



### Άσκηση 1

Από το Packet Lengths με κατάλληλα filters βρίσκουμε ότι τα πακέτα TCP είναι 946 και UDP 6.

Wireshark · Packet Lengths · diktya2vol2.pcapng

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Packet Lengths	946	1027,19	54	1506	0,0974	100%	0,7400	8,916
0-19	0	-	-	-	0,0000	0,00%	-	-
20-39	0	-	-	-	0,0000	0,00%	-	-
40-79	295	54,89	54	66	0,0304	31,18%	0,2500	9,496
80-159	4	109,50	93	135	0,0004	0,42%	0,0200	8,518
160-319	5	205,40	188	220	0,0005	0,53%	0,0200	8,520
320-639	5	541,20	370	599	0,0005	0,53%	0,0200	8,323
640-1279	10	786,20	641	1175	0,0010	1,06%	0,0300	8,308
1280-2559	627	1504,77	1298	1506	0,0645	66,28%	0,5200	8,806
2560-5119	0	-	-	-	0,0000	0,00%	-	-
5120 and greater	0	-	-	-	0,0000	0,00%	-	-

Display filter: tcp

Copy Save as... Close

Wireshark · Packet Lengths · diktya2vol2.pcapng

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Packet Lengths	6	105,17	76	144	0,0377	100%	0,0400	9,306
0-19	0	-	-	-	0,0000	0,00%	-	-
20-39	0	-	-	-	0,0000	0,00%	-	-
40-79	1	76,00	76	76	0,0063	16,67%	0,0100	9,306
80-159	5	111,00	80	144	0,0314	83,33%	0,0300	9,307
160-319	0	-	-	-	0,0000	0,00%	-	-
320-639	0	-	-	-	0,0000	0,00%	-	-
640-1279	0	-	-	-	0,0000	0,00%	-	-
1280-2559	0	-	-	-	0,0000	0,00%	-	-
2560-5119	0	-	-	-	0,0000	0,00%	-	-
5120 and greater	0	-	-	-	0,0000	0,00%	-	-

Display filter: udp

Copy Save as... Close

### Άσκηση 2

Τα διαφορετικά Endpoints με τα οποία υπάρχει επικοινωνία σε επίπεδο Ethernet είναι 3 και αντιστοιχούν στις συσκευές που επικοινωνεί το δίκτυο μιας και αυτά τα endpoints αναφέρονται σε MAC διευθύνσεις. Η πρώτη διεύθυνση αντιστοιχίζεται σε υπολογιστή, η δεύτερη σε router και η τρίτη είναι η broadcast MAC διεύθυνση του δικτύου Ethernet.

Ethernet · 3	IPv4 · 10	IPv6 · 3	TCP · 20	UDP · 4		
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
74:40:bb:e0:ed:e7	967	973k	303	27k	664	
d4:60:e3:b9:72:80	961	972k	664	946k	297	
ff:ff:ff:ff:ff:ff	6	252	0	0	6	

### Άσκηση 3

Τα διαφορετικά endpoints με τα οποία υπάρχει επικοινωνία σε επίπεδο iP είναι 10 σε IPv4 και 3 σε IPv6.

#### IPv4

5.62.53.133	3	1248	1	595	2	653	—	—	—	—
51.144.113.175	34	20k	17	16k	17	3897	—	—	—	—
65.55.44.109	3	2125	1	773	2	1352	—	—	—	—
116.202.208.24	2	114	1	60	1	54	—	—	—	—
142.250.74.206	1	66	1	66	0	0	—	—	—	—
172.217.18.110	4	830	1	66	3	764	—	—	—	—
172.217.22.110	12	4310	7	1450	5	2860	—	—	—	—
192.168.1.1	6	631	3	391	3	240	—	—	—	—
192.168.1.7	952	972k	296	26k	656	945k	—	—	—	—
195.201.241.83	887	942k	624	926k	263	16k	—	—	—	—

#### IPv6

fe80::1	3	258	2	172	1	86	—	—	—	—
fe80::2dd9:b5ee:d88a:c0d6	2	172	1	86	1	86	—	—	—	—
ff02::1	1	86	0	0	1	86	—	—	—	—

Αυτά τα endpoints δεν ταυτίζονται με τα αντίστοιχα στο επίπεδο του Ethernet αφού αυτά αναφέρονται σε διευθύνσεις iP ενώ στο επίπεδο Ethernet αναφέρονται σε MAC διευθύνσεις. Επίσης το Ethernet αναφέρεται στο layer 2, ενώ οι iPs στο layer 3 του TCP/IP μοντέλου.

#### Άσκηση 4

Οι θύρες (ports) που χρησιμοποιήθηκαν για την ερώτηση από τον υπολογιστή μου προς τον DNS Server:

Source Port	Destination Port
56102	53
53763	
62556	

Οι θύρες (ports) που χρησιμοποιήθηκαν για την απάντηση από τον DNS Server προς τον υπολογιστή μου:

Source Port	Destination Port
53	56102
	53763
	62556

Είναι λογικό να χρησιμοποιεί ο DNS μόνο την θύρα 53, μιας και είναι η default port του.

#### Άσκηση 5

Το πακέτο που περιέχει απάντηση σε ερώτηση καθορίζεται από το γεγονός το destination IP είναι η δική μας διεύθυνση IP, το Source Port είναι το 53 και επίσης αναγράφεται ότι είναι Standard query response.

```
> Frame 741: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface \Device\NPF_{EC2353D6-2D06-4EFA-B9F9-A2FD7A36F825}, id 0
> Ethernet II, Src: Sercomm_b9:72:80 (d4:60:e3:b9:72:80), Dst: HonHaiPr_e0:ed:e7 (74:40:bb:e0:ed:e7)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.7
> User Datagram Protocol, Src Port: 53, Dst Port: 56102
> Domain Name System (response)
```

Αν το πακέτο περιέχει αίτημα, η source IP είναι η δική μας διεύθυνση IP, το Destination Port είναι το 53 και επίσης αναγράφεται στο Info ότι είναι Standard query.

```
> Frame 681: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF_{EC2353D6-2D06-4EFA-B9F9-A2FD7A36F825}, id 0
> Ethernet II, Src: HonHaiPr_e0:ed:e7 (74:40:bb:e0:ed:e7), Dst: Sercomm_b9:72:80 (d4:60:e3:b9:72:80)
> Internet Protocol Version 4, Src: 192.168.1.7, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 56102, Dst Port: 53
> Domain Name System (query)
```

Το πακέτο μιας ερώτησης και μιας απάντησης συνδέονται μέσω του source port και του destination port στην ερώτηση και στην απάντηση αντίστοιχα.

### Άσκηση 6

Υπάρχει flag που μας πληροφορεί αν ο server που μας απαντάει είναι authoritative και για αυτό το domain, δεν είναι.

```
▼ Domain Name System (response)
  Transaction ID: 0x97f9
  ▼ Flags: 0x8183 Standard query response, No such name
    1... .. = Response: Message is a response
    .000 0... .. = Opcode: Standard query (0)
    .... 0... .. = Authoritative: Server is not an authority for domain
```

### Άσκηση 7

Το [www.book4book.gr](http://www.book4book.gr) είναι canonical name, το domain name είναι το book4book.gr. Η ip διεύθυνση είναι η 195.201.241.83

```
C:\Users\Μαρίνα Σαμ>tracert book4book.gr

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

Ως εναλλακτική, μέσω του Wireshark, βρίσκουμε ένα DNS Reply και στην καρτέλα Answer βρίσκουμε την εν λόγω ip.

```
▼ Answers
  > www.book4book.gr: type CNAME, class IN, cname book4book.gr
  > book4book.gr: type A, class IN, addr 195.201.241.83
```

### Άσκηση 8

Η εγκαθίδρυση της σύνδεσης υλοποιείται μέσω του 3-way-handshake.

Βήματα:

1. **[SYN]:** Ο client θέλει να εγκαθιδρύσει σύνδεση με τον server. Στέλνει ένα segment με SYN (Synchronize Sequence Number) σε αυτόν, το οποίο πληροφορεί τον server ότι ο client θέλει να ξεκινήσει την επικοινωνία. Μέσω του SYN δηλώνεται με ποιόν αριθμό ξεκινάει τα segments του client.
2. **[SYN, ACK]:** Ο server απαντάει στο αίτημα του client με ένα σετ από SYN-ACK signal bits. Το ACK(acknowledgement) δηλώνει την απάντηση του server στο segment που έλαβε από τον client και το SYN δηλώνει με ποιόν αριθμό ξεκινάει τα segments του.
3. **[ACK]:** Ο client αναγνωρίζει το απάντηση του server και πλέον εγκαθιδρύουν μια αξιόπιστη σύνδεση μεταξύ τους με την οποία θα ξεκινήσουν την μεταφορά των δεδομένων.

192.168.1.7	216.58.212.173	TCP	66 2470 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
216.58.212.173	192.168.1.7	TCP	66 443 → 2470 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1430 SACK_PERM=1 WS=256
216.58.212.173	192.168.1.7	TCP	66 443 → 2470 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1430 SACK_PERM=1 WS=256

### Για 1<sup>ο</sup> βήμα:

Το sequence number που στέλνει ο client είναι αρχικοποιημένο, άρα είναι το SYN που στέλνει στον server. Παρατηρούμε ότι στην ενότητα Flags, το SYN:set. Τέλος, το SEQ=0. Συνεπώς αυτό επιβεβαιώνει ότι είμαστε στο 1<sup>ο</sup> βήμα του 3-way-handshake.

Transmission Control Protocol, Src Port: 2470, Dst Port: 443, Seq: 0, Len: 0
Source Port: 2470
Destination Port: 443
[Stream index: 2]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 1012642138
[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 .... = Nonce: Not set
...0... .... = Congestion Window Reduced (CWR): Not set
....0... .... = ECN-Echo: Not set
....0... .... = Urgent: Not set
....0... .... = Acknowledgment: Not set
....0... .... = Push: Not set
....0... .... = Reset: Not set
> ....0...1. = Syn: Set
....0...0... = Fin: Not set
[TCP Flags: .....S.]

Για το 2<sup>ο</sup> βήμα:

Το sequence number που στέλνει ο server είναι αρχικοποιημένο, άρα είναι το SYN που στέλνεται στον client, ώστε να γνωρίζει με ποιόν αριθμό θα ξεκινάει τα segments του ο server. Ακόμα το acknowledgement number είναι επίσης αρχικοποιημένο, οπότε δηλώνει response προς το αίτημα του client. Παρατηρούμε ότι στην ενότητα Flags, το SYN:set και το ACK:set. Τέλος, το SEQ=0 και ACK=1. Συνεπώς αυτό επιβεβαιώνει ότι είμαστε στο 2<sup>ο</sup> βήμα του 3-way-handshake.

```
Transmission Control Protocol, Src Port: 443, Dst Port: 2470, Seq: 0, Ack: 1, Len: 0
  Source Port: 443
  Destination Port: 2470
  [Stream index: 2]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 3019902269
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 1012642139
  1000 .... = Header Length: 32 bytes (8)
  Flags: 0x012 (SYN, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    .... 0... = Congestion Window Reduced (CWR): 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
```

### Για το 3<sup>ο</sup> βήμα:

Το sequence number είναι ίδιο με το αρχικό που έστειλε ο client. Αυτό είναι λογικό μιας και με αυτό αναγνωρίζεται ότι το segment που στέλνει ο server αντιστοιχεί στον client. Το acknowledgement number είναι αρχικοποιημένο, άρα δηλώνει response του πελάτη στον server. Το γεγονός αυτό επαληθεύει την επιτυχία εγκαθίδρυσης της σύνδεσης. Παρατηρούμε ότι στην ενότητα Flags, το ACK: set. Τέλος, το SEQ=1 και ACK=1. Συνεπώς αυτό επιβεβαιώνει ότι είμαστε στο 3<sup>ο</sup> βήμα του 3-way-handshake.

```
▼ Transmission Control Protocol, Src Port: 2470, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
  Source Port: 2470
  Destination Port: 443
  [Stream index: 2]
  [TCP Segment Len: 0]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 1012642139
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 3019902270
  0101 .... = Header Length: 20 bytes (5)
  ▼ Flags: 0x010 (ACK)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    .... 0... = Congestion Window Reduced (CWR): 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
```

### Άσκηση 9

#### Για GET:

Source Port	Destination Port
56102	80
53763	
62556	

#### Για !GET:

Source Port	Destination Port
80	56102
	53763
	62556

Είναι αναμενόμενο από τον HTTP server να χρησιμοποιεί το port 80 μιας και είναι το default port του. Εμείς χρησιμοποιούμε τα ports 56102,53763,62556 και η επικοινωνία γίνεται μέσω

αυτών των θυρών. Το πρωτόκολλο HTTP χρησιμοποιείται από το επίπεδο εφαρμογών του TCP/IP μοντέλου.

### Άσκηση 10

Ο browser έστειλε 4 HTTP GET Requests προς την IP του [www.book4book.gr](http://www.book4book.gr) [195.201.241.83]

33	6.064308	192.168.1.7	195.201.241.83	HTTP	701 GET / HTTP/1.1
102	8.144240	192.168.1.7	195.201.241.83	HTTP	670 GET /wp-content/plugins/jquery-vertical-accordion-menu/skin.php?widget_id=3&skin=clean HTTP/1.1
101	8.135203	192.168.1.7	195.201.241.83	HTTP	737 GET /wp-content/plugins/sitepress-multilingual-cms/res/css/language-selector.css?v=2.8.2 HTTP/1.1
159	8.404606	192.168.1.7	195.201.241.83	HTTP	737 GET /wp-content/plugins/sitepress-multilingual-cms/res/css/language-selector.css?v=2.8.2 HTTP/1.1

### Άσκηση 11

Η έκδοση του HTTP που τρέχει ο browser μου είναι η HTTP/1.1

```
Hypertext Transfer Protocol
> GET / HTTP/1.1\r\n
```

Η έκδοση που τρέχει ο server είναι επίσης η HTTP/1.1 και το λογισμικό που μας απάντησε στο αίτημα είναι ο Apache.

```
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Mon, 14 Dec 2020 16:56:57 GMT\r\n
    Server: Apache\r\n
```