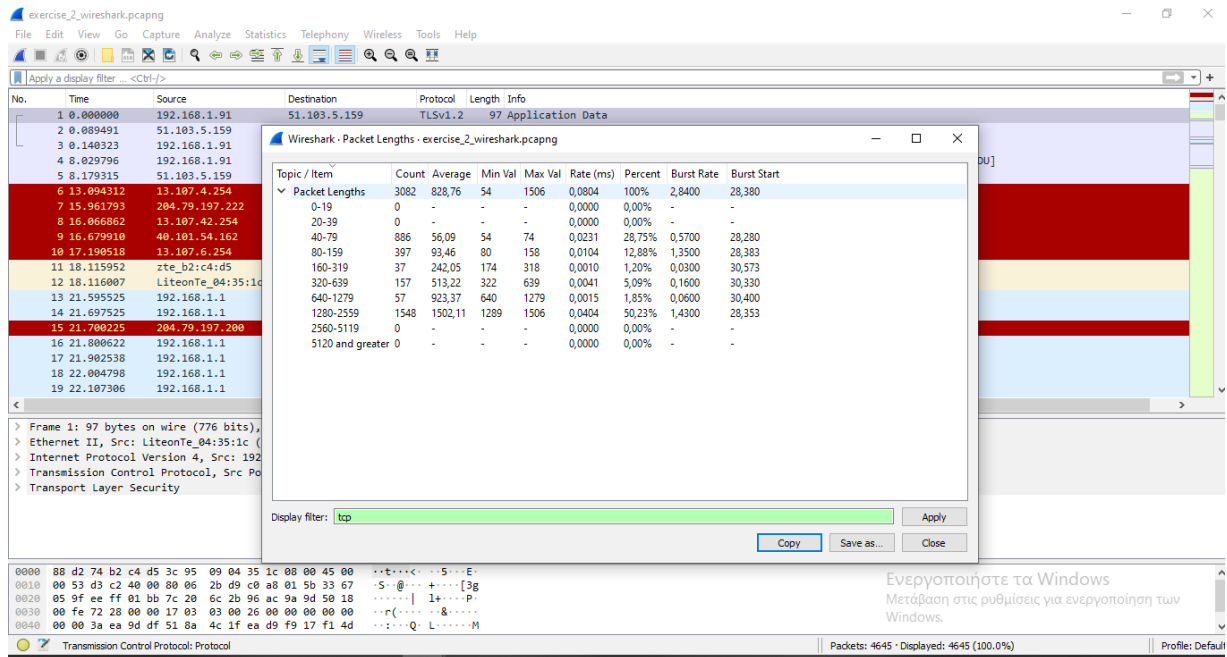


Wireshark Exercise 1

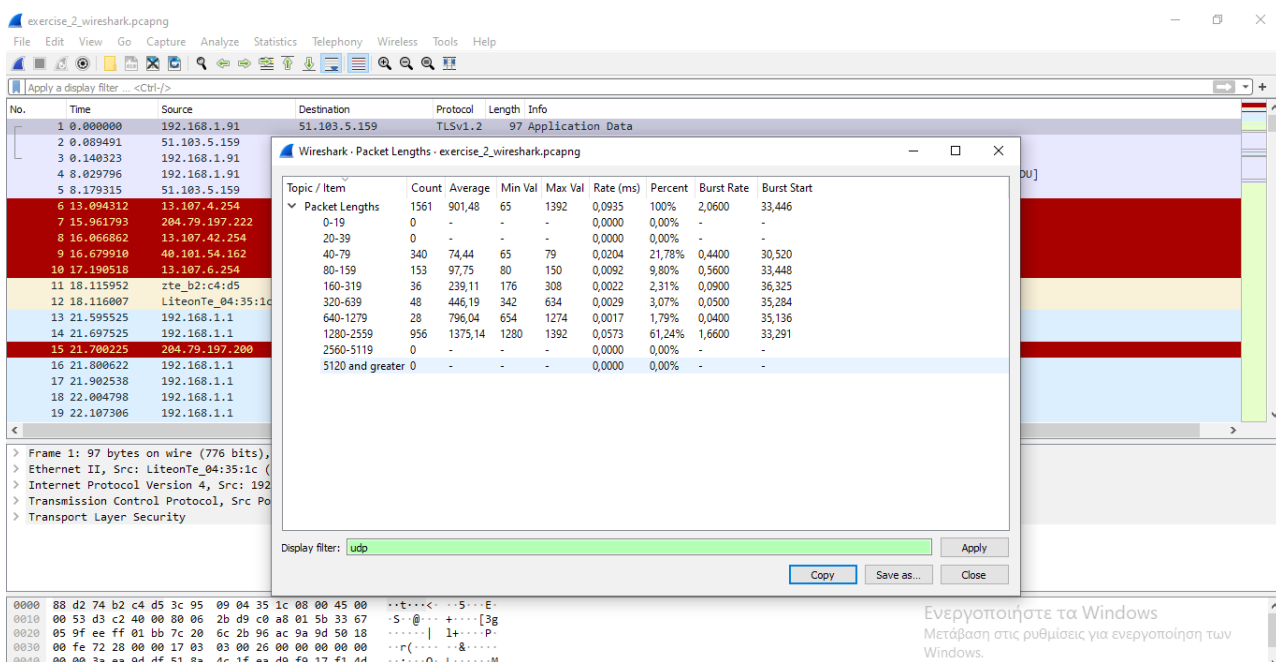
ΕΡΩΤΗΣΕΙΣ

1. Για την εύρεση των πακέτων TCP και UDP έκανα χρήση των φίλτρων tcp κι udp αντίστοιχα.

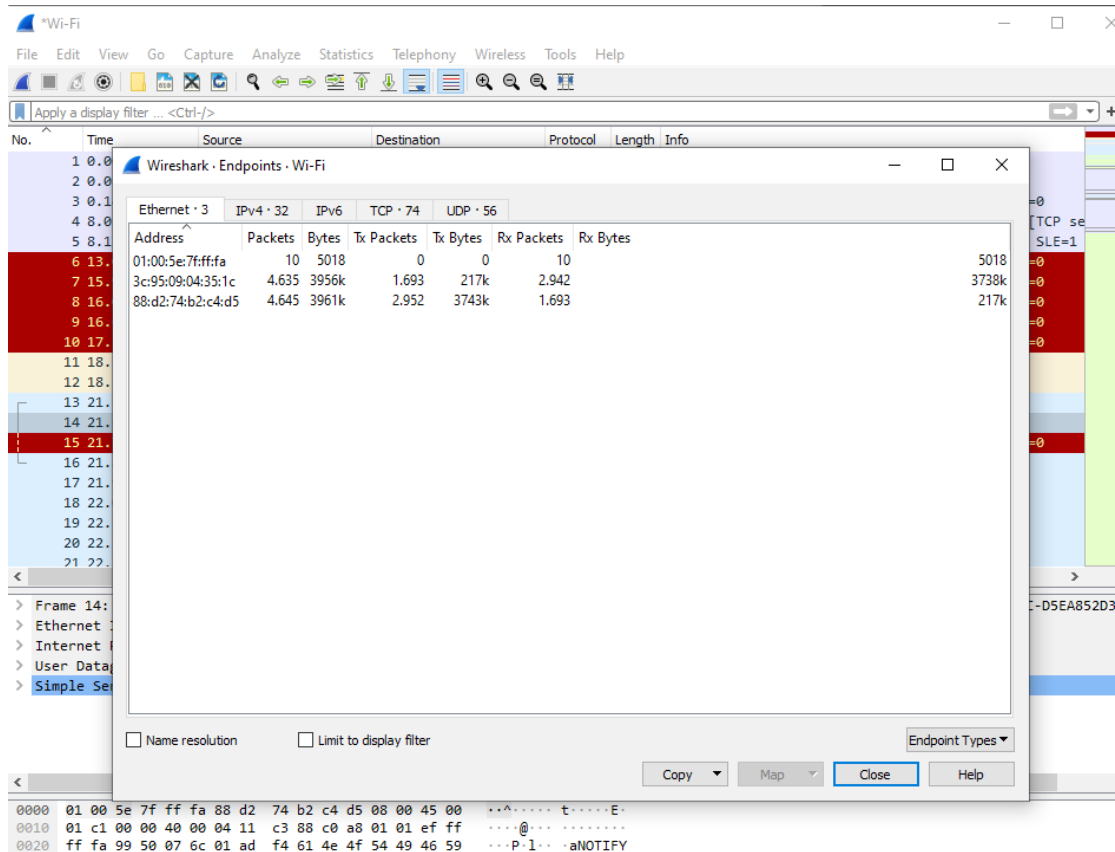
TCP: στάλθηκαν 3082



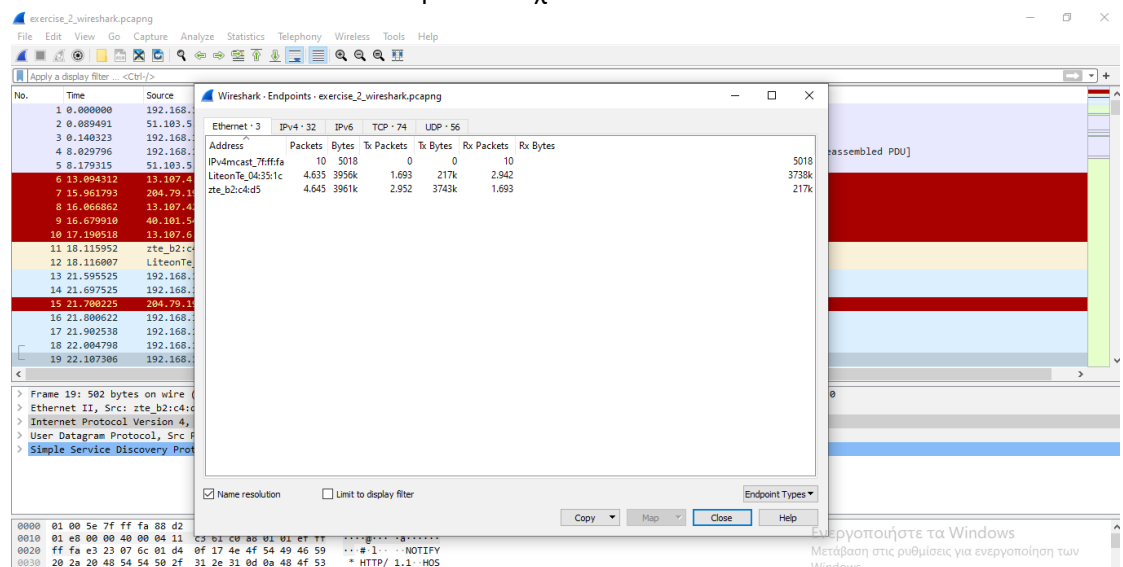
UDP: στάλθηκαν 1561



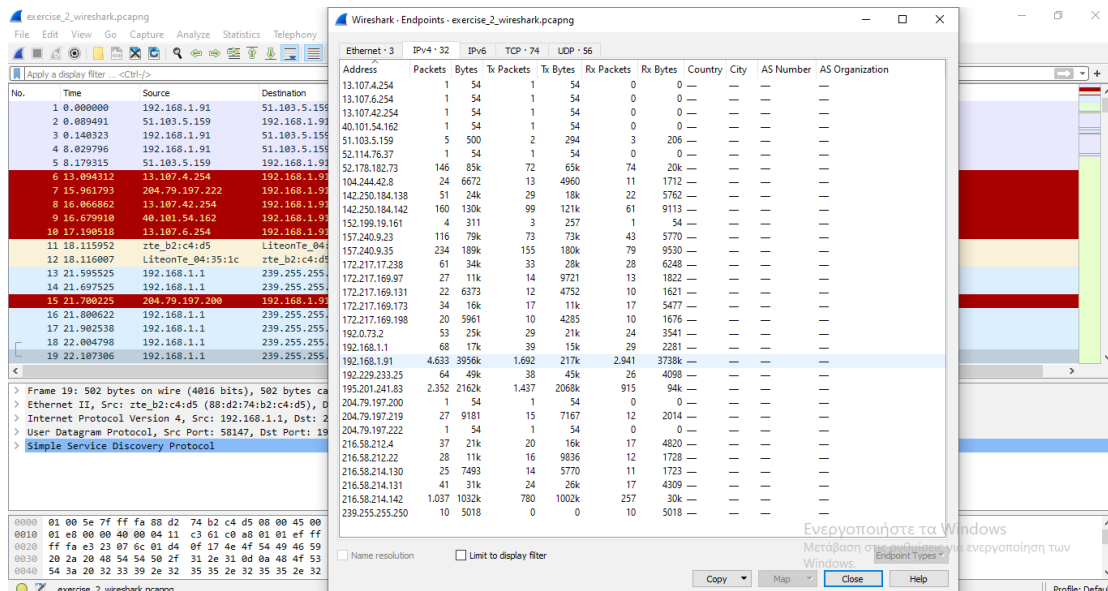
2. Τα endpoints με τα οποία υπάρχει επικοινωνία σε επίπεδο Ethernet είναι τα εξής τρία με τις ακόλουθες διευθύνσεις :



Πατώντας το name resolution βλέπουμε τα ονόματα και τις μάρκες των συσκευών .Η τελευταία διεύθυνση αντιστοιχεί στο modem.



3. Τα endpoints με τα οποία υπάρχει επικοινωνία σε επίπεδο IP είναι 32:



The image shows the Wireshark interface with a packet capture of 'exercise_2_wireshark.pcapng'. The packet list on the left shows several packets, with packet 19 selected. The packet details pane on the right shows the 'Endpoints' table for the selected packet. The table lists the source and destination IP addresses for the packet, along with the number of packets and bytes transmitted and received.

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
13.107.4.254	1	54	1	54	0	0	—	—	—	—
13.107.6.254	1	54	1	54	0	0	—	—	—	—
13.107.42.254	1	54	1	54	0	0	—	—	—	—
40.101.54.162	1	54	1	54	0	0	—	—	—	—
51.103.5.159	5	500	2	294	3	206	—	—	—	—
52.114.76.37	1	54	1	54	0	0	—	—	—	—
52.178.182.73	146	85k	72	65k	74	20k	—	—	—	—
104.244.42.8	24	6672	13	4960	11	1712	—	—	—	—
142.250.184.138	51	24k	29	18k	22	5762	—	—	—	—
142.250.184.142	160	130k	99	121k	61	9113	—	—	—	—
152.199.19.161	4	311	3	257	1	54	—	—	—	—
157.240.9.23	116	79k	73	73k	43	5770	—	—	—	—
157.240.9.35	234	189k	155	180k	79	9530	—	—	—	—
172.217.17.238	61	34k	33	28k	28	6248	—	—	—	—
172.217.169.97	27	11k	14	9721	13	1822	—	—	—	—
172.217.169.131	22	6373	12	4752	10	1621	—	—	—	—
172.217.169.173	34	16k	17	11k	17	5477	—	—	—	—
172.217.169.198	20	5961	10	4285	10	1676	—	—	—	—
192.0.73.2	53	25k	29	21k	24	3541	—	—	—	—
192.168.1.1	68	17k	39	15k	29	2281	—	—	—	—
192.168.1.91	4,633	3956k	1,692	217k	2,941	3738k	—	—	—	—
192.229.233.25	64	49k	38	45k	26	4098	—	—	—	—
195.201.241.83	2,352	2162k	1,437	2068k	915	94k	—	—	—	—
204.79.197.200	1	54	1	54	0	0	—	—	—	—
204.79.197.219	27	9181	15	7167	12	2014	—	—	—	—
204.79.197.222	1	54	1	54	0	0	—	—	—	—
216.58.212.4	37	21k	20	16k	17	4820	—	—	—	—
216.58.212.22	28	11k	16	9836	12	1728	—	—	—	—
216.58.214.130	25	7493	14	5770	11	1723	—	—	—	—
216.58.214.131	41	31k	24	26k	17	4309	—	—	—	—
216.58.214.142	1,037	1032k	780	1002k	257	30k	—	—	—	—
239.255.255.250	10	5018	0	0	10	5018	—	—	—	—

4. Χρησιμοποίησα το φίλτρο “dnsserver” και βρήκα τα ports της σελίδας <http://www.book4book.gr/> όπου :

Για την ερώτηση:

Destination: zte_b2:c4:d5 (88:d2:74:b2:c4:d5)

Source: LiteonTe_04:35:1c (3c:95:09:04:35:1c)

Για την απάντηση:

Destination: LiteonTe_04:35:1c (3c:95:09:04:35:1c)

Source: zte_b2:c4:d5 (88:d2:74:b2:c4:d5)

5. Διακρίνουμε αν ένα πακέτο περιέχει αίτημα προς τον DNS server ή απάντηση σε ερώτημα που έχει κάνει πατώντας Domain Name System ,όπου θα αναγράφεται αν είναι response ή query.
Συγκεκριμένα :

Query:

exercise_2_wireshark.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dnsserver

Time	Source	Destination	Protocol	Length	Info
24	25.569349	192.168.1.91	DNS	76	Standard query 0x2fde A www.book4book.gr
25	25.690223	192.168.1.1	DNS	182	Standard query response 0x2fde A www.book4book.gr CNAME book4book.gr A 195.201.241.83 NS ns82.ipdns.gr NS ns81...
28	25.725450	192.168.1.1	DNS	89	Standard query 0x18aa A nav.smartscreen.microsoft.com
34	25.797017	192.168.1.1	DNS	473	Standard query response 0x18aa A nav.smartscreen.microsoft.com CNAME wd-prod-ss.trafficmanager.net CNAME wd-pro...
59	26.191770	192.168.1.91	DNS	90	Standard query 0x33b5 A smartscreen-prod.microsoft.com
61	26.272225	192.168.1.1	DNS	475	Standard query response 0x33b5 A smartscreen-prod.microsoft.com CNAME wd-prod-ss.trafficmanager.net CNAME wd-pr...
1271	28.960597	192.168.1.91	DNS	75	Standard query 0x473a A maps.google.com
1282	29.031946	192.168.1.1	DNS	365	Standard query response 0x473a A maps.google.com A 216.58.214.142 NS ns4.googIE.coM NS ns3.googIE.coM NS ns1.go...
1505	29.689939	192.168.1.91	DNS	80	Standard query 0xa478 A platform.twitter.com
1533	29.758307	192.168.1.1	DNS	513	Standard query response 0xa478 A platform.twitter.com CNAME cs472.wac.edgecastcdn.net CNAME cs1-apr-8315.wac.ed...
1776	30.119733	192.168.1.91	DNS	80	Standard query 0x5ec6 A www.book4book.com.cy
1782	30.122225	192.168.1.1	DNS	76	Standard query 0x02a0 A www.book4book.lk
1877	30.168332	192.168.1.91	DNS	76	Standard query 0xacda A www.gravatar.com
1966	30.246385	192.168.1.1	DNS	490	Standard query response 0x02a0 A www.book4book.lk A 192.248.8.30 NS ns1.ac.lk NS m.nic.lk NS ns1.nic.lk NS d.nic...
1969	30.247283	192.168.1.1	DNS	289	Standard query response 0xacda A www.gravatar.com A 192.0.73.2 NS ns3.automattic.com NS ns2.automattic.com NS n...
2523	30.955430	192.168.1.1	DNS	139	Standard query response 0x5ec6 No such name A www.book4book.com.cy SOA cynic.dns.cy
2528	32.247681	192.168.1.1	DNS	84	Standard query 0x0c71 A www.google-analytics.com
2529	32.310078	192.168.1.1	DNS	429	Standard query response 0x0c71 A www.google-analytics.com CNAME www-google-analytics.l.google.coM A 172.217.17...
2531	32.324919	192.168.1.91	DNS	75	Standard query 0x010c A www.youtube.com

< >

[Timestamps]
UDP payload (34 bytes)
Domain Name System (query)
Transaction ID: 0x2fde
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0

Response:

exercise_2_wireshark.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dnsserver

Time	Source	Destination	Protocol	Length	Info
24	25.569349	192.168.1.91	DNS	76	Standard query 0x2fde A www.book4book.gr
25	25.690223	192.168.1.1	DNS	182	Standard query response 0x2fde A www.book4book.gr CNAME book4book.gr A 195.201.241.83 NS ns82.ipdns.gr NS ns81...
28	25.725450	192.168.1.1	DNS	89	Standard query 0x18aa A nav.smartscreen.microsoft.com
34	25.797017	192.168.1.1	DNS	473	Standard query response 0x18aa A nav.smartscreen.microsoft.com CNAME wd-prod-ss.trafficmanager.net CNAME wd-pro...
59	26.191770	192.168.1.91	DNS	90	Standard query 0x33b5 A smartscreen-prod.microsoft.com
61	26.272225	192.168.1.1	DNS	475	Standard query response 0x33b5 A smartscreen-prod.microsoft.com CNAME wd-prod-ss.trafficmanager.net CNAME wd-pr...
1271	28.960597	192.168.1.91	DNS	75	Standard query 0x473a A maps.google.com
1282	29.031946	192.168.1.1	DNS	365	Standard query response 0x473a A maps.google.com A 216.58.214.142 NS ns4.googIE.coM NS ns3.googIE.coM NS ns1.go...
1505	29.689939	192.168.1.91	DNS	80	Standard query 0xa478 A platform.twitter.com
1533	29.758307	192.168.1.1	DNS	513	Standard query response 0xa478 A platform.twitter.com CNAME cs472.wac.edgecastcdn.net CNAME cs1-apr-8315.wac.ed...
1776	30.119733	192.168.1.91	DNS	80	Standard query 0x5ec6 A www.book4book.com.cy
1782	30.122225	192.168.1.91	DNS	76	Standard query 0x02a0 A www.book4book.lk
1877	30.168332	192.168.1.91	DNS	76	Standard query 0xacda A www.gravatar.com
1966	30.246385	192.168.1.1	DNS	490	Standard query response 0x02a0 A www.book4book.lk A 192.248.8.30 NS ns1.ac.lk NS m.nic.lk NS ns1.nic.lk NS d.nic...
1969	30.247283	192.168.1.1	DNS	289	Standard query response 0xacda A www.gravatar.com A 192.0.73.2 NS ns3.automattic.com NS ns2.automattic.com NS n...
2523	30.955430	192.168.1.1	DNS	139	Standard query response 0x5ec6 No such name A www.book4book.com.cy SOA cynic.dns.cy
2528	32.247681	192.168.1.91	DNS	84	Standard query 0x0c71 A www.google-analytics.com
2529	32.310078	192.168.1.1	DNS	429	Standard query response 0x0c71 A www.google-analytics.com CNAME www-google-analytics.l.google.coM A 172.217.17...
2531	32.324919	192.168.1.91	DNS	75	Standard query 0x010c A www.youtube.com

< >

[Timestamps]
UDP payload (140 bytes)
Domain Name System (response)
Transaction ID: 0x2fde
Flags: 0x0100 Standard query response, No error
Questions: 1
Answer RRs: 2
Authority RRs: 2
Additional RRs: 2

Όπου παρατηρούμε πώς η διεύθυνση source της ερώτησης είναι ίδια με την destination της απάντησης και η destination της ερώτησης με την source της απάντησης.

- Υπάρχει flag που να προσδιορίζει αν ο name server που μας απαντάει είναι authoritative για το συγκεκριμένο domain στο Domain Name System και συγκεκριμένα σε αυτό που μας έχει απαντήσει φαίνεται παρακάτω ότι είναι .

exercise_2_wireshark.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dnsserver

No.	Time	Source	Destination	Protocol	Length	Info
24	25.569349	192.168.1.91	192.168.1.1	DNS	76	Standard query 0x2fde A www.book4book.gr
25	25.690223	192.168.1.1	192.168.1.91	DNS	182	Standard query response 0x2fde A www.book4book.gr CNAME book4book.gr A 195.201.241.83 NS ns82.ipdns.gr NS ns61...
28	25.725450	192.168.1.91	192.168.1.1	DNS	89	Standard query 0x18aa A nav.smartscreen.microsoft.com
34	25.797017	192.168.1.1	192.168.1.91	DNS	473	Standard query response 0x18aa A nav.smartscreen.microsoft.com CNAME wd-prod-ss.trafficmanager.net CNAME wd-pro...
59	26.191770	192.168.1.91	192.168.1.1	DNS	90	Standard query 0x33b5 A smartscreen-prod.microsoft.com
61	26.272225	192.168.1.1	192.168.1.91	DNS	475	Standard query response 0x33b5 A smartscreen-prod.microsoft.com CNAME wd-prod-ss.trafficmanager.net CNAME wd-pr...
1271	28.960597	192.168.1.91	192.168.1.1	DNS	75	Standard query 0x473a A maps.google.com
1282	29.031946	192.168.1.1	192.168.1.91	DNS	365	Standard query response 0x473a A maps.google.com A 216.58.214.142 NS ns4.go0G1E.coM NS ns3.go0G1E.coM NS ns1.go...
1505	29.689939	192.168.1.91	192.168.1.1	DNS	80	Standard query 0xa478 A platform.twitter.com
1533	29.758387	192.168.1.1	192.168.1.91	DNS	513	Standard query response 0xa478 A platform.twitter.com CNAME cs472.wac.edgestcdn.net CNAME cs1-apr-8315.wac.ed...
1776	30.119733	192.168.1.91	192.168.1.1	DNS	80	Standard query 0x5ec6 A www.book4book.com.cy
1782	30.122225	192.168.1.91	192.168.1.1	DNS	76	Standard query 0x02a0 A www.book4book.lk
1877	30.168333	192.168.1.91	192.168.1.1	DNS	76	Standard query 0x02a0 A www.book4book.lk

Domain Name System (response)
Transaction ID: 0x2fde
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 2
Authority RRs: 2
Additional RRs: 2
Queries
Answers
Authoritative nameservers
book4book.gr: type NS, class IN, ns ns82.ipdns.gr
book4book.gr: type NS, class IN, ns ns81.ipdns.gr
Additional records
[Request In: 24]
[Time: 0.120874000 seconds]

0030 00 02 00 02 00 02 03 77 77 77 09 62 6f 6f 6b 3dw ww-book4
0040 62 6f 6f 6b 02 67 72 00 00 01 00 01 c0 0c 00 05book.gr.....
0050 00 01 00 00 0c d7 00 02 c0 10 c0 10 00 01 00 01S.....
0060 00 00 0c d7 00 04 c3 c9 f1 53 c0 10 00 02 00 01n s82-ipdn
0070 00 00 c0 d7 00 0d 04 6e 73 38 32 05 69 70 64 6e

Number of authoritative records in packet (dns.count.auth_rr), 2 byte(s)

Packets: 4645 · Displayed: 58 (1.2%)

Profile: Default

10:05 μμ
15/1/2021

7. Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.91
- 8.

exercise_2_wireshark.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
4240	37.102261	195.201.241.83	192.168.1.91	HTTP	570	HTTP/1.1 404 Not Found (text/html)
938	28.601918	195.201.241.83	192.168.1.91	HTTP	1506	[TCP Fast Retransmission] Continuation
1238	28.846275	195.201.241.83	192.168.1.91	HTTP	1506	[TCP Fast Retransmission] Continuation
442	28.378643	195.201.241.83	192.168.1.91	HTTP	1506	[TCP Previous segment not captured] Continuation
444	28.374592	195.201.241.83	192.168.1.91	HTTP	1506	[TCP Previous segment not captured] Continuation
466	28.382526	195.201.241.83	192.168.1.91	HTTP	1506	[TCP Previous segment not captured] Continuation
496	28.394565	195.201.241.83	192.168.1.91	HTTP	1506	[TCP Previous segment not captured] Continuation
504	28.396994	195.201.241.83	192.168.1.91	HTTP	1506	[TCP Previous segment not captured] Continuation
580	28.398369	195.201.241.83	192.168.1.91	HTTP	1506	[TCP Previous segment not captured] Continuation
511	28.399354	195.201.241.83	192.168.1.91	HTTP	1506	[TCP Previous segment not captured] Continuation
514	28.399643	195.201.241.83	192.168.1.91	HTTP	1506	[TCP Previous segment not captured] Continuation
516	28.399955	195.201.241.83	192.168.1.91	HTTP	1506	[TCP Previous segment not captured] Continuation
518	28.400893	195.201.241.83	192.168.1.91	HTTP	1506	[TCP Previous segment not captured] Continuation
520	28.401458	195.201.241.83	192.168.1.91	HTTP	1506	[TCP Previous segment not captured] Continuation
522	28.402353	195.201.241.83	192.168.1.91	HTTP	1506	[TCP Previous segment not captured] Continuation
524	28.402823	195.201.241.83	192.168.1.91	HTTP	1506	[TCP Previous segment not captured] Continuation
607	28.432492	195.201.241.83	192.168.1.91	HTTP	1506	[TCP Previous segment not captured] Continuation
633	28.441959	195.201.241.83	192.168.1.91	HTTP	1506	[TCP Previous segment not captured] Continuation
646	28.446175	195.201.241.83	192.168.1.91	HTTP	138	[TCP Previous segment not captured] Continuation
649	28.447386	195.201.241.83	192.168.1.91	HTTP	1506	[TCP Previous segment not captured] Continuation
651	28.447777	195.201.241.83	192.168.1.91	HTTP	1506	[TCP Previous segment not captured] Continuation

Frame 3859: 474 bytes on wire (3792 bits), 474 bytes captured (3792 bits) on interface \Device\NPF_{C800D679-685D-488A-951C-D5EAB52D3109}, id 0
Ethernet II, Src: LiteonTe_04:35:1c (3c:95:09:04:35:1c), Dst: zte_b2:c4:d5 (88:d2:74:b2:c4:d5)
Internet Protocol Version 4, Src: 192.168.1.91, Dst: 216.58.214.142
0000 = Version: 4
... 0001 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 468
Identification: 0x0000 (00000000)
0000 88 d2 74 b2 c4 d5 3c 95 09 04 35 1c 08 00 45 00<...5...
0010 01 cc 68 ef 40 00 00 06 1f 70 c0 a8 01 5b d8 3ah@...p...
0020 d6 8e f6 de 00 50 66 b9 a5 89 da 24 22 6e 50 18PF...\$nP
0030 01 00 39 62 00 00 47 45 54 20 2f 6d 61 70 66 699b-GE T /mapf
0040 6c 65 73 2f 6b 6d 6c 2f 70 61 64 64 6c 65 2f 70 les/kml/ paddle/p

Version (p.version), 1 byte(s)

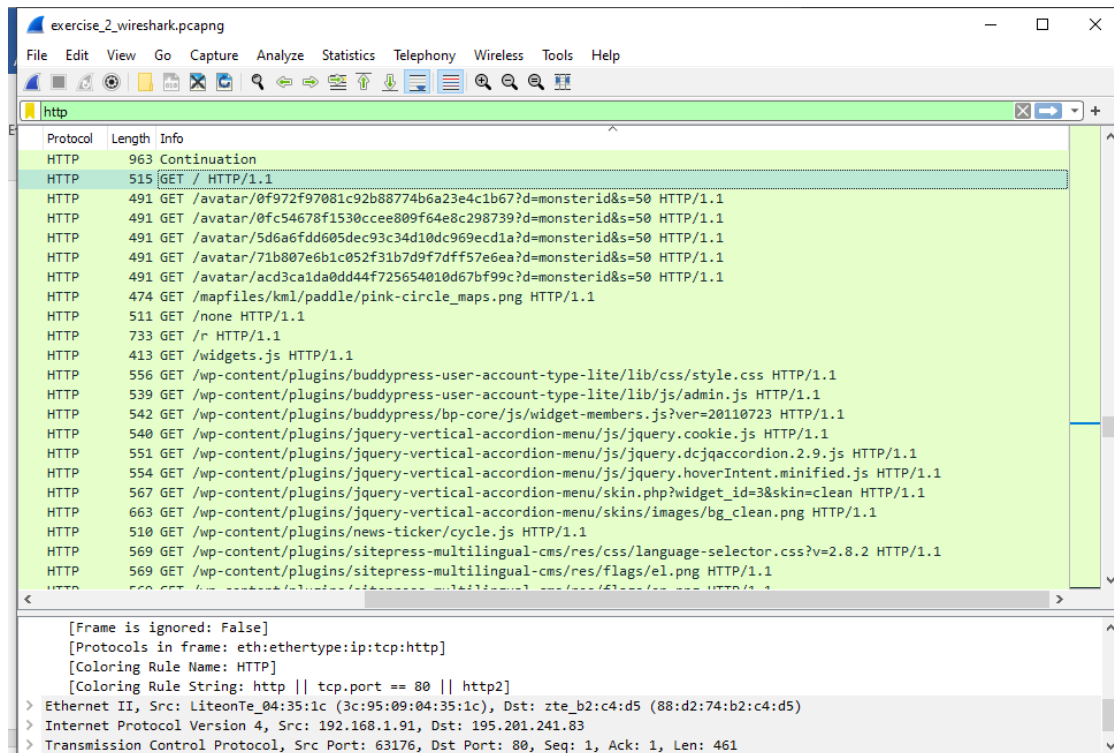
Packets: 4645 · Displayed: 512 (11.0%)

Profile: Default

11:35 μμ
15/1/2021

9. Βάζοντας σε σειρά τις source θύρες που χρησιμοποιήθηκαν από το HTTP πρωτόκολλο παρατηρούμε πως κάθε αριθμός source θύρας αντιστοιχεί σε συγκεκριμένο destination. Το πρωτόκολλο επιπέδου μεταφοράς που χρησιμοποιεί το HTTP είναι το TCP.

10. 76 Πακέτα HTTP περιείχαν GET αίτημα



Οι IP διευθύνσεις είναι τρεις:

- i. 195.201.241.83
- ii. 192.0.73.2
- iii. 216.58.214.142