Wrocław 01.10.2022

C Y B E R S E C U R I T Y

L A B 9

1. Introduction.

Secure network transmission is investigated in the laboratory. The security issues addressed in the lab focus on SSH communication, VPN networks, and their performance of encryption algorithms, TLS/SSL (OpenSSL) authentication, and firewall configuration. In IT, secure transmission refers to the transmission of data, such as confidential or proprietary information, through a secure channel. Many secure transmission methods require the use of encryption algorithms.

First, get acquainted with the following terms:

Authentication - is the process of confirming the declared identity of the entity involved in the communication process. The purpose of authentication is to obtain a level of certainty that a given entity is the one it claims to be.

Authorization - the purpose of the authorization is access control, which confirms that the entity is authorized to use the requested resource.

Encryption - is the transformation of data in such a way that the data becomes unintelligible without knowing the specific key. This allows protecting data as it passes over the network.

Integrity - The property that confirms that the data has not been compromised or altered in an unauthorized way. If a third party captures and modifies your data, it should be noticed.

Confidentiality - is the protection against unauthorized access, while providing authorized users access to resources without obstruction. Confidentiality ensures that data is not intentionally or unintentionally disclosed to anyone without a valid need to know.

SSH, Secure Shell, is a popular, powerful, software-based approach to network security. Whenever data is sent by a computer to the network, SSH automatically encrypts it. Then, when the data reaches its intended recipient, SSH automatically decrypts it. The result is *transparent* encryption: users can work normally, unaware that their communications are safely encrypted on the network. Besides, SSH uses modern, secure encryption algorithms and is effective enough to be found within mission-critical applications at major corporations.

VPN is the acronym for "**virtual private network.**" A short and direct definition is that a VPN is a mechanism to establish a secure remote access connection across an **intermediary network**, often the Internet. VPNs allow remote access, remote control, and highly secured communications within a private network. VPNs employ encryption and authentication to provide confidentiality, integrity, and privacy protection for network communications. An example diagram of a VPN network:

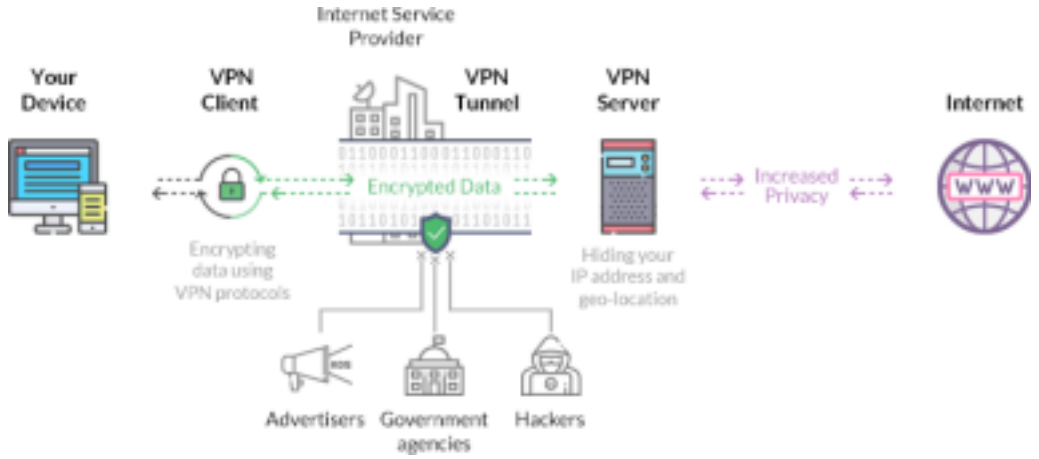


Figure 1 VPN architecture - source https://www.rossco.org/SecureOffice_Images/how-does-a-vpn-work-diagram.png

There are many VPN products available on the market, both commercial and open source. Almost all of these VPN products can be separated into the following four categories:

- PPTP-protocol based VPNs,
- IPSec-protocol based VPNs,
- SSL-based VPNs,
- OpenVPN,

In our laboratory, OpenVPN is used. OpenVPN is often called an SSL-based VPN, as it uses the SSL/TLS protocol to secure the connection. However, OpenVPN also uses HMAC in combination with a digest (or hashing) algorithm for ensuring the integrity of the packets delivered. It can be configured to use pre-shared keys as well as X.509 certificates. These features are not typically offered by other SSL-based VPNs.

SSL/TLS is a protocol that ensures the confidentiality and integrity of data transmission as well as server and sometimes client authentication. It is based on asymmetric encryption and X.509 certificates. SSL is used by web browsers and servers for transmission of sensitive information. SSL is a part of an overall protocol known as Transport Layer Security (TLS). SSL and its successor TLS make use of certificate authorities. When a browser requests a secure web page, 's' is added onto 'HTTP' in the URL of the browser which sends out the public key and the certificate by checking whether the certificate comes from a trusted party which is currently valid and has a relationship with the site from which it comes. The most familiar use of TLS is to secure online transactions. TLS can also be used for security purposes in servers such as mail, database, or directory. A virtual private network uses TLS to encrypt the connection between the user's device and the network being accessed.

2. Environment configuration.

To configure the environment, you need to download three images of virtual machines. All the necessary files can be found on the portal in the attachments to this laboratory. Two of the virtual machines (VMs) are configured as clients. The third one is a VPN server and a firewall. There is also a set of certificates and configuration files for VPNs in the package. The network topology is configured as follows:

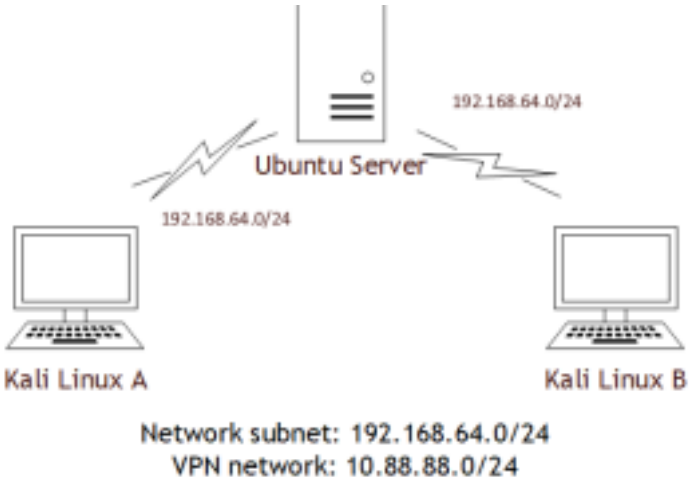


Figure 2 Network topology

1. Run Virtualbox and import virtual machine images.
2. Log in to the server (login: server, pass: student).
3. Log in the clients (login: client, pass: student).

Server configuration:

1. Check if the configuration file exists in /etc/openvpn and see the content of server.conf.
2. There should be the following files in /etc/openvpn/:
   - server.crt - server certificate,
   - server.key - server key,
   - ta.key - HMAC signature – TLS authentication,
   - dh.key - Diffie-Hellman key,
   - ca.crt – CA certificate,
3. To start the VPN server, run:
   sudo systemctl start openvpn@server.service
   To check the status of the VPN service, type:
   sudo systemctl status openvpn@server

Client's configuration:

1. Check if the configuration file exists in /etc/openvpn and see the content of client.conf.
2. There should be the following files in /etc/openvpn/:
   - clientA.key and clientB.key – client key,
   - clientA.crt and clientB.crt – client certificate,
   - ta.key - HMAC signature – TLS authentication,
   - client.conf – configuration file,
   - ca.crt – CA certificate,
3. Adjust client.conf file.
   - Check the IP (Figure 3) of the Server (run ifconfig command on the Server and check IP of network interface, should be from NAT subnet confidured in VirtualBox, in the above example the subnet should be 192.168.64.0/24)
   - Copy the IP of the Server and past it in the client.conf – line:
     remote X.X.X.X 1194
     instead of X.X.X.X.

   Note: to edit file use *nano* editor, but you need root privileges, so add *sudo* before *nano*, e.g.:

```
sudo nano /etc/openvpn/client.conf
```

To save a file push Crtl + X, type ‘Yes’ and push Enter.

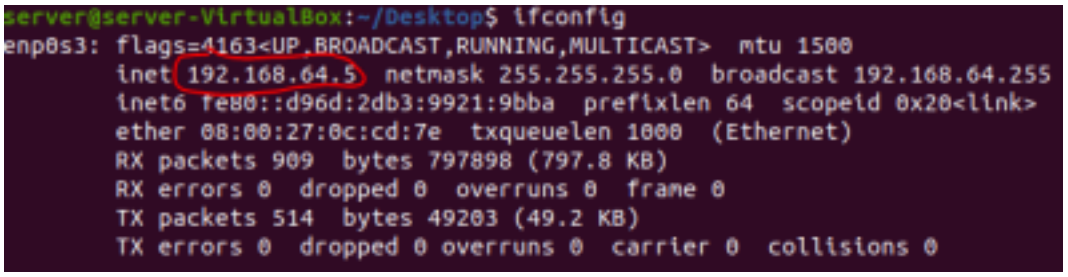


Figure 3 How to check IP of a VM.

4. Remember to change the name of the client certificate and key in client.conf for both clients Kali A and Kali B.
5. To start the VPN connection, type:
   sudo openvpn --config /etc/openvpn/client.conf

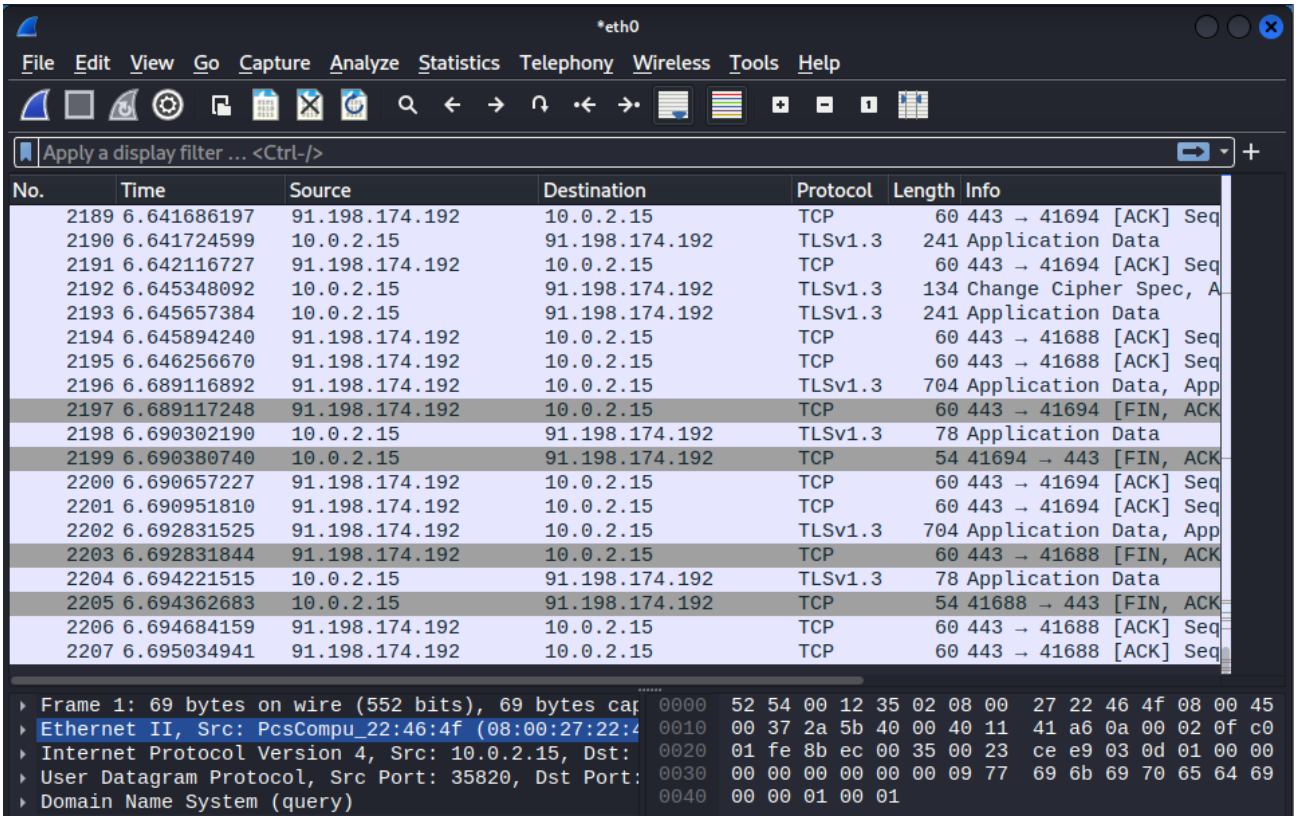
3. TLS communications

The point aims to analyze the TLS 1.2/TLS 1.3 communications. Get acquainted with TLS/SSL versions 1.2 and 1.3, find the advantages and disadvantages of each version.

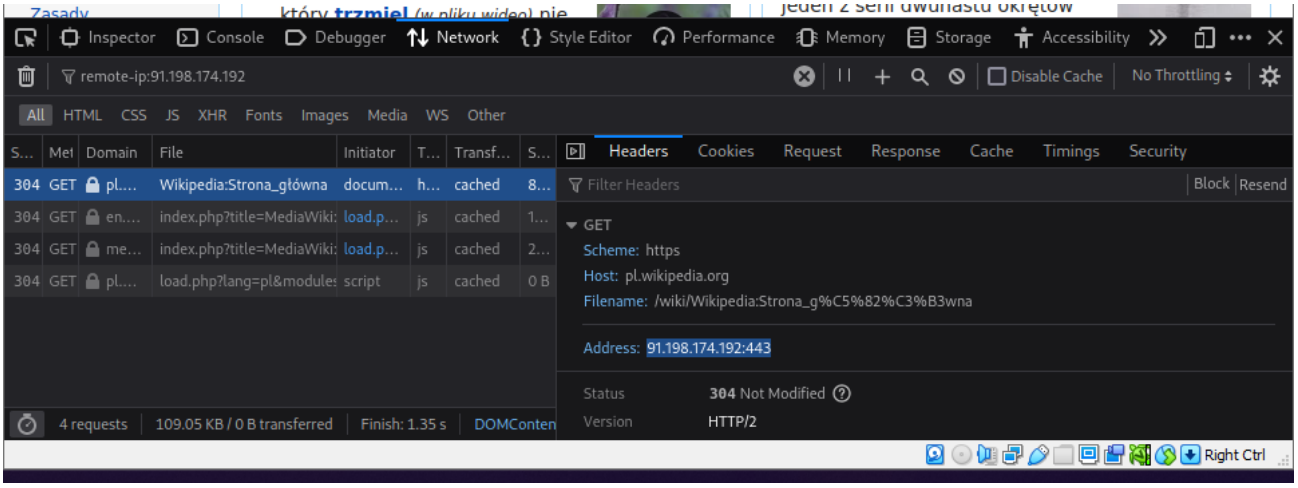
I. Task 1:

- Capture the network traffic on the physical network interface (usually, the name starts with *en*…),

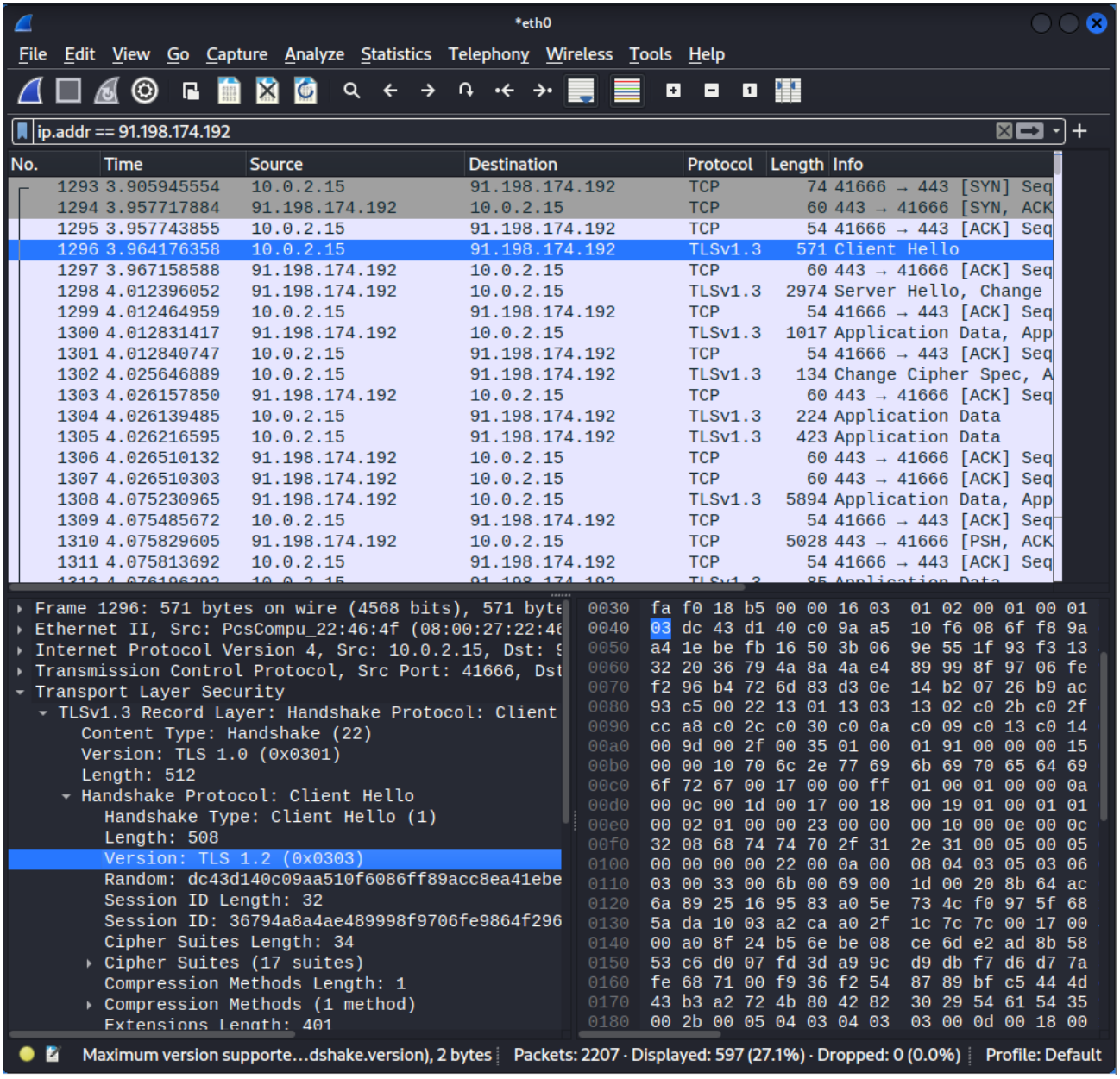
>> Captured packets in eth0 wireshark for Wikipedia,



We can check the remote address from the network on inspection and check the ip to filter onWireShark;

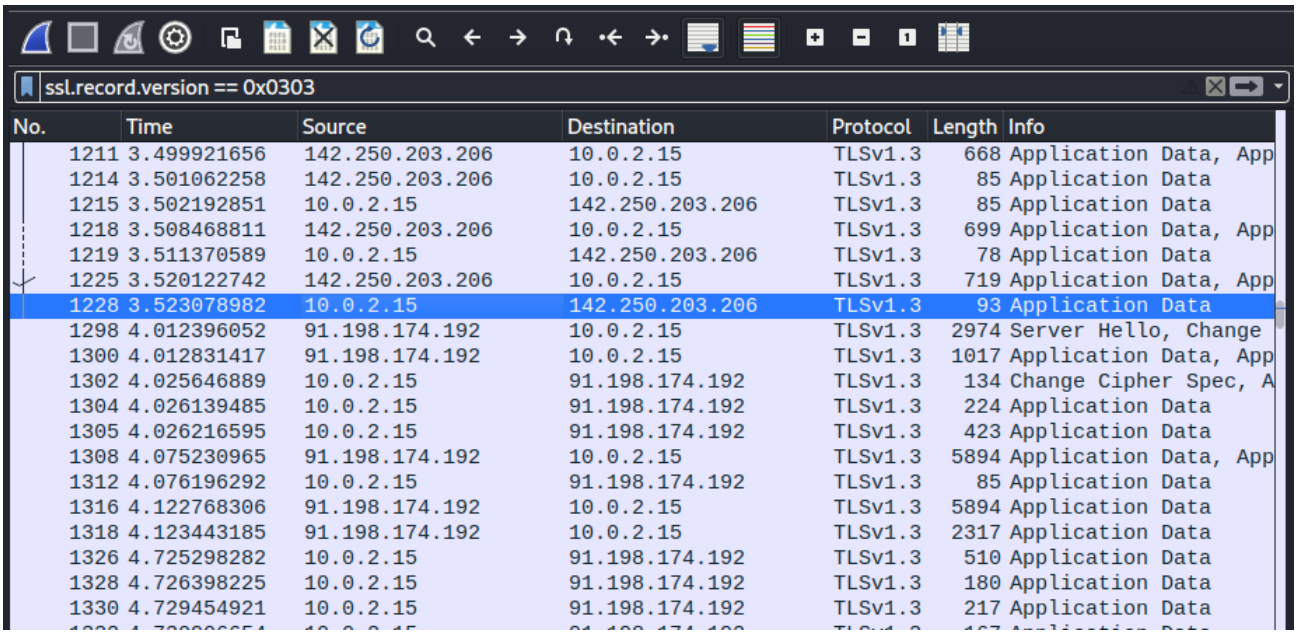


And upon checking the TLS packet we can see,



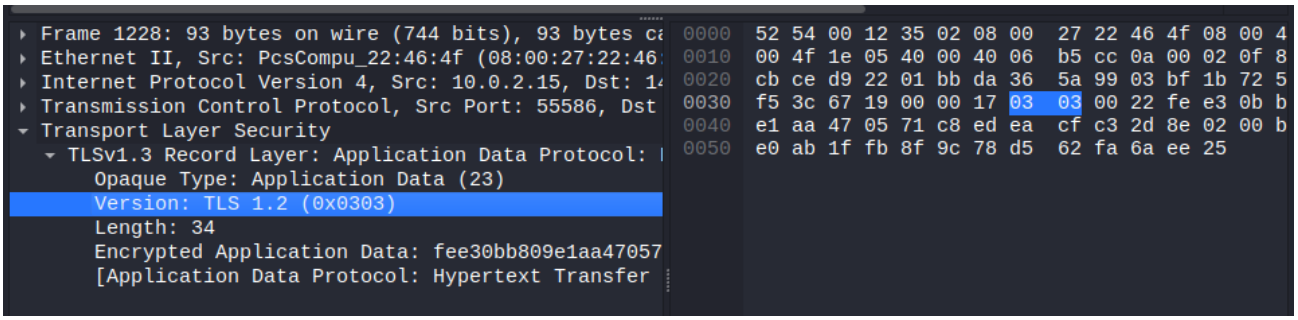
• Filter only the records for TLS/SSL communication. Filter expression for TLS/SSL in Wireshark: ssl.record.version == 0x0303,

>>



• Study the TLS/SSL records in detail.

>>



II. Questions:

• Is TLS and SSL the same protocol?
>No, TLS (Transport Layer Security) and SSL (Secure Sockets Layer) are different protocols.

• What is a TLS/SSL handshake?
>A TLS/SSL handshake is the process of negotiating a secure connection between two parties. It involves the setup of cryptographic parameters and authentication of the server and client.

• What does the TLS/SSL protocol provide, give examples of its applications (at least 2)?
>The TLS/SSL protocol provides secure communication over a computer network and is used for authentication, encryption, and data integrity. Examples of its applications include web browsing, e-mail, instant messaging, and voice over IP.

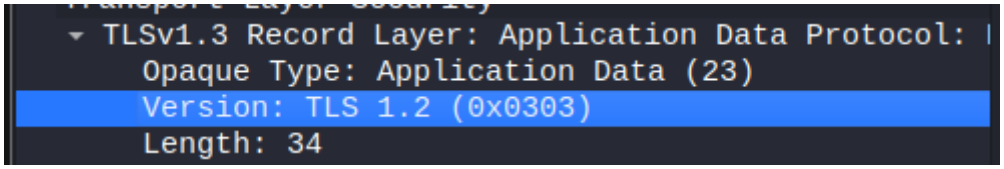
• Which versions of the protocol are currently the most popular?
>The most popular versions of the protocol are TLS 1.3 and TLS 1.2.

• Which version offers higher security and why?
> TLS 1.3 offers higher security due to its improved encryption algorithms and more efficient handshake process.

• Which version offers higher performance?
>TLS 1.2 offers higher performance as it requires fewer round trips to establish a connection.

Based on the traffic captured, analyze the recorded TLS/SSL traffic.

• Which version of the protocol has been captured?

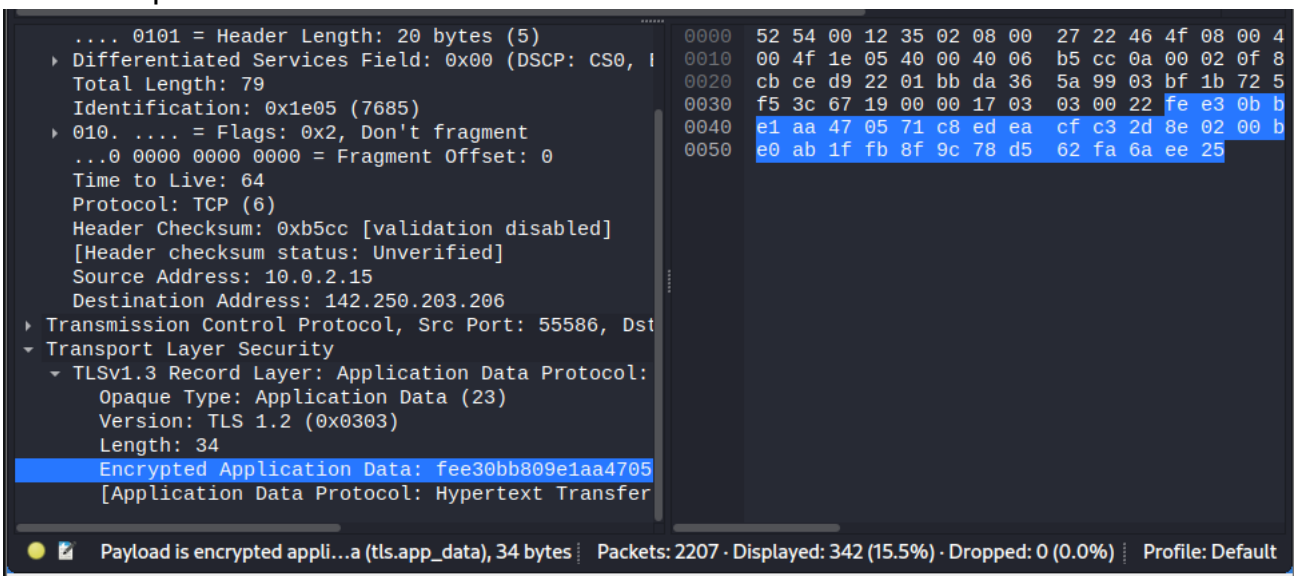


>

• What kind of messages does a handshake consist of (connection establishment)?
> A handshake usually consists of a series of messages that establish a connection between two parties. This includes messages that verify each party's identity and parameters for the connection. The messages may also include messages that inform each party of the current state and any errors that have occurred.

• What does the version of the protocol use depend on?
> The version of the protocol used depends on the type of communication taking place, the capabilities of the two devices communicating, and the environment in which the communication is taking place.

Take a print screen of what type of encryption was used for encryption and put it into the report.

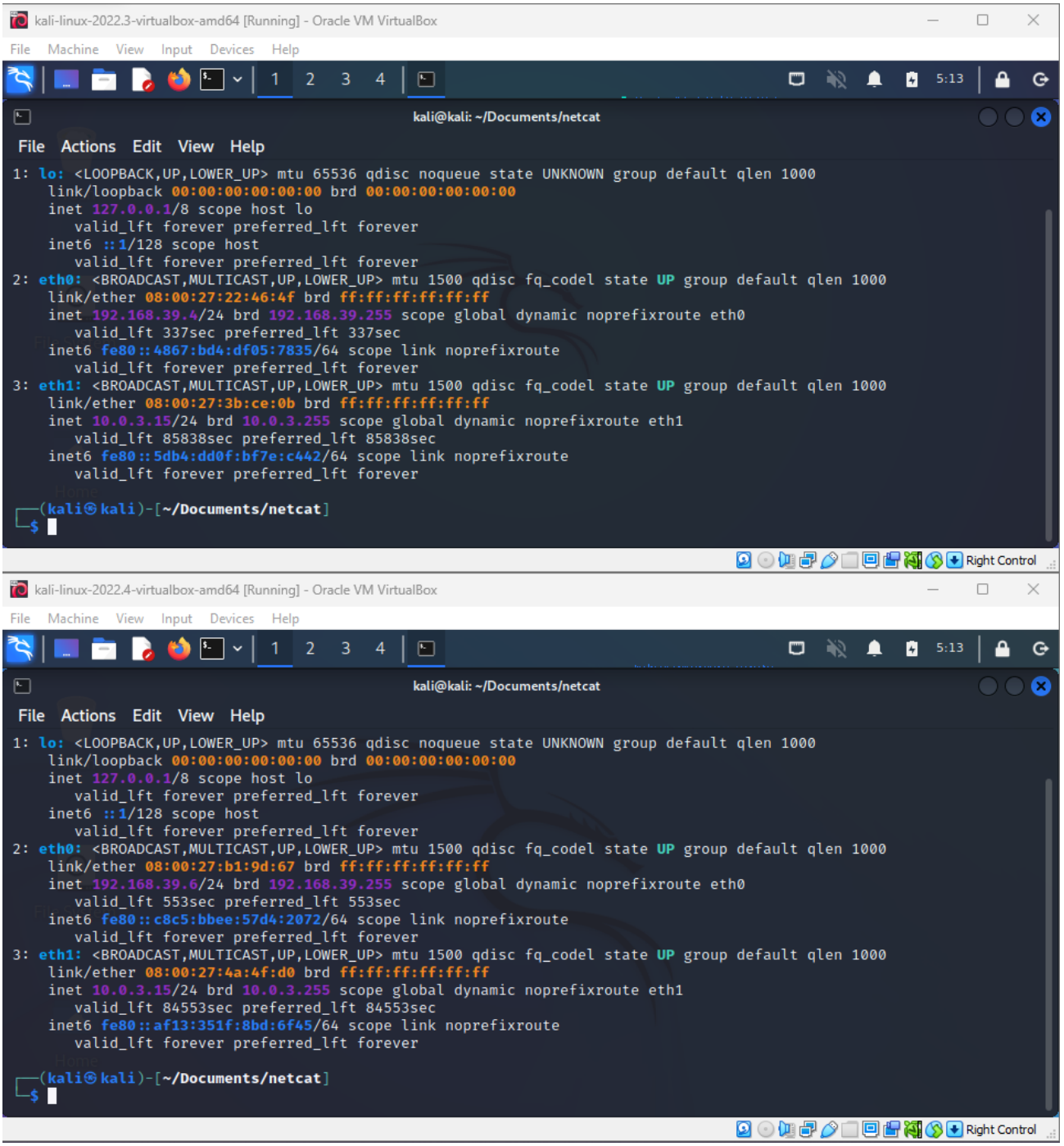


4. OpenVPN.

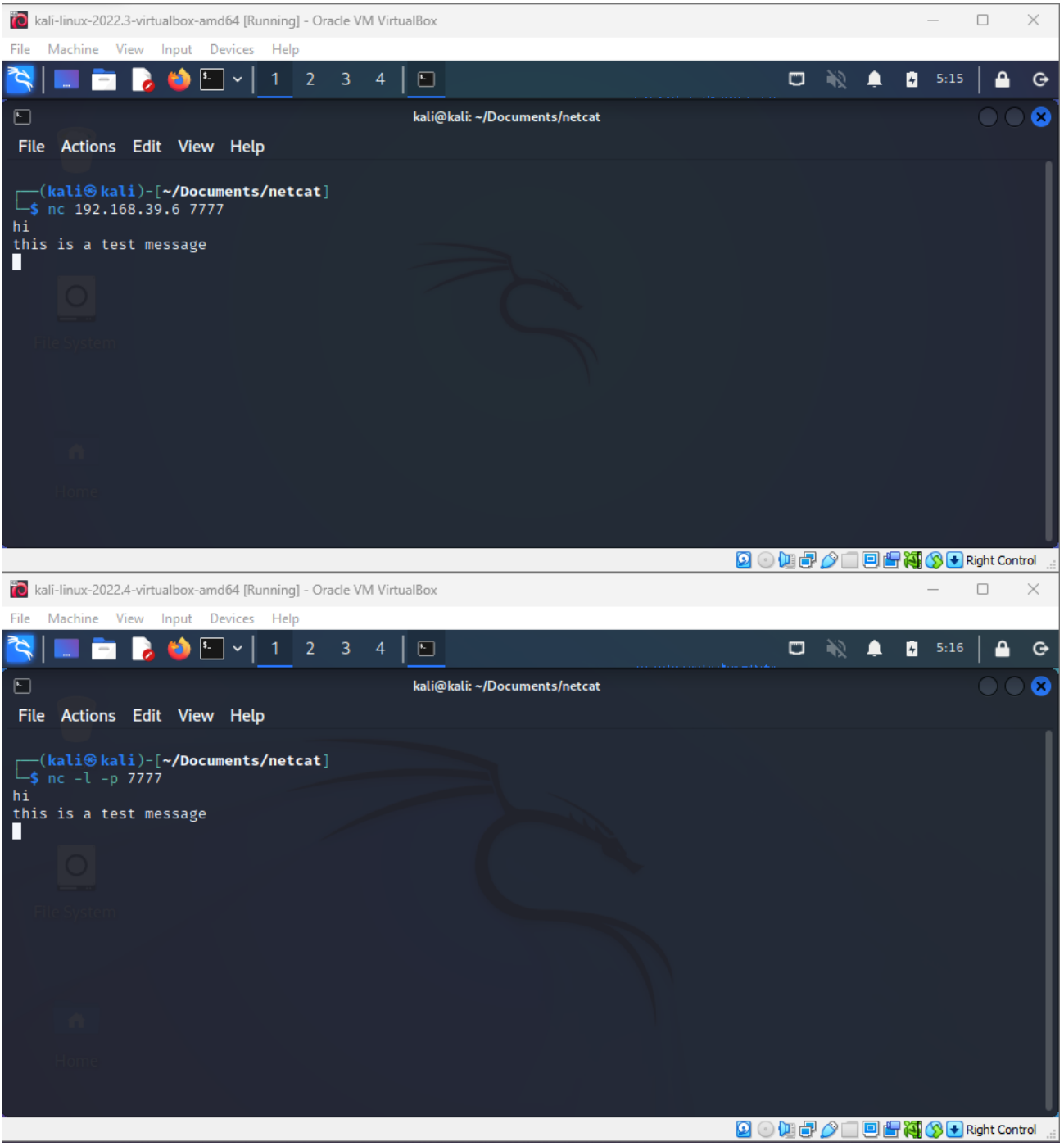
Netcat is a tool that is used to send data between clients, below is an example configuration:

- Sending a text message
  - clientB: run the command: ***nc -l -p 7777***,
  - clientA: run the command: *nc X.X.X.X 7777* (X.X.X.X - is the ip address of the clientB, 7777 is the port used for Netcat communication),
  - type a text in a terminal,
- Sending a file,
  - clientB: ***nc -l -p 7777 > file_name***
  - clientA: cilentA: ***cat ./file_name | nc X.X.X.X 7777***

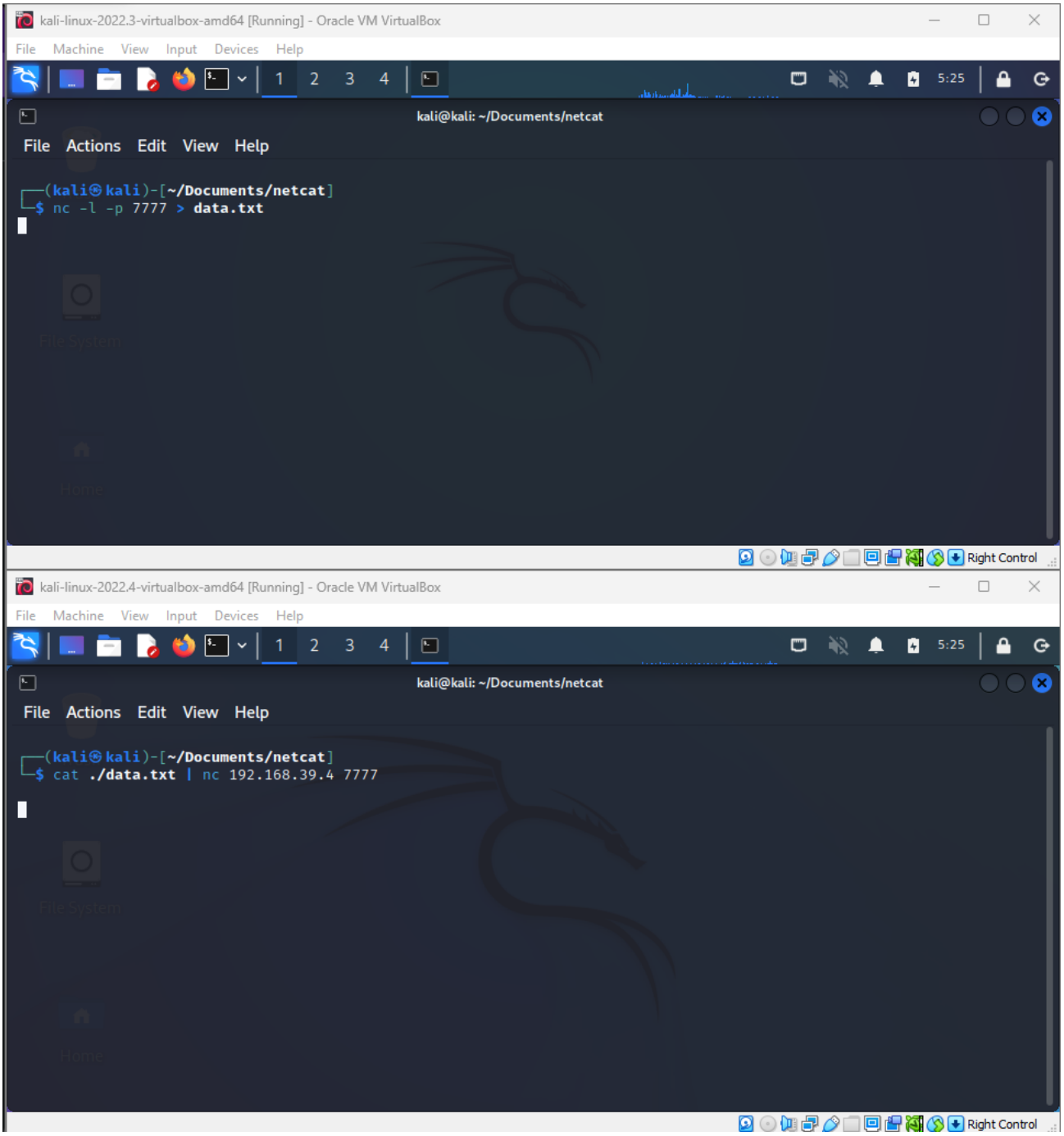
The Wireshark is used to capture the traffic on network interfaces.



192.168.39.4 as ClientA && 192.168.39.6 as ClientB



Transferring file,

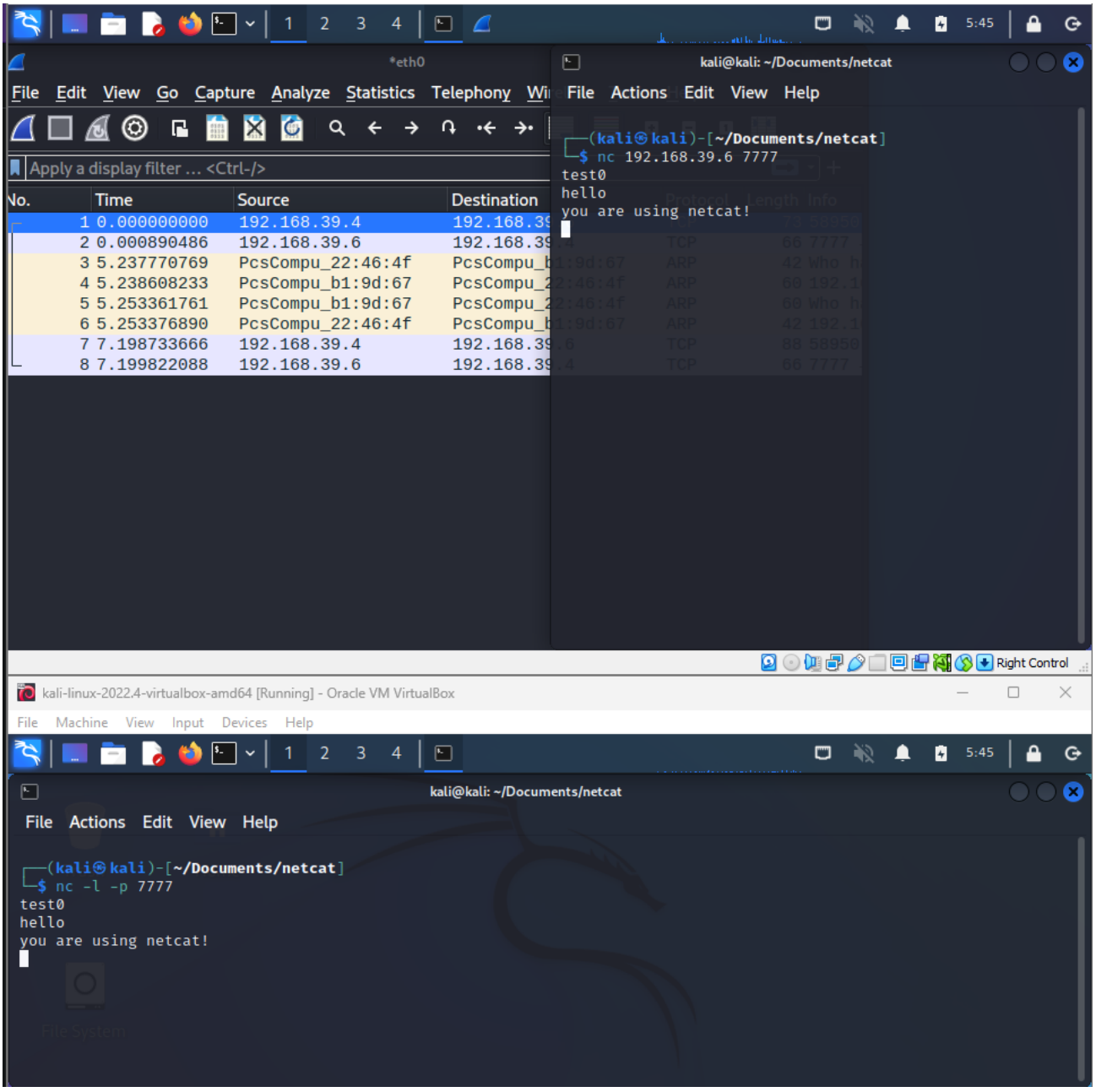


>>>>> In the document ClientA and ClientB are reversed<<<<<<

I. Task 1:

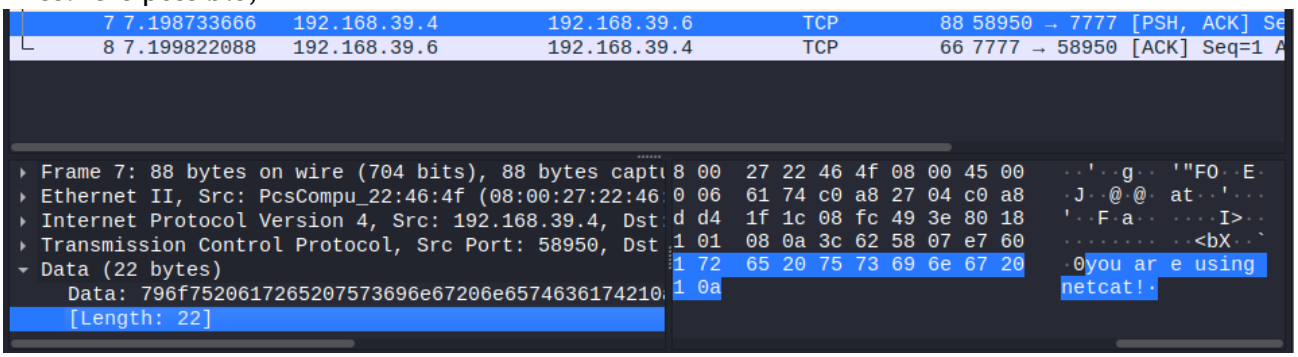
- Capture the network traffic on the VPN network interface (usually, the name is tun0, check it using *ifconfig* command).
- Send a few messages using *netcat* between clients A and B.

> >



• Observe and analyze the communication process and it is content in the WS. • Find and verify the data sent by netcat in the WS. Is it possible to read the message that was sent by netcat? Take a print screen of the data contained in the packets.

> Yes! It is possible,

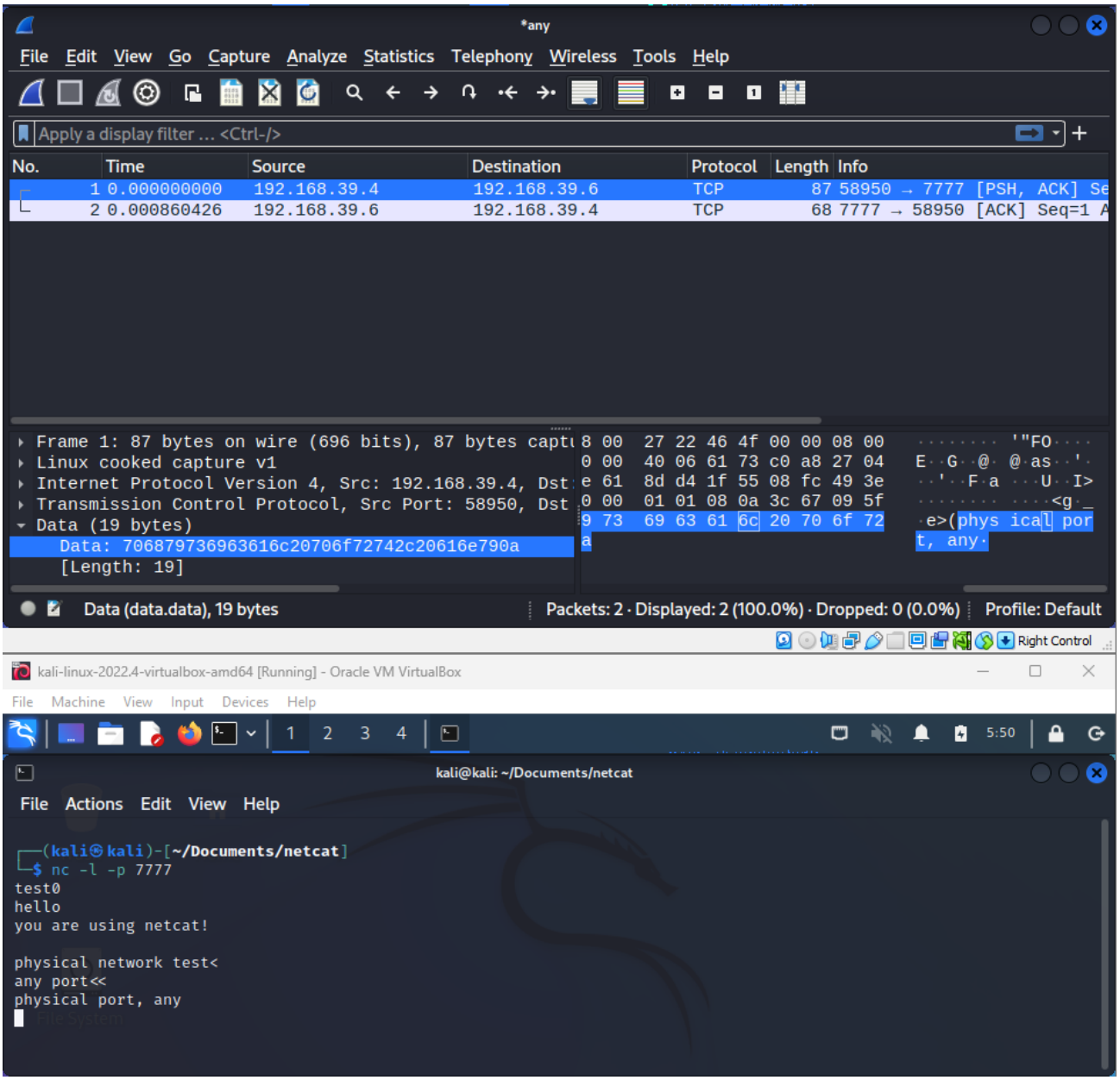


II. Task 2:

- Capture the network traffic on the physical network interface (usually, the name starts with *en*…)
- Send a few messages using *netcat* between clients A and B.

• Observe and analyze the communication process and it is content in the WS. • Find and verify the data sent by netcat in the WS. Take a print screen of the data contained in the packets.

> > >



Questions to task 1 and 2:

1. Is it possible to read the message that was sent via netcat?

> Yes, it is possible to read the message that was sent via netcat. The netcat utility creates a connection between two systems and sends data over the connection which can then be read by the receiving system.

2. What is the characteristic of captured traffic on the VPN network interface and the host interface?

> The characteristic of captured traffic on the VPN network interface would be encrypted data, while the host interface would have plaintext data.

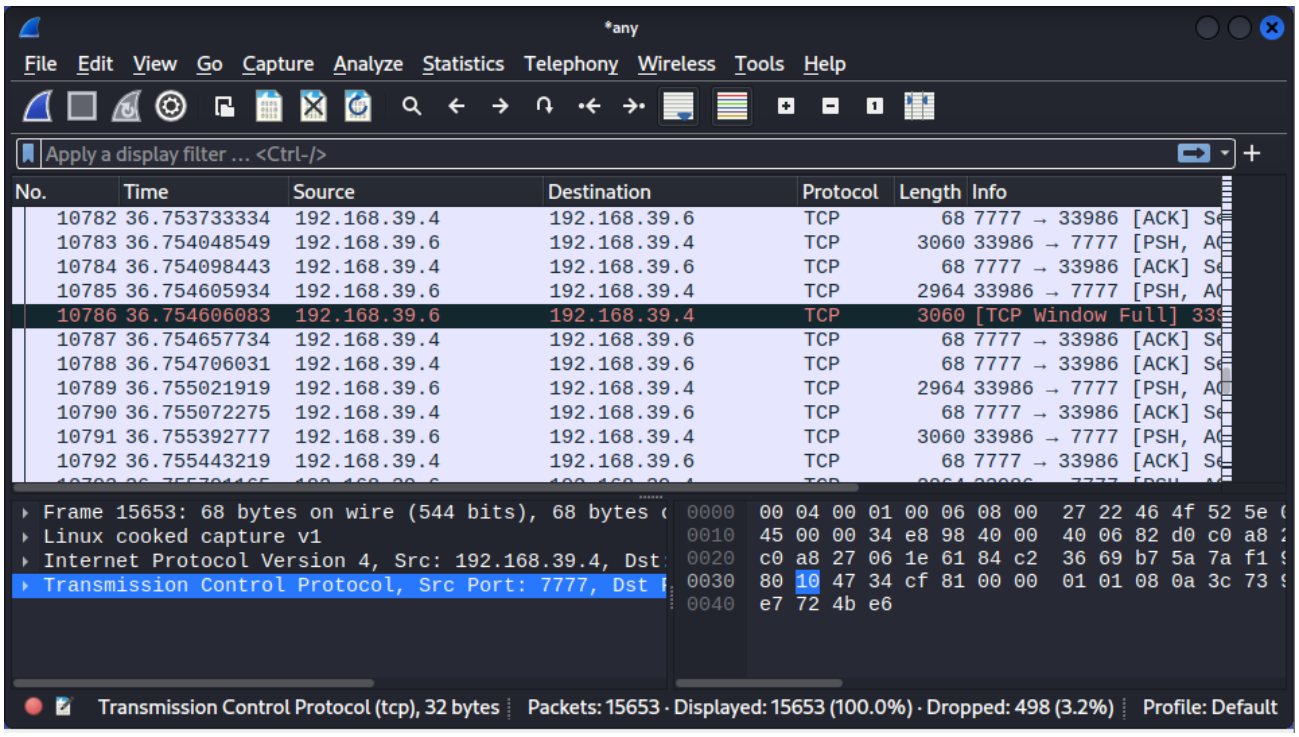
3. What relevant information can you see analyzing the traffic for both cases?

> Analyzing the traffic for both cases, relevant information such as IP addresses, port numbers, protocol type, and other relevant data can be seen. Additionally, the encrypted data of the VPN network interface can be decrypted to reveal the original content of the data.

III. Task 3:

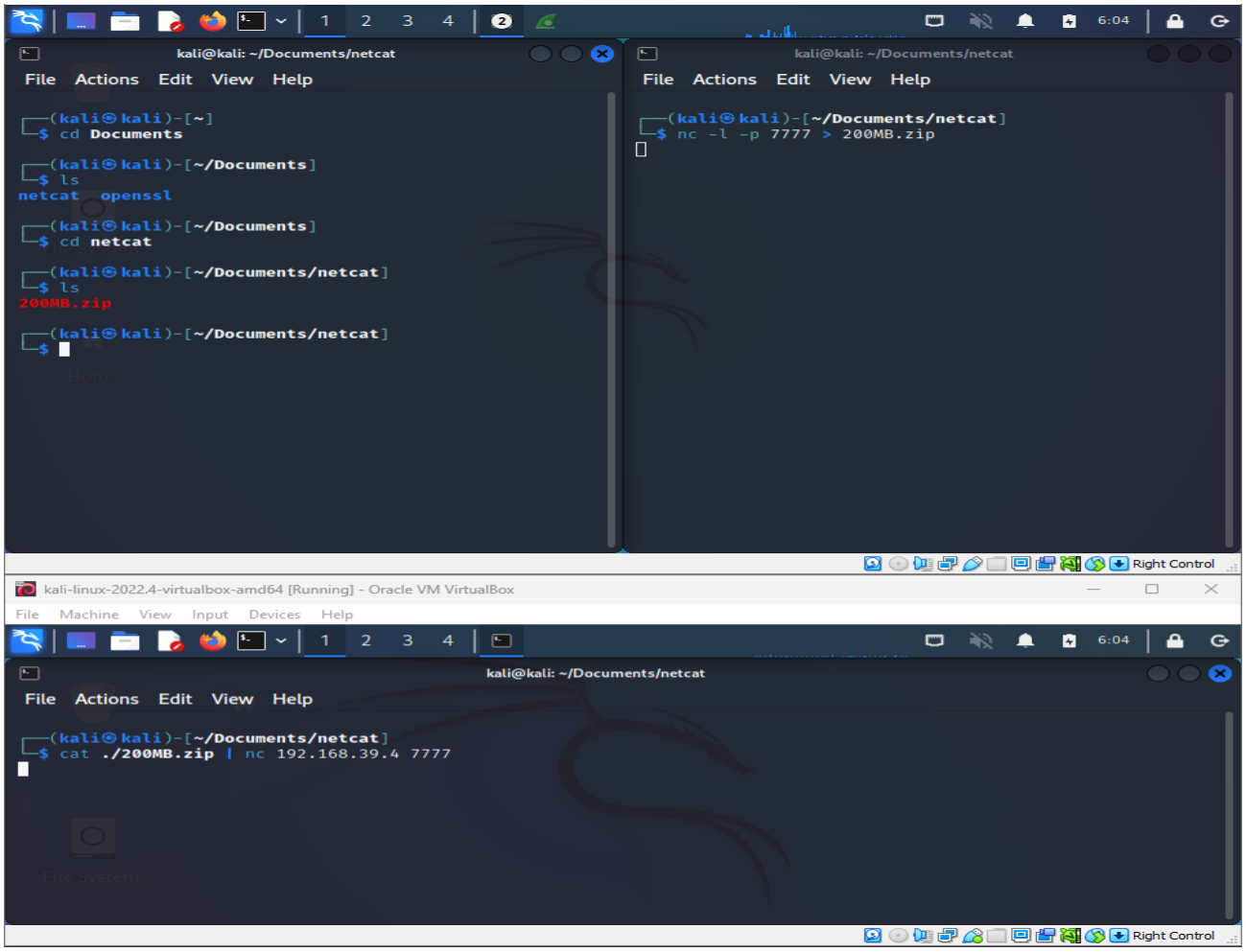
- Capture the network traffic on the physical network interface (usually, the name starts with *en*…),

>



- Send a large file via netcat. The file is located on the client's VM. (in directory: /home/kali/Desktop/FILES/ubuntu.iso, ubuntu.iso ~900MB)

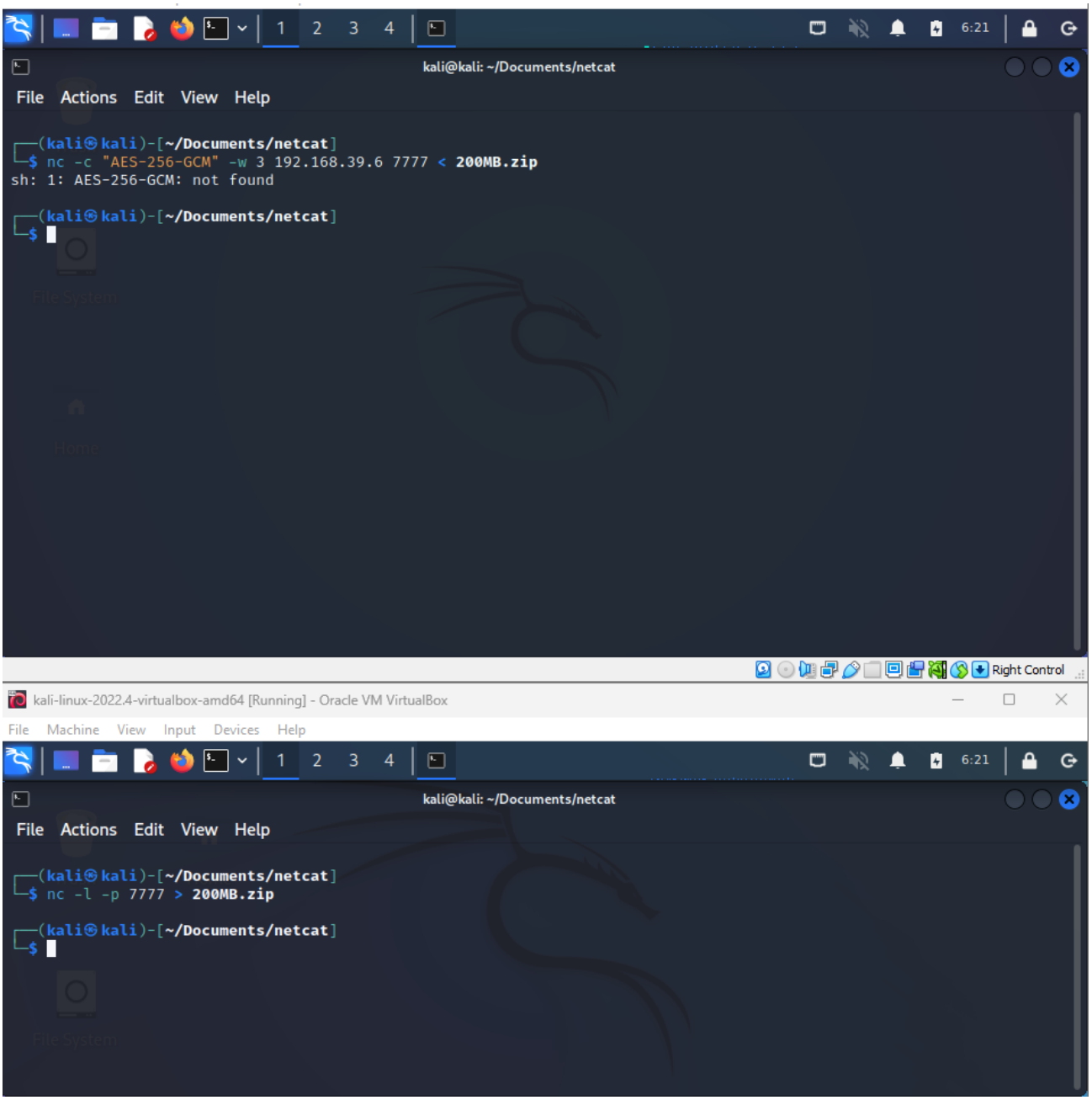
> i used 200MB (bad home internet)



• Transfer the file 4 times, each time change the encryption and authentication algorithm. Edit **client.conf** for both clients and change the following parameters simultaneously:

1. Setting 1
    a. cipher AES-256-GCM,
    b. auth SHA512,cat
2. Setting 2
    a. Cipher AES-128-CBC,
    b. Auth SHA1,
3. Setting 3
    a. Cipher DES-EDE-CBC,
    b. Auth MD5,
4. Setting 4
    a. Cipher DES-CBC,
    b. Auth MD5,

• Observe and analyze the communication process and it is content in the WS. • Measure the time of data transfer.



For different commands it says “not found”, if there was better documentation on the file - it would help a lot!

IV. Questions:

1. Is there a difference in data transfer times? What can affect them?

> it would differ as different algorithms use different hash functions.

2. What can we say about the encryption and authentication algorithms used?

> an educated guess would be - it depends on different algorithms used.

3. Which set of settings is the worst and which is the best in terms of security?

> simple google search shows, the cipher AES-256-GCM is the best one & the Cipher DES-CBC tends to be the worst one.