Exercise 1 – Basic network stuff

Difficulty: **Easy**

Use the `arp` command and paste the output from the arp table on your system:
Use the `route` command and paste the output from the routing table on your system:
Use the `traceroute` command on your system and observe the hops to Google's DNS, 8.8.8.8. Paste the full output from the command bellow showing all the hops from your system to 8.8.8.8.

arp command - ARP stands for "Address Resolution Protocol". Displays and modifies entries in the Address Resolution Protocol (ARP) cache. The ARP cache contains one or more tables.
Running arp without any arguments will display a list of the command's parameters.

```
C:\Users\Nikki>arp

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a            Displays current ARP entries by interrogating the current
                protocol data.  If inet_addr is specified, the IP and Physical
                addresses for only the specified computer are displayed.  If
                more than one network interface uses ARP, entries for each ARP
                table are displayed.
  -g            Same as -a.
  -v            Displays current ARP entries in verbose mode.  All invalid
                entries and entries on the loop-back interface will be shown.
  inet_addr     Specifies an internet address.
  -N if_addr    Displays the ARP entries for the network interface specified
                by if_addr.
  -d            Deletes the host specified by inet_addr. inet_addr may be
                wildcarded with * to delete all hosts.
  -s            Adds the host and associates the Internet address inet_addr
                with the Physical address eth_addr.  The Physical address is
                given as 6 hexadecimal bytes separated by hyphens. The entry
                is permanent.
  eth_addr      Specifies a physical address.
  if_addr       If present, this specifies the Internet address of the
                interface whose address translation table should be modified.
                If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.
```

To properly use the arp command and to display the complete ARP cache we use the arp -a command.

```
C:\Users\Nikki>arp -a

Interface: 192.168.234.121 --- 0x12
  Internet Address      Physical Address      Type
  192.168.234.35        9e-52-b7-4b-55-ab     dynamic
  192.168.234.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 172.26.208.1 --- 0x1b
  Internet Address      Physical Address      Type
  172.26.223.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 172.29.160.1 --- 0x29
  Internet Address      Physical Address      Type
  172.29.175.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

route command - allows us to make manual entries into the network routing tables.

Route print displays the entire contents of the IP routing table.

```
C:\Users\Nikki>route print
===========================================================================
Interface List
  3...02 45 e2 71 7a 67 ......Microsoft Wi-Fi Direct Virtual Adapter
 10...82 45 e2 71 7a 67 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 18...00 45 e2 71 7a 67 ......Realtek 8822CE Wireless LAN 802.11ac PCI-E NIC
  1...........................Software Loopback Interface 1
 27...00 15 5d 77 2b 5b ......Hyper-V Virtual Ethernet Adapter
 41...00 15 5d 1b 34 c5 ......Hyper-V Virtual Ethernet Adapter #2
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0   192.168.234.35  192.168.234.121     50
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
     172.26.208.0    255.255.240.0         On-link      172.26.208.1   5256
     172.26.208.1  255.255.255.255         On-link      172.26.208.1   5256
   172.26.223.255  255.255.255.255         On-link      172.26.208.1   5256
     172.29.160.0    255.255.240.0         On-link      172.29.160.1   5256
     172.29.160.1  255.255.255.255         On-link      172.29.160.1   5256
   172.29.175.255  255.255.255.255         On-link      172.29.160.1   5256
    192.168.234.0    255.255.255.0         On-link   192.168.234.121    306
  192.168.234.121  255.255.255.255         On-link   192.168.234.121    306
  192.168.234.255  255.255.255.255         On-link   192.168.234.121    306
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link   192.168.234.121    306
        224.0.0.0        240.0.0.0         On-link      172.26.208.1   5256
        224.0.0.0        240.0.0.0         On-link      172.29.160.1   5256
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link   192.168.234.121    306
  255.255.255.255  255.255.255.255         On-link      172.26.208.1   5256
  255.255.255.255  255.255.255.255         On-link      172.29.160.1   5256
===========================================================================
Persistent Routes:
  None
```

```
IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
 18    306 fe80::/64                On-link
 27   5256 fe80::/64                On-link
 41   5256 fe80::/64                On-link
 27   5256 fe80::40ff:15f4:505d:76f5/128
                                    On-link
 41   5256 fe80::8eb8:18a9:c6c3:d26a/128
                                    On-link
 18    306 fe80::aec9:e417:62a2:fe3a/128
                                    On-link
  1    331 ff00::/8                 On-link
 18    306 ff00::/8                 On-link
 27   5256 ff00::/8                 On-link
 41   5256 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

traceroute command – in Windows CLI is **tracert.** We will be using tracert to Google's DNS, 8.8.8.8. This command shows all the hops from my system to 8.8.8.8.

```
C:\Users\Nikki>tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:

  1    32 ms     4 ms     4 ms  192.168.234.35
  2   157 ms   234 ms    37 ms  10.91.2.224
  3    53 ms    38 ms    42 ms  10.91.2.42
  4    64 ms    26 ms    28 ms  10.91.2.153
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7    41 ms    35 ms    41 ms  ctel-78-157-17-26.cabletel.com.mk [78.157.17.26]
  8     *       60 ms    39 ms  195.3.114.153
  9     *        *       45 ms  lg22-9070.as8447.a1.net [195.3.64.57]
 10     *        *        *     Request timed out.
 11    75 ms    43 ms    61 ms  lg59-9071.as8447.a1.net [80.120.167.46]
 12    65 ms    47 ms    56 ms  209.85.245.45
 13    69 ms    72 ms    77 ms  142.251.228.27
 14    85 ms    50 ms    54 ms  dns.google [8.8.8.8]

Trace complete.
```

Why would you need to use the `ping` command?
Answer: We use the **ping** command, first and foremost, to determine whether a machine has internet access. But this command can be also, used, for troubleshooting, exploration, observing, security. The ping command sends Internet Control Message Protocol (ICMP) packets to the destination. Then it waits for the echo reply. It can show statistic for this request, errors and packet loss.

When we use this command, we will send echo requests. Usually there are 4 echo requests. Then we will receive a result for each of them. Like, for example, that indicates if they were successful, how much data was received, the time it took for the response.

```
C:\Users\Nikki>ping google.com

Pinging google.com [142.250.180.238] with 32 bytes of data:
Reply from 142.250.180.238: bytes=32 time=49ms TTL=111
Reply from 142.250.180.238: bytes=32 time=52ms TTL=111
Reply from 142.250.180.238: bytes=32 time=56ms TTL=111
Reply from 142.250.180.238: bytes=32 time=63ms TTL=111

Ping statistics for 142.250.180.238:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 49ms, Maximum = 63ms, Average = 55ms
```

Write down the TCP/UDP ports of the most commonly used services bellow in the form of TCP[PORT] or UDP[PORT].
As an example, the first two answers have been filled in:

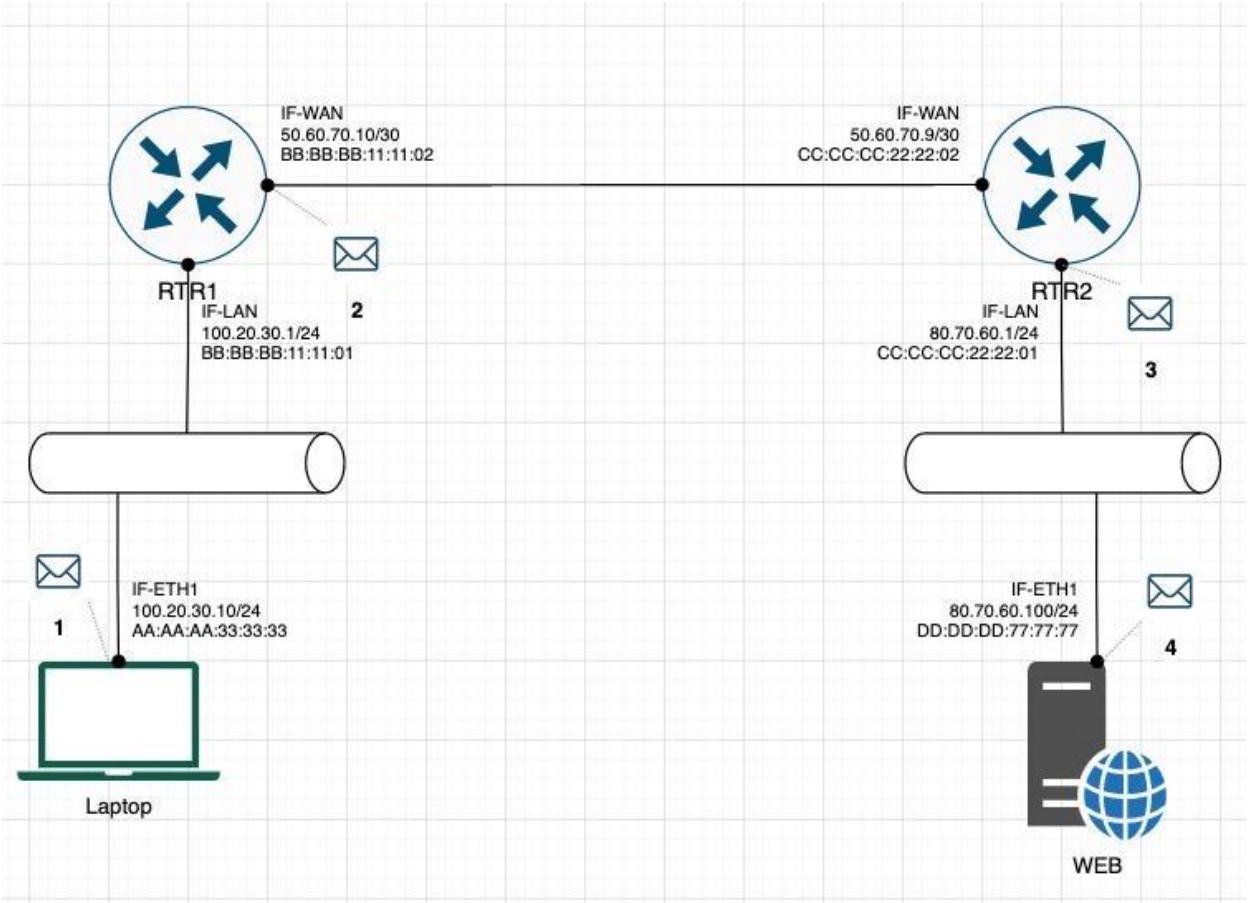
- HTTP – TCP80
- SNMP – UDP161
- HTTPS - TCP443
- DNS client – UDP53
- DNS zone transfer – TCP53
- SMTP – TCP25
- SSH – TCP22
- FTP – TCP21 (command port), TCP20 (data port)
- Telnet – TCP23
- MSSQL – TCP1433
- MySQL – TCP3306
- PostreSQL – TCP5432
- RDP (Remote Desktop Protocol) – UDP3389
- NTP – UDP123
- NFS – TCP2049

Exercise 2 – TCP/IP Basics

Difficulty: **Medium**

Refer to the exhibit and answer the questions below.

The letter symbol ✉, represents the IP packet as it travels across the network.
In the example shown, the laptop attempts to communicate with the web server in question. During its travel the packet will be forwarded across the network nodes and will eventually end up across six network interfaces before it reaches the web server. Each packet as part of the TCP/IP Stack contains fields for the source and destination MAC Address, IP Address and the TCP/UDP Port.



For each of the packet locations shown, 1 to 4 write down the source and destination MAC addresses of the packet as it travels across the network interfaces.

1. The laptop initiates communication with the web server and prepares a packet. What would the packet look like at this stage?
   - SRC IP: 100.20.30.10
   - DST IP: 80.70.60.100
   - SRC MAC: AA:AA:AA:33:33:33
   - DST MAC: BB:BB:BB:11:11:01

2. RTR1 receives the packet on its IF-LAN interface, prepares it accordingly and forwards it out its IF-WAN. What would the packet look like at this stage?
   - SRC IP: 100.20.30.10
   - DST IP: 80.70.60.100
   - SRC MAC: BB:BB:BB:11:11:02
   - DST MAC: CC:CC:CC:22.22.02

3. RTR2 receives the packet on its IF-WAN interface, prepares it accordingly and forwards it out via IF-LAN. What would the packet look like at this stage?
   - SRC IP: 100.20.30.10
   - DST IP: 80.70.60.100
   - SRC MAC: CC:CC:CC:22:22:01
   - DST MAC: DD:DD:DD:77:77:77

4. The web server receives the packet and prepares a response packet back. What would the packet look like at this stage?
   - SRC IP: 80.70.60.100
   - DST IP: 100.20.30.10
   - SRC MAC: DD:DD:DD:77:77:77
   - DST MAC: CC:CC:CC:22:22.01

Since we are talking about web traffic (www) in the example, which transport layer protocol will most probably be used?

- ❑ TCP – WWW relays on TCP protocol
- ❑ UDP

If we do a traffic analysis with a network packet monitoring tool like WireShark, what can we expect to see for the source and destination ports when the laptop sends the packet?

- SRC PORT: Port 1024 and above
- DST PORT: Port 443 for HTTPS or port 80 http

Similarly, and vice versa, what can we expect to see as destination ports when the Web server sends a response packet back?

- SRC PORT: Port 443 for HTTPS or port 80 http
- DST PORT: Port 1024 and above

How many broadcast domains are there in the exhibit shown?

There are 3 broadcast domains in the exhibit shown above. The first broadcast domain is between the laptop and the router 1, the second broadcast domain is between the router 1 and router 2 and the third broadcast domain is between the router 2 and the server. The routers separate the broadcast domains, thus giving us 3 broadcast domains. In other words, all ports on a router are in a different broadcast domain.

Exercise 3 – Traffic analysis and identifying the OSI layers of the network packets

Difficulty: **Hard**

Prerequisite:
Search online and get familiar with the TCP's three-way handshake. Learn how to capture the three-way handshake using Wireshark.
Install Wireshark on your computer and use it to capture traffic against a website or a server or your choice. It is recommended that you capture traffic against a simple website. Name and the IP address of the website you plan to capture traffic:

Analyze the TCP's three-way handshake and using screenshots from the Wireshark window answer the questions bellow:

1. What is the source IP (of the initiating host): 192.168.234

Current filter: tcp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.234.121	52.112.120.189	TCP	55	49270 → 443 [ACK] Seq=1 Ack=1 Win=507 Len=1 [TCP segment of a reassembled PDU]
2	0.091333	52.112.120.189	192.168.234.121	TCP	66	443 → 49270 [ACK] Seq=1 Ack=2 Win=16383 Len=0 SLE=1 SRE=2
3	1.887384	192.168.234.121	52.97.181.34	TCP	66	49273 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
4	1.942782	52.97.181.34	192.168.234.121	TCP	66	443 → 49273 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 WS=256 SACK_PERM
5	1.942906	192.168.234.121	52.97.181.34	TCP	54	49273 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
6	1.943453	192.168.234.121	52.97.181.34	TLSv1.2	260	Client Hello
7	2.002668	52.97.181.34	192.168.234.121	TCP	1434	443 → 49273 [ACK] Seq=1 Ack=207 Win=4194816 Len=1380 [TCP segment of a reassembled PDU]
8	2.005264	52.97.181.34	192.168.234.121	TCP	2814	443 → 49273 [ACK] Seq=1381 Ack=207 Win=4194816 Len=2760 [TCP segment of a reassembled PDU]
9	2.005264	52.97.181.34	192.168.234.121	TLSv1.2	348	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done

2. What is the destination IP? (target website):52.97.181.34

Current filter: tcp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.234.121	52.112.120.189	TCP	55	49270 → 443 [ACK] Seq=1 Ack=1 Win=507 Len=1 [TCP segment of a reassembled PDU]
2	0.091333	52.112.120.189	192.168.234.121	TCP	66	443 → 49270 [ACK] Seq=1 Ack=2 Win=16383 Len=0 SLE=1 SRE=2
3	1.887384	192.168.234.121	52.97.181.34	TCP	66	49273 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
4	1.942782	52.97.181.34	192.168.234.121	TCP	66	443 → 49273 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 WS=256 SACK_PERM
5	1.942906	192.168.234.121	52.97.181.34	TCP	54	49273 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
6	1.943453	192.168.234.121	52.97.181.34	TLSv1.2	260	Client Hello
7	2.002668	52.97.181.34	192.168.234.121	TCP	1434	443 → 49273 [ACK] Seq=1 Ack=207 Win=4194816 Len=1380 [TCP segment of a reassembled PDU]
8	2.005264	52.97.181.34	192.168.234.121	TCP	2814	443 → 49273 [ACK] Seq=1381 Ack=207 Win=4194816 Len=2760 [TCP segment of a reassembled PDU]
9	2.005264	52.97.181.34	192.168.234.121	TLSv1.2	348	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
10	2.005372	192.168.234.121	52.97.181.34	TCP	54	49273 → 443 [ACK] Seq=207 Ack=4435 Win=131072 Len=0

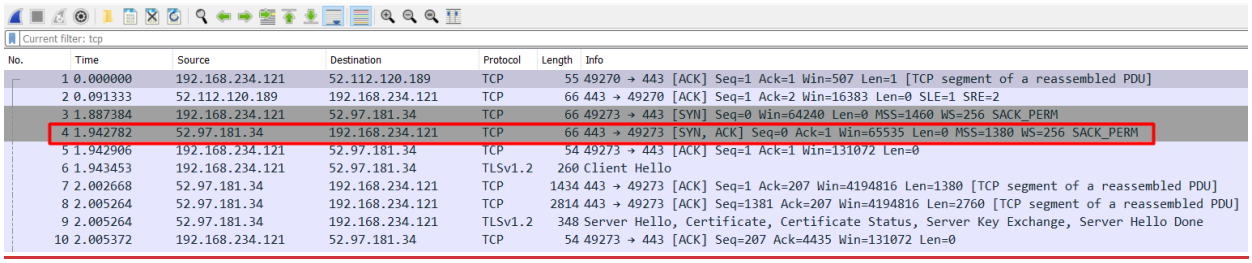
Identify the Network Interface (Layer 1 & 2) section of the SYN packet and paste a screenshot from it:
<- Paste a screenshot of the Layer 2 details section here ->

Current filter: tcp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.234.121	52.112.120.189	TCP	55	49270 → 443 [ACK] Seq=1 Ack=1 Win=507 Len=1 [TCP segment of a reassembled PDU]
2	0.091333	52.112.120.189	192.168.234.121	TCP	66	443 → 49270 [ACK] Seq=1 Ack=2 Win=16383 Len=0 SLE=1 SRE=2
3	1.887384	192.168.234.121	52.97.181.34	TCP	66	49273 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
4	1.942782	52.97.181.34	192.168.234.121	TCP	66	443 → 49273 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 WS=256 SACK_PERM
5	1.942906	192.168.234.121	52.97.181.34	TCP	54	49273 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
6	1.943453	192.168.234.121	52.97.181.34	TLSv1.2	260	Client Hello
7	2.002668	52.97.181.34	192.168.234.121	TCP	1434	443 → 49273 [ACK] Seq=1 Ack=207 Win=4194816 Len=1380 [TCP segment of a reassembled PDU]
8	2.005264	52.97.181.34	192.168.234.121	TCP	2814	443 → 49273 [ACK] Seq=1381 Ack=207 Win=4194816 Len=2760 [TCP segment of a reassembled PDU]
9	2.005264	52.97.181.34	192.168.234.121	TLSv1.2	348	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
10	2.005372	192.168.234.121	52.97.181.34	TCP	54	49273 → 443 [ACK] Seq=207 Ack=4435 Win=131072 Len=0
11	2.008540	192.168.234.121	52.97.181.34	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message

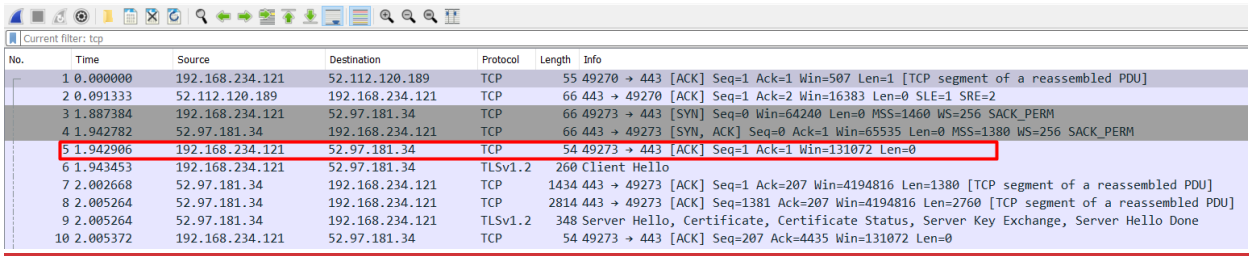
Identify the Network Layer 3 section of the SYN/ACK packet and paste a screenshot from it:

<- Paste a screenshot of the Layer 3 details section here ->



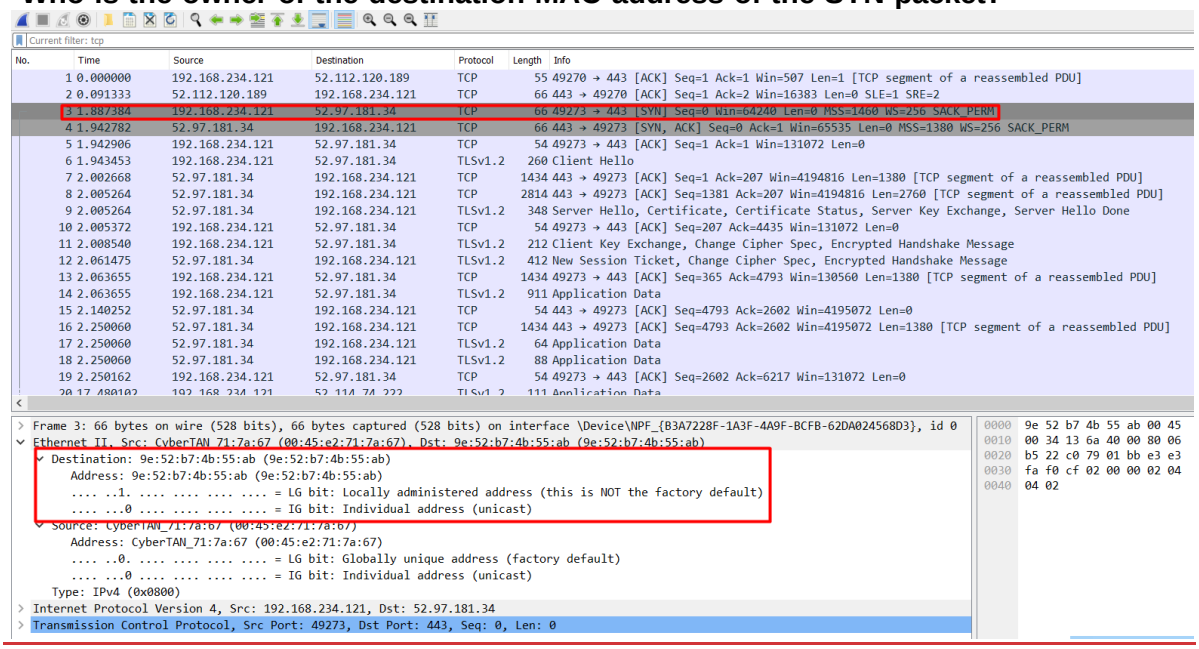
Identify the Transport Layer 4 section of the ACK packet and paste a screenshot from it bellow:

<- Paste a screenshot of the Layer 4 details section here ->



Look closely at the L2 section of the three-way handshake packet details. Each of them shows the source and destination MAC address of the packets.

Who is the owner of the destination MAC address of the SYN packet?



Exercise 4 – Hacking mockup (for Bonus points)

Difficulty: **Very hard**

Use Wireshark to capture the packet's application layer data and discover the implications of using unencrypted communication over a network.
It is recommended that you use your own Linux Virtual Machine on your system on which you need to confiture a telnet server.
From your own system try to login with a Telnet on the target VM all while capturing the traffic with a Wireshark. As a proof of competition for this exercise paste in bellow a screenshot of the application layer data containing visible username and password.

- I am not able to do the bonus exercise now , but I will tray to do it and attach it later on GitHub.