Ονοματεπώνυμο: ΔΗΜΗΤΡΙΟΣ ΓΕΩΡΓΟΥΣΗΣ	ΑΜ: 03119005	Ομάδα: 4
Όνομα PC/ΛΣ: LAPTOP-R71DG51G / WINDOWS 10 HOME		Ημερομηνία: 08/10/2022
Διεύθυνση IP: 192.168.2.11	Διεύθυνση MAC: 10-63-C8-94-47-9D	

Άσκηση 1:

Ανοίγουμε το menu στο taskbar που δείχνει το εικονίδιο της σύνδεσης στο διαδίκτυο και πάμε στα properties. Παίρνουμε τα παρακάτω δεδομένα:

SSID:	VODAFONE_5G_5108
Protocol:	Wi-Fi 5 (802.11ac)
Security type:	WPA2-Personal
Network band:	5 GHz
Network channel:	36
Link speed (Receive/Transmit):	866/433 (Mbps)
Link-local IPv6 address:	fe80::bc8d:87f8:e810:3db6%11
IPv4 address:	192.168.2.11
IPv4 DNS servers:	192.168.2.1
Manufacturer:	Qualcomm Atheros Communications Inc.
Description:	Qualcomm Atheros QCA9377 Wireless Network Adapter
Driver version:	12.0.0.929
Physical address (MAC):	10-63-C8-94-47-9D

1.1: Ονομασία κάρτας δικτύου μέσω της οποίας συνδέομαι στο διαδίκτυο
Qualcomm Atheros QCA9377 Wireless Network Adapter
1.2: Το είδος της σύνδεσης: Η σύνδεση είναι ασύρματη (Wi-Fi)
1.3: Η σύνδεση αυτή έχει ταχύτητα 866(Receive)/433(Transmit) Mbps
1.4: MAC Address: 10-63-C8-94-47-9D
1.5: IPv4 του Wi-Fi: 192.168.2.11
1.6: IPv6: fe80::bc8d:87f8:e810:3db6%11

Τώρα πάμε στον υπολογιστή μας στις εξής ρυθμίσεις
"Control Panel\All Control Panel Items\Network and Sharing Center" και πατάμε πάνω στο connection που αντιστοιχεί στο παραπάνω SSID. Έπειτα διαλέγουμε details και έχουμε τα παρακάτω:

1.7: IPv4 DNS: 192.168.2.1
IPv6 DNS: δεν έχει
1.8: IPv4 Default Gateway: 192.168.2.1
IPv6 Default Gateway: δεν έχει

Άσκηση 2:

Χρησιμοποιούμε το windows powershell και το command prompt για τα παρακάτω.

2.1: Όνομα του υπολογιστή μου: LAPTOP-R71DG51G

Βρέθηκε με την εντολή “hostname” στο powershell.

2.2: Τα ονόματα των καρτών δικτύου που διαθέτει ο υπολογιστής μου:

Realtek PCIe GbE Family Controller (Ethernet adapter Ethernet)
Microsoft Wi-Fi Direct Virtual Adapter #3 (Wireless LAN adapter Local connection* 1)
Microsoft Wi-Fi Direct Virtual Adapter #4 (Wireless LAN adapter Local connection* 2)
Qualcomm Atheros QCA9377 Wireless Network Adapter (Wireless LAN adapter Wi-Fi)

Η τελευταία κάρτα δικτύου είναι μάλιστα αυτή που είναι χρησιμοποιούμε κατά τη σύνταξη αυτής της αναφοράς.
Τα αποτελέσματα του 2.2 ερωτήματος βρέθηκαν με την εντολή “ipconfig/all” στο command prompt.

2.3: MAC Address: 10-63-C8-94-47-9D

Η MAC Address βρέθηκε από το πεδίο physical Address του μόνο adapter που δεν έχει disconnected στο πεδίο Media State και είναι, δηλαδή, η κάρτα δικτύου που χρησιμοποιεί ο υπολογιστής αυτή τη στιγμή. Τα δεδομένα τα παίρνουμε από την ίδια εντολή με το ερώτημα 2.2.

2.4: Ταχύτητα αυτής της σύνδεσης σε Mbps: 433.3 Mbps

Το παραπάνω αποτέλεσμα το παίρνουμε τρέχοντας την εντολή
“Get-NetAdapter | where Status -eq "Up" | select InterfaceDescription, LinkSpeed” στο Windows Powershell.

Για τα 2.5 έως 2.10 χρησιμοποιούμε τα αποτελέσματα της εντολής “ipconfig/all” που τρέξαμε νωρίτερα.

2.5: IPv4 Wi-Fi: 192.168.2.11

2.6: Μάσκα υποδικτύου: 255.255.255.0

2.6.i: Το τμήμα δικτύου της διεύθυνσης είναι ουσιαστικά οι συνεχόμενοι άσσοι από το MSB προς το LSB της μάσκας, αν την αναπαραστούμε σε bits. Η μάσκα μας έχει άσσους στα πρώτα 3 byte άρα το τμήμα δικτύου της διεύθυνσης είναι 24 bit.

2.6.ii: Διεύθυνση υποδικτύου: 192.168.2.0

Για να πάρουμε αυτή τη διεύθυνση κάνουμε λογικό AND της μάσκας με την αρχική διεύθυνση.

2.7: IPv6: fe80::bc8d:87f8:e810:3db6%11 (Link-local)

2.8: IPv4 Default Gateway: 192.168.2.1
IPv6 Default Gateway: Δεν έχει

2.9: IPv4 DNS: 192.168.2.1
IPv6 DNS: δεν έχει

2.10: IPv4 DHCP: 192.168.2.1

2.11:

Πλήθος πλαισίων που στάλθηκαν:	51583 + 7196	(unicast + non-unicast packets)
Πλήθος πλαισίων που λάβαμε:	59206 + 0	(unicast + non-unicast packets)
Πλήθος byte που στάλθηκαν:	14683424	
Πλήθος byte που λάβαμε:	49374808	

Για το ερώτημα αυτό χρησιμοποιήσαμε την εντολή “netstat -e”.

2.12:

IPv4 packets sent:	8797 (Output Requests)
IPv4 packets received:	8216

Χρησιμοποιήσαμε την εντολή “netstat -s -p -IP”.

2.13: Πλήθος εγκατεστημένων συνδέσεων TCP του υπολογιστή μου με άλλους υπολογιστές.

Τρέχουμε την εντολή “netstat -n -p TCP”.

Index	Proto	Local Address	Foreign Address	State
1	TCP	127.0.0.1:55771	127.0.0.1:55772	ESTABLISHED
2	TCP	127.0.0.1:55772	127.0.0.1:55771	ESTABLISHED
3	TCP	127.0.0.1:55773	127.0.0.1:55774	ESTABLISHED
4	TCP	127.0.0.1:55774	127.0.0.1:55773	ESTABLISHED
5	TCP	192.168.2.11:55715	20.199.120.151:443	ESTABLISHED
6	TCP	192.168.2.11:55785	52.13.69.101:443	ESTABLISHED
7	TCP	192.168.2.11:55852	104.42.50.130:443	ESTABLISHED
8	TCP	192.168.2.11:55943	34.117.237.239:443	ESTABLISHED
9	TCP	192.168.2.11:55945	52.97.173.18:443	ESTABLISHED
10	TCP	192.168.2.11:57825	144.2.14.25:443	CLOSE_WAIT
11	TCP	192.168.2.11:57834	20.199.120.151:443	ESTABLISHED

Παίρνουμε τα παραπάνω αποτελέσματα (το πεδίο index συμπληρώθηκε από εμένα).
Βλέπουμε ότι οι πρώτες 4 συνδέσεις TCP είναι από θύρες του ίδιου μας του υπολογιστή στον εαυτό του. Τις αγνοούμε λοιπόν. Άρα έχουμε 11 – 4 – 1 = 6 συνδέσεις με άλλους υπολογιστές.

2.14:

Index	Source	Destination
5	55715	443
6	55785	443

Άσκηση 3:

3.1: Καταγραφή διαφορετιών πρωτοκόλλων που εμφανίζονται στην οθόνη: Βλέπουμε μηνύματα πρωτοκόλλων TCP και HTTP.

3.2: MAC Address (my computer's): 10:63:c8:94:47:9d

Έχουμε ταξινομήσει τα μηνύματα με βάση το frame number. Πάμε στο πρώτο μήνυμα που στάλθηκε (εμείς το στείλαμε) και κοιτάζουμε το value του πεδίου Source αυτού του μηνύματος.

3.3: Κατασκευαστής της κάρτας δίκτυου μας: LiteonTe (LITE-ON Technology Corporation)

Αυτή την πληροφορία μας την δίνει το Wireshark στην αναπάρασταση του MAC Address. Γνώριζουμε ότι προσπερνώντας τα 2 πρώτα bit της διεύθυνσης τα επόμενα 22 bit προσδιορίζουν τον κατασκευαστή. Το Wireshark μας δείχνει ποιος είναι ο κατασκευαστής από μόνο του.

3.4: IPV4 (my computer's): 192.168.2.11

Εξετάζοντας τα στοιχεία του ίδιου πακέτου, αφού είμαστε βεβαιομένοι εξαιτίας της προηγηθείσας ανάλυσης ότι εμείς το στείλαμε, βλέπουμε ότι το Wireshark δείχνει το IP του source και άρα γνωρίζουμε το IP address μας.

3.5: IPv4 (edu-dy.cn.ntua.gr): 147.102.40.15

Είναι το Dst (destination) στο παραπάνω πακέτο.

3.6: Σύνταξη φίλτρου που εμφανίζεται τώρα: tcp.stream eq 2

3.7.i: τύπος εξυπηρετητή ιστού της ιστοσελίδας:

Server: Apache/2.2.22 (FreeBSD) mod_ssl/2.2.22 OpenSSL/0.9.8zh-freebsd DAV/2

3.7.ii: τίτλος και το αντίστοιχο HTML tag της σελίδας που επισκέφτηκα:

τίτλος: CN Lab

HTML tag:

```
<html>
    <head>
        <title>CN Lab</title>
    </head>
    <body>
        <h1>It works!</h1>
        <h2>Computer Networks 2022-23</h2>
        <h3>Lab1</h3>
    </body>
</html>
```

3.7.iii: σημείο παραθύρου όπου εμφανίζεται αυτός ο τίτλος: ο τίτλος εμφανίζεται πάνω πάνω στο παράθυρο. Στο σημείο του φυλλομετρητή όπου βλέπουμε όλα τα ανοικτά μας παράθυρα.

3.8: Σύνταξη φίλτρου για εμφάνιση μόνο HTTP μηνυμάτων: ip.addr==147.102.40.15 && http

3.9: Πλήθος μηνυμάτων HTTP που στάλθηκαν: 2

Πλήθος μηνυμάτων HTTP που λήφθηκαν: 2

3.10: Χρόνος που πέρασε από την στιγμή που στάλθηκε το πρώτο GET μέχρι να ληφθεί η απόκριση 200 OK είναι 0.016944 (+ 0) seconds. Χρησιμοποιώντας τις ρυθμίσεις για το Time Display Format της υπόδειξης η απάντηση είναι άμεσα εμφανής.

```
2888 0.001040 192.168.2.11    147.102.40.15    HTTP     522 GET / HTTP/1.1
2891 0.016944 147.102.40.15    192.168.2.11     TCP       66 80 → 54671 [SYN, ACK] Seq=0 A
2892 0.000000 147.102.40.15    192.168.2.11     HTTP     585 HTTP/1.1 200 OK  (text/html)
```

Στο σημείο αυτό αφαιρούμε το προηγούμενο φίλτρο και δείχνουμε όλα τα πακέτα TCP που στάλθηκαν.

	Time	Source	Destination	Protocol	Length	Info
2883	0.000000	192.168.2.11	147.102.40.15	TCP	66	54670 → 80 [SYN] Seq=0 Win=64240
2884	0.002423	192.168.2.11	147.102.40.15	TCP	66	54671 → 80 [SYN] Seq=0 Win=64240
2886	0.013195	147.102.40.15	192.168.2.11	TCP	66	80 → 54670 [SYN, ACK] Seq=0 Ack=1
2887	0.000369	192.168.2.11	147.102.40.15	TCP	54	54670 → 80 [ACK] Seq=1 Ack=1 Win=
2888	0.001040	192.168.2.11	147.102.40.15	HTTP	522	GET / HTTP/1.1
2891	0.016944	147.102.40.15	192.168.2.11	TCP	66	80 → 54671 [SYN, ACK] Seq=0 Ack=1
2892	0.000000	147.102.40.15	192.168.2.11	HTTP	585	HTTP/1.1 200 OK (text/html)
2893	0.000996	192.168.2.11	147.102.40.15	TCP	54	54671 → 80 [ACK] Seq=1 Ack=1 Win=
2980	0.041715	192.168.2.11	147.102.40.15	TCP	54	54670 → 80 [ACK] Seq=469 Ack=532
3105	0.081009	192.168.2.11	147.102.40.15	HTTP	468	GET /favicon.ico HTTP/1.1
3109	0.018771	147.102.40.15	192.168.2.11	TCP	590	80 → 54670 [ACK] Seq=532 Ack=883
3110	0.000000	147.102.40.15	192.168.2.11	TCP	590	[TCP Previous segment not capture
3111	0.000497	192.168.2.11	147.102.40.15	TCP	66	54670 → 80 [ACK] Seq=883 Ack=1068
3112	0.000214	147.102.40.15	192.168.2.11	TCP	590	[TCP Out-Of-Order] 80 → 54670 [AC
3113	0.000075	192.168.2.11	147.102.40.15	TCP	66	54670 → 80 [ACK] Seq=883 Ack=1604
3114	0.000092	147.102.40.15	192.168.2.11	TCP	590	[TCP Out-Of-Order] 80 → 54670 [AC
3115	0.000000	147.102.40.15	192.168.2.11	TCP	590	80 → 54670 [ACK] Seq=2676 Ack=883
3116	0.000060	192.168.2.11	147.102.40.15	TCP	54	54670 → 80 [ACK] Seq=883 Ack=2676
3117	0.000055	192.168.2.11	147.102.40.15	TCP	54	54670 → 80 [ACK] Seq=883 Ack=3212
3118	0.000227	147.102.40.15	192.168.2.11	TCP	590	80 → 54670 [ACK] Seq=3212 Ack=883
3119	0.015767	147.102.40.15	192.168.2.11	TCP	590	80 → 54670 [ACK] Seq=3748 Ack=883
3120	0.000000	147.102.40.15	192.168.2.11	HTTP	319	HTTP/1.1 200 OK (image/x-icon)
3121	0.000260	192.168.2.11	147.102.40.15	TCP	54	54670 → 80 [ACK] Seq=883 Ack=4549
4404	5.006782	147.102.40.15	192.168.2.11	TCP	54	80 → 54670 [FIN, ACK] Seq=4549 Ac
4405	0.000141	192.168.2.11	147.102.40.15	TCP	54	54670 → 80 [ACK] Seq=883 Ack=4550

3.11: Πόσα πακέτα χρειάστηκαν για την ολοκλήρωση της μετάδοσης: 8

Το GET για την εικόνα “favicon.ico” είναι στο πακέτο 3105. Το αντίστοιχο 200 OK για την αποστολή σε εμάς της εικόνας είναι στο πακέτο 3120.

Τα πακέτα που χρειάζονται να σταλούν για να λάβουμε την εικόνα είναι αυτά που έχουν στο πεδίο πληροφοριών τους [TCP segment of a reassembled PDU]. Μετράμε 7 τέτοια πακέτα (δεν φαίνεται παραπάνω) και το τελευταίο κομμάτι πληροφορίας μεταφέρεται από το HTTP πακέτο με την απόκριση 200 OK. Χρειάζεται να λάβουμε 8 πακέτα για να ολοκληρωθεί η διαδικασία. Στη διαδικασία μετάδοσης της εικόνας δεν μετράμε το πακέτο που στείλαμε εμείς αρχικά, διότι με αυτό μόνον ζητούσαμε την εικόνα. Άρα 8 πακέτα.

Βέβαια στην συνέχεια ανταλλάσσονται κάποια acknowledgments, ωστόσο, αυτά δεν μετέφεραν πληροφοριές για την εικόνα άρα τα αγνοούμε στην παραπάνω καταμέτρηση.

3.12: Φίλτρο για εμφάνιση μόνο πακέτων TCP: το χρησιμοποιήσαμε ήδη παραπάνω. Η σύνταξή του είναι:
“ip.addr==147.102.40.15 && tcp”

3.13: A Χρόνος μέχρι να ληφθεί το πρώτο εξ αυτών = 0.018771 seconds
B Χρόνος υπόλοιπης μετάδοσης = 8.166276 – 8.149289 = 0.016987 seconds
C Χρόνος ολοκλήρωσης απόκρισης στο αίτημα GET = 8.166276 – 8.130518 = 0.035758 seconds

Για τον πρώτο χρόνο χρησιμοποιήσαμε το “Seconds since Previous Displayed Packet” και για τα επόμενα 2 χρησιμοποιήσαμε το “Seconds since first captured Packet”.

3.14: 1 Service Time = 0.018771 seconds
2 Response Spread = 0.016987 seconds
3 Application PDU Response Time = 0.035758 seconds

Διακρίνουμε την αντιστοιχία: A B C
1 2 3
Service Time είναι ο χρόνος μέχρι να εξυπηρετηθούμε (να πάρουμε το 1ο πακέτο). Response Spread είναι η διάρκεια της υπόλοιπης απόκρισης και Application PDU Response Time είναι ο χρόνος που χρειάστηκε για να ολοκληρωθεί το αίτημά μας.

3.15: Σύνταξη φίλτρου για να δω μόνο μηνύματα HTTP που έστειλε ο υπολογιστής μου:
"ip.src==192.168.2.11 && http"

Ή στην συγκεκριμένη άσκηση μας νοιάζει μόνο η επικοινωνία μας με τον εξυπηρετητή ιστό για την πρόσβαση στο "edu-dy.cn.ntua.gr". Παραπάνω βρήκαμε ότι η IPv4 του είναι 147.102.40.15 άρα μπορούμε να χρησιμοποιήσουμε και το φίλτρο:
"ip.addr==147.102.40.15 && ip.src==192.168.2.11 && http"