Εργαστηριακή Άσκηση 1
Αναλυτής Πρωτοκόλλων Wireshark

ΟΝΟΜΑΤΕΠΩΝΥΜΟ: ΚΟΥΣΤΕΝΗΣ ΧΡΙΣΤΟΣ (03120227)

ΟΜΑΔΑ: 3

ΟΝΟΜΑ PC/ΛΣ: LAPTOP-TK5Q3T95 /WINDOWS 11

ΗΜΕΡΟΜΗΝΙΑ: 10/10/2023(ΑΝΑΠΛΗΡΩΣΗ)

ΔΙΕΥΘΥΝΣΗ IP: 147.102.203.51/192.168.1.250

ΔΙΕΥΘΥΝΣΗ MAC: B4-B5-B6-79-4B-09

Σημείωση: Το 1ο και 2ο μέρος(εκτός των 2.13, 2.14) της άσκησης έγιναν στο δίκτυο της σχολής ενώ τα υπόλοιπα ερωτήματα στο τοπικό δίκτυο της οικίας μου. Εκεί οφείλονται οι διαφορετικές IP addresses της ίδιας συσκευής που χρησιμοποιώ.

1.1 Την ονομασία της κάρτας δικτύου (network adapter) μέσω της οποίας συνδέστε στο διαδίκτυο.

“Settings” -> “Network & Internet” -> “eduroam” ->

Description: MediaTek Wi-Fi 6 MT7921 Wireless LAN Card

1.2 Το είδος της σύνδεσης, ενσύρματη (Ethernet) ή ασύρματη (WiFi).

Wifi

1.3 Την ταχύτητα σύνδεσης αυτής σε Mbps.

“Settings” -> “Network & Internet” -> “eduroam” ->
Link speed(Receive/Transmit) : 300/300 (Mbps)

1.4 Τη διεύθυνση υπο-στρώματος MAC σε δεκαεξαδική μορφή. [Συμπληρώστε με την πληροφορία αυτή και το αντίστοιχο πεδίο στην επικεφαλίδα του φύλλου απαντήσεων.]

“Settings” -> “Network & Internet” -> “eduroam” ->

Physical address(Mac) : B4-B5-B6-79-4B-09

1.5 Τη διεύθυνση IPv4 της διεπαφής Ethernet ή WiFi του υπολογιστή σας. [Συμπληρώστε με την πληροφορία αυτή και το αντίστοιχο πεδίο στην επικεφαλίδα του φύλλου απαντήσεων.]

"Settings" -> "Network & Internet" -> "eduroam" ->

IPv4 address: 147.102.203.51

1.6 Εάν έχει ορισθεί, τη διεύθυνση IPv6 της διεπαφής Ethernet ή WiFi του υπολογιστή σας;
"Settings" -> "Network & Internet" -> "eduroam" ->

IPv6 address: 2001:648:2000:e9:363d:34dc:bfe2:df77

1.7 Τη διεύθυνση IPv4/IPv6 του εξυπηρετητή DNS.

8.8.8.8(Primary), 8.8.4.4(Secondary) /

2001:4860:4860::8888(Primary), 2001:4860:4860::8844 (Secondary)

1.8 Τη διεύθυνση IPv4/IPv6 της προκαθορισμένης πύλης (default gateway/route).
Win->type "control panel"-> click "Control Panel" -> "Network and Internet" ->
"Network and Sharing Center"-> Click "wifi eduroam" -> "Details"

IPv4 Default Gateway: 147.102.200.200

IPv6 Default Gateway: fe80::aec:f5ff:fed0:d91d%22

2.1 Το όνομα του υπολογιστή σας. [Συμπληρώστε το όνομα μαζί με το είδος λειτουργικού συστήματος το αντίστοιχο πεδίο της επικεφαλίδας του φύλλου απαντήσεων.]
Command: "**hostname**".

LAPTOP-TK5Q3T95

2.2 Τα ονόματα των καρτών δικτύου (φυσικών και/ή εικονικών) που διαθέτει ο υπολογιστής σας.
Command: "**ipconfig /all**".

Ethernet(Physical) : Realtek PCIe GbE Family Controller

Wireless LAN adapter Local Area Connection* 1 (Virtual) : Microsoft Wi-Fi Direct Virtual Adapter

Wireless LAN adapter Local Area Connection* 2(Virtual) : Microsoft Wi-Fi Direct Virtual Adapter

Wireless LAN adapter Wi-Fi(Physical) : MediaTek Wi-Fi 6 MT7921 Wireless LAN Card

2.3 Τη διεύθυνση υπο-στρώματος MAC της κάρτας δικτύου μέσω της οποίας συνδέστε στο διαδίκτυο.
Command: "**ipconfig /all**".

Physical address: B0-DC-0B-98-9C-3D

2.4 Την ταχύτητα σύνδεσης αυτής σε Mbps.

Command: wmic nic where netEnabled=true get name, speed

Name	Speed
MediaTek Wi-Fi 6 MT7921 Wireless LAN Card	300000000

Δηλαδή, 300 Mbps.

2.5 Τη διεύθυνση IPv4 της διεπαφής Ethernet ή WiFi του υπολογιστή σας.
Command: **“ipconfig /all”**.

IPv4 Address: 147.102.203.51

2.6 Τη μάσκα υποδικτύου και χωρίς την εκτέλεση επιπλέον εντολών:

Command: **“ipconfig /all”**.

Subnet Mask : 255.255.252.0

i. το μέγεθος σε bit του τμήματος δικτύου της διεύθυνσης IPv4 του υπολογιστή σας, και

255_{10} -> 11111111_2

252_{10} -> 11111100_2

Άρα το subnet mask θα κρατήσει τα πρώτα 22 bits.

ii. τη διεύθυνση του υποδικτύου.

11001011(=203_{10}) AND 11111100(=252_{10}) = 11001000_{10} = 200_{10}

Προφανώς, η πράξη AND διατηρεί ίδια τα κομμάτια του mask με 255_{10} = 11111111_2 και απαλοίφει λόγω των μηδενικών το τελευταίο δεκαδικό μέρος του host.

Subnet address : 147.102.200.0

2.7 Εάν έχει ορισθεί, τη διεύθυνση IPv6 της διεπαφής Ethernet ή WiFi του υπολογιστή σας.

Command: **“ipconfig /all”**.

IPv6 Address : 2001:648:2000:e9:363d:34dc:bfe2:df77

2.8 Τη διεύθυνση IPv4/IPv6 της προκαθορισμένης πύλης (default gateway). [Υπόδειξη: Στο οικιακό περιβάλλον προκαθορισμένη πύλη είναι ο δρομολογητής (router).]

Command: **"ipconfig /all"**.

Default Gateway : 147.102.200.200 / fe80::aec:f5ff:fed0:d91d%22

2.9 Τη διεύθυνση IPv4/IPv6 των εξυπηρετητών DNS.

Command: **"ipconfig /all"**.

8.8.8.8(Primary), 8.8.4.4(Secondary) /

2001:4860:4860::8888(Primary), 2001:4860:4860::8844 (Secondary)

2.10 Τη διεύθυνση IPv4 του εξυπηρετητή DHCP. [Υπόδειξη: Στο οικιακό περιβάλλον τυπικά ταυτίζεται με τον δρομολογητή.]

Command: **"ipconfig /all"**.

DHCP Server : 147.102.236.230

2.11 Τον αριθμό πλαισίων Ethernet (πακέτων) και το πλήθος byte που έστειλε και έλαβε η κάρτα δικτύου του υπολογιστή σας.

Command : "netstat -e"

	Received	Sent
Bytes	2906707384	158650200
Unicast packets	1180736	599768
Non-unicast packets	29106280	119976
Discards	0	0
Errors	0	0
Unknown protocols	0	

2.12 Τον αριθμό πακέτων IPv4 που έστειλε και έλαβε η κάρτα δικτύου του υπολογιστής σας.

Command : **netstat -e -s**

Packets Received = 2420534

```
Output Requests                    = 78209
```

2.13 Τον αριθμό εγκατεστημένων (established) συνδέσεων TCP του υπολογιστή σας με άλλους υπολογιστές. [Υπόδειξη. Η διεύθυνση 127.0.0.1 είναι ο ίδιος ο υπολογιστής σας.]

```
Command : netstat -n
```

Αφαιρέσαμε από τη λίστα τις not established connections και αυτές που είχανε τη local address διαφορετική του 127.0.0.1.

1.	TCP	192.168.1.250:54557	23.102.0.171:443	ESTABLISHED
2.	TCP	192.168.1.250:54558	192.168.1.190:8009	ESTABLISHED
3.	TCP	192.168.1.250:54559	192.168.1.90:8009	ESTABLISHED
4.	TCP	192.168.1.250:54589	35.186.224.47:443	ESTABLISHED
5.	TCP	192.168.1.250:54593	34.107.221.82:80	ESTABLISHED
6.	TCP	192.168.1.250:54594	34.107.221.82:80	ESTABLISHED
7.	TCP	192.168.1.250:54597	34.107.141.31:443	ESTABLISHED
8.	TCP	192.168.1.250:54603	104.199.65.124:443	ESTABLISHED
9.	TCP	192.168.1.250:54605	35.186.227.140:443	ESTABLISHED
10.	TCP	192.168.1.250:54606	192.229.221.95:80	ESTABLISHED
11.	TCP	192.168.1.250:54608	34.117.65.55:443	ESTABLISHED
12.	TCP	192.168.1.250:54609	40.79.150.121:443	ESTABLISHED
13.	TCP	192.168.1.250:54610	34.117.65.55:443	ESTABLISHED
14.	TCP	192.168.1.250:54611	34.117.14.220:443	ESTABLISHED
15.	TCP	192.168.1.250:54645	20.90.153.243:443	ESTABLISHED
16.	TCP	192.168.1.250:54651	192.168.1.90:8009	ESTABLISHED
17.	TCP	192.168.1.250:54655	20.54.232.160:443	ESTABLISHED
18.	TCP	192.168.1.250:54656	20.54.232.160:443	ESTABLISHED
19.	TCP	192.168.1.250:54659	192.168.1.190:8008	ESTABLISHED
20.	TCP	192.168.1.250:54660	192.168.1.90:8008	ESTABLISHED
21.	TCP	192.168.1.250:54662	192.168.1.190:8008	ESTABLISHED
22.	TCP	192.168.1.250:54663	192.168.1.90:8008	ESTABLISHED
23.	TCP	192.168.1.250:54667	104.122.24.86:443	ESTABLISHED
24.	TCP	192.168.1.250:54670	40.118.94.234:443	ESTABLISHED
25.	TCP	192.168.1.250:54673	192.168.1.190:8009	ESTABLISHED
26.	TCP	192.168.1.250:54679	20.103.143.137:443	ESTABLISHED
27.	TCP	192.168.1.250:54684	20.189.173.10:443	ESTABLISHED
28.	TCP	192.168.1.250:54690	13.107.42.12:443	ESTABLISHED
29.	TCP	192.168.1.250:54693	20.60.58.161:443	ESTABLISHED
30.	TCP	192.168.1.250:54707	192.168.1.190:9080	ESTABLISHED
31.	TCP	192.168.1.250:54711	192.168.1.90:9080	ESTABLISHED
32.	TCP	192.168.1.250:54735	20.90.152.133:443	ESTABLISHED
33.	TCP	192.168.1.250:54736	34.117.237.239:443	ESTABLISHED
34.	TCP	192.168.1.250:54737	34.120.208.123:443	ESTABLISHED
35.	TCP	192.168.1.250:54739	44.214.229.86:443	ESTABLISHED
36.	TCP	192.168.1.250:54740	13.107.42.12:443	ESTABLISHED
37.	TCP	192.168.1.250:54741	13.107.42.12:443	ESTABLISHED
38.	TCP	[::1]:5426	[::1]:54564	ESTABLISHED
39.	TCP	[::1]:5426	[::1]:54565	ESTABLISHED

```
40. TCP    [::1]:5426             [::1]:54566            ESTABLISHED
41. TCP    [::1]:5426             [::1]:54567            ESTABLISHED
42. TCP    [::1]:5426             [::1]:54568            ESTABLISHED
43. TCP    [::1]:5426             [::1]:54590            ESTABLISHED
44. TCP    [::1]:5426             [::1]:54591            ESTABLISHED
45. TCP    [::1]:5426             [::1]:54592            ESTABLISHED
46. TCP    [::1]:5426             [::1]:54721            ESTABLISHED
47. TCP    [::1]:5426             [::1]:54722            ESTABLISHED
48. TCP    [::1]:5426             [::1]:54723            ESTABLISHED
49. TCP    [::1]:5426             [::1]:54724            ESTABLISHED
50. TCP    [::1]:5426             [::1]:54725            ESTABLISHED
51. TCP    [::1]:5426             [::1]:54726            ESTABLISHED
52. TCP    [::1]:5426             [::1]:54727            ESTABLISHED
53. TCP    [::1]:5426             [::1]:54728            ESTABLISHED
54. TCP    [::1]:5426             [::1]:54729            ESTABLISHED
55. TCP    [::1]:5426             [::1]:54730            ESTABLISHED
56. TCP    [::1]:5426             [::1]:54731            ESTABLISHED
57. TCP    [::1]:5426             [::1]:54732            ESTABLISHED
58. TCP    [::1]:54564            [::1]:5426             ESTABLISHED
59. TCP    [::1]:54565            [::1]:5426             ESTABLISHED
60. TCP    [::1]:54566            [::1]:5426             ESTABLISHED
61. TCP    [::1]:54567            [::1]:5426             ESTABLISHED
62. TCP    [::1]:54568            [::1]:5426             ESTABLISHED
63. TCP    [::1]:54590            [::1]:5426             ESTABLISHED
64. TCP    [::1]:54591            [::1]:5426             ESTABLISHED
65. TCP    [::1]:54592            [::1]:5426             ESTABLISHED
66. TCP    [::1]:54721            [::1]:5426             ESTABLISHED
67. TCP    [::1]:54722            [::1]:5426             ESTABLISHED
68. TCP    [::1]:54723            [::1]:5426             ESTABLISHED
69. TCP    [::1]:54724            [::1]:5426             ESTABLISHED
70. TCP    [::1]:54725            [::1]:5426             ESTABLISHED
71. TCP    [::1]:54726            [::1]:5426             ESTABLISHED
72. TCP    [::1]:54727            [::1]:5426             ESTABLISHED
73. TCP    [::1]:54728            [::1]:5426             ESTABLISHED
74. TCP    [::1]:54729            [::1]:5426             ESTABLISHED
75. TCP    [::1]:54730            [::1]:5426             ESTABLISHED
76. TCP    [::1]:54731            [::1]:5426             ESTABLISHED
77. TCP    [::1]:54732            [::1]:5426             ESTABLISHED
78. TCP    [2a02:587:460d:500:9510:6e7c:4a27:b25d]:54595  [2600:1901:0:38d7::]:80
    ESTABLISHED
79. TCP    [2a02:587:460d:500:9510:6e7c:4a27:b25d]:54601
    [2a02:26f0:c000:295::21cc]:80  ESTABLISHED
80. TCP    [2a02:587:460d:500:9510:6e7c:4a27:b25d]:54646  [2600:1901:1:c36::]:443
    ESTABLISHED
81. TCP    [2a02:587:460d:500:9510:6e7c:4a27:b25d]:54647  [2600:1901:0:524d::]:443
    ESTABLISHED
```

82. TCP [2a02:587:460d:500:9510:6e7c:4a27:b25d]:54650 [2600:1901:1:5ca::]:443 ESTABLISHED
83. TCP [2a02:587:460d:500:9510:6e7c:4a27:b25d]:54653 [2600:1901:1:a98::]:443 ESTABLISHED
84. TCP [2a02:587:460d:500:9510:6e7c:4a27:b25d]:54676 [2a02:26f0:3500:589::52c]:443 ESTABLISHED
85. TCP [2a02:587:460d:500:9510:6e7c:4a27:b25d]:54677 [2620:1ec:42::132]:443 ESTABLISHED
86. TCP [2a02:587:460d:500:9510:6e7c:4a27:b25d]:54680 [2603:1026:c0d:807::2]:443 ESTABLISHED
87. TCP [2a02:587:460d:500:9510:6e7c:4a27:b25d]:54682 [2620:1ec:42::132]:443 ESTABLISHED
88. TCP [2a02:587:460d:500:9510:6e7c:4a27:b25d]:54769 [2606:4700:4400::6812:28cd]:443 ESTABLISHED
89. TCP [2a02:587:460d:500:9510:6e7c:4a27:b25d]:54779 [2a02:582:a00::d4cd:7e22]:80 ESTABLISHED
90. TCP [2a02:587:460d:500:9510:6e7c:4a27:b25d]:54780 [2a02:582:a00::d4cd:7e22]:80 ESTABLISHED
91. TCP [fe80::4662:2891:4015:3485%22]:54768 [fe80::cad9:d2ff:fee6:2a48%22]:443 ESTABLISHED
92. TCP [fe80::4662:2891:4015:3485%22]:54770 [fe80::cad9:d2ff:fee6:2a48%22]:443 ESTABLISHED

92 Established connections(77 IPv4 & 15 IPv6)

2.14 Για δύο από τις παραπάνω συνδέσεις TCP, τις θύρες πηγής και προορισμού.

1.54558 (θύρα πηγής), 8009 (θύρα προορισμού)

2.54559 (θύρα πηγής), 8009 (θύρα προορισμού)

(Σημείωση υπογραμμίστηκαν στο παραπάνω ερώτημα)

3.1 Καταγράψτε τα διαφορετικά πρωτόκολλα που εμφανίζονται στη λίστα.

Σε αλφαβητική σειρά τα διαφορετικά πρωτόκολλα είναι:

- ARP
- HTTP
- ICMPv6
- IGMPv3
- MDNS
- SNMP
- SSDP
- TCP
- TLSv1.2
- UDP

Για τον εξυπηρετητή ιστού edu-dy.cn.ntua.gr είναι μόνο TCP και HTTP όπως διαπιστώνεται έπειτα από εφαρμογή του φίλτρου ip.addr==147.102.40.15.

3.2 Ποια είναι η διεύθυνση MAC του υπολογιστή σας σε δεκαεξαδική μορφή;

B4-B5-B6-79-4B-09

3.3 Ποιος είναι ο κατασκευαστής της κάρτας δικτύου όπως προκύπτει από τις επικεφαλίδες του πλαισίου Ethernet; [Υπόδειξη: Βεβαιωθείτε ότι η επιλογή Resolve Physical Addresses στο μενού View-> Name Resolution είναι ενεργοποιημένη.]

CHONGQING FUGUI ELECTRONICS CO.,LTD.

3.4 Ποια είναι η διεύθυνση IPv4 του υπολογιστή σας;
Internet Protocol Version 4 -> **Source Address: 192.168.1.250**

3.5 Ποια είναι η διεύθυνση IPv4 του edu-dy.cn.ntua.gr;
Internet Protocol Version 4 -> **Destination Address: 147.102.40.15**

3.6 Ποια είναι η σύνταξη του φίλτρου που εμφανίζεται τώρα στο πεδίο του φίλτρου απεικόνισης;

tcp.stream eq 5

3.7 Με βάση τα αποτελέσματα της προηγούμενης καταγραφής βρείτε:

i. τον τύπο του εξυπηρετητή ιστού που φιλοξενεί τη σελίδα που επισκεφθήκατε,

Apache/2.2.22

ii. τον τίτλο και το αντίστοιχο HTML tag της σελίδας που επισκεφθήκατε,

<title>CN Lab1</title>

iii. σε ποιο σημείο του παραθύρου του φυλλομετρητή εμφανίζεται αυτός ο τίτλος;
Πάνω στο label της συγκεκριμένης καρτέλας

3.8 Με εφαρμογή κατάλληλου φίλτρου εμφανίστε τώρα μόνο τα μηνύματα HTTP με τον edu-dy.cn.ntua.gr. Ποια είναι η σύνταξή του; [Υπόδειξη: Θα πρέπει να σχηματίσετε μια έκφραση με τον λογικό τελεστή ΚΑΙ (and ή &&) εμπλέκοντας τη διεύθυνση IP του edu-dy.cn.ntua.gr.]

ip.addr == 147.102.40.15 && http

3.9 Πόσα μηνύματα HTTP στάλθηκαν και πόσα λήφθηκαν;

2 Received(192.168.1.250 -> 147.102.40.15)

2 Sent(147.102.40.15 -> 192.168.1.250)

3.10 Πόσος χρόνος πέρασε από τη στιγμή που στάλθηκε το πρώτο αίτημα GET μέχρι να ληφθεί η απόκριση 200 OK; [Υπόδειξη: Από το μενού View επιλέξτε Time Display Format Seconds Since Previous Displayed Packet.]

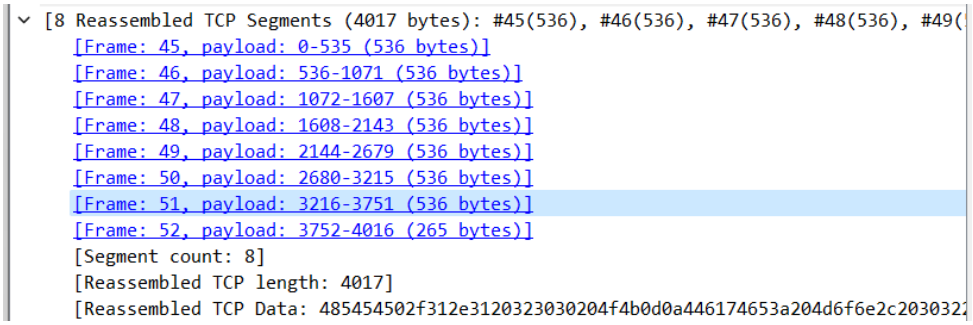
0.009910 seconds

33	0.000163	192.168.1.250	147.102.40.15	HTTP	417	GET / HTTP/1.1
34	0.009910	147.102.40.15	192.168.1.250	HTTP	587	HTTP/1.1 200 OK (text/html)

3.11 Πόσα πακέτα χρειάστηκαν για την ολοκλήρωση της μετάδοσης; Καταγράψτε τους αύξοντες αριθμούς τους.

Οι αύξοντες αριθμοί των πακέτων είναι:

45
46
47
48
49
50
51
52



Άρα απαιτούνται 8 πλαίσια όπου το τελευταίο στέλνει την επιβεβαίωση 200 OK και είναι τύπου http ενώ τα άλλα είναι τύπου tcp.

3.12 Με εφαρμογή κατάλληλου φίλτρου εμφανίστε μόνο τεμάχια TCP. Ποια είναι η σύνταξή του;

ip.addr == 147.102.40.15 && tcp

3.13 .Εντοπίστε το πρώτο πακέτο (τεμάχιο TCP) της μετάδοσης για το κατέβασμα της εικόνας favicon.ico, Πόσος χρόνος πέρασε μέχρι να ληφθεί το πρώτο εξ αυτών, πόσος από την προηγούμενη στιγμή μέχρι να ολοκληρωθεί η μετάδοση των επόμενων και πόσος για να ολοκληρωθεί η απόκριση στο αίτημα GET;

- 0.010853 seconds μετά το αίτημα GET για να ληφθεί το πρώτο πακέτο.
- 0.001132 seconds μεταξύ της στιγμής που φτάνει το πρώτο και της στιγμής που φτάνει το τελευταίο.
- 0.001132 + 0.010853 = 0.011985 seconds για να ολοκληρωθεί η απαίτηση στο αίτημα GET.

3.14.Συγκρίνατε αυτούς χρόνους Service Time, Response Spread και Application PDU (APDU) Response Time με αυτούς που καταγράψατε προηγουμένως.

[Service Time: 0.010853 seconds]

[Rsp Spread: 0.001132 seconds]

[APDU Rsp Time: 0.011985 seconds]

Άρα ταυτίζονται

3.15.Θέλετε τώρα να δείτε μόνο τα μηνύματα HTTP που έστειλε ο υπολογιστής σας. Ποια είναι η σύνταξή του;

ip.src==192.168.1.250 and http