

Τεχνολογίες και Υπηρεσίες Διαδικτύου

Εργασία με χρήση του εργαλείου Wireshark

Φίλιππος Δουραχαλής, 3312205

Άσκηση 1)

1.

Πρωτόκολλο	Επίπεδο	Πρωτόκολλο Επιπέδου Μεταφοράς
ARP	Ζεύξης Δεδομένων	
IPv4	Δικτύου	
IPv6	Δικτύου	
ICMPv6	Δικτύου	
TCP	Μεταφοράς	
UDP	Μεταφοράς	
TLSv1.2	Μεταφοράς-Εφαρμογής	TCP
TLSv1.3	Μεταφοράς-Εφαρμογής	TCP
DNS	Εφαρμογής	UDP
MDNS	Εφαρμογής	UDP
LLMNR	Εφαρμογής	UDP
SSDP	Εφαρμογής	UDP
HTTP	Εφαρμογής	TCP

2.

Καταγράφηκαν 14 endpoints σε επίπεδο Ethernet και συνολικά 68 endpoints σε επίπεδο IP (44 IPv4 και 24 IPv6). Τα συγκεκριμένα endpoints της επικοινωνίας με τον υπολογιστή είναι τα ακόλουθα.

Ethernet Endpoints	IPv4 Endpoints	IPv6 Endpoints
a4:91:b1:5a:cc:a0	192.168.1.221	fdfd:3427:2509:0:93b:6bc7:26ec:fedf
ff:ff:ff:ff:ff:ff	255.255.255.255	fdfd:3427:2509::1
7c:f6:66:19:f4:86	192.168.1.60	2a02:2149:8ad2:6a00:93b:6bc7:26ec:fedf
7c:f6:66:17:0e:7d	192.168.1.165	2a00:1450:4017:815::200a
34:e1:2d:51:6a:80	195.122.177.184	fe80::a684:1dbf:eff8:881a
fe:70:e3:ff:b6:c4	192.168.1.10	ff02::fb
01:00:5e:00:00:fb	224.0.0.251	ff02::1:3
ec:fa:bc:c7:6b:ea	172.217.17.228	fe80::a691:b1ff:fe5a:cca0

a8:93:4a:ea:4b:1f	130.117.190.213	2a00:1450:4017:80e::200e
33:33:00:00:00:fb	13.107.237.44	fe80::87ce:3730:68c4:b10c
33:33:00:01:00:03	192.168.1.14	2a00:1450:4017:800::200a
01:00:5e:00:00:fc	142.250.187.106	2620:1ec:42::132
01:00:5e:7f:ff:fa	192.168.1.125	2a00:1450:4017:80d::200a
00:a0:96:e5:4f:0a	224.0.0.252	2620:1ec:4e:1::44
	195.251.255.227	2a00:1450:4017:804::200a
	192.168.1.1	2a00:1450:4017:80d::2003
	239.255.255.250	2a00:1450:4017:814::2003
	52.111.231.17	2a00:1450:4017:808::200e
	20.189.173.11	2a00:1450:4017:804::200e
	142.250.187.142	2a00:1450:4017:810::2003
	199.231.164.68	2a00:1450:4017:816::2016
	216.58.212.3	2a00:1450:4017:816::2001
	142.251.140.74	2a00:1450:4017:816::200e
	52.113.194.132	2a02:2149:3::c2db:5a0
	40.126.31.72	
	20.190.159.22	
	204.79.197.203	
	195.251.252.250	
	142.250.187.163	
	216.58.214.141	
	216.58.212.42	
	142.250.187.174	
	142.250.187.99	
	172.217.17.227	
	152.199.21.118	
	23.50.174.96	
	142.251.140.78	
	20.54.24.69	
	142.251.140.14	
	172.217.169.118	
	172.217.169.97	
	131.253.33.254	
	142.250.187.110	
	194.219.5.160	

Παρατηρούμε ότι δεν ταυτίζονται τα endpoints του Ethernet με τα endpoints του internet. Αυτό διότι οι διευθύνσεις του Ethernet χρησιμοποιούνται μόνο για την προώθηση πλαισίων μεταξύ των κόμβων εντός του τοπικού δικτύου. Αντίθετα οι διευθύνσεις IP χρησιμοποιούνται στο επίπεδο δικτύου για την επικοινωνία του υπολογιστή με άλλους κόμβους στο διαδίκτυο, το πλήθος το οποίων είναι αρκετές φορές μεγαλύτερο σε σύγκριση με τους κόμβους του τοπικού μας δικτύου.

Σημείωση: Η ιδιωτική IPv4 διεύθυνση του υπολογιστή μας είναι η “192.168.1.165”, ενώ ως IPv6 διευθύνσεις χρησιμοποιούνται οι “2a02:2149:8ad2:6a00:93b:6bc7:26ec:fedf”, “ fe80::87ce:3730:68c4:b10c” και “fdfd:3427:2509:0:93b:6bc7:26ec:fedf”

3.

Για να λάβουμε όλα τα πακέτα TCP που έχουν σταλεί από τον υπολογιστή εφαρμόζουμε το φίλτρο

```
"tcp && (ip.src == 192.168.1.165 || ipv6.src == 2a02:2149:8ad2:6a00:93b:6bc7:26ec:fedf || ipv6.src == fdfd:3427:2509:0:93b:6bc7:26ec:fedf || ipv6.src == fe80::87ce:3730:68c4:b10c)"
```

Αυτά είναι συνολικά 3.256

tcp && (ip.src == 192.168.1.165 ipv6.src == 2a02:2149:8ad2:6a00:93b:6bc7:26ec:fedf ipv6.src == fdfd:3427:2509:0:93b:6bc7:26ec:fedf ipv6.src == fe80::87ce:3730:68c4:b10c)						
No.	Time	Source	Destination	Protocol	Length	Info
5	0.864959	192.168.1.165	195.122.177.184	TLSv1.2	132	Application Data
6	0.865030	192.168.1.165	195.122.177.184	TLSv1.2	831	Application Data
15	1.186536	192.168.1.165	195.122.177.184	TCP	54	60522 → 443 [ACK] Seq=856 Ack=235 Win=64404 Len=0
18	2.462097	192.168.1.165	172.217.17.228	TLSv1.2	227	Application Data
19	2.462992	192.168.1.165	130.117.190.213	TLSv1.2	131	Application Data
20	2.463052	192.168.1.165	130.117.190.213	TLSv1.2	296	Application Data
21	2.542375	192.168.1.165	172.217.17.228	TLSv1.2	89	Application Data
22	2.563646	192.168.1.165	172.217.17.228	TLSv1.2	228	Application Data
23	2.604467	192.168.1.165	172.217.17.228	TLSv1.2	89	Application Data
24	2.667641	192.168.1.165	172.217.17.228	TLSv1.2	229	Application Data
25	2.672222	192.168.1.165	130.117.190.213	TLSv1.2	131	Application Data
26	2.672465	192.168.1.165	130.117.190.213	TLSv1.2	297	Application Data
> Frame 6: 831 bytes on wire (6648 bits), 831 bytes captured (6648 bits) on interface 0						
> Ethernet II, Src: IntelCor_51:6a:80 (34:e1:2d:51:6a:80), Dst: Technico_5a:cc:01:00:00:00						
> Internet Protocol Version 4, Src: 192.168.1.165, Dst: 195.122.177.184						
> Transmission Control Protocol, Src Port: 60522, Dst Port: 443, Seq: 79, Ack: 235, Win: 64404, Len: 0						
> Transport Layer Security						
0000 a4 91 b1 5a cc a0 34 e1 2d 51 6a 80 08 00 45 00						
0010 03 31 cf bb 40 00 80 06 00 00 c0 a8 01 a5 c3 70						
0020 b1 b8 ec 6a 01 bb 39 20 52 94 3f b1 f5 50 50 10						
0030 fc 7e 3a a4 00 00 17 03 03 03 04 c1 97 e9 64 a0						
0040 87 1e 5c 1c 49 aa 54 34 1f c8 f9 69 81 c1 23 20						
0050 22 25 6c 2c 2b 76 ab 1c 68 2d 55 20 6b 73 e9 20						
0060 42 d6 fb 28 ab 00 33 2a cc a5 e1 49 79 8e 6f 50						
0070 1f 29 bc c7 48 f0 01 b9 0a 0e e5 55 d0 c5 d5 f0						
0080 2b e1 ba b6 23 0c d6 00 fa 8f 7a c1 82 bb 90 c0						
0090 a9 7e 20 8b 9d 47 27 e2 6f 45 00 50 a2 13 ad a0						
00a0 24 cf ea ee a8 22 b8 23 89 8e 90 79 0c 84 c6 f0						
00b0 d2 82 a8 3b d5 b1 da 61 c6 91 2e f4 3b 8c 7c 60						
00c0 80 9d 9f 19 0b 20 94 1d 2a 14 3a 68 f7 5e a9 70						
00d0 9d 86 6a 16 ed 93 ae be 73 bc 2c 10 d9 7b 83 e0						

Εφαρμόζοντας αντίστοιχο φίλτρο, δηλαδή

```
"udp && (ip.src == 192.168.1.165 || ipv6.src == 2a02:2149:8ad2:6a00:93b:6bc7:26ec:fedf || ipv6.src == fdfd:3427:2509:0:93b:6bc7:26ec:fedf || ipv6.src == fe80::87ce:3730:68c4:b10c)"
```

παίρνουμε όλα τα πακέτα UDP τα οποία έχουν ως πηγή τον υπολογιστή μας, τα οποία είναι 87 στο πλήθος.

udp && (p.src == 192.168.1.165 ipv6.src == 2a02:2149:8ad2:6a00:93b:6bc7:26ec:fedf ipv6.src == fdff:3427:2509:0:93b:6bc7:26ec:fedf ipv6.src == fe80::87ce:3730:68c4:b10c)						
No.	Time	Source	Destination	Protocol	Length	Info
7	1.078002	fdff:3427:2509:0:93...	fdff:3427:2509::1	DNS	88	Standard query 0xcdad A wpad.lan
8	1.078207	fdff:3427:2509:0:93...	fdff:3427:2509::1	DNS	88	Standard query 0x30f8 AAAA wpad.lan
270	5.297793	fdff:3427:2509:0:93...	fdff:3427:2509::1	DNS	115	Standard query 0x73f4 A optimizationguide-pa.googleapis.c
271	5.298380	fdff:3427:2509:0:93...	fdff:3427:2509::1	DNS	115	Standard query 0x38d5 AAAA optimizationguide-pa.googleapi
272	5.298891	fdff:3427:2509:0:93...	fdff:3427:2509::1	DNS	115	Standard query 0xf95f HTTPS optimizationguide-pa.googleap
332	5.848995	fdff:3427:2509:0:93...	fdff:3427:2509::1	DNS	94	Standard query 0x2842 A eclass.aueb.gr
333	5.849103	fdff:3427:2509:0:93...	fdff:3427:2509::1	DNS	94	Standard query 0x233a AAAA eclass.aueb.gr
335	5.849337	fdff:3427:2509:0:93...	fdff:3427:2509::1	DNS	94	Standard query 0x2d14 HTTPS eclass.aueb.gr
1516	6.493092	fdff:3427:2509:0:93...	fdff:3427:2509::1	DNS	111	Standard query 0x9f37 A content-autofill.googleapis.com
1517	6.493230	fdff:3427:2509:0:93...	fdff:3427:2509::1	DNS	111	Standard query 0xa9f2 AAAA content-autofill.googleapis.cc
1518	6.493354	fdff:3427:2509:0:93...	fdff:3427:2509::1	DNS	111	Standard query 0x1642 HTTPS content-autofill.googleapis.c
1911	6.623913	fdff:3427:2509:0:93...	fdff:3427:2509::1	ICMPv6	216	Destination Unreachable (Port unreachable)
> Frame 7: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interfa > Ethernet II, Src: IntelCor_51:6a:80 (34:e1:2d:51:6a:80), Dst: Technico_5a:cc: > Internet Protocol Version 6, Src: fdff:3427:2509:0:93b:6bc7:26ec:fedf, Dst: f > User Datagram Protocol, Src Port: 50176, Dst Port: 53 > Domain Name System (query)						
				0000	a4 91 b1 5a cc a0 34 e1 2d 51 6a 80 86 dd 60 00	
				0010	00 00 00 22 11 40 fd fd 34 27 25 09 00 00 09 3b	
				0020	6b c7 26 ec fe df fd fd 34 27 25 09 00 00 00 00	
				0030	00 00 00 00 00 01 c4 00 00 35 00 22 49 5f cd ac	
				0040	01 00 00 01 00 00 00 00 00 00 04 77 70 61 64 03	
				0050	6c 61 6e 00 00 01 00 01	
User Datagram Protocol: Protocol						
Packets: 11205 · Displayed: 87 (0.8%)						

4.

Γνωρίζουμε ότι η τριπλή χειραψία TCP πραγματοποιείται ακριβώς πριν την αποστολή του πρώτου HTTP GET αιτήματος προς τον διακομιστή. Εφαρμόζοντας το φίλτρο “tcp” μπορούμε να εντοπίσουμε τα τμήματα αυτά που προηγούνται του συγκεκριμένου HTTP αιτήματος και εγκαθιδρύουν τη σύνδεση με τον υπολογιστή μας. Η διαδικασία του TCP 3-way handshake φαίνεται παρακάτω.

3330	23.591456	192.168.1.165	199.231.164.68	TCP	66	60657 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
3331	23.597883	192.168.1.165	199.231.164.68	TCP	66	60658 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
3332	23.792051	199.231.164.68	192.168.1.165	TCP	66	80 → 60657 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1452 SACK_PERM W
3333	23.792368	192.168.1.165	199.231.164.68	TCP	54	60657 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0

Για την εγκαθίδρυση της σύνδεσης:

1. Ο υπολογιστής μας (client) στέλνει αρχικά ένα τμήμα TCP στην (γνωστή) θύρα 80 του web server που γνωρίζει ότι ακούει, με ενεργοποιημένο SYN flag και έναν αρχικό αριθμό ακολουθίας x (εδώ Seq = 0), το οποίο αποτελεί την αίτηση σύνδεσης.

3331	23.597883	192.168.1.165	199.231.164.68	TCP	66	60658 → 80	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM																			
Internet Protocol Version 4, Src: 192.168.1.165, Dst: 199.231.164.68									0000	a4	91	b1	5a	cc	a0	34	e1	2d	51	6a	00	00	45	00	...	Z...	
Transmission Control Protocol, Src Port: 60658, Dst Port: 80, Seq: 0, Len: 0									0010	00	34	39	9f	40	00	80	06	00	00	c0	a8	01	a5	c7	e7	...	49@
Source Port: 60658									0020	a4	44	ec	f2	00	50	b5	43	38	aa	00	00	00	00	80	02	D...	
Destination Port: 80									0030	fa	f0	2e	a0	00	00	02	04	05	b4	01	03	03	08	01	01	...	
[Stream index: 29]									0040	04	02													..			
[Conversation completeness: Complete, WITH_DATA (31)]																											
[TCP Segment Len: 0]																											
Sequence Number: 0 (relative sequence number)																											
Sequence Number (raw): 3041081514																											
[Next Sequence Number: 1 (relative sequence number)]																											
Acknowledgment Number: 0																											
Acknowledgment number (raw): 0																											
1000 = Header Length: 32 bytes (8)																											
Flags: 0x002 (SYN)																											
000. = Reserved: Not set																											
...0 = Accurate ECN: Not set																											
.... 0... = Congestion Window Reduced: Not set																											
.... .0.. = ECN-Echo: Not set																											
.... ..0. = Urgent: Not set																											
.... ...0 = Acknowledgment: Not set																											
..... 0... = Push: Not set																											
..... .0.. = Reset: Not set																											
>1. = Syn: Set																											
..... ...0 = Fin: Not set																											
[TCP Flags:S.]																											
Window: 64240																											
[Calculated window size: 64240]																											
Checksum: 0x2ea0 [unverified]																											
[Checksum Status: Unverified]																											
Urgent Pointer: 0																											
> Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window sc																											
> [Timestamps]																											

2. Ο web server επιβεβαιώνει το αίτημα του πελάτη με αριθμό 0, προσauζάνοντας τον αριθμό ακολουθίας κατά 1 (Ack=1). Το τμήμα έχει ενεργοποιημένα τα SYN και ACK flags, ενώ ανακοινώνει επίσης και τον δικό του αρχικό αριθμό ακολουθίας γ (Seq = 0)

3332	23.792051	199.231.164.68	192.168.1.165	TCP	66	80 → 60657	[SYN, ACK]	Seq=0 Ack=1 Win=64240 Len=0 MSS=1452 SACK_PERM WS=128		
>	Ethernet II, Src: Technico_5a:cc:a0 (a4:91:b1:5a:cc:a0), Dst: IntelCor_51:6							0000	34 e1 2d 51 6a 80 a4 91 b1 5a cc a0 08 00 45 00	4-Qj...Z...E
>	Internet Protocol Version 4, Src: 199.231.164.68, Dst: 192.168.1.165							0010	00 34 00 00 40 00 2e 06 1e 4b c7 e7 a4 44 c0 a8	4...@...K...D
▼	Transmission Control Protocol, Src Port: 80, Dst Port: 60657, Seq: 0, Ack:							0020	01 a5 00 50 ec f1 17 db a3 69 50 b1 01 2b 80 12	...P...iP...+
	Source Port: 80							0030	fa f0 4b 3c 00 00 02 04 05 ac 01 01 04 02 01 03	...K<...
	Destination Port: 60657							0040	03 07	..
	[Stream index: 28]									
	[Conversation completeness: Complete, WITH_DATA (31)]									
	[TCP Segment Len: 0]									
	Sequence Number: 0 (relative sequence number)									
	Sequence Number (raw): 400270185									
	[Next Sequence Number: 1 (relative sequence number)]									
	Acknowledgment Number: 1 (relative ack number)									
	Acknowledgment number (raw): 1353777451									
	1000 = Header Length: 32 bytes (8)									
▼	Flags: 0x012 (SYN, ACK)									
	000. = Reserved: Not set									
	...0 = Accurate ECN: Not set									
 0... = Congestion Window Reduced: Not set									
0.. = ECN-Echo: Not set									
0. = Urgent: Not set									
1 = Acknowledgment: Set									
0 = Push: Not set									
 0... = Reset: Not set									
>1. = Syn: Set									
0 = Fin: Not set									
	[TCP Flags:A..S.]									
	Window: 64240									
	[Calculated window size: 64240]									
	Checksum: 0x4b3c [unverified]									
	[Checksum Status: Unverified]									
	Urgent Pointer: 0									
>	Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operat									
>	[Timestamps]									
>	[SEQ/ACK analysis]									

3. Τέλος, ο υπολογιστής μας επιβεβαιώνει με τη σειρά του τον αριθμό ακολουθίας του προηγούμενου τμήματος στέλνοντας ένα τμήμα ACK για αυτόν (Ack = 1) και αυξάνει τον δικό του αριθμό ακολουθίας κατά ένα (Seq = 1). Σε αυτό το στάδιο η σύνδεση έχει εγκαθιδρυθεί και τα δύο άκρα μπορούν να ξεκινήσουν την ανταλλαγή δεδομένων.

3333	23.792368	192.168.1.165	199.231.164.68	TCP	54	60657 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0
>	Frame 3333:	54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface			0000	a4 91 b1 5a cc a0 34 e1 2d 51 6a 80 0
>	Ethernet II, Src:	IntelCor_51:6a:80 (34:e1:2d:51:6a:80), Dst: Technico_5a:cc:a0:34:e1:2d:51:6a:80			0010	00 28 39 a0 40 00 80 06 00 00 c0 a8 0
>	Internet Protocol Version 4, Src:	192.168.1.165, Dst: 199.231.164.68			0020	a4 44 ec f1 00 50 50 b1 01 2b 17 db a
▼	Transmission Control Protocol, Src Port:	60657, Dst Port: 80, Seq: 1, Ack: 1, Len: 0			0030	02 04 2e 94 00 00
	Source Port:	60657				
	Destination Port:	80				
	[Stream index:	28]				
	[Conversation completeness:	Complete, WITH_DATA (31)]				
	[TCP Segment Len:	0]				
	Sequence Number:	1 (relative sequence number)				
	Sequence Number (raw):	1353777451				
	[Next Sequence Number:	1 (relative sequence number)]				
	Acknowledgment Number:	1 (relative ack number)				
	Acknowledgment number (raw):	400270186				
	0101 = Header Length:	20 bytes (5)				
▼	Flags:	0x010 (ACK)				
	000. = Reserved:	Not set				
	...0 = Accurate ECN:	Not set				
 0... = Congestion Window Reduced:	Not set				
0.. = ECN-Echo:	Not set				
0. = Urgent:	Not set				
1 = Acknowledgment:	Set				
 0... = Push:	Not set				
0.. = Reset:	Not set				
0. = Syn:	Not set				
0 = Fin:	Not set				
	[TCP Flags:A....]				
	Window:	516				
	[Calculated window size:	132096]				
	[Window size scaling factor:	256]				
	Checksum:	0x2e94 [unverified]				
	[Checksum Status:	Unverified]				
	Urgent Pointer:	0				
>	[Timestamps]					
>	[SEQ/ACK analysis]					

5.

Εφαρμόζοντας το φίλτρο `"tcp.dstport == 443"` παίρνουμε όλα τα τμήματα TCP που έχουν ως θύρα προορισμού την 443. Αυτά είναι στο σύνολό τους 3.226.

tcp.dstport == 443						
No.	Time	Source	Destination	Protocol	Length	Info
3313	22.681444	192.168.1.165	172.217.17.228	TCP	54	60614 → 443 [ACK] Seq=8561 Ack=20090 Win=509 Len=0
3314	22.682267	192.168.1.165	172.217.17.228	TLSv1.2	89	Application Data
3316	22.696056	192.168.1.165	172.217.17.228	TCP	66	[TCP Dup ACK 3313#1] 60614 → 443 [ACK] Seq=8596 Ack=20090 Win=509 Len=0 SL...
3317	22.699211	192.168.1.165	172.217.17.228	TLSv1.2	93	Application Data
3322	22.800798	192.168.1.165	130.117.190.213	TCP	54	60512 → 443 [ACK] Seq=11287 Ack=9340 Win=64000 Len=0
3355	24.546694	192.168.1.165	172.217.17.228	TLSv1.2	161	Application Data
3368	24.833155	192.168.1.165	172.217.17.228	TCP	66	60614 → 443 [ACK] Seq=8742 Ack=20567 Win=508 Len=0 SLE=20528 SRE=20567
3369	24.834723	192.168.1.165	172.217.17.228	TLSv1.2	93	Application Data
3370	24.841876	192.168.1.165	216.58.212.3	TLSv1.2	132	Application Data
3371	24.841947	192.168.1.165	216.58.212.3	TLSv1.2	93	Application Data
3378	24.970933	192.168.1.165	216.58.212.3	TCP	54	60622 → 443 [ACK] Seq=118 Ack=3225 Win=512 Len=0
3379	24.972428	192.168.1.165	216.58.212.3	TLSv1.2	89	Application Data
3383	24.973609	192.168.1.165	216.58.212.3	TCP	54	60622 → 443 [ACK] Seq=153 Ack=6366 Win=512 Len=0
3384	24.973894	192.168.1.165	216.58.212.3	TLSv1.2	93	Application Data
3385	24.984747	192.168.1.165	172.217.17.228	TLSv1.2	333	Application Data
Frame 3322: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface						
Ethernet II, Src: IntelCor_51:6a:80 (34:e1:2d:51:6a:80), Dst: Technico_5a:cc:a0:34:e1:2d:51:6a:80						
Internet Protocol Version 4, Src: 192.168.1.165, Dst: 130.117.190.213						
Transmission Control Protocol, Src Port: 60512, Dst Port: 443, Seq: 11287, Len: 0						
Source Port: 60512						
Destination Port: 443						
[Stream index: 2]						
[Conversation completeness: Incomplete (12)]						
[TCP Segment Len: 0]						
0000 a4 91 b1 5a cc a0 34 e1 2d 51 6a 80 08 00 45 0c ...Z...4...Qj...E						
0010 00 28 99 4d 40 00 80 06 00 00 c0 a8 01 a5 82 75 ...(.H@.....						
0020 be d5 ec 60 01 bb 6c 17 9f da 3d 51 65 67 50 101...=QegP						
0030 fa 00 03 b3 00 00						
ex1.pcapng						
Packets: 11205 · Displayed: 3226 (28.8%)						
Profile: D						

Εφαρμόζοντας το φίλτρο `"tcp.srcport == 443"` βλέπουμε όλα τα τμήματα TCP που είχαν ως θύρα προέλευσης την 443. Συνολικά αυτά είναι 7.567

No.	Time	Source	Destination	Protocol	Length	Info
3332	23.792051	199.231.164.68	192.168.1.165	TCP	66	80 → 60657 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1452 SACK_PERM WS=128
3335	23.814175	199.231.164.68	192.168.1.165	TCP	66	80 → 60658 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1452 SACK_PERM WS=128
3338	24.017387	199.231.164.68	192.168.1.165	TCP	54	80 → 60657 [ACK] Seq=1 Ack=428 Win=64128 Len=0
3339	24.023975	199.231.164.68	192.168.1.165	HTTP	629	HTTP/1.1 301 Moved Permanently (text/html)
3341	24.211928	199.231.164.68	192.168.1.165	TCP	1506	80 → 60657 [ACK] Seq=576 Ack=860 Win=64128 Len=1452 [TCP segment of a reas...
3342	24.234918	199.231.164.68	192.168.1.165	HTTP	1211	HTTP/1.1 200 OK (text/html)
3347	24.469982	199.231.164.68	192.168.1.165	TCP	1506	80 → 60657 [ACK] Seq=3185 Ack=1190 Win=64128 Len=1452 [TCP segment of a re...
3349	24.524436	199.231.164.68	192.168.1.165	HTTP	552	HTTP/1.1 200 OK (text/css)
3350	24.524436	199.231.164.68	192.168.1.165	TCP	54	80 → 60658 [ACK] Seq=1 Ack=313 Win=64128 Len=0
3351	24.524436	199.231.164.68	192.168.1.165	HTTP	715	HTTP/1.1 200 OK (application/javascript)
3352	24.524436	199.231.164.68	192.168.1.165	TCP	66	80 → 60659 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1452 SACK_PERM WS=128
3358	24.726781	199.231.164.68	192.168.1.165	TCP	54	80 → 60659 [ACK] Seq=1 Ack=310 Win=64128 Len=0
3359	24.793218	199.231.164.68	192.168.1.165	HTTP	898	HTTP/1.1 200 OK (application/javascript)
3388	25.010270	199.231.164.68	192.168.1.165	TCP	1506	80 → 60658 [ACK] Seq=662 Ack=693 Win=64128 Len=1452 [TCP segment of a reas...
3393	25.057570	199.231.164.68	192.168.1.165	TCP	1506	80 → 60658 [ACK] Seq=2114 Ack=693 Win=64128 Len=1452 [TCP segment of a reas...

> Frame 3332: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on in

> Ethernet II, Src: Technico_5a:cc:a0 (a4:91:b1:5a:cc:a0), Dst: IntelCor_51:6

> Internet Protocol Version 4, Src: 199.231.164.68, Dst: 192.168.1.165

> Transmission Control Protocol, Src Port: 80, Dst Port: 60657, Seq: 0, Ack:

Source Port: 80

Destination Port: 60657

[Stream index: 28]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 0]

0000 34 e1 2d 51 6a 80 a4 91 b1 5a cc a0 08 00 45 00 4 -Qj...Z....E

0010 00 34 00 00 40 00 2e 06 1e 4b c7 e7 a4 44 c0 a8 4 @...K...D

0020 01 a5 00 50 ec f1 17 db a3 69 50 b1 01 2b 80 12 ...P...iP...+

0030 fa f0 4b 3c 00 00 02 04 05 ac 01 01 04 02 01 03 ..K<... ..

0040 03 07 ..

ex1.pcapng Packets: 11205 · Displayed: 32 (0.3%) Profile: De

7.

Από τα προηγούμενα ερωτήματα παρατηρούμε ότι η IP διεύθυνση του διακομιστή που φιλοξενεί τον ιστότοπο είναι η 199.231.164.68. Επομένως θέτοντας το φίλτρο *“ip.addr == 199.231.164.68 && tcp”*, μπορούμε να εξετάσουμε ποιες θύρες χρησιμοποιήθηκαν από το TCP για την επικοινωνία με τον server (σημειώνεται ότι δεν εφαρμόζεται φίλτρο επί του domain name καθώς κάτι τέτοιο θα μας εμφανίσει μόνο τα HTTP πακέτα κι όχι όλα τα TCP τμήματα που ανταλλάχθηκαν με τον server).

Οι θύρες προέλευσης και προορισμού που χρησιμοποιήθηκαν από το πρωτόκολλο κατά την επικοινωνία είναι οι **80** (η θύρα στην οποία ακούει ο web server), **60657**, **60658** και **60659** (επιλέχθηκαν ως θύρες προέλευσης από τον υπολογιστή μας).

No.	Time	Source	Destination	Protocol	Length	Info
3330	23.591456	192.168.1.165	199.231.164.68	TCP	66	60657 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
3331	23.597883	192.168.1.165	199.231.164.68	TCP	66	60658 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
3332	23.792051	199.231.164.68	192.168.1.165	TCP	66	80 → 60657 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1452 SACK_PERM WS=128
3333	23.792368	192.168.1.165	199.231.164.68	TCP	54	60657 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0
3334	23.793818	192.168.1.165	199.231.164.68	HTTP	481	GET / HTTP/1.1
3335	23.814175	199.231.164.68	192.168.1.165	TCP	66	80 → 60658 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1452 SACK_PERM WS=128
3336	23.814352	192.168.1.165	199.231.164.68	TCP	54	60658 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0
3338	24.017387	199.231.164.68	192.168.1.165	TCP	54	80 → 60657 [ACK] Seq=1 Ack=428 Win=64128 Len=0
3339	24.023975	199.231.164.68	192.168.1.165	HTTP	629	HTTP/1.1 301 Moved Permanently (text/html)
3340	24.028217	192.168.1.165	199.231.164.68	HTTP	486	GET /faqs/ HTTP/1.1
3341	24.211928	199.231.164.68	192.168.1.165	TCP	1506	80 → 60657 [ACK] Seq=576 Ack=860 Win=64128 Len=1452 [TCP segment of a reas...
3342	24.234918	199.231.164.68	192.168.1.165	HTTP	1211	HTTP/1.1 200 OK (text/html)
3343	24.235029	192.168.1.165	199.231.164.68	TCP	54	60657 → 80 [ACK] Seq=860 Ack=3185 Win=132096 Len=0
3344	24.275348	192.168.1.165	199.231.164.68	HTTP	384	GET /style/faqs.css HTTP/1.1
3345	24.276667	192.168.1.165	199.231.164.68	TCP	66	60659 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

8.

Χρησιμοποιούμε το φίλτρο *“tls”* για να εμφανιστούν μόνο τα αντίστοιχα πακέτα.

Συνολικά αυτά είναι στο πλήθος 4.983, όπως φαίνεται στην παρακάτω εικόνα.

No.	Time	Source	Destination	Protocol	Length	Info
3633	28.127090	130.117.190.213	192.168.1.165	TLSv1.2	156	Application Data
3635	28.127090	130.117.190.213	192.168.1.165	TLSv1.2	109	Application Data
3637	28.127323	192.168.1.165	130.117.190.213	TLSv1.2	131	Application Data
3638	28.127401	192.168.1.165	130.117.190.213	TLSv1.2	300	Application Data
3639	28.144973	172.217.17.228	192.168.1.165	TLSv1.2	385	Application Data
3640	28.148931	172.217.17.228	192.168.1.165	TLSv1.2	319	Application Data
3641	28.148931	172.217.17.228	192.168.1.165	TLSv1.2	86	Application Data
3642	28.148931	172.217.17.228	192.168.1.165	TLSv1.2	85	Application Data
3643	28.148931	172.217.17.228	192.168.1.165	TLSv1.2	93	Application Data
3645	28.149566	192.168.1.165	172.217.17.228	TLSv1.2	89	Application Data
3646	28.160805	192.168.1.165	172.217.17.228	TLSv1.2	93	Application Data
3647	28.189477	130.117.190.213	192.168.1.165	TLSv1.2	267	Application Data, Application Data
3649	28.192392	130.117.190.213	192.168.1.165	TLSv1.2	109	Application Data
3650	28.192392	130.117.190.213	192.168.1.165	TLSv1.2	165	Application Data
3651	28.192392	130.117.190.213	192.168.1.165	TLSv1.2	156	Application Data

> Frame 3651: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits) on 0

> Ethernet II, Src: Technico_5a:cc:a0 (a4:91:b1:5a:cc:a0), Dst: IntelCor_51:6

> Internet Protocol Version 4, Src: 130.117.190.213, Dst: 192.168.1.165

▼ Transmission Control Protocol, Src Port: 443, Dst Port: 60512, Seq: 10834,

Source Port: 443

Destination Port: 60512

[Stream index: 2]

[Conversation completeness: Incomplete (12)]

[TCP Segment Len: 102]

0000 34 e1 2d 51 6a 80 a4 91 b1 5a cc a0 08 00 45 00

0010 00 8e c4 cb 40 00 37 06 7b 06 82 75 be d5 c0 a8

0020 01 a5 01 bb ec 60 3d 51 6b 3d 6c 17 a6 bd 50 18

0030 f9 cd 17 24 00 00 17 03 03 00 61 03 8a 26 d2 33

0040 2d cc d1 f0 78 1c a5 96 79 d4 27 a0 94 09 5f 1f

0050 a4 a1 d9 e0 aa 47 0a e1 fe 56 46 b6 50 ea a1 67

0060 f3 e9 2d 87 0f a7 06 66 39 35 3a be 74 0c d2 a7

0070 82 86 21 2d e1 ab ee 4e 91 32 a5 8a 60 b4 48 6c

0080 4c 3c f1 6b ef 50 5b ec 7c c7 bb 49 d3 bb c4 c0

0090 0a 1f d3 19 d5 be ea 62 bd 24 03 3f

Transport Layer Security: Protocol

Packets: 11205 · Displayed: 4983 (44.5%)

Το TLS μεταφέρει κρυπτογραφημένα δεδομένα για το πρωτόκολλο HTTP.

▼ Transport Layer Security
▼ TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 527
Encrypted Application Data: 0efaca5244f2d3990cd1192bcc6f1c72973c32bb827d85da311f9a6090605c
[Application Data Protocol: Hypertext Transfer Protocol]

9.

Χρησιμοποιώντας το φίλτρο "http" παίρνουμε ότι ανταλλάχθηκαν συνολικά 18 πακέτα HTTP

No.	Time	Source	Destination	Protocol	Length	Info
3344	24.275348	192.168.1.165	199.231.164.68	HTTP	384	GET /style/faqs.css HTTP/1.1
3346	24.276785	192.168.1.165	199.231.164.68	HTTP	366	GET /style/rs.js HTTP/1.1
3349	24.524436	199.231.164.68	192.168.1.165	HTTP	552	HTTP/1.1 200 OK (text/css)
3351	24.524436	199.231.164.68	192.168.1.165	HTTP	715	HTTP/1.1 200 OK (application/javascript)
3354	24.526264	192.168.1.165	199.231.164.68	HTTP	363	GET /utils.js HTTP/1.1
3359	24.793218	199.231.164.68	192.168.1.165	HTTP	898	HTTP/1.1 200 OK (application/javascript)
3361	24.806944	192.168.1.165	199.231.164.68	HTTP	435	GET /images/faqs.org.png HTTP/1.1
3362	24.806961	192.168.1.165	199.231.164.68	HTTP	434	GET /images/library.jpg HTTP/1.1
3363	24.808890	192.168.1.165	199.231.164.68	HTTP	448	GET /style/i/faqs-header.png HTTP/1.1
3395	25.057570	199.231.164.68	192.168.1.165	HTTP	1109	HTTP/1.1 200 OK (JPEG JFIF image)
3396	25.057570	199.231.164.68	192.168.1.165	HTTP	717	HTTP/1.1 200 OK (PNG)
3401	25.057570	199.231.164.68	192.168.1.165	HTTP	614	HTTP/1.1 200 OK (PNG)
3412	25.065981	192.168.1.165	199.231.164.68	HTTP	427	GET /favicon.ico HTTP/1.1
3437	25.299621	199.231.164.68	192.168.1.165	HTTP	1073	HTTP/1.1 200 OK (image/vnd.microsoft.icon)

10.

Μπορούμε να προβάλλουμε μόνο τα HTTP GET requests που γίνονται προς σελίδες οι οποίες δεν υποστηρίζουν κρυπτογράφηση με TLS, καθώς σε διαφορετική περίπτωση το Wireshark δεν μπορεί να αποκρυπτογραφήσει τα μηνύματα και άρα να εξετάσει το περιεχόμενό τους.

Παρατηρούμε ότι ο ιστότοπος www.faqs.org δεν υποστηρίζει κρυπτογράφηση των HTTP μηνυμάτων, επομένως μπορούμε να τα φιλτράρουμε με την έκφραση “*http.request.method = “GET”*” και να προβάλλουμε κανονικά τα περιεχόμενα τους.

Τα αιτήματα αυτά στέλνονται στην IP διεύθυνση 199.231.164.68

http.request.method == "GET"						
No.	Time	Source	Destination	Protocol	Length	Info
3334	23.793818	192.168.1.165	199.231.164.68	HTTP	481	GET / HTTP/1.1
3340	24.028217	192.168.1.165	199.231.164.68	HTTP	486	GET /faqs/ HTTP/1.1
3344	24.275348	192.168.1.165	199.231.164.68	HTTP	384	GET /style/faqs.css HTTP/1.1
3346	24.276785	192.168.1.165	199.231.164.68	HTTP	366	GET /style/rs.js HTTP/1.1
3354	24.526264	192.168.1.165	199.231.164.68	HTTP	363	GET /utils.js HTTP/1.1
3361	24.806944	192.168.1.165	199.231.164.68	HTTP	435	GET /images/faqs.org.png HTTP/1.1
3362	24.806961	192.168.1.165	199.231.164.68	HTTP	434	GET /images/library.jpg HTTP/1.1
3363	24.808890	192.168.1.165	199.231.164.68	HTTP	448	GET /style/i/faqs-header.png HTTP/1.1
3412	25.065981	192.168.1.165	199.231.164.68	HTTP	427	GET /favicon.ico HTTP/1.1

Window: 516
[Calculated window size: 132096]
[Window size scaling factor: 256]
Checksum: 0x303f [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
TCP payload (427 bytes)
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
Request Method: GET
Request URI: /
Request Version: HTTP/1.1

0000 a4 91 b1 5a cc a0 34 e1 2d 51 6a 80 08 00 45 00 ...Z...4...Qj...E...
0010 01 d3 39 a1 40 00 00 06 00 00 c0 a8 01 a5 c7 e7 ...9...@...=...D...
0020 a4 44 ec f1 00 50 50 b1 01 2b 17 db a3 6a 50 18 ...D...PP...+...jP...
0030 02 04 30 3f 00 00 47 45 54 20 2f 20 48 54 50 50 ...0?...GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e .../1.1...Ho st: www...
0050 66 61 71 73 2e 6f 72 67 0d 0a 43 6f 6e 6e 65 63 ...faqs.org...Connec...
0060 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 ...tion: ke ep-alive...
0070 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 ...re-Upgrade-Insecu...
0080 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a ...re-Request: 1...
0090 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 ...User-Agent: Mozi...
00a0 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 ...lla/5.0 (Windows...
00b0 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b ...NT 10.0 ; Win64...
00c0 20 78 36 34 29 20 41 70 70 6c 65 57 65 62 4b 69 ...x64) AppleWebKit...
00d0 74 2f 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c ...t/537.36 (KHTML...
00e0 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 ...like Gecko) Chr...
00f0 6f 6d 65 2f 31 30 38 2e 30 2e 30 2e 30 20 53 61 ...ome/108.0.0.0 Sa...
0100 66 61 72 69 2f 35 33 37 2e 33 36 0d 0a 41 63 63 ...fari/537.36...Acc

11.

Εξετάζοντας μια οποιαδήποτε απάντηση του server προς το μηχάνημά μας, διαπιστώνουμε ότι το μηχάνημα που φιλοξενεί τον ιστότοπο τρέχει τον Apache HTTP server.

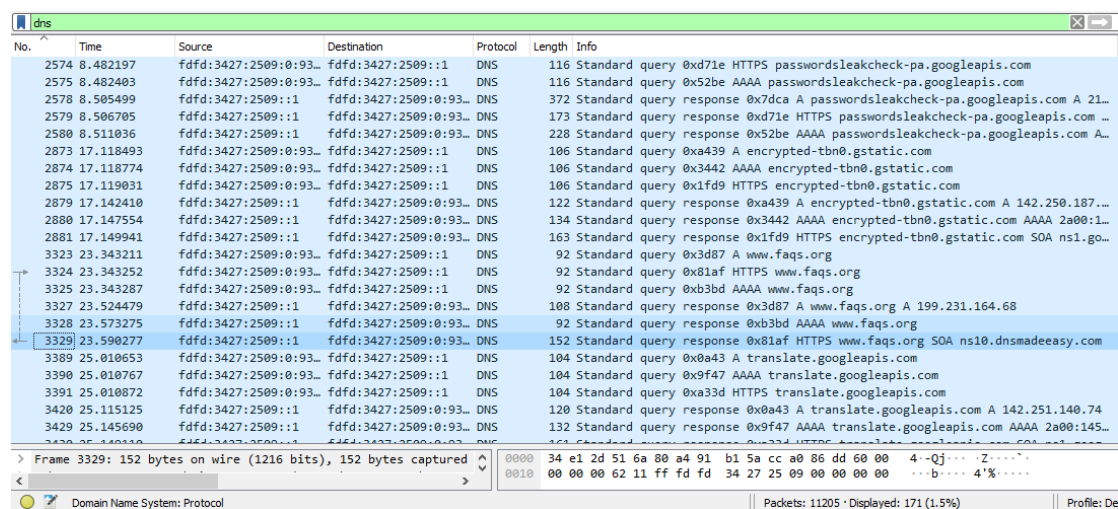
Η σύνδεση είναι persistent, όπως φαίνεται από την τιμή του πεδίου Connection που είναι Keep-Alive.

3342	24.234918	199.231.164.68	192.168.1.165	HTTP	1211	HTTP/1.1 200 OK (text/html)
TCP segment data (1157 bytes)						
[2 Reassembled TCP Segments (2609 bytes): #3341(1452), #3342(1157)]						
Hypertext Transfer Protocol						
HTTP/1.1 200 OK\r\n						
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]						
Response Version: HTTP/1.1						
Status Code: 200						
[Status Code Description: OK]						
Response Phrase: OK						
Date: Sun, 25 Dec 2022 23:05:59 GMT\r\n						
Server: Apache\r\n						
X-Frame-Options: SAMEORIGIN\r\n						
X-XSS-Protection: 1; mode=block\r\n						
X-Content-Type-Options: nosniff\r\n						
Vary: Accept-Encoding\r\n						
Content-Encoding: gzip\r\n						
Content-Length: 2277\r\n						
Keep-Alive: timeout=10, max=99\r\n						
Connection: Keep-Alive\r\n						
Content-Type: text/html; charset=UTF-8\r\n						
\r\n						
[HTTP response 2/4]						

0000 34 e1 2d 51 6a 80 a4 91 b1 5a cc a0 08 00 45 00 4...Qj...Z...E...
0010 04 ad dc 1f 40 00 2e 06 3d b2 c7 e7 a4 44 c0 a8 ...@...=...D...
0020 01 a5 00 50 ec f1 17 db ab 55 50 b1 04 86 50 18 ...P...UP...P...
0030 01 f5 58 aa 00 00 60 80 2e e6 e4 42 7f 65 09 f9 ...X...B...e...
0040 a3 62 1a 53 59 93 7d 88 c1 01 29 25 2c 8b 54 13 ...bSY...)%...T...
0050 5e 10 3b 56 a2 2a d4 10 d0 0a 41 68 93 07 b5 08 ...;V...Ah...
0060 ca c3 96 67 9f 0f 4c b0 d8 d8 60 7a 12 93 c1 63 ...g...L...z...c...
0070 02 ec 89 66 0a 9b db 5c 56 8a 94 95 02 19 4c b7 ...f...V...L...
0080 c8 6b d0 a1 32 99 54 96 39 ae bc d2 1f 20 2e 44 ...k...2...9...D...
0090 70 af 08 55 0c ba 89 96 04 3c c9 05 3a 1c 24 63 ...p...U...<...\$c...
00a0 45 7f 56 0b ed c6 9b cc c3 82 cd 74 aa 64 55 42 ...E...t...t...dUB...
00b0 c1 00 b6 1f ea a5 2d 1a 84 bb 2a bd b5 a4 03 03 ...f...E...a...
00c0 e8 21 2c 95 d0 ca ec d6 45 1e 97 1e b2 ce 61 13 ...f...ux...r...
00d0 83 1c 76 3d c7 01 c5 93 bf c7 75 78 0f 00 72 c5 ...Q...p...|...>...
00e0 a1 51 1a 70 7b 5d fc 9b ef 7c 21 5b a9 3e 5d 5f ...}...G...q[8...;r...X...
00f0 7d 60 47 b8 ae 71 5b 38 bc ba c9 a0 3b 72 8e 58 ...N...M...t...
0100 d7 83 4e 34 0c f4 b1 c1 a6 ac 4d ab cc ca 60 74 ...Q...M...j...m...
0110 51 c3 b6 f6 92 92 e2 5c 80 dd e4 de 7d 6d c5 9c ...Q...M...j...l...
0120 b1 09 1c 16 18 a2 fe e9 3e c1 90 86 62 5b 5b 60 ...B...H...I...r...z...
0130 39 57 d8 dd 6d 27 f0 df 04 cb fb 84 6a b6 95 6c ...H...E...O...w...
0140 42 8b af b6 d5 3e 90 d7 f0 49 ee 95 9c 72 e1 7a ...C...s...h...s...
0150 08 d9 5f c7 83 48 63 e2 84 45 95 4f 98 f2 e5 77 ...d...s...L...
0160 e4 a1 c4 43 91 f4 60 73 12 68 16 87 c0 1e 73 0f ...ye...\$...8...M...I...
0170 64 3e 5c 5f 92 1b b7 aa f3 73 ab 9e 1a 0e 2d 4c ...
0180 79 65 c7 b2 24 ef c0 f9 38 d3 bd c6 4d 80 49 fe ...

12.

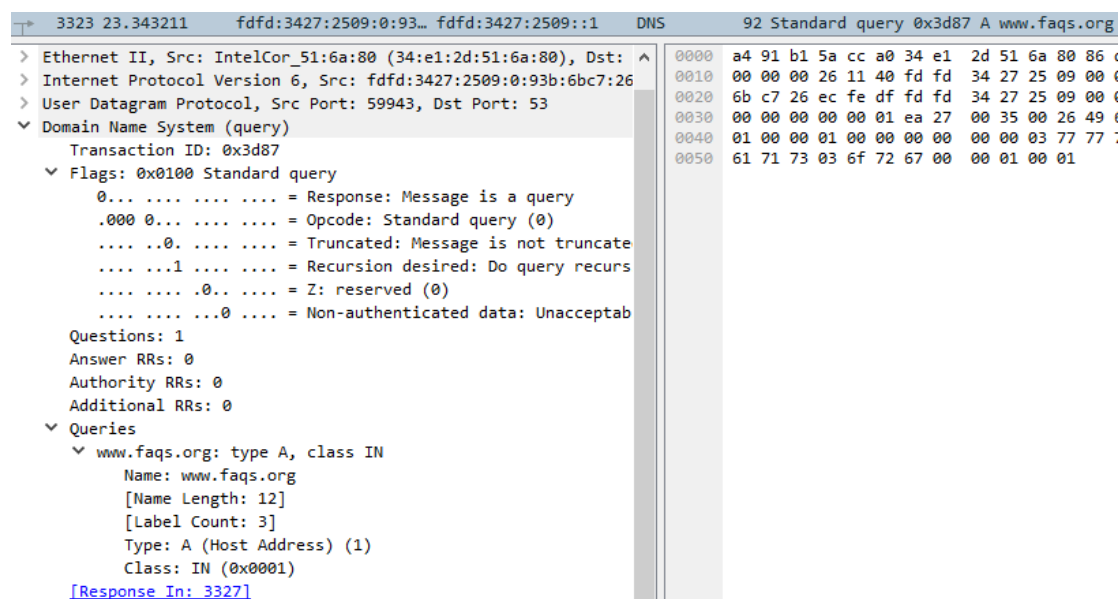
Εφαρμόζοντας το φίλτρο “dns”, εμφανίζονται όλα τα πακέτα DNS που καταγράφηκαν, τα οποία είναι συνολικά 171.



No.	Time	Source	Destination	Protocol	Length	Info
2574	8.482197	fdfd:3427:2509:0:93...	fdfd:3427:2509::1	DNS	116	Standard query 0xd71e HTTPS passwordsleakcheck-pa.googleapis.com
2575	8.482463	fdfd:3427:2509:0:93...	fdfd:3427:2509::1	DNS	116	Standard query 0x52be AAAA passwordsleakcheck-pa.googleapis.com
2578	8.505499	fdfd:3427:2509::1	fdfd:3427:2509:0:93...	DNS	372	Standard query response 0x7dca A passwordsleakcheck-pa.googleapis.com A 21...
2579	8.506705	fdfd:3427:2509::1	fdfd:3427:2509:0:93...	DNS	173	Standard query response 0xd71e HTTPS passwordsleakcheck-pa.googleapis.com
2580	8.511036	fdfd:3427:2509::1	fdfd:3427:2509:0:93...	DNS	228	Standard query response 0x52be AAAA passwordsleakcheck-pa.googleapis.com A...
2873	17.118493	fdfd:3427:2509:0:93...	fdfd:3427:2509::1	DNS	106	Standard query 0xa439 A encrypted-tbn0.gstatic.com
2874	17.118774	fdfd:3427:2509:0:93...	fdfd:3427:2509::1	DNS	106	Standard query 0x3442 AAAA encrypted-tbn0.gstatic.com
2875	17.119031	fdfd:3427:2509:0:93...	fdfd:3427:2509::1	DNS	106	Standard query 0x1fd9 HTTPS encrypted-tbn0.gstatic.com
2879	17.142410	fdfd:3427:2509::1	fdfd:3427:2509:0:93...	DNS	122	Standard query response 0xa439 A encrypted-tbn0.gstatic.com A 142.250.187...
2880	17.147554	fdfd:3427:2509::1	fdfd:3427:2509:0:93...	DNS	134	Standard query response 0x3442 AAAA encrypted-tbn0.gstatic.com AAAA 2a00:1...
2881	17.149941	fdfd:3427:2509::1	fdfd:3427:2509:0:93...	DNS	163	Standard query response 0x1fd9 HTTPS encrypted-tbn0.gstatic.com SOA ns1.go...
3323	23.343211	fdfd:3427:2509:0:93...	fdfd:3427:2509::1	DNS	92	Standard query 0x3d87 A www.faqs.org
3324	23.343252	fdfd:3427:2509:0:93...	fdfd:3427:2509::1	DNS	92	Standard query 0x81af HTTPS www.faqs.org
3325	23.343287	fdfd:3427:2509:0:93...	fdfd:3427:2509::1	DNS	92	Standard query 0xb3bd AAAA www.faqs.org
3327	23.524479	fdfd:3427:2509::1	fdfd:3427:2509:0:93...	DNS	108	Standard query response 0x3d87 A www.faqs.org A 199.231.164.68
3328	23.573275	fdfd:3427:2509::1	fdfd:3427:2509:0:93...	DNS	92	Standard query response 0xb3bd AAAA www.faqs.org
3329	23.598277	fdfd:3427:2509::1	fdfd:3427:2509:0:93...	DNS	152	Standard query response 0x81af HTTPS www.faqs.org SOA ns10.dnsmadeeasy.com
3389	25.010653	fdfd:3427:2509:0:93...	fdfd:3427:2509::1	DNS	104	Standard query 0x0a43 A translate.googleapis.com
3390	25.010767	fdfd:3427:2509:0:93...	fdfd:3427:2509::1	DNS	104	Standard query 0x9f47 AAAA translate.googleapis.com
3391	25.010872	fdfd:3427:2509:0:93...	fdfd:3427:2509::1	DNS	104	Standard query 0xa33d HTTPS translate.googleapis.com
3420	25.115125	fdfd:3427:2509::1	fdfd:3427:2509:0:93...	DNS	120	Standard query response 0x0a43 A translate.googleapis.com A 142.251.140.74
3429	25.145690	fdfd:3427:2509::1	fdfd:3427:2509:0:93...	DNS	132	Standard query response 0x9f47 AAAA translate.googleapis.com AAAA 2a00:145...

13.

Όπως φαίνεται στην προηγούμενη εικόνα, αλλά και από την εξέταση του εκάστοτε πακέτου, μπορούμε να διακρίνουμε τα DNS queries από τα responses μέσω των αντίστοιχων πεδίων των πακέτων. Για παράδειγμα σε ένα αίτημα παρατηρούμε ότι το Response flag είναι απενεργοποιημένο, υποδεικνύοντας ότι πρόκειται για query, ενώ επιπλέον το πακέτο περιέχει μια ή περισσότερες ερωτήσεις, αλλά καμία απάντηση.



No.	Time	Source	Destination	Protocol	Length	Info
3323	23.343211	fdfd:3427:2509:0:93...	fdfd:3427:2509::1	DNS	92	Standard query 0x3d87 A www.faqs.org

Details	Hex
Ethernet II, Src: IntelCor_51:6a:80 (34:e1:2d:51:6a:80), Dst: 00:00:00:00:00:00	34 e1 2d 51 6a 80 a4 91 b1 5a cc a0 86 dd 60 00
Internet Protocol Version 6, Src: fdfd:3427:2509:0:93b:6bc7:26, Dst: fdfd:3427:2509:0:93b:6bc7:26	00 00 00 26 11 40 fd fd 34 27 25 09 00 00 00 00
User Datagram Protocol, Src Port: 59943, Dst Port: 53	6b c7 26 ec fe df fd fd 34 27 25 09 00 00 00 00
Domain Name System (query)	00 00 00 00 00 00 01 ea 27 00 35 00 26 49 00 00
Transaction ID: 0x3d87	00 00 01 00 00 00 00 00 00 00 03 77 77 00 00 00
Flags: 0x0100 Standard query	61 71 73 03 6f 72 67 00 00 01 00 01
0... .. = Response: Message is a query	
.000 0... .. = Opcode: Standard query (0)	
.... .0. = Truncated: Message is not truncate	
.... ..1 = Recursion desired: Do query recurs	
....0... = Z: reserved (0)	
....0... = Non-authenticated data: Unacceptab	
Questions: 1	
Answer RRs: 0	
Authority RRs: 0	
Additional RRs: 0	
Queries	
www.faqs.org: type A, class IN	
Name: www.faqs.org	
[Name Length: 12]	
[Label Count: 3]	
Type: A (Host Address) (1)	
Class: IN (0x0001)	

Αντίθετα σε μια DNS απάντηση προς ένα αίτημα, το Response flag είναι ενεργοποιημένο και το πακέτο περιέχει τις απαντήσεις προς τα ερωτήματα του αιτήματος.

```

3327 23.524479 fdfd:3427:2509::1 fdfd:3427:2509:0:93... DNS 108 Standard query response 0x3d87 A www.faqs.org A 199.231.164.68
> User Datagram Protocol, Src Port: 53, Dst Port: 59943
  Domain Name System (response)
    Transaction ID: 0x3d87
    Flags: 0x8180 Standard query response, No error
      1... .. = Response: Message is a response
      .000 0... .. = Opcode: Standard query (0)
      .... 0... .. = Authoritative: Server is not an au
      .... 0... .. = Truncated: Message is not truncate
      .... 1... .. = Recursion desired: Do query recurs
      .... 1... .. = Recursion available: Server can do
      .... 0... .. = Z: reserved (0)
      .... 0... .. = Answer authenticated: Answer/autho
      .... 0... .. = Non-authenticated data: Unacceptab
      .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
    Queries
      > www.faqs.org: type A, class IN
    Answers
      > www.faqs.org: type A, class IN, addr 199.231.164.68
      [Request In: 3323]
      [Time: 0.181268000 seconds]

```

Η απάντηση συνδέεται με το αίτημα μέσω του Transaction ID το οποίο για ένα response είναι το ίδιο με του query στο οποίο απευθύνεται.

14.

Το www.faqs.org δεν είναι alias καθώς όπως παρατηρούμε στην προηγούμενη εικόνα, η απάντησή στο DNS αίτημα που έστειλε το μηχανήμα μας επιστρέφει απευθείας μια εγγραφή τύπου A όπως ζητήθηκε, δηλ. την διεύθυνση του μηχανήματος που φιλοξενεί τον ιστότοπο, και όχι κάποια εγγραφή τύπου CNAME, η οποία θα υποδείκνυε ότι το όνομα αυτό αποτελεί ψευδώνυμο για κάποιο άλλο domain. Η διεύθυνση που αντιστοιχεί στον server είναι η 199.231.164.68

Αν ήταν alias θα απαιτούνταν επιπρόσθετα επαναληπτικά ή αναδρομικά ερωτήματα για το CNAME που επιστράφηκε προκειμένου ο DNS server να μας επιστρέψει τελικά τη διεύθυνση του server, όπως φαίνεται ενδεικτικά στην παρακάτω εικόνα.

```

348 5.874477 fdfd:3427:2509::1 fdfd:3427:2509:0:93b:6bc7:26ec:fedf DNS 147 Standard query response 0x2842
> Internet Protocol Version 6, Src: fdfd:3427:2509::1, Dst: fdfd:3427:2509:0:93b:6bc7:26ec:fedf
> User Datagram Protocol, Src Port: 53, Dst Port: 54728
  Domain Name System (response)
    Transaction ID: 0x2842
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
    Queries
      > eclass.aueb.gr: type A, class IN
    Answers
      > eclass.aueb.gr: type CNAME, class IN, cname openeclass-web.servers.aueb.gr
      > openeclass-web.servers.aueb.gr: type A, class IN, addr 195.251.255.227
      [Request In: 332]
      [Time: 0.025482000 seconds]

```

15.

Οι απαντήσεις DNS περιέχουν το flag “authoritative” το οποίο υποδεικνύει εάν ο name server που μας απαντάει είναι υπεύθυνος για το συγκεκριμένη ζώνη στην

οποία ανήκει το domain ή όχι. Εξετάζοντας το συγκεκριμένο flag της απάντησης που λάβαμε για το domain αυτό, παρατηρούμε ότι είναι απενεργοποιημένο, το οποίο σημαίνει ότι ο name server δεν είναι authoritative για αυτό.

```
▼ Domain Name System (response)
  Transaction ID: 0x3d87
  ▼ Flags: 0x8180 Standard query response, No error
    1... .. = Response: Message is a response
    .000 0... .. = Opcode: Standard query (0)
    .... .0.. .. = Authoritative: Server is not an authority for domain
    .... ..0. .... = Truncated: Message is not truncated
    .... ..1 .... = Recursion desired: Do query recursively
    .... ..1... .. = Recursion available: Server can do recursive queries
    .... ..0.. .... = Z: reserved (0)
    .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the
    .... ..0 .... = Non-authenticated data: Unacceptable
    .... ..0000 = Reply code: No error (0)

  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    > www.faqs.org: type A, class IN
  ▼ Answers
    ▼ www.faqs.org: type A, class IN, addr 199.231.164.68
      Name: www.faqs.org
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 17882 (4 hours, 58 minutes, 2 seconds)
      Data length: 4
      Address: 199.231.164.68
      [Request In: 3323]
      [Time: 0.181268000 seconds]
```

Άσκηση 2)

1.

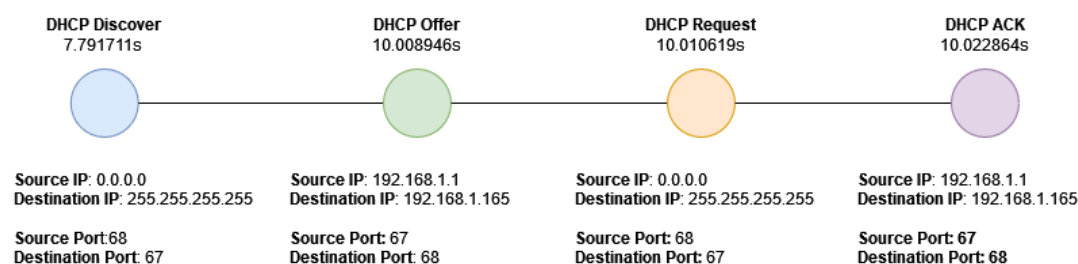
Όπως φαίνεται στην εικόνα, τα DHCP μηνύματα στέλνονται πάνω από UDP.

```
▼
Protocol
▼ Frame
  ▼ Ethernet
    ▼ Internet Protocol Version 4
      ▼ User Datagram Protocol
        Dynamic Host Configuration Protocol
```

2.

dhcp						
No.	Time	Source	Destination	Protocol	Length	Info
146	7.791711s	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x136b9e8
189	10.008946	192.168.1.1	192.168.1.165	DHCP	342	DHCP Offer - Transaction ID 0x136b9e8
190	10.010619	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x136b9e8
191	10.022864	192.168.1.1	192.168.1.165	DHCP	363	DHCP ACK - Transaction ID 0x136b9e8

Κατασκευάζουμε το χρονοδιάγραμμα όπου φαίνονται τα διαδοχικά DHCP μηνύματα που ανταλλάσσονται βάσει της καταγεγραμμένης κίνησης που φαίνεται στην ανωτέρω εικόνα.



3.

Η MAC διεύθυνση του υπολογιστή είναι η 34-E1-2D-51-6A-80

```
Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x0136b9e8
  Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: IntelCor 51:6a:80 (34:e1:2d:51:6a:80)
```

4.

Το μήνυμα Discover διαφοροποιείται από το Request μέσω των options που ορίζει το καθένα, όπως φαίνεται στις παρακάτω εικόνες.

146	7.791711	0.0.0.0	255.255.255.255	DHCP	344 DHCP Discover
> Frame 146: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface \Dev > Ethernet II, Src: IntelCor_51:6a:80 (34:e1:2d:51:6a:80), 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)					
Message type: Boot Request (1) Hardware type: Ethernet (0x01) Hardware address length: 6 Hops: 0 Transaction ID: 0x0136b9e8 Seconds elapsed: 0					
> Bootp flags: 0x0000 (Unicast) Client IP address: 0.0.0.0 Your (client) IP address: 0.0.0.0 Next server IP address: 0.0.0.0 Relay agent IP address: 0.0.0.0 Client MAC address: IntelCor_51:6a:80 (34:e1:2d:51:6a:80) Client hardware address padding: 00000000000000000000 Server host name not given Boot file name not given Magic cookie: DHCP					
> Option: (53) DHCP Message Type (Discover) > Option: (61) Client identifier > Option: (50) Requested IP Address (192.168.1.165) > Option: (12) Host Name > Option: (60) Vendor class identifier > Option: (55) Parameter Request List > Option: (255) End Option End: 255					

190	10.010619	0.0.0.0	255.255.255.255	DHCP	370 DHCP Request
> Frame 190: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on interface \Dev > Ethernet II, Src: IntelCor_51:6a:80 (34:e1:2d:51:6a:80), 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 (Request)					
Message type: Boot Request (1) Hardware type: Ethernet (0x01) Hardware address length: 6 Hops: 0 Transaction ID: 0x0136b9e8 Seconds elapsed: 0					
> Bootp flags: 0x0000 (Unicast) Client IP address: 0.0.0.0 Your (client) IP address: 0.0.0.0 Next server IP address: 0.0.0.0 Relay agent IP address: 0.0.0.0 Client MAC address: IntelCor_51:6a:80 (34:e1:2d:51:6a:80) Client hardware address padding: 00000000000000000000 Server host name not given Boot file name not given Magic cookie: DHCP					
> Option: (53) DHCP Message Type (Request) > Option: (61) Client identifier > Option: (50) Requested IP Address (192.168.1.165) > Option: (54) DHCP Server Identifier (192.168.1.1) > Option: (12) Host Name > Option: (81) Client Fully Qualified Domain Name > Option: (60) Vendor class identifier > Option: (55) Parameter Request List > Option: (255) End					

Πιο συγκεκριμένα, παρατηρούμε αρχικά ότι υπάρχει διαφορά στο Option 53 το οποίο προσδιορίζει και το είδος του μηνύματος (Discover και Request αντίστοιχα). Εκτός αυτού, στο DHCP Request μήνυμα περιέχει επιπλέον το option 54 που προσδιορίζει τον DHCP server που επέλεξε ο client για την αποδοχή του DHCP Offer. Αυτή η διαφορά είναι σημαντική καθώς στο DHCP Discover ο client δεν γνωρίζει τους διαθέσιμους DHCP servers, οπότε στέλνει ένα broadcast μήνυμα προς όλους, με αποτέλεσμα να λάβει -ενδεχομένως- πολλαπλά DHCP Offers από αυτούς, εκ των οποίων θα πρέπει να αποδεχθεί μόνο το ένα.

Σημειώνεται ότι και στα δύο μηνύματα ζητάει την εκχώρηση των ίδιων παραμέτρων δικτύου.

5.

Το Transaction ID στην αλληλουχία των 4 πρώτων μηνυμάτων DHCP είναι 0x136b9e8

146	7.791711	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover	- Transaction ID 0x136b9e8
189	10.008946	192.168.1.1	192.168.1.165	DHCP	342	DHCP Offer	- Transaction ID 0x136b9e8
190	10.010619	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request	- Transaction ID 0x136b9e8
191	10.022864	192.168.1.1	192.168.1.165	DHCP	363	DHCP ACK	- Transaction ID 0x136b9e8

Στα επόμενα δύο μηνύματα (Request, ACK) το Transaction ID είναι 0xdc20e0d4

420	17.345246	192.168.1.165	192.168.1.1	DHCP	358	DHCP Request	- Transaction ID 0xdc20e0d4
421	17.389279	192.168.1.1	192.168.1.165	DHCP	363	DHCP ACK	- Transaction ID 0xdc20e0d4

Το Transaction ID επιλέγεται από τον client προκειμένου να μπορεί να αντιστοιχίσει τις αποκρίσεις του DHCP server με τα αιτήματα που έχει υποβάλλει.

6.

Η IP διεύθυνση του DHCP server, όπως αυτή φαίνεται στην απάντηση του (DHCP Offer) είναι η 192.168.1.1

189	10.008946	192.168.1.1	192.168.1.165	DHCP	342 DHCP Offer
>	Frame 189: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \N				
>	Ethernet II, Src: Technico_5a:cc:a0 (a4:91:b1:5a:cc:a0), Dst: IntelCor_51:6a:80 (34:e1:2d:51:6a:80)				
>	Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.165				
>	User Datagram Protocol, Src Port: 67, Dst Port: 68				
▼	Dynamic Host Configuration Protocol (Offer)				
	Message type: Boot Reply (2)				
	Hardware type: Ethernet (0x01)				
	Hardware address length: 6				
	Hops: 0				
	Transaction ID: 0x0136b9e8				
	Seconds elapsed: 0				
>	Bootp flags: 0x0000 (Unicast)				
	Client IP address: 0.0.0.0				
	Your (client) IP address: 192.168.1.165				
	Next server IP address: 192.168.1.1				
	Relay agent IP address: 0.0.0.0				
	Client MAC address: IntelCor_51:6a:80 (34:e1:2d:51:6a:80)				
	Client hardware address padding: 00000000000000000000				
	Server host name not given				
	Boot file name not given				
	Magic cookie: DHCP				
>	Option: (53) DHCP Message Type (Offer)				
>	Option: (54) DHCP Server Identifier (192.168.1.1)				
>	Option: (51) IP Address Lease Time				
>	Option: (58) Renewal Time Value				
>	Option: (59) Rebinding Time Value				
>	Option: (1) Subnet Mask (255.255.255.0)				
>	Option: (28) Broadcast Address (192.168.1.255)				
>	Option: (3) Router				
>	Option: (6) Domain Name Server				
>	Option: (15) Domain Name				
>	Option: (255) End				
	Padding: 000000				

7.

Η IP διεύθυνση που προσφέρει ο DHCP server στο DHCP Offer μήνυμα που φαίνεται στην προηγούμενη εικόνα είναι η 192.168.1.165

Αυτή είναι και η διεύθυνση που είχε αιτηθεί ο υπολογιστής μας στο DHCP Discover μήνυμα (option 50).

8.

Μεταξύ των παραμέτρων του δικτύου που ζητάει ο client και στέλνει ο DHCP server είναι το subnet mask, ώστε να μπορέσει ο υπολογιστής να προσδιορίσει το υποδίκτυο στο οποίο ανήκει και επομένως να επικοινωνήσει με τους υπόλοιπους κόμβους σε αυτό, και έπειτα η διεύθυνση του default gateway (δηλαδή του router), ώστε να γνωρίζει που θα πρέπει να διαβιβάσει τα πακέτα που έχουν προορισμό εκτός του δικτύου του.

189	10.008946	192.168.1.1	192.168.1.165	DHCP	342 DHCP Offer
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.165					
User Datagram Protocol, Src Port: 67, Dst Port: 68					
Dynamic Host Configuration Protocol (Offer)					
Message type: Boot Reply (2)					
Hardware type: Ethernet (0x01)					
Hardware address length: 6					
Hops: 0					
Transaction ID: 0x0136b9e8					
Seconds elapsed: 0					
> Bootp flags: 0x0000 (Unicast)					
Client IP address: 0.0.0.0					
Your (client) IP address: 192.168.1.165					
Next server IP address: 192.168.1.1					
Relay agent IP address: 0.0.0.0					
Client MAC address: IntelCor_51:6a:80 (34:e1:2d:51:6a:80)					
Client hardware address padding: 000000000000000000000000					
Server host name not given					
Boot file name not given					
Magic cookie: DHCP					
> Option: (53) DHCP Message Type (Offer)					
> Option: (54) DHCP Server Identifier (192.168.1.1)					
> Option: (51) IP Address Lease Time					
> Option: (58) Renewal Time Value					
> Option: (59) Rebinding Time Value					
v Option: (1) Subnet Mask (255.255.255.0)					
Length: 4					
Subnet Mask: 255.255.255.0					
> Option: (28) Broadcast Address (192.168.1.255)					
v Option: (3) Router					
Length: 4					
Router: 192.168.1.1					

9.

Το lease time προσδιορίζεται στο option 51 όπως βλέπουμε στο DHCP Offer μήνυμα. Αυτό χρησιμοποιείται προκειμένου οι IP που παραχωρεί ο DHCP server να μην δεσμεύονται επ' αόριστον από τις συσκευές που τις ζητάνε, παρά μόνο εάν αυτές συνεχίζουν να είναι συνδεδεμένες στο ίδιο δίκτυο. Μόλις μια συσκευή που είχε ζητήσει μια συγκεκριμένη IP αποσυνδεθεί για ένα ορισμένο χρονικό διάστημα, αυτή η IP γίνεται ξανά διαθέσιμη προκειμένου να γίνει εξοικονόμηση διευθύνσεων. Εφόσον ένα μηχάνημα θέλει να συνεχίσει να χρησιμοποιεί την ίδια IP πρέπει να ξανά-υποβάλλει ένα DHCP Request είτε όταν έχει περάσει το 50% της περιόδου που καθορίζει το lease time (στο option 58 – renewal time value) ή, αν δεν ήταν δυνατό το renewal, όταν έχει περάσει το 87.5% του χρόνου αυτού (καθορίζεται στο option 59 –rebinding time value).

Το lease time για το οποίο ο DHCP server μας έχει εκχωρήσει την IP, όπως φαίνεται στην παρακάτω εικόνα, είναι μια ημέρα.

189	10.008946	192.168.1.1	192.168.1.165	DHCP	342	DHCP Offer
-----	-----------	-------------	---------------	------	-----	------------

```

Relay agent IP address: 0.0.0.0
Client MAC address: IntelCor_51:6a:80 (34:e1:2d:51:6a:80)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
> Option: (53) DHCP Message Type (Offer)
> Option: (54) DHCP Server Identifier (192.168.1.1)
v Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: (86400s) 1 day
v Option: (58) Renewal Time Value
    Length: 4
    Renewal Time Value: (43200s) 12 hours
v Option: (59) Rebinding Time Value
    Length: 4
    Rebinding Time Value: (75600s) 21 hours

```

10.

Εφαρμόζοντας το φίλτρο “arp” εμφανίζονται όλα τα ARP broadcast πλαίσια που λαμβάνει ο υπολογιστής μας καθώς και αυτά που στέλνει για να μάθει τις Ethernet διευθύνσεις των υπόλοιπων κόμβων του υποδικτύου μας. Αυτά φαίνονται στην εικόνα που ακολουθεί:

arp						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Technico_5a:cc:a0	Broadcast	ARP	42	Who has 192.168.1.165? Tell 192.168.1.1
3	0.527118	IntelCor_51:6a:80	Broadcast	ARP	42	ARP Announcement for 169.254.176.81
41	1.539044	Espressi_c7:6b:ea	Broadcast	ARP	42	ARP Announcement for 192.168.1.14
47	2.053620	Technico_5a:cc:a0	Broadcast	ARP	42	Who has 192.168.1.216? Tell 192.168.1.1
51	2.253372	Technico_5a:cc:a0	Broadcast	ARP	42	Who has 192.168.1.165? Tell 192.168.1.1
54	2.770710	MitsumiE_e5:4f:0a	Broadcast	ARP	42	Who has 192.168.1.30? Tell 192.168.1.216
59	3.076235	MitsumiE_e5:4f:0a	Broadcast	ARP	42	Who has 192.168.1.30? Tell 192.168.1.216
66	3.282291	Technico_5a:cc:a0	Broadcast	ARP	42	Who has 192.168.1.165? Tell 192.168.1.1
70	3.385560	MitsumiE_e5:4f:0a	Broadcast	ARP	42	Who has 192.168.1.30? Tell 192.168.1.216
75	4.305643	Technico_5a:cc:a0	Broadcast	ARP	42	Who has 192.168.1.165? Tell 192.168.1.1
77	5.331615	Technico_5a:cc:a0	Broadcast	ARP	42	Who has 192.168.1.165? Tell 192.168.1.1
110	6.351486	Technico_5a:cc:a0	Broadcast	ARP	42	Who has 192.168.1.165? Tell 192.168.1.1
138	7.283686	Technico_5a:cc:a0	Broadcast	ARP	42	Who has 192.168.1.165? Tell 192.168.1.1
155	8.294229	Technico_5a:cc:a0	Broadcast	ARP	42	Who has 192.168.1.165? Tell 192.168.1.1
181	9.318354	Technico_5a:cc:a0	Broadcast	ARP	42	Who has 192.168.1.165? Tell 192.168.1.1
194	10.044170	IntelCor_51:6a:80	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.165
197	10.053478	Technico_5a:cc:a0	IntelCor_51:6a:80	ARP	42	192.168.1.1 is at a4:91:b1:5a:cc:a0
230	10.251034	Technico_5a:cc:a0	Broadcast	ARP	42	Who has 192.168.1.165? Tell 192.168.1.1
231	10.251044	IntelCor_51:6a:80	Technico_5a:cc:a0	ARP	42	192.168.1.165 is at 34:e1:2d:51:6a:80
236	10.337055	IntelCor_51:6a:80	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.165
237	10.348103	Technico_5a:cc:a0	IntelCor_51:6a:80	ARP	42	192.168.1.1 is at a4:91:b1:5a:cc:a0
247	10.512421	IntelCor_51:6a:80	Broadcast	ARP	42	Who has 192.168.1.165? (ARP Probe)
318	11.527354	IntelCor_51:6a:80	Broadcast	ARP	42	Who has 192.168.1.165? (ARP Probe)
322	11.571219	Espressi_c7:6b:ea	Broadcast	ARP	42	ARP Announcement for 192.168.1.14
351	12.525796	IntelCor_51:6a:80	Broadcast	ARP	42	Who has 192.168.1.165? (ARP Probe)
355	12.817626	MitsumiE_e5:4f:0a	Broadcast	ARP	42	Who has 192.168.1.30? Tell 192.168.1.216
362	13.109651	MitsumiE_e5:4f:0a	Broadcast	ARP	42	Who has 192.168.1.30? Tell 192.168.1.216
363	13.209721	MitsumiE_e5:4f:0a	Broadcast	ARP	42	Who has 192.168.1.165? Tell 192.168.1.216
364	13.209731	IntelCor_51:6a:80	MitsumiE_e5:4f:0a	ARP	42	192.168.1.165 is at 34:e1:2d:51:6a:80
368	13.414283	MitsumiE_e5:4f:0a	Broadcast	ARP	42	Who has 192.168.1.30? Tell 192.168.1.216
371	13.523453	IntelCor_51:6a:80	Broadcast	ARP	42	ARP Announcement for 192.168.1.165
395	15.464875	MitsumiE_e5:4f:0a	Broadcast	ARP	42	Who has 192.168.1.165? Tell 192.168.1.216
396	15.464903	IntelCor_51:6a:80	MitsumiE_e5:4f:0a	ARP	42	192.168.1.165 is at 34:e1:2d:51:6a:80
398	15.566631	MitsumiE_e5:4f:0a	Broadcast	ARP	42	Who has 192.168.1.165? Tell 192.168.1.216
399	15.566655	IntelCor_51:6a:80	MitsumiE_e5:4f:0a	ARP	42	192.168.1.165 is at 34:e1:2d:51:6a:80
468	17.612746	Technico_5a:cc:a0	Broadcast	ARP	42	Who has 192.168.1.14? Tell 192.168.1.1
469	17.614271	Technico_5a:cc:a0	Broadcast	ARP	42	Who has 192.168.1.30? Tell 192.168.1.1
470	17.616071	Technico_5a:cc:a0	Broadcast	ARP	42	Who has 192.168.1.221? Tell 192.168.1.1

Στην εικόνα φαίνονται αρκετά πλαίσια ARP τα οποία έχουν άμεση σχέση με το πρωτόκολλο DHCP και τη διαδικασία που περιεγράφηκε νωρίτερα.

Το πρώτο ARP πλαίσιο που μας ενδιαφέρει στέλνεται από τον DHCP server, αφότου ο υπολογιστής μας καθορίσει την IP που θέλει να του εκχωρηθεί με το DHCP Discover, προκειμένου ο server να διαπιστώσει εάν η συγκεκριμένη διεύθυνση χρησιμοποιείται από κάποιον άλλο κόμβο στο δίκτυο, έτσι ώστε να την διαθέσει στο DHCP Offer.

146	7.791711	0.0.0.0	255.255.255.255	DHCP	344 DHCP Discover - Transaction ID 0x136b9e8
147	7.946870	fdfd:3427:2509:0:93...	fdfd:3427:2509::1	DNS	102 Standard query 0x26ee AAAA client.wns.window
148	7.950040	fe80::87ce:3730:68c...	ff02::c	UDP	718 57691 → 3702 Len=656
149	7.954201	fdfd:3427:2509::1	fdfd:3427:2509:0:93...	DNS	145 Standard query response 0x26ee AAAA client.w
150	7.954837	fdfd:3427:2509:0:93...	fdfd:3427:2509::1	DNS	109 Standard query 0xe3f8 AAAA wns.notify.traffi
151	7.960432	fdfd:3427:2509::1	fdfd:3427:2509:0:93...	DNS	109 Standard query response 0xe3f8 AAAA wns.noti
152	7.961208	fdfd:3427:2509:0:93...	fdfd:3427:2509::1	DNS	102 Standard query 0x8a69 AAAA client.wns.window
153	7.967617	fdfd:3427:2509::1	fdfd:3427:2509:0:93...	DNS	145 Standard query response 0x8a69 AAAA client.w
154	8.166068	169.254.176.81	239.255.255.250	UDP	698 57690 → 3702 Len=656
155	8.294229	Technico_5a:cc:a0	Broadcast	ARP	42 Who has 192.168.1.165? Tell 192.168.1.1

Τα επόμενα ARP πλαίσια που έχουν νόημα στην καταγραφή μας παρατηρούνται μόλις ολοκληρωθεί η διαδικασία εκχώρησης παραμέτρων δικτύου από τον DHCP server. Ο υπολογιστής μας στέλνει ένα ARP Request για να μάθει την διεύθυνση επιπέδου Ethernet του default gateway που έλαβε από τον DHCP server. Το αμέσως επόμενο πλαίσιο φέρει το ARP reply του αιτήματος μας από το router. Τα πλαίσια αυτά είναι τα ακόλουθα 2:

189	10.008946	192.168.1.1	192.168.1.165	DHCP	342 DHCP Offer - Transaction ID 0x136b9e8
190	10.010619	0.0.0.0	255.255.255.255	DHCP	370 DHCP Request - Transaction ID 0x136b9e8
191	10.022864	192.168.1.1	192.168.1.165	DHCP	363 DHCP ACK - Transaction ID 0x136b9e8
192	10.040000	fe80::87ce:3730:68c...	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
193	10.040112	192.168.1.165	224.0.0.22	IGMPv3	54 Membership Report / Leave group 224.0.0.252
194	10.044170	IntelCor_51:6a:80	Broadcast	ARP	42 Who has 192.168.1.1? Tell 192.168.1.165
195	10.050904	192.168.1.165	224.0.0.22	IGMPv3	54 Membership Report / Leave group 239.255.255.250
196	10.051326	192.168.1.165	224.0.0.22	IGMPv3	54 Membership Report / Join group 239.255.255.250 for any sources
197	10.053478	Technico_5a:cc:a0	IntelCor_51:6a:80	ARP	42 192.168.1.1 is at a4:91:b1:5a:cc:a0

Με τη σειρά του το router ζητάει να μάθει την ethernet διεύθυνση του υπολογιστή μας με ξεχωριστό ARP request. Ο υπολογιστής αποκρίνεται με τη διεύθυνση MAC του προκειμένου το router να ενημερώσει την ARP cache του και να μπορέσει να προωθήσει πλαίσια που προορίζονται για αυτόν.

230	10.251034	Technico_5a:cc:a0	Broadcast	ARP	42 Who has 192.168.1.165? Tell 192.168.1.1
231	10.251044	IntelCor_51:6a:80	Technico_5a:cc:a0	ARP	42 192.168.1.165 is at 34:e1:2d:51:6a:80

Τέλος ο υπολογιστής μας, δηλαδή ο client κάνει έναν έλεγχο (ARP probe) για να διαπιστώσει εάν υπάρχει κι άλλος κόμβος στο δίκτυο με την ίδια IP διεύθυνση. Αν δεν λάβει καμία απάντηση σημαίνει ότι αυτή η διεύθυνση δεν χρησιμοποιείται από κάποιον άλλο εκτός από τον ίδιο και μπορεί να ξεκινήσει να τη χρησιμοποιεί.

247	10.512421	IntelCor_51:6a:80	Broadcast	ARP	42 Who has 192.168.1.165? (ARP Probe)
-----	-----------	-------------------	-----------	-----	---------------------------------------

Σημειώνεται ότι το ARP Probe έχει ως IP διεύθυνση αποστολής την 0.0.0.0, προκειμένου οι υπόλοιποι κόμβοι να μην ενημερώσουν τις ARP cache τους με τις πληροφορίες του πλαισίου αυτού (η διεύθυνση IP αγνοείται)