Exercise 1 – Basic network stuff

# Difficulty: Easy

Use the arp command and paste the output from the arp table on your system:

*Interface: 192.168.1.106 --- 0x11*

*Internet Address Physical Address Type*

*192.168.1.1 c8-3a-35-ba-55-d0 dynamic*

*192.168.1.255 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*

Use the route command and paste the output from the routing table on your system:

*Interface List*

*24...00 ff da 96 48 c9 ........TAP-Surfshark Windows Adapter V9*

*17...50 eb f6 b5 96 cc …....Realtek PCIe 2.5GbE Family Controller*

*1........................................Software Loopback Interface 1*

*39...00 15 5d bb 3f d0 .......Hyper-V Virtual Ethernet Adapter*

*51...00 15 5d 36 45 ea ......Hyper-V Virtual Ethernet Adapter #2*

*===========================================================================*

*IPv4 Route Table*

*===========================================================================*

*Active Routes:*

*Network Destination Netmask Gateway Interface Metric*

*0.0.0.0 0.0.0.0 192.168.1.1 192.168.1.106 35*

*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*

*172.29.144.0 255.255.240.0 On-link 172.29.144.1 5256*

*172.29.144.1 255.255.255.255 On-link 172.29.144.1 5256*

*172.29.159.255 255.255.255.255 On-link 172.29.144.1 5256*

*172.31.208.0 255.255.240.0 On-link 172.31.208.1 5256*

*172.31.208.1 255.255.255.255 On-link 172.31.208.1 5256*

*172.31.223.255 255.255.255.255 On-link 172.31.208.1 5256*

*192.168.1.0 255.255.255.0 On-link 192.168.1.106 291*

*192.168.1.106 255.255.255.255 On-link 192.168.1.106 291*

*192.168.1.255 255.255.255.255 On-link 192.168.1.106 291*

*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 192.168.1.106 291*

*224.0.0.0 240.0.0.0 On-link 172.29.144.1 5256*

*224.0.0.0 240.0.0.0 On-link 172.31.208.1 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 192.168.1.106 291*

*255.255.255.255 255.255.255.255 On-link 172.29.144.1 5256*

*255.255.255.255 255.255.255.255 On-link 172.31.208.1 5256*

*===========================================================================*

*Persistent Routes:*

*None*

*IPv6 Route Table*

*===========================================================================*

*Active Routes:*

*If Metric Network Destination Gateway*

*1 331 ::1/128 On-link*

*17 291 fe80::/64 On-link*

*39 5256 fe80::/64 On-link*

*51 5256 fe80::/64 On-link*

*39 5256 fe80::f45:6f2b:21bf:d856/128*

*On-link*

*17 291 fe80::6c07:1a2b:2933:449f/128*

*On-link*

*51 5256 fe80::9983:2f1b:bacc:2138/128*

*On-link*

*1 331 ff00::/8 On-link*

*17 291 ff00::/8 On-link*

*39 5256 ff00::/8 On-link*

*51 5256 f f00::/8 On-link*

*===========================================================================*

*Persistent Routes:*

*None*

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.

*Tracing route to dns.google [8.8.8.8]*

*over a maximum of 30 hops:*

*1 <1 ms <1 ms <1 ms 192.168.1.1*

*2 <1 ms <1 ms <1 ms 192.168.0.1*

*3 10 ms 7 ms 6 ms 10.180.224.1*

*4 \* \* \* Request timed out.*

*5 \* \* \* Request timed out.*

*6 \* \* \* Request timed out.*

*7 \* \* \* Request timed out.*

*8 9 ms 9 ms 9 ms ctel-78-157-16-209.cabletel.com.mk [78.157.16.209]*

*9 26 ms 27 ms 29 ms 195.3.114.153*

*10 \* 28 ms 27 ms lag33-9073.as8447.a1.net [195.3.64.57]*

*11 \* \* \* Request timed out.*

*12 35 ms 31 ms 31 ms lg59-9071.as8447.a1.net [80.120.167.46]*

*13 31 ms 31 ms 33 ms 209.85.245.45*

*14 31 ms 30 ms 32 ms 216.239.49.77*

*15 32 ms 31 ms 32 ms dns.google [8.8.8.8]*

*Trace complete.*

## Why would you need to use the ping command?

Answer: *We use the ping command to determine whether a networked device is reachable or not. This command can be used to diagnose connectivity problems on the network, check for packet loss and latency and verify network performance. It can also be used to check whether a server or webpage is operational.*

## 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*
* Telnet – *TCP23*
* MSSQL – *TCP1433*
* MySQL – *TCP3306*
* PostreSQL – *TCP5432*
* RDP (Remote Desktop Protocol) – *TCP3389*
* NTP – *UDP123*
* NFS – *TCP2049*

Exercise 2 – TCP/IP Basics

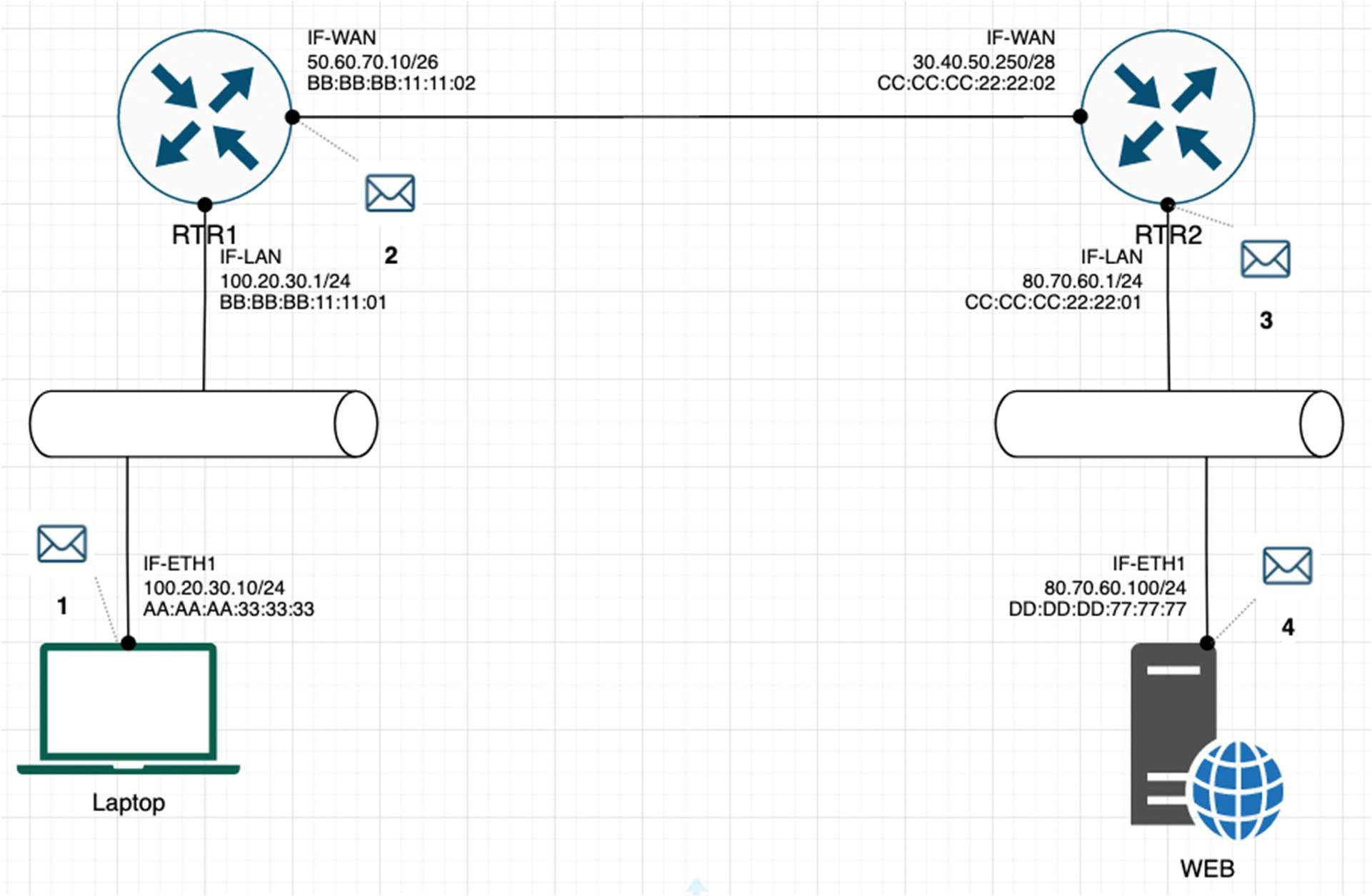
# Difficulty: Medium

## 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*

1. 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**
* 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: *Randomly generated port number*
* DST PORT: *80 (HTTP) or 443 (HTTPS)*

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

* SRC PORT: *80 (HTTP) or 443 (HTTPS)*
* DST PORT: *The same random port number that was generated before*

**How many broadcast domains are there in the exhibit shown?** *THREE*

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:

[www.reklama5.mk](http://www.reklama5.mk) *37.61.200.238*

## 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):

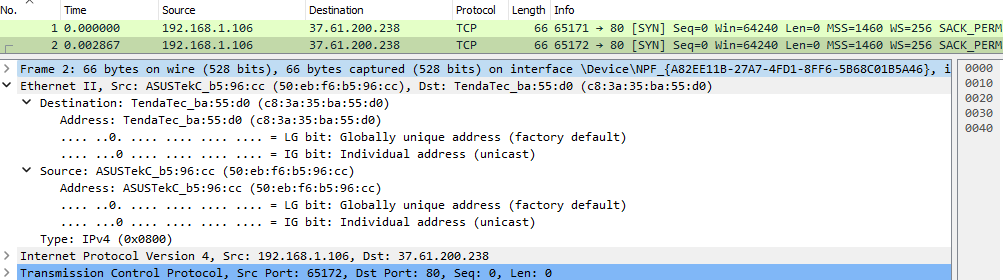
*192.168.1.106*

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

*37.61.200.238*

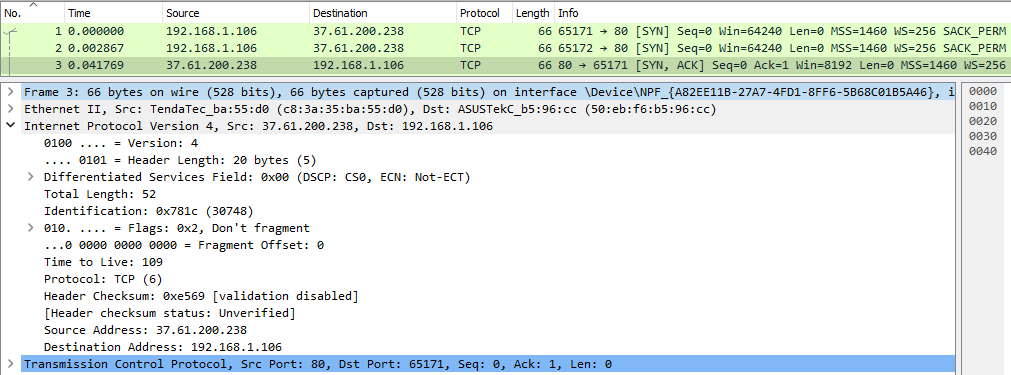
## Identify the Network Interface (Layer 1 & 2) section of the SYN packet and paste a screenshot from it:

<- Paste a screenshot of the Layer 2 details section here ->



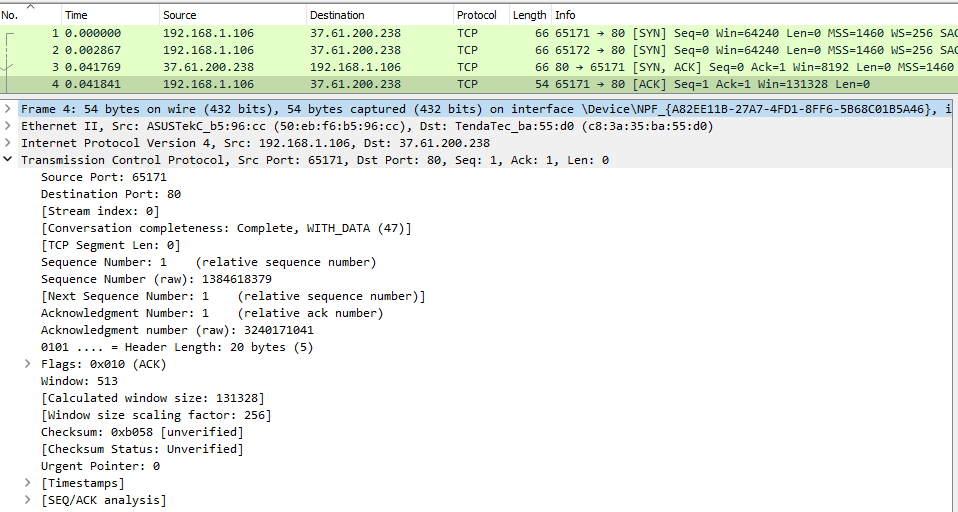
## Identify the Network Layer 3 section of the SYN/ACK packet and paste a screenshot from it:

<- 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?**

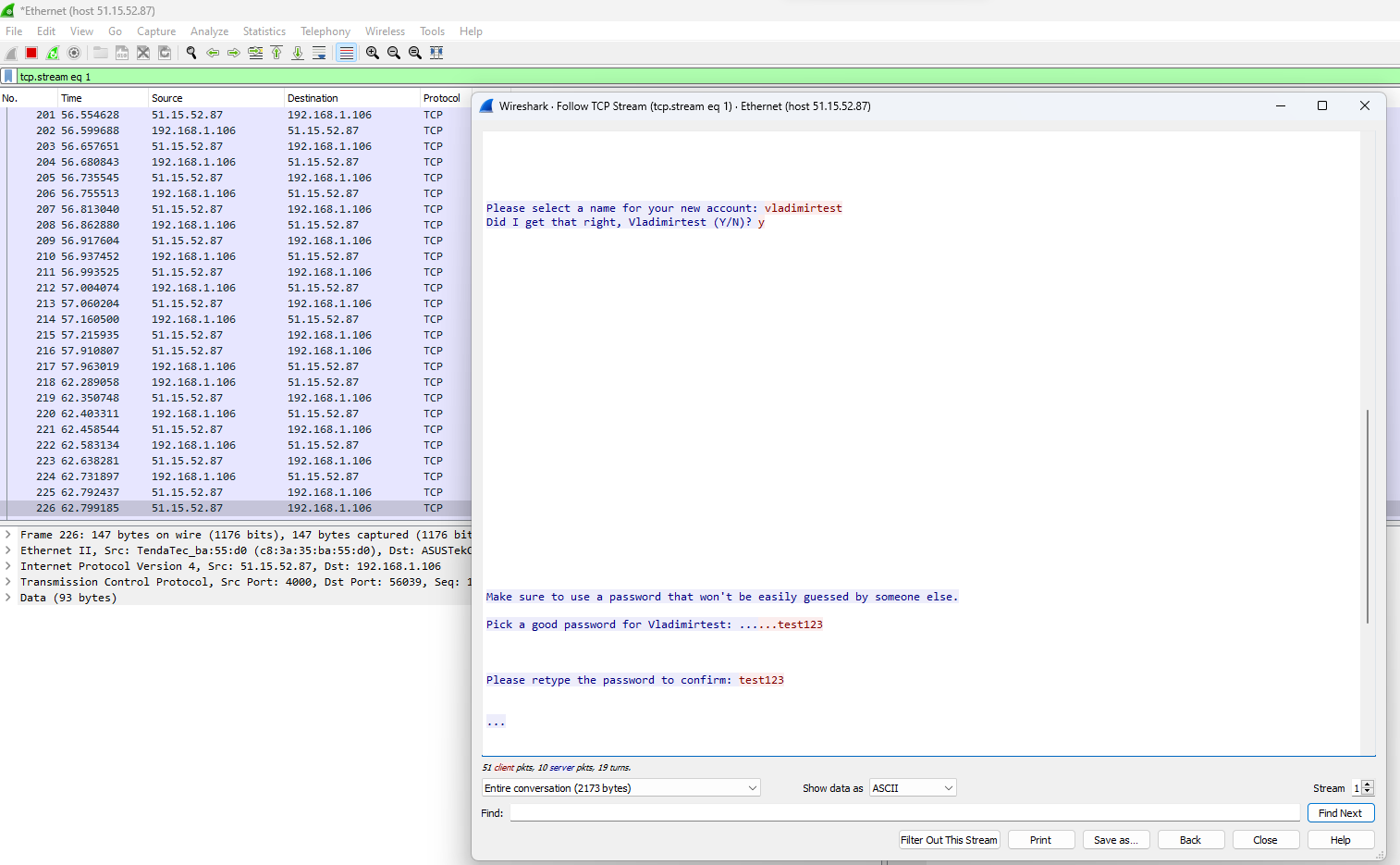
*TendaTec – It is my router.*

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.