

## Δίκτυα Επικοινωνιών:

### 2<sup>η</sup> Εργασία:

Γεωργίου Αλέξιος-Λάζαρος 3180027

*DNS flush:*

```
Command Prompt
Microsoft Windows [Version 10.0.18362.900]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Alexis>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

### 1<sup>η</sup> Ερώτηση:

Εφαρμόζουμε το καταλληλο displaying filter (tcp και udp). Στην συνέχεια πατάμε statistics > Capture file properties και βλέπουμε πόσα πακέτα είναι displayed.

Για το tcp: 958

Statistics			
Measurement	Captured	Displayed	Marked
Packets	1422	958 (67.4%)	—
Time span, s	9.727	5.493	—
Average pps	146.2	174.4	—
Average packet size, B	900	1078	—
Bytes	1279383	1032850 (80.7%)	0
Average bytes/s	131k	188k	—
Average bits/s	1052k	1504k	—

Για το udp: 459

Statistics			
Measurement	Captured	Displayed	Marked
Packets	1422	459 (32.3%)	—
Time span, s	9.727	9.013	—
Average pps	146.2	50.9	—
Average packet size, B	900	537	—
Bytes	1279383	246269 (19.2%)	0
Average bytes/s	131k	27k	—
Average bits/s	1052k	218k	—

## 2<sup>η</sup> Ερώτηση:

Wireshark · Endpoints · ergasia2capture.pcapng

Ethernet · 8		IPv4 · 23		IPv6		TCP · 25		UDP · 57	
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes			
IPv4mcast_7f:ff:fa	3	321	0	0	3				
Tp-LinkT_85:96:bc	1	60	1	60	0				
Tp-LinkT_ce:e8:6b	1,414	1278k	631	103k	783				
Tp-LinkT_d0:d1:f8	2	209	2	209	0				
Tp-LinkT_ee:2c:da	1	60	1	60	0				
Sercomm_43:30:80	1,414	1278k	783	1175k	631				
SamsungE_f2:b9:77	4	308	4	308	0				
Broadcast	5	316	0	0	5				

8 διαφορετικές συσκευές endpoints

Smart tv, router, pc

## 3<sup>η</sup> Ερώτηση:

Ethernet · 8	IPv4 · 23	IPv6	TCP · 25	UDP · 57						
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
93.184.220.66	26	31k	16	30k	10	1352	—	—	—	—
104.244.42.200	25	8055	13	5634	12	2421	—	—	—	—
142.250.184.131	17	7797	10	5099	7	2698	—	—	—	—
142.250.184.138	13	7107	7	3945	6	3162	—	—	—	—
142.250.184.142	74	41k	42	32k	32	9263	—	—	—	—
157.240.9.23	44	13k	26	9839	18	3857	—	—	—	—
157.240.9.35	67	45k	42	38k	25	6601	—	—	—	—
172.217.17.170	29	10k	14	6052	15	4931	—	—	—	—
172.217.17.206	73	53k	44	47k	29	6337	—	—	—	—
172.217.17.234	51	20k	27	15k	24	5964	—	—	—	—
172.217.17.238	20	8582	10	4441	10	4141	—	—	—	—
172.217.169.131	24	13k	14	7892	10	6097	—	—	—	—
192.0.73.2	25	5710	11	2528	14	3182	—	—	—	—
192.168.2.1	44	9315	22	7597	22	1718	—	—	—	—
192.168.2.3	4	308	4	308	0	0	—	—	—	—
192.168.2.8	1,412	1278k	630	103k	782	1175k	—	—	—	—
192.168.2.12	1	167	1	167	0	0	—	—	—	—
192.168.2.255	2	154	0	0	2	154	—	—	—	—
195.201.241.83	808	971k	449	942k	359	29k	—	—	—	—
216.58.212.13	29	12k	14	6874	15	6077	—	—	—	—
216.58.212.14	40	15k	20	9542	20	5663	—	—	—	—
216.58.214.142	3	168	1	60	2	108	—	—	—	—
239.255.255.250	3	321	0	0	3	321	—	—	—	—

23 endpoints IPv4 και 0 για IPv6

Δεν ταυτίζονται όλα πλην του IPv4mcast με IP 239.255.255.250. Στο ethernet έχουμε mac addresses ενώ στο IPv4 έχουμε IPs.

## 4<sup>η</sup> Ερώτηση:

No.	Time	Source	Destination	Protocol	Length	Info
4	2.579882	192.168.2.8	192.168.2.1	DNS	76	Standard query 0x27cc A www.book4book.gr
5	2.579882	192.168.2.8	192.168.2.1	DNS	80	Standard query 0x3672 A fonts.googleapis.com
6	2.577214	192.168.2.8	192.168.2.1	DNS	77	Standard query 0x88d7 A fonts.gstatic.com
7	2.588865	192.168.2.8	192.168.2.1	DNS	78	Standard query 0x698e A www.googleapis.com
8	2.778978	192.168.2.8	192.168.2.1	DNS	80	Standard query 0x015a A beacon.gcp.gvt2.com
9	2.779487	192.168.2.8	192.168.2.1	DNS	83	Standard query 0x6829 A safebrowsing.google.com
194	4.695250	192.168.2.8	192.168.2.1	DNS	75	Standard query 0x9471 A maps.google.com
205	4.791958	192.168.2.8	192.168.2.1	DNS	76	Standard query 0xf45 A www.book4book.lk
206	4.791958	192.168.2.8	192.168.2.1	DNS	80	Standard query 0x7656 A www.book4book.com.cy
428	4.877847	192.168.2.8	192.168.2.1	DNS	84	Standard query 0x679f A www.google-analytics.com
1014	5.582488	192.168.2.8	192.168.2.1	DNS	75	Standard query 0x4e68 A www.youtube.com
1024	5.719412	192.168.2.8	192.168.2.1	DNS	80	Standard query 0x9d22 A platform.twitter.com
1025	5.720084	192.168.2.8	192.168.2.1	DNS	71	Standard query 0x8c48 A twitter.com
1031	5.742449	192.168.2.8	192.168.2.1	DNS	76	Standard query 0x65f6 A www.gravatar.com
1106	6.055124	192.168.2.8	192.168.2.1	DNS	79	Standard query 0xf75b A maps.googleapis.com
1107	6.061764	192.168.2.8	192.168.2.1	DNS	75	Standard query 0xe686 A apis.google.com
1117	6.097877	192.168.2.8	192.168.2.1	DNS	83	Standard query 0x533a A syndication.twitter.com
1117	6.134681	192.168.2.8	192.168.2.1	DNS	80	Standard query 0x0548 A connect.facebook.net
1215	6.335748	192.168.2.8	192.168.2.1	DNS	79	Standard query 0x23c9 A accounts.google.com
1273	6.733384	192.168.2.8	192.168.2.1	DNS	76	Standard query 0x1068 A www.facebook.com
1393	7.977883	192.168.2.8	192.168.2.1	DNS	74	Standard query 0x79a7 A www.google.com
1420	8.273179	192.168.2.8	192.168.2.1	DNS	81	Standard query 0x561c A developers.google.com
9	2.598910	192.168.2.1	192.168.2.8	DNS	174	Standard query response 0x698e A www.googleapis.com A 172.217.17.170 A 216.58.206.202 A 172.217.17.202 A 172.217.169.186 A 142.250.184.138 A 172.217.169.138
11	2.612203	192.168.2.1	192.168.2.8	DNS	371	Standard query response 0x3672 A fonts.googleapis.com A 142.250.184.138 NS ns3.google.com NS ns4.google.com NS ns1.google.com NS ns2.google.com A 216.239.32.18 AAAA 2001:4860:4802:32::a
12	2.612203	192.168.2.1	192.168.2.8	DNS	394	Standard query response 0x88d7 A fonts.gstatic.com CNAME gstaticdis11.google.com A 172.217.169.131 NS ns3.google.com NS ns2.google.com NS ns1.google.com NS ns4.google.com A 216.239.32.18
44	2.721881	192.168.2.1	192.168.2.8	DNS	208	Standard query response 0x27cc A www.book4book.gr CNAME book4book.gr A 195.201.241.83 NS ns2.ipdns.gr NS ns1.ipdns.gr A 195.201.241.83 A 95.217.177.141
75	2.789272	192.168.2.1	192.168.2.8	DNS	138	Standard query response 0x015a A beacon.gcp.gvt2.com CNAME beacon-handoff.gcp.gvt2.com A 142.250.184.131
79	2.808466	192.168.2.1	192.168.2.8	DNS	389	Standard query response 0x6829 A safebrowsing.google.com CNAME sb1.google.com A 172.217.17.206 NS ns4.google.com NS ns2.google.com NS ns3.google.com NS ns1.google.com A 216.239.32.18 A
195	4.718565	192.168.2.1	192.168.2.8	DNS	354	Standard query response 0x9471 A maps.google.com A 172.217.17.206 NS ns2.google.com NS ns3.google.com NS ns4.google.com NS ns1.google.com A 216.239.32.18 AAAA 2001:4860:4802:32::a A 216.239.32.18
201	4.798410	192.168.2.1	192.168.2.8	DNS	80	Standard query response 0x7656 No such name A www.book4book.com.cy

Total Length: 42  
Identification: 0x1d6d (53613)  
Flags: 0x00  
Fragment Offset: 0  
Time to Live: 128  
Protocol: UDP (17)  
Header Checksum: 0xe3e7 [validation disabled]  
[Header checksum status: Unverified]  
Source Address: 192.168.2.8  
Destination Address: 192.168.2.1  
User Datagram Protocol, Src Port: 52178, Dst Port: 53  
Domain Name System (query)

Φιλτράρουμε με DNS τα πακέτα, βρίσκουμε το πακέτο για το book4book.gr και βλέπουμε τις 2 θύρες στην περιγραφή του.

Src Port: 52178, Dst Port: 53

## 5<sup>η</sup> Ερώτηση:

Αν περιέχει αίτημα στο DNS server τότε το τοπικό IP μας είναι (192.168.2.8) το source ενώ αν λαμβάνουμε την απάντηση είναι το destination. Τα δύο πακέτα συνδέονται με τα δύο Ports. Στο ένα είναι το 52178 το src και το 53 το dst ενώ στο άλλο πακέτο ανάποδα.

## 6<sup>η</sup> Ερώτηση:

```
> Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF_{C13952AE-03D8-4E64-BB5D-E46CC24E16BF}, id 0
> Ethernet II, Src: Tp-LinkT_ce:e8:6b (50:3e:aa:ce:e8:6b), Dst: Sercomm_43:30:80 (e8:1b:69:43:30:80)
> Internet Protocol Version 4, Src: 192.168.2.8, Dst: 192.168.2.1
> User Datagram Protocol, Src Port: 52178, Dst Port: 53
  Source Port: 52178
  Destination Port: 53
  Length: 42
  Checksum: 0xe032 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 1]
  > [Timestamps]
    UDP payload (34 bytes)
  > Domain Name System (query)
    Transaction ID: 0x27cc
    > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    > Queries
      [Response In: 44]
```

Το flag λέγεται “Authority RRs”, είναι 0 για τα πακέτα μας με το book4book άρα είναι authoritative domain.

```
C:\Users\Alexis>tracert 192.168.2.1

Tracing route to vodafone.station [192.168.2.1]
over a maximum of 30 hops:

  1    5 ms    5 ms    33 ms  vodafone.station [192.168.2.1]

Trace complete.
```

## 7<sup>η</sup> Ερώτηση:

Το όνομα `www.book4book.gr` είναι domain name αφού είναι το ψευδώνυμο (alias) της διεύθυνσης του site.

Η διεύθυνση IP είναι 195.201.241.83

```
C:\Users\Alexis>tracert www.book4book.gr

Tracing route to book4book.gr [195.201.241.83]
over a maximum of 30 hops:

  1    11 ms    4 ms    8 ms    vodafone.station [192.168.2.1]
  2    15 ms    29 ms    27 ms    loopback2004.med01.dsl.hol.gr [62.38.0.170]
  3    13 ms    24 ms    13 ms    62.38.96.150
  4    11 ms    21 ms    14 ms    ae3-100-ucr.ata.cw.net [195.89.103.69]
  5    12 ms    14 ms    14 ms    ae4-ucr1.atm.cw.net [195.2.2.70]
  6    27 ms    29 ms    29 ms    195.2.21.57
  7    43 ms    30 ms    28 ms    ae-11.r01.sofibu01.bg.bb.gin.ntt.net [129.250.66.57]
  8    62 ms    51 ms    47 ms    ae-3.r20.mlanit02.it.bb.gin.ntt.net [129.250.6.203]
  9    51 ms    52 ms    63 ms    ae-0.r21.mlanit02.it.bb.gin.ntt.net [129.250.3.157]
 10    61 ms    60 ms    67 ms    ae-6.r21.frnkge13.de.bb.gin.ntt.net [129.250.3.183]
 11    58 ms    59 ms    67 ms    ae-8.r01.frnkge13.de.bb.gin.ntt.net [129.250.6.51]
 12    56 ms    68 ms    75 ms    213.198.82.130
 13    *        77 ms    117 ms    core23.fsn1.hetzner.com [213.239.252.38]
 14    80 ms    86 ms    76 ms    ex9k1.dc14.fsn1.hetzner.com [213.239.245.82]
 15    70 ms    68 ms    69 ms    ns81.ipdns.gr [195.201.241.83]

Trace complete.
```

## 8<sup>η</sup> Ερώτηση:

tcp && ( ip.dst == 195.201.241.83    ip.src == 195.201.241.83)						
No.	Time	Source	Destination	Protocol	Length	Info
45	2.721619	192.168.2.8	195.201.241.83	TCP	66	56392 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
46	2.721905	192.168.2.8	195.201.241.83	TCP	66	56393 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
70	2.783299	195.201.241.83	192.168.2.8	TCP	66	80 → 56392 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1416 SACK_PERM=1 WS=128
71	2.783358	192.168.2.8	195.201.241.83	TCP	54	56392 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0

Βάζουμε displaying filter για tcp και το ip του book4book να είναι είτε dst είτε src.

```
tcp && ( ip.dst == 195.201.241.83 || ip.src == 195.201.241.83)
```

Στο πρώτο πακέτο (45) στέλνουμε αίτημα σύνδεσης στο book4book.

Το δεύτερο πακέτο (46) στάλθηκε για τον ίδιο σκοπό αλλά σε άλλο port στο οποίο δεν έγινε τελικά σύνδεση.

Στο τρίτο πακέτο (70) το γίνεται το acknowledge από τον υπολογιστή που φιλοξένει το book4book ότι έλαβε το πρώτο πακέτο.

Στο τέταρτο πακέτο (71) στέλνουμε στο book4book ότι λάβαμε το δεύτερο πακέτο (το acknowledge του book4book).

## 9<sup>η</sup> Ερώτηση:

Βάζουμε displaying filter για http και το ip του book4book να είναι είτε dst είτε src.

```
http && ( ip.dst == 195.201.241.83 || ip.src == 195.201.241.83)
```

Τα ports των πακέτων είναι 80, 56392 κατά κύριο λόγο και 56393 στην προσπάθεια σύνδεσης.

▼ Transmission Control Protocol, Src Port: 80, Dst Port: 56392, Seq: 506929, Ack: 708, Len: 1416  
Source Port: 80  
Destination Port: 56392

Το HTTP χρησιμοποιεί TCP πρωτόκολλο επιπέδου μεταφοράς, αφού η ανταλλαγή πακέτων πρέπει να είναι αξιόπιστη.

## 10<sup>η</sup> Ερώτηση:

Time	Source	Destination	Protocol	Length	Info
173 4.678573	192.168.2.8	195.201.241.83	HTTP	730	GET /wp-content/plugins/jquery-vertical-accordion-menu/skin.php?widget_id=3&skin=clean HTTP/1.1
1270 6.785708	192.168.2.8	93.184.220.66	HTTP	409	GET /widgets.js?_1607700809255 HTTP/1.1
1045 5.786362	192.168.2.8	93.184.220.66	HTTP	499	GET /widgets.js HTTP/1.1
1180 5.990999	192.168.2.8	195.201.241.83	HTTP	712	GET /r HTTP/1.1
385 4.826125	192.168.2.8	195.201.241.83	HTTP	718	GET /none HTTP/1.1
1056 5.881245	192.168.2.8	192.0.73.2	HTTP	532	GET /avatar/acd3c0da0dd44f725654010d67bf99c?d=monsterid&s=50 HTTP/1.1
1094 5.951936	192.168.2.8	192.0.73.2	HTTP	532	GET /avatar/71b807e6b1c052f31b7d9f7dfff57e6a?d=monsterid&s=50 HTTP/1.1
1049 5.820317	192.168.2.8	192.0.73.2	HTTP	532	GET /avatar/5d6a6fdd605dec93c34d10dc969ecd1a?d=monsterid&s=50 HTTP/1.1
1092 5.937920	192.168.2.8	192.0.73.2	HTTP	532	GET /avatar/0fc54678f1530ccee809f64e8c298739?d=monsterid&s=50 HTTP/1.1
1088 5.932061	192.168.2.8	192.0.73.2	HTTP	532	GET /avatar/0f972f97081c92b8774b6a23e4c1b67?d=monsterid&s=50 HTTP/1.1
72 2.783509	192.168.2.8	195.201.241.83	HTTP	761	GET / HTTP/1.1

11 πακέτα http get.

Προς

195.201.241.83

93.184.220.66

192.0.73.2

## 11<sup>η</sup> Ερώτηση:

No.	Time	Source	Destination	Protocol	Length	Info
72	2.783509	192.168.2.8	195.201.241.83	HTTP	761	GET / HTTP/1.1
173	4.678573	192.168.2.8	195.201.241.83	HTTP	730	GET /wp-content/plugins/jquery-vertical-accordion-menu/skin.php?widget_id=3&skin=clean HTTP/1.1
283	4.770454	195.201.241.83	192.168.2.8	HTTP	1371	HTTP/1.1 200 OK (text/css)
385	4.826125	192.168.2.8	195.201.241.83	HTTP	718	GET /none HTTP/1.1
514	4.907739	195.201.241.83	192.168.2.8	HTTP	1470	[TCP Previous segment not captured] Continuation
516	4.913794	195.201.241.83	192.168.2.8	HTTP	2886	Continuation
518	4.913893	195.201.241.83	192.168.2.8	HTTP	1470	[TCP Previous segment not captured] Continuation
520	4.914039	195.201.241.83	192.168.2.8	HTTP	1470	Continuation

> Frame 72: 761 bytes on wire (6088 bits), 761 bytes captured (6088 bits) on interface \Device\NPF\_{C13952AE-03D8-4E64-B85D-E46CC24E16BF}, id 0  
> Ethernet II, Src: Tp-LinkT\_ce:e8:6b (50:3e:aa:ce:e8:6b), Dst: Sercomm\_43:30:80 (e8:1b:69:43:30:80)  
> Internet Protocol Version 4, Src: 192.168.2.8, Dst: 195.201.241.83  
> Transmission Control Protocol, Src Port: 56392, Dst Port: 80, Seq: 1, Ack: 1, Len: 707  
▼ Hypertext Transfer Protocol  
> GET / HTTP/1.1\r\n

Έκδοση HTTP1.1 και ο browser και ο server του book4book.

No.	Time	Source	Destination	Protocol	Length	Info
72	2.783509	192.168.2.8	195.201.241.83	HTTP	761	GET / HTTP/1.1
173	4.678573	192.168.2.8	195.201.241.83	HTTP	730	GET /wp-content/plugins/jquery-vertical-accordion-menu/skin.php?widget_id=3&skin=clean HTTP/1.1
283	4.770454	195.201.241.83	192.168.2.8	HTTP	1371	HTTP/1.1 200 OK (text/css)
385	4.826125	192.168.2.8	195.201.241.83	HTTP	718	GET /none HTTP/1.1
514	4.907739	195.201.241.83	192.168.2.8	HTTP	1470	[TCP Previous segment not captured] Continuation
516	4.913794	195.201.241.83	192.168.2.8	HTTP	2886	Continuation
518	4.913893	195.201.241.83	192.168.2.8	HTTP	1470	[TCP Previous segment not captured] Continuation
520	4.914039	195.201.241.83	192.168.2.8	HTTP	1470	Continuation

> Frame 283: 1371 bytes on wire (10968 bits), 1371 bytes captured (10968 bits) on interface \Device\NPF\_{C13952AE-03D8-4E64-B85D-E46CC24E16BF}, id 0  
> Ethernet II, Src: Sercomm\_43:30:80 (e8:1b:69:43:30:80), Dst: Tp-LinkT\_ce:e8:6b (50:3e:aa:ce:e8:6b)  
> Internet Protocol Version 4, Src: 195.201.241.83, Dst: 192.168.2.8  
> Transmission Control Protocol, Src Port: 80, Dst Port: 56393, Seq: 1, Ack: 677, Len: 1317  
▼ 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 Phrases: OK  
Date: Fri, 11 Dec 2020 15:33:31 GMT\r\n  
Server: Apache\r\n

Web server software book4book: Apache