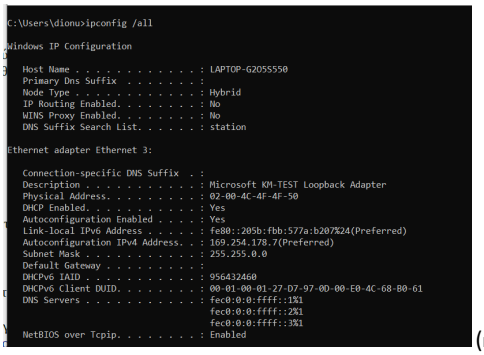
nslookup www.ceid.upatras.gr: Χρησιμοποιείται για την αναζήτηση πληροφοριών από εξυπηρετητές του Συστήματος Ονομάτων Τομέα (DNS). Οι πρώτες 2 γραμμές είναι πληροφορίες για τον εξυπηρετητή ονομάτων που δίνει απάντηση. Οι επόμενες 2 γραμμές δείχνουν το όνομα και τη διεύθυνση IP του υπολογιστή με βάση τον οποίο γίνεται η αναζήτηση.

ipconfig /all: (σημαίνει "Διαμόρφωση πρωτοκόλλου Διαδικτύου ") είναι ένα πρόγραμμα εφαρμογής κονσόλας ορισμένων λειτουργικών συστημάτων υπολογιστών που εμφανίζει όλες τις τρέχουσες τιμές διαμόρφωσης δικτύου TCP / IP και ανανεώνει τις ρυθμίσεις Dynamic Host Configuration Protocol (DHCP) και Domain Name System (DNS).

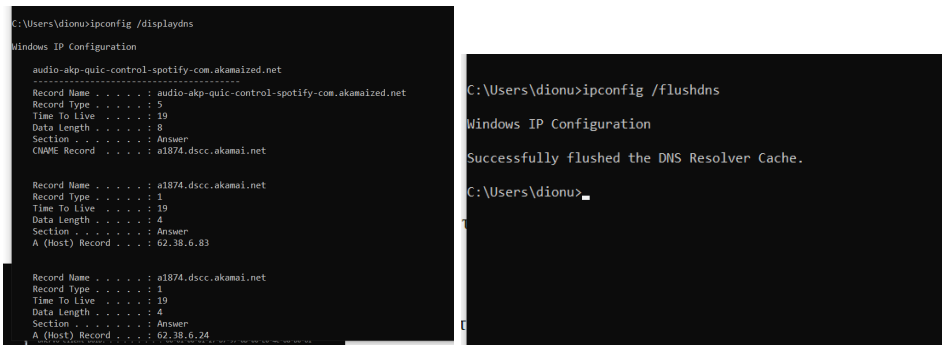
ipconfig /displaydns: Εμφανίζει τα περιεχόμενα της προσωρινής μνήμης του προγράμματος-πελάτη επίλυσης DNS, η οποία περιλαμβάνει και τις δύο καταχωρήσεις προφορτωμένες από την τοπική. Αρχείο κεντρικών υπολογιστών και τυχόν εγγραφές πόρων που αποκτήθηκαν πρόσφατα για ερωτήματα ονόματος που επιλύονται από τον υπολογιστή, το DNS. Η υπηρεσία πελάτη χρησιμοποιεί αυτές τις πληροφορίες για να επιλύσει γρήγορα τα ονόματα που υποβάλλονται συχνά σε ερωτήσεις, πριν υποβάλει ερώτημα διαμορφωμένους διακομιστές DNS

ipconfig /flushdns: Το σύστημά εκκαθαρίζει την προσωρινή μνήμη του προγράμματος-πελάτη επίλυσης DNS. Επίσης μπορούμε να χρησιμοποιήσουμε αυτή την διαδικασία για την απόρριψη αρνητικών καταχωρήσεων προσωρινής μνήμης από τη μνήμη cache.

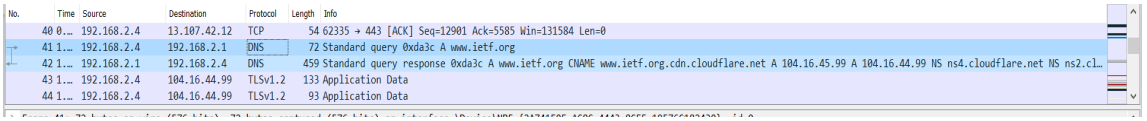




(και είχε κι άλλα προς τα κάτω)



1.



Ανάλυση μηνυμάτων: Το περιβάλλον του Wireshark χωρίζεται σε 3 πεδία: Τη λίστα με τα μηνύματα και τις αποκρίσεις, τις λεπτομέρειές τους και τα bytes.

Ανάλυση του πακέτου: Το πακέτο αποτελείται από 1 μηνύμα και 1 αποκρίση.

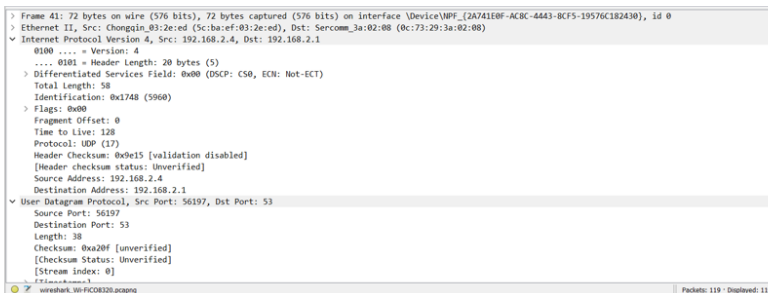
1^{ο} μήνυμα: Standard query 0xda3c A www.ietf.org
Το 0xda3c αποτελέι το transaction id

Τα πρώτα 14 ψηφία (σε δεκαεξαδικό) είναι το Ethernet header, και δίπλα υπάρχει και η μετάφραση σε κώδικα Ascii. Τα επόμενα 20 ψηφία είναι η ip header. Τα επόμενα 8 αφορούν το UDP πρωτόκολλο, ενώ τα 36 τελευταία αφορούν το DNS query. Το πρωτόκολλο που έχει χρησιμοποιηθεί είναι το UDP.

1^{η} απόκριση: Το 0xda3c είναι το transaction ID.
Τα πρώτα 14 ψηφία είναι το Ethernet ID και δίπλα βρίσκεται αντίστοιχα η μετάφραση σε κώδικα Ascii. Τα επόμενα 40 ψηφία είναι η IP header. Τα επόμενα 8 είναι για το UDP πρωτόκολλο, ενώ τα τελευταία 64 είναι για την απόκριση του DNS.

Έχει χρησιμοποιηθεί το UDP πρωτόκολλο.

2.

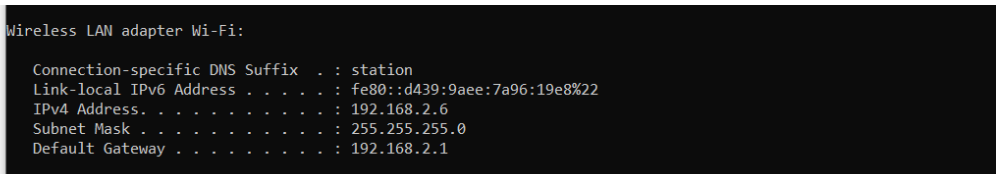


Η θήρα προορισμού για το μήνυμα ερώτησης του DNS είναι: Destination Port: 53
Η θήρα προέλευσης για το μήνυμα απόκρισης του DNS είναι: Source Port: 56197

3.

IP εμφανίζεται το μήνυμα ερώτησης DNS: **192.168.2.1**

Παρατηρώ ότι οι διεύθυνσεις δεν είναι ίδιες.



4. Το μήνυμα ερώτησης είναι τύπου A Standart Query και δεν περιέχει απαντήσεις
5. Υπάρχει μια απάντηση:
www.ietf.org: type AAAA, class IN
Name: www.ietf.org
[Name Length: 12]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)

6. Αντιστοιχεί στο destination.

7. Το Header ενός DNS πακέτου: όπως φαίνεται, αποτελείται από 6 πεδία.
Το πρώτο πεδίο είναι το Transaction ID, το οποίο πρέπει να είναι ίδιο στο μηνυμα ερώτησης και στο μήνυμα απάντησης.
Στη συνέχεια υπάρχει ένα πεδίο με flags τα οποία δείχνουν (με τη σειρά):
Εάν το μήνυμα αποτελεί μήνυμα ερώτησης ή απάντησης
Το Opcode
Εάν ο server είναι authoritative
Truncated: Message is not truncated
Αίτηση για να είναι το query recursive.
Απάντηση αν το query μπορεί να είναι recursive.
Z: reserved
Εάν η απάντηση είναι authenticated
Εάν επιτρέπονται non-authenticated data
Το Reply code που δείχνει εάν υπάρχει κάποιο error.
Μετά το πεδίο των flags έχουμε τον αριθμό των ερωτήσεων, τον αριθμό των απαντήσεων RR, τον αριθμό
των authority RRs και τον αριθμό τον επιπρόσθετων RRs.

8. 48 F8 B3 26 DF 49 BA BA BA BA BA BA 08 00 45 00 00 38 66 BD 00 00 80 11
02 0C C0 A8 01 34 08 08 08 08 D5 39 00 35 00 24 44 8F 00 03 01 00 00 01 00 00
00 00 00 00 06 67 6F 6F 67 6C 65 03 63 6F 6D 00 00 01 00 01

192.168.1.52 → 8.8.8.8 DNS Standard query 0x0003 A google.com
Τα πρώτα 13 bytes αποτελούν το Ethernet, τα επόμενα 20 την IP, τα επόμενα
8 το UDP και τέλος, τα τελευταία 28 το DNS.

Για το Ethernet:Destination: Cisco-Li_26:df:49 (48:f8:b3:26:df:49)
Source: ba:ba:ba:ba:ba:ba (ba:ba:ba:ba:ba:ba)
Type: IPv4 (0x0800)

Για το IPv4:

0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 56
Identification: 0x66bd (26301)
Flags: 0x0000
Fragment offset: 0
Time to live: 128
Protocol: UDP (17)
Header checksum: 0x020c
Header checksum status: Unverified
Source: 192.168.1.52
Destination: 8.8.8.8

Για το UDP:
Source Port: 54585
Destination Port: 53
Length: 36
Checksum: 0x448f
Checksum Status: Unverified
Stream index: 0

Για το DNS:
Transaction ID: 0x0003
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Το DNS μήνυμα αποτελεί μήνυμα ερώτησης.
Ερώτηση:
google.com: type A, class IN

Το query ζητάει την IP για το google.com

9. BA BA BA BA BA BA 48 F8 B3 26 DF 49 08 00 45 08 00 E8 B2 EF 00 00 37 11

FE 21 08 08 08 08 C0 A8 01 34 00 35 D5 39 00 D4 28 A2 00 03 81 80 00 01 00 0B

00 00 00 00 06 67 6F 6F 67 6C 65 03 63 6F 6D 00 00 01 00 01 C0 0C 00 01 00 01

00 00 00 04 00 04 4A 7D EC 23 C0 0C 00 01 00 01 00 00 00 04 00 04 4A 7D EC

25 C0 0C 00 01 00 01 00 00 00 04 00 04 4A 7D EC 27 C0 0C 00 01 00 01 00 00 00

04 00 04 4A 7D EC 20 C0 0C 00 01 00 01 00 00 00 04 00 04 4A 7D EC 28 C0 0C

00 01 00 01 00 00 00 04 00 04 4A 7D EC 21 C0 0C 00 01 00 01 00 00 00 04 00 04

4A 7D EC 29 C0 0C 00 01 00 01 00 00 00 04 00 04 4A 7D EC 22 C0 0C 00 01 00

01 00 00 00 04 00 04 4A 7D EC 24 C0 0C 00 01 00 01 00 00 00 04 00 04 4A 7D

EC 2E C0 0C 00 01 00 01 00 00 00 04 00 04 4A 7D EC 26

8.8.8.8 → 192.168.1.52
DNS Standard query response 0x0003 A google.com
A 74.125.236.35
A 74.125.236.37
A 74.125.236.39
A 74.125.236.32
A 74.125.236.40
A 74.125.236.33A 74.125.236.34
A 74.125.236.36
A 74.125.236.46
A 74.125.236.38
Τα πρώτα 13 bytes αποτελούν το Ethernet, τα επόμενα 20 την IP, τα επόμενα 8 το UDP και τέλος, τα τελευταία 204 το DNS.

Για το Ethernet:
Destination: ba:ba:ba:ba:ba:ba (ba:ba:ba:ba:ba:ba)
Source: Cisco-Li_26:df:49 (48:f8:b3:26:df:49)
Type: IPv4 (0x0800)

Για την IPv4:
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x08 (DSCP: Unknown, ECN: Not-ECT)
Total Length: 232
Identification: 0xb2ef (45807)
Flags: 0x0000
Fragment offset: 0
Time to live: 55
Protocol: UDP (17)
Header checksum: 0xfe21
Header checksum status: Unverified
Source: 8.8.8.8
Destination: 192.168.1.52

Για το UDP:
Source Port: 53
Destination Port: 54585
Length: 212
Checksum: 0x28a2
Checksum Status: Unverified
Stream index: 0

Για το DNS:

Transaction ID: 0x0003

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 11

Authority RRs: 0

Additional RRs: 0

Το DNS μήνυμα αποτελεί μήνυμα απάντησης.

Οι απαντήσεις:

google.com: type A, class IN, addr 74.125.236.35

google.com: type A, class IN, addr 74.125.236.37

google.com: type A, class IN, addr 74.125.236.39

google.com: type A, class IN, addr 74.125.236.32

google.com: type A, class IN, addr 74.125.236.40

google.com: type A, class IN, addr 74.125.236.33

google.com: type A, class IN, addr 74.125.236.41

google.com: type A, class IN, addr 74.125.236.34

google.com: type A, class IN, addr 74.125.236.36

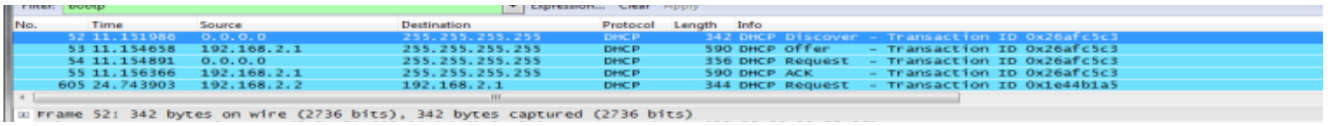
google.com: type A, class IN, addr 74.125.236.46

google.com: type A, class IN, addr 74.125.236.38

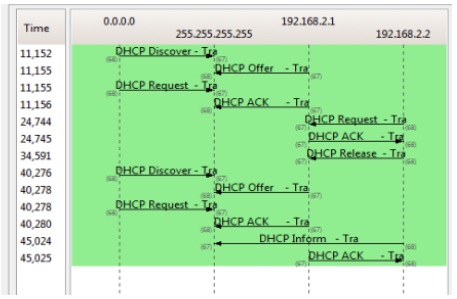
Ανάλυση DHCP πρωτοκόλλου:

ipconfig /release: Αυτή η εντολή αποδεσμεύει την IP διεύθυνση που είχε εκχωρηθεί δυναμικά τη δεδομένη στιγμή στον υπολογιστή (host) από τον διακομιστή DHCP

Ipconfig /renew: Η εντολή αυτή οδηγεί τον host να ζητήσει από τον διακομιστή DHCP να εκχωρήσει μια δυναμική διεύθυνσης IP



1.



2. θύρα:bootps

Πρωτόκολλο:UDP

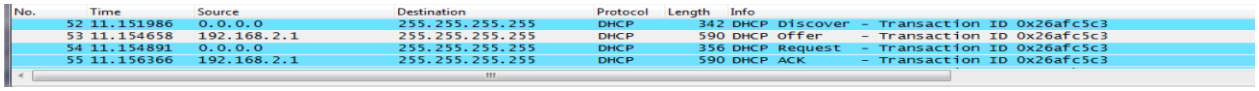
3. 192.168.2.1

4. Οι τιμές που διαφοροποιούν το DHCP Discover μήνυμα από το DHCP Request μήνυμα είναι στο πεδίο Option 53. Όπου στο πρώτο πακέτο έχει την τιμή DHCP Discover και στο

δεύτερο DHCP Request. Σε ότι αφορά τα υπόλοιπα πεδία, αυτά δεν παρουσιάζουν διαφοροποιήσεις.

5. στα τέσσερα πρώτα πακέτα η διεύθυνση αποστολής είναι κοινή, η 255.255.255.255.

6. Η διεύθυνση πηγής για τον πελάτη είναι η προκαθορισμένη 0.0.0.0. Ενώ ο διακομιστής DHCP χρησιμοποιεί την πραγματική του διεύθυνση, την 192.168.2.1.



No.	Time	Source	Destination	Protocol	Length	Info
52	11.151986	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x26afc5c3
53	11.154658	192.168.2.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x26afc5c3
54	11.154891	0.0.0.0	255.255.255.255	DHCP	356	DHCP Request - Transaction ID 0x26afc5c3
55	11.156366	192.168.2.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x26afc5c3

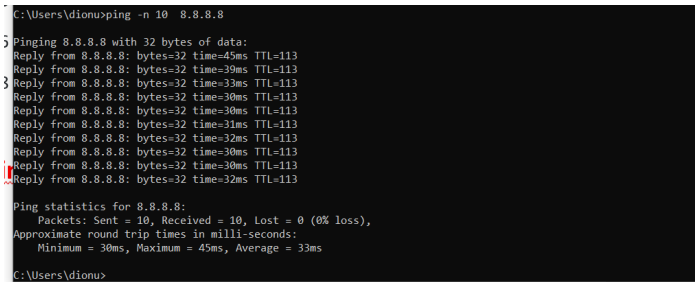
7. το IP Address Lease Time που έχει τιμή 1 ώρα. Είναι ο χρόνος για τον οποίο ο DHCP διακομιστής δίνει μία IP διεύθυνση σε ένα πελάτη. Δεσμεύοντας την απέναντι σε αιτήσεις από άλλους πελάτες.

8. Ο σκοπός των μηνυμάτων DHCP release είναι για να καταργήσουν την δυναμική εκχώρηση μίας διεύθυνσης IP σε πελάτη και να την απελευθερώσουν για κάποια επόμενη αίτηση. Σε περίπτωση που δεν σταλεί αυτό το μήνυμα θα πρέπει να περάσει ο χρόνος lease time προκειμένου να απελευθερωθεί η διεύθυνση

9.Ναι ανταλλάχθηκαν, όσον αφορά τα ARP μηνύματα, αυτά πραγματοποιούνται κατόπιν αίτησης του DHCP διακομιστή. Προκειμένου να βεβαιωθεί ότι η διεύθυνση IP που προτίθεται να αποδώσει σε ένα πελάτη δεν είναι δεσμευμένη από άλλον υπολογιστή (host)

Ανάλυση ICMP πρωτοκόλλου – Ping:

1.



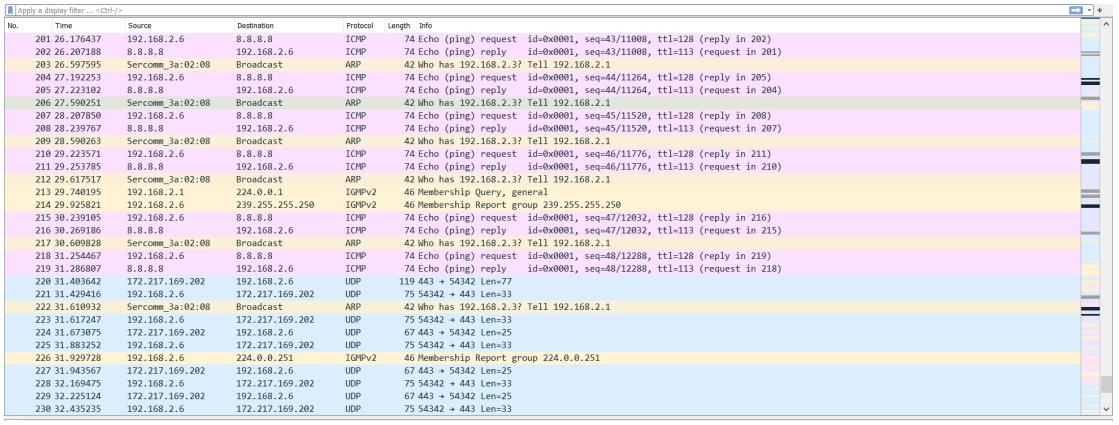
```
C:\Users\dionu>ping -n 10  8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=45ms TTL=113
Reply from 8.8.8.8: bytes=32 time=39ms TTL=113
Reply from 8.8.8.8: bytes=32 time=33ms TTL=113
Reply from 8.8.8.8: bytes=32 time=30ms TTL=113
Reply from 8.8.8.8: bytes=32 time=30ms TTL=113
Reply from 8.8.8.8: bytes=32 time=31ms TTL=113
Reply from 8.8.8.8: bytes=32 time=32ms TTL=113
Reply from 8.8.8.8: bytes=32 time=30ms TTL=113
Reply from 8.8.8.8: bytes=32 time=30ms TTL=113
Reply from 8.8.8.8: bytes=32 time=32ms TTL=113

Ping statistics for 8.8.8.8:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 30ms, Maximum = 45ms, Average = 33ms

C:\Users\dionu>
```

2.



No.	Time	Source	Destination	Protocol	Length	Info
201	26.176437	192.168.2.6	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=43/11008, ttl=128 (reply in 202)
202	26.207188	8.8.8.8	192.168.2.6	ICMP	74	Echo (ping) reply id=0x0001, seq=43/11008, ttl=113 (request in 201)
203	26.597595	Sercomm_3a:02:08	Broadcast	ARP	42	Who has 192.168.2.3? Tell 192.168.2.1
204	27.192253	192.168.2.6	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=44/11264, ttl=128 (reply in 205)
205	27.223102	8.8.8.8	192.168.2.6	ICMP	74	Echo (ping) reply id=0x0001, seq=44/11264, ttl=113 (request in 204)
206	27.590251	Sercomm_3a:02:08	Broadcast	ARP	42	Who has 192.168.2.3? Tell 192.168.2.1
207	28.207850	192.168.2.6	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=45/11520, ttl=128 (reply in 208)
208	28.239767	8.8.8.8	192.168.2.6	ICMP	74	Echo (ping) reply id=0x0001, seq=45/11520, ttl=113 (request in 207)
209	28.590263	Sercomm_3a:02:08	Broadcast	ARP	42	Who has 192.168.2.3? Tell 192.168.2.1
210	29.223571	192.168.2.6	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=46/11776, ttl=128 (reply in 211)
211	29.253785	8.8.8.8	192.168.2.6	ICMP	74	Echo (ping) reply id=0x0001, seq=46/11776, ttl=113 (request in 210)
212	29.617517	Sercomm_3a:02:08	Broadcast	ARP	42	Who has 192.168.2.3? Tell 192.168.2.1
213	29.740195	192.168.2.1	224.0.0.1	IGMPv2	46	Membership Query, general
214	29.925821	192.168.2.6	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
215	30.239105	192.168.2.6	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=47/12032, ttl=128 (reply in 216)
216	30.269186	8.8.8.8	192.168.2.6	ICMP	74	Echo (ping) reply id=0x0001, seq=47/12032, ttl=113 (request in 215)
217	30.609828	Sercomm_3a:02:08	Broadcast	ARP	42	Who has 192.168.2.3? Tell 192.168.2.1
218	31.254467	192.168.2.6	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=48/12288, ttl=128 (reply in 219)
219	31.286807	8.8.8.8	192.168.2.6	ICMP	74	Echo (ping) reply id=0x0001, seq=48/12288, ttl=113 (request in 218)
220	31.403642	172.217.169.202	192.168.2.6	UDP	119	443 → 54342 Len=77
221	31.429416	192.168.2.6	172.217.169.202	UDP	75	54342 → 443 Len=33
222	31.610932	Sercomm_3a:02:08	Broadcast	ARP	42	Who has 192.168.2.3? Tell 192.168.2.1
223	31.617247	192.168.2.6	172.217.169.202	UDP	75	54342 → 443 Len=33
224	31.673075	172.217.169.202	192.168.2.6	UDP	67	443 → 54342 Len=25
225	31.883252	192.168.2.6	172.217.169.202	UDP	75	54342 → 443 Len=33
226	31.929728	192.168.2.6	224.0.0.251	IGMPv2	46	Membership Report group 224.0.0.251
227	31.943567	172.217.169.202	192.168.2.6	UDP	67	443 → 54342 Len=25
228	32.169475	192.168.2.6	172.217.169.202	UDP	75	54342 → 443 Len=33
229	32.225124	172.217.169.202	192.168.2.6	UDP	67	443 → 54342 Len=25
230	32.435235	192.168.2.6	172.217.169.202	UDP	75	54342 → 443 Len=33

Ανάλυση: Η IP διεύθυνση του αποστολέα είναι 192.168.2.6, αντιστοιχεί στον υπολογιστή όπου γίνεται το πείραμα

Ο παραλήπτης έχει τη διεύθυνση 8.8.8.8

– Το πεδίο type έχει την τιμή 8.

– Το πεδίο code number την τιμή 0.

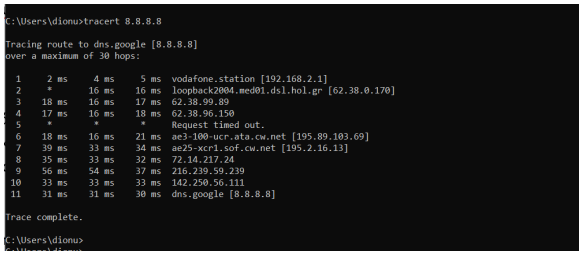
– Τα πεδία checksum, identifier, sequence number καταλαμβάνουν 2 bytes έκαστο.

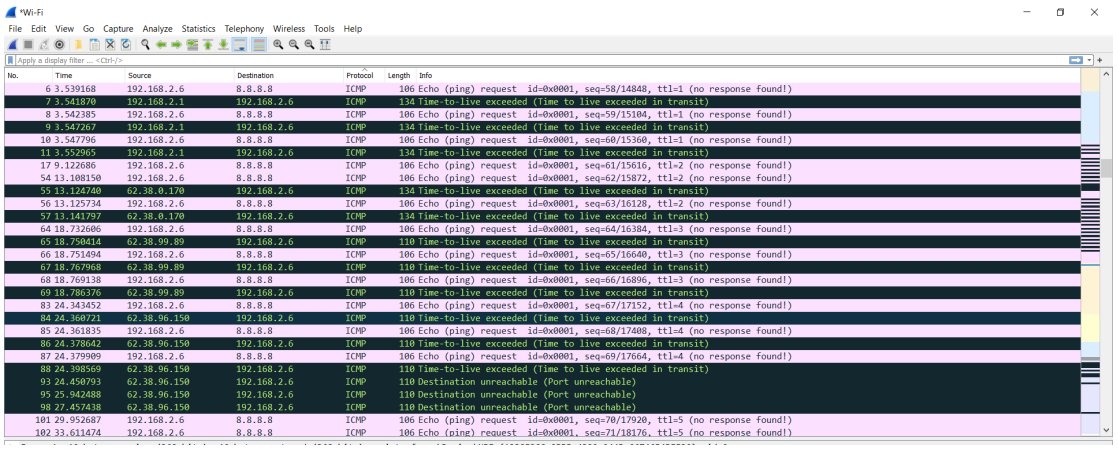
– Τα δεδομένα καταλαμβάνουν 32 bytes

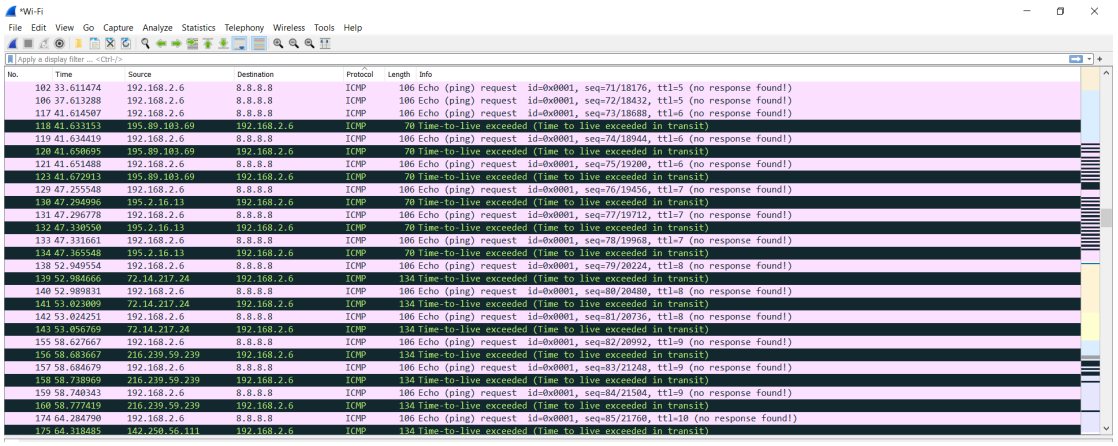
3. Οι θύρες πηγής και προορισμού από την άλλη δεν φαίνονται πουθενά. Αυτό συμβαίνει γιατί το ICMP πακέτο έχει σχεδιαστεί να επικοινωνεί σε επίπεδο δικτύου μεταξύ του υπολογιστή και του δρομολογητή και όχι μέσω εφαρμογών στο επίπεδο εφαρμογής.

4. Διαπιστώσα ότι το πεδίο type έχει την τιμή 0, ενώ στο μήνυμα ερώτησης ήταν 8. Από εκεί και πέρα, τα υπόλοιπα πεδία είναι τα ίδια με το ICMP μήνυμα ερώτησης.

Ανάλυση ICMP πρωτοκόλλου – Traceroute:







6. ICMP echo πακέτο στο οποίο διακρίνονται τα ίδια πεδία με τα πακέτα που εντοπίστηκαν και στο ICMP ping

7. Παρατηρείται ότι αυτό το ICMP πακέτο λάθους [Time-to-Live exceeded] περιέχει περισσότερα πεδία από ότι ένα Ping ICMP μήνυμα. Τα παραπάνω πεδία περιέχουν την IP επικεφαλίδα και τα πρώτα 8 bytes από το αρχικό ICMP πακέτο. Για το οποίο στάλθηκε το μήνυμα λάθους.

8. Εξετάζοντας τα τελευταία τρία πακέτα ICMP που στάλθηκαν στον υπολογιστή από όπου έγιναν οι μετρήσεις του πειράματος: Διαπιστώνεται ότι η τιμή του πεδίου message type είναι 0 και όχι 11. Αυτό συνέβη γιατί τα τελευταία μηνύματα πρόλαβαν να φτάσουν στον προορισμό τους, προτού να λήξει ο χρόνος TTL. Με βάση τα παραπάνω, θα αναδειχθούν τα πλεονεκτήματα χρήσης ενός δικτύου διανομής περιεχομένου.

Ανάλυση IP πρωτοκόλλου:

Τα πρώτα 13 και τα τελευταία 9 ψηφία αποτελούν το Ethernet header. Τα επόμενα 20 ψηφία είναι το IPv4 header (14ο εώς 33ο). Τα επόμενα 21 είναι το TCP header (34ο εώς 54ο).

1. Η διεύθυνση IP του προορισμού αποστολής είναι: 129.110.2.17.

2. Το μήκος του IP μέρους είναι συνολικά 41 bytes.

3. Το frame μας αποτελείται από 64 byte, επομένως είναι ολόκληρο πακέτο και οχι μέρος κάποιου

μεγαλύτερου.

4. Η TCP θύρα του αποστολέα είναι η 515 ενώ του δέκτη η 80.

5. Η τιμή του header checksum είναι 0x7dcb. Το header checksum είναι ουσιαστικά το άθροισμα όλων των προηγούμενων πεδίων της IP header. Στο frame μας το άθροισμα αυτό είναι 22.010(10) ενώ το header checksum είναι 17.728(10). Αρα είναι σωστή