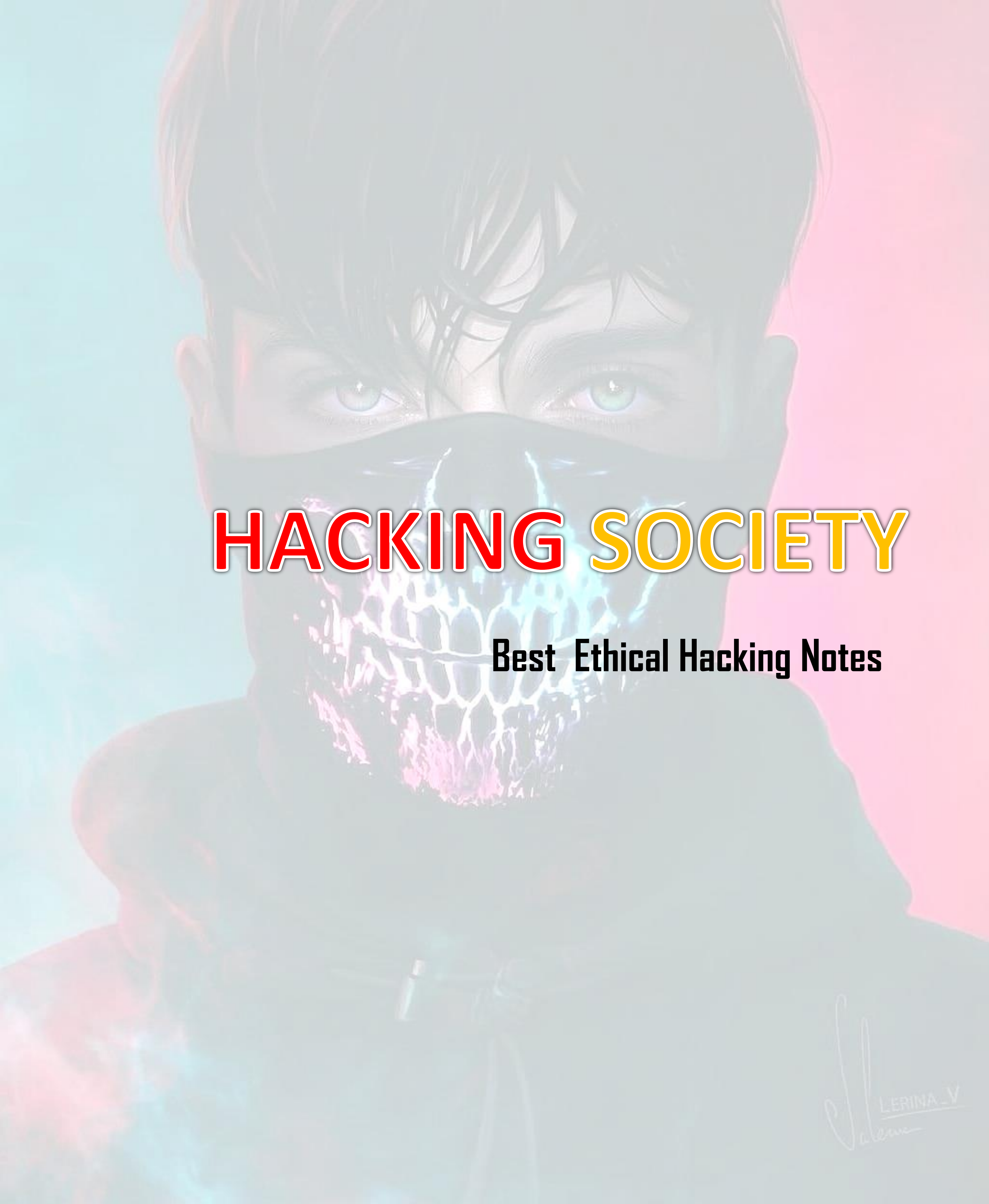
HackitTech

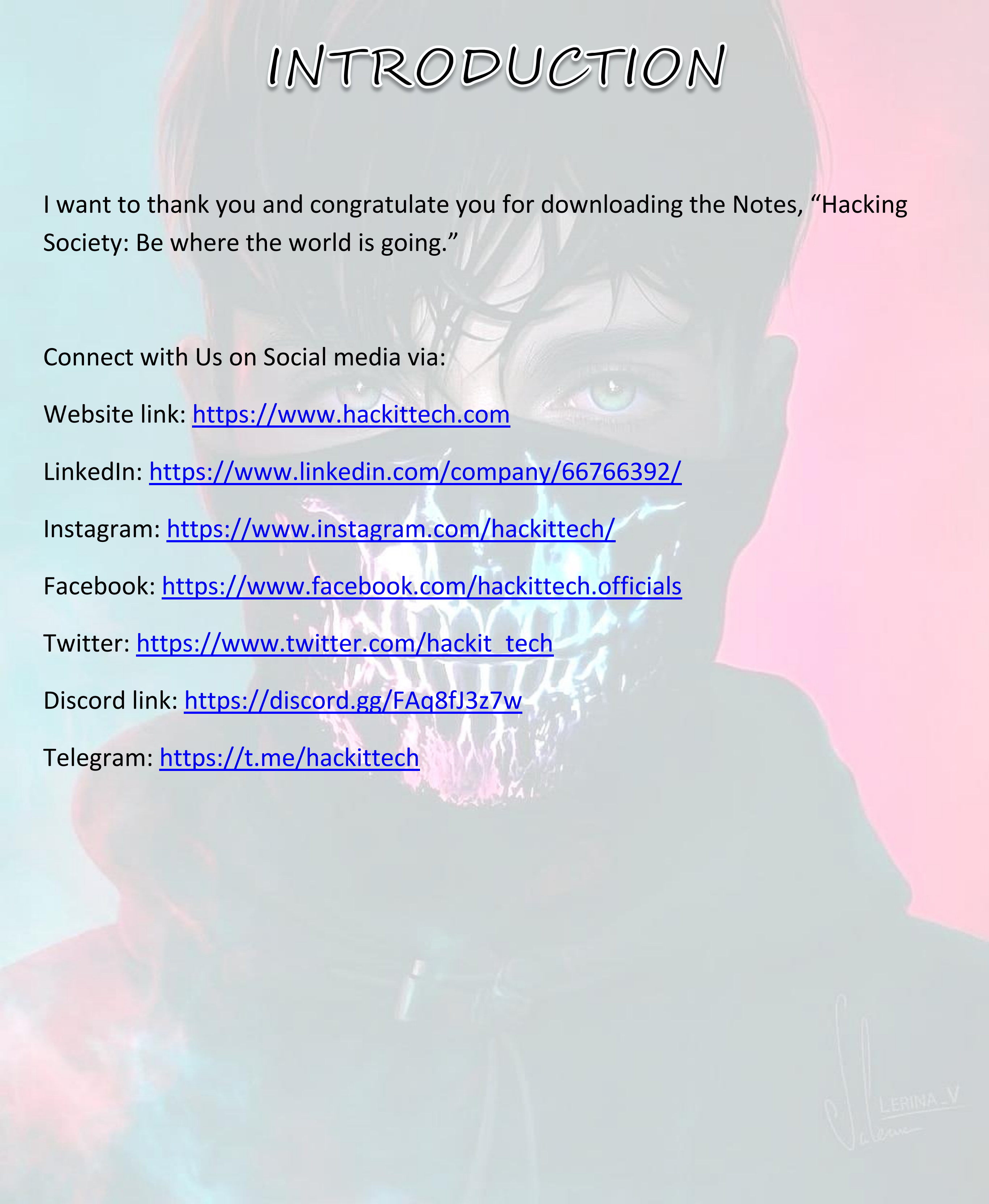


HACKING SOCIETY

Best Ethical Hacking Notes

By Sandeep Kumar

Insta [@admirerr_20]



INTRODUCTION

I want to thank you and congratulate you for downloading the Notes, “Hacking Society: Be where the world is going.”

Connect with Us on Social media via:

Website link: https://www.hackittech.com

LinkedIn: https://www.linkedin.com/company/66766392/

Instagram: https://www.instagram.com/hackittech/

Facebook: https://www.facebook.com/hackittech.officials

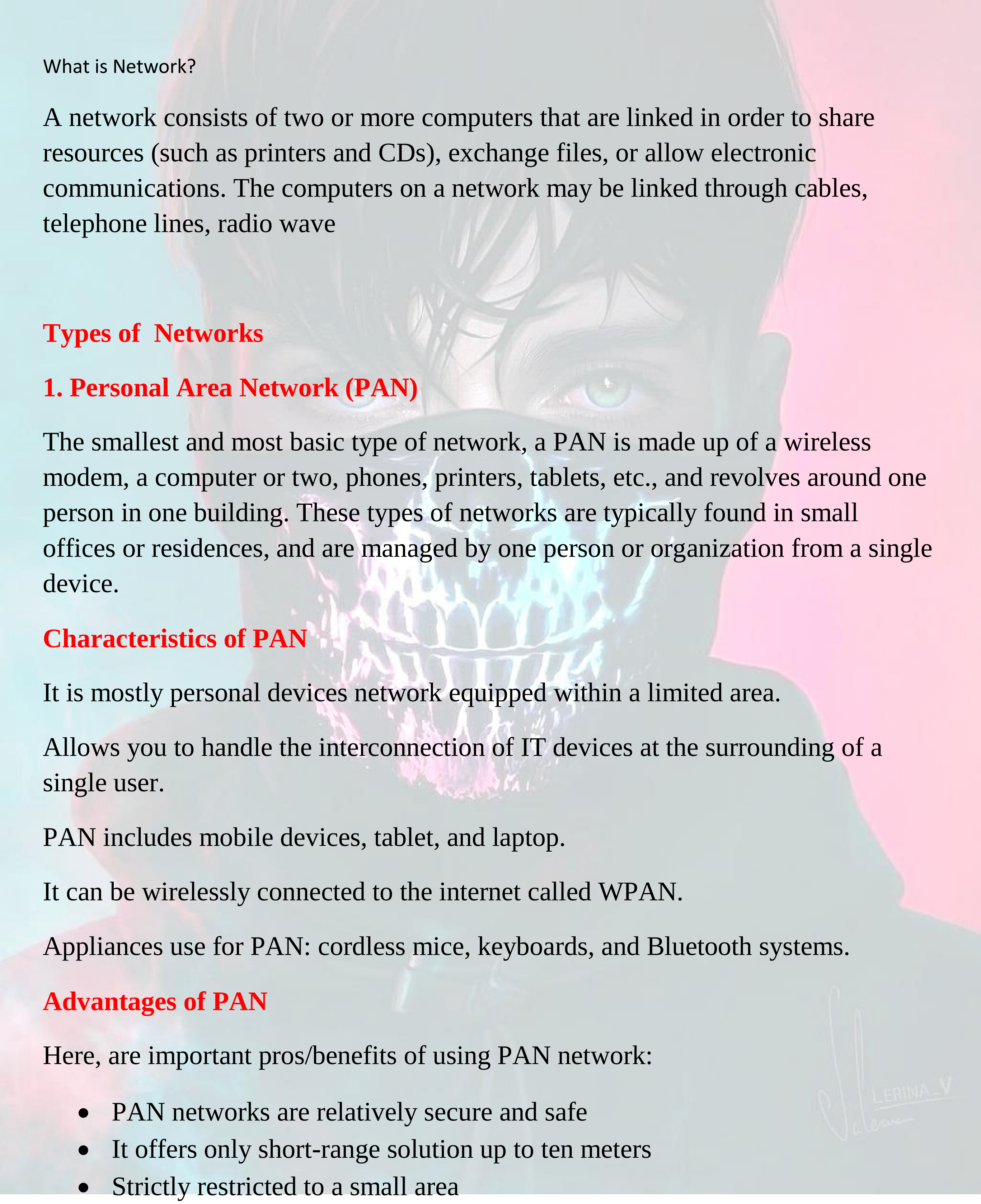
Twitter: https://www.twitter.com/hackit_tech

Discord link: https://discord.gg/FAq8fJ3z7w

Telegram: https://t.me/hackittech

By Sandeep Kumar

Insta @admirerr_20



What is Network?

A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio wave

Types of Networks

1. Personal Area Network (PAN)

The smallest and most basic type of network, a PAN is made up of a wireless modem, a computer or two, phones, printers, tablets, etc., and revolves around one person in one building. These types of networks are typically found in small offices or residences, and are managed by one person or organization from a single device.

Characteristics of PAN

It is mostly personal devices network equipped within a limited area.

Allows you to handle the interconnection of IT devices at the surrounding of a single user.

PAN includes mobile devices, tablet, and laptop.

It can be wirelessly connected to the internet called WPAN.

Appliances use for PAN: cordless mice, keyboards, and Bluetooth systems.

Advantages of PAN

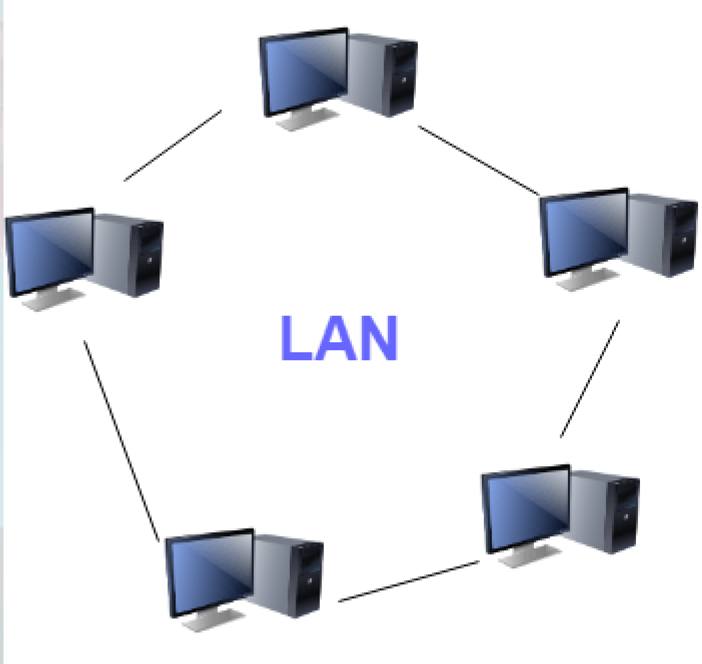
Here, are important pros/benefits of using PAN network:

- PAN networks are relatively secure and safe
- It offers only short-range solution up to ten meters
- Strictly restricted to a small area

Disadvantages of PAN

- Here are important cons/ drawback of using PAN network:
- It may establish a bad connection to other networks at the same radio bands.
- Distance limits.

2. Local Area Network (LAN)



We're confident that you've heard of these types of networks before – LANs are the most frequently discussed networks, one of the most common, one of the most original and one of the simplest types of networks. LANs connect groups of computers and low-voltage devices together across short distances (within a building or between a group of two or three buildings in close proximity to each other) to share information and resources. Enterprises typically manage and maintain LANs.

Using routers, LANs can connect to wide area networks (WANs, explained below) to rapidly and safely transfer data.

Characteristics of LAN

Here are important characteristics of a LAN network:

- It is a private network, so an outside regulatory body never controls it.
- LAN operates at a relatively higher speed compared to other WAN systems.
- There are various kinds of media access control methods like token ring and ethernet.

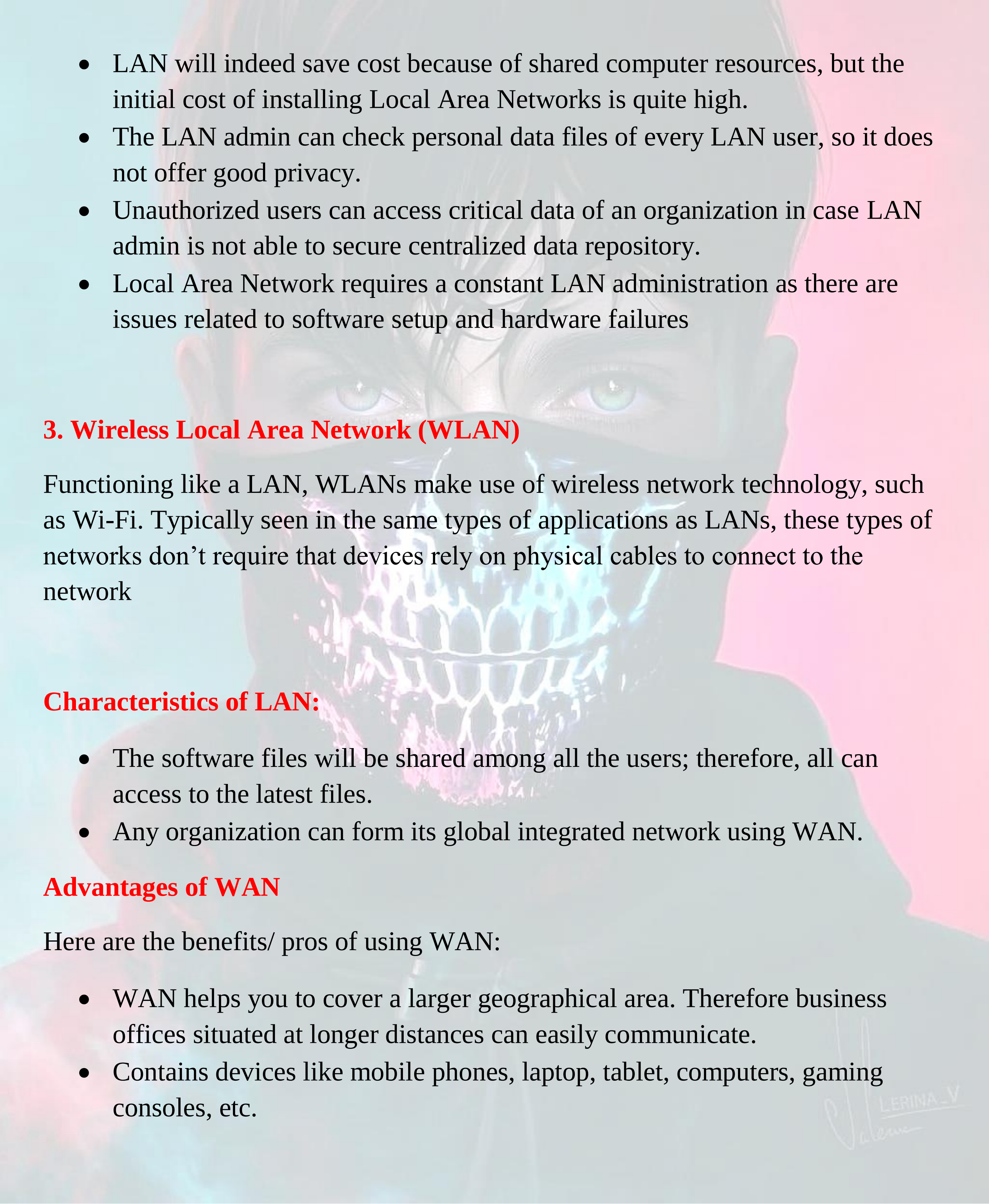
Advantages of LAN

Here are pros/benefits of using LAN:

- Computer resources like hard-disks, DVD-ROM, and printers can share local area networks. This significantly reduces the cost of hardware purchases.
- You can use the same software over the network instead of purchasing the licensed software for each client in the network.
- Data of all network users can be stored on a single hard disk of the server computer.
- You can easily transfer data and messages over networked computers.
- It will be easy to manage data at only one place, which makes data more secure.
- Local Area Network offers the facility to share a single internet connection among all the LAN users.

Disadvantages of LAN

Here are the important cons/ drawbacks of LAN:



- LAN will indeed save cost because of shared computer resources, but the initial cost of installing Local Area Networks is quite high.
- The LAN admin can check personal data files of every LAN user, so it does not offer good privacy.
- Unauthorized users can access critical data of an organization in case LAN admin is not able to secure centralized data repository.
- Local Area Network requires a constant LAN administration as there are issues related to software setup and hardware failures

3. Wireless Local Area Network (WLAN)

Functioning like a LAN, WLANs make use of wireless network technology, such as Wi-Fi. Typically seen in the same types of applications as LANs, these types of networks don’t require that devices rely on physical cables to connect to the network

Characteristics of LAN:

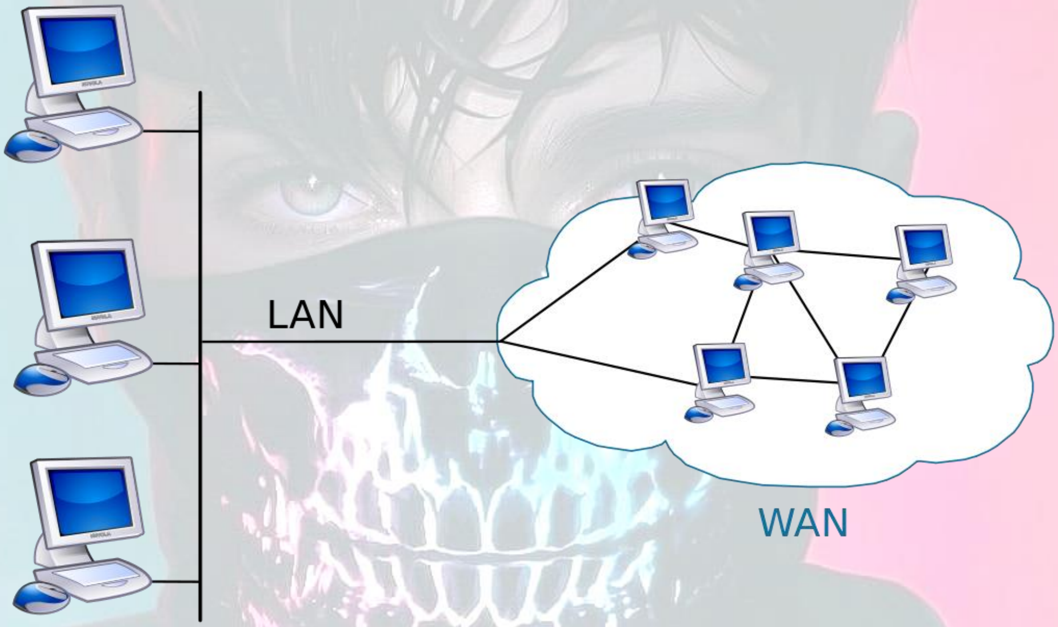
- The software files will be shared among all the users; therefore, all can access to the latest files.
- Any organization can form its global integrated network using WAN.

Advantages of WAN

Here are the benefits/ pros of using WAN:

- WAN helps you to cover a larger geographical area. Therefore business offices situated at longer distances can easily communicate.
- Contains devices like mobile phones, laptop, tablet, computers, gaming consoles, etc.

- WLAN connections work using radio transmitters and receivers built into client devices.



Disadvantage of WAN

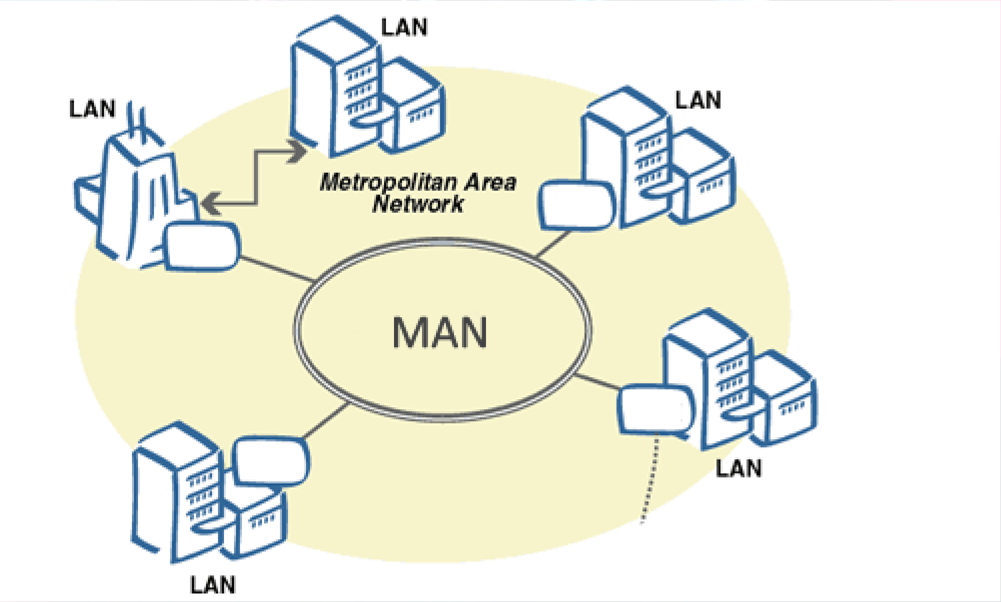
Here are drawbacks/cons of using WAN:

- The initial setup cost of investment is very high.
- It is difficult to maintain the WAN network. You need skilled technicians and network administrators.
- There are more errors and issues because of the wide coverage and the use of different technologies.

- It requires more time to resolve issues because of the involvement of multiple wired and wireless technologies.
- Offers lower security compared to other types of networks.

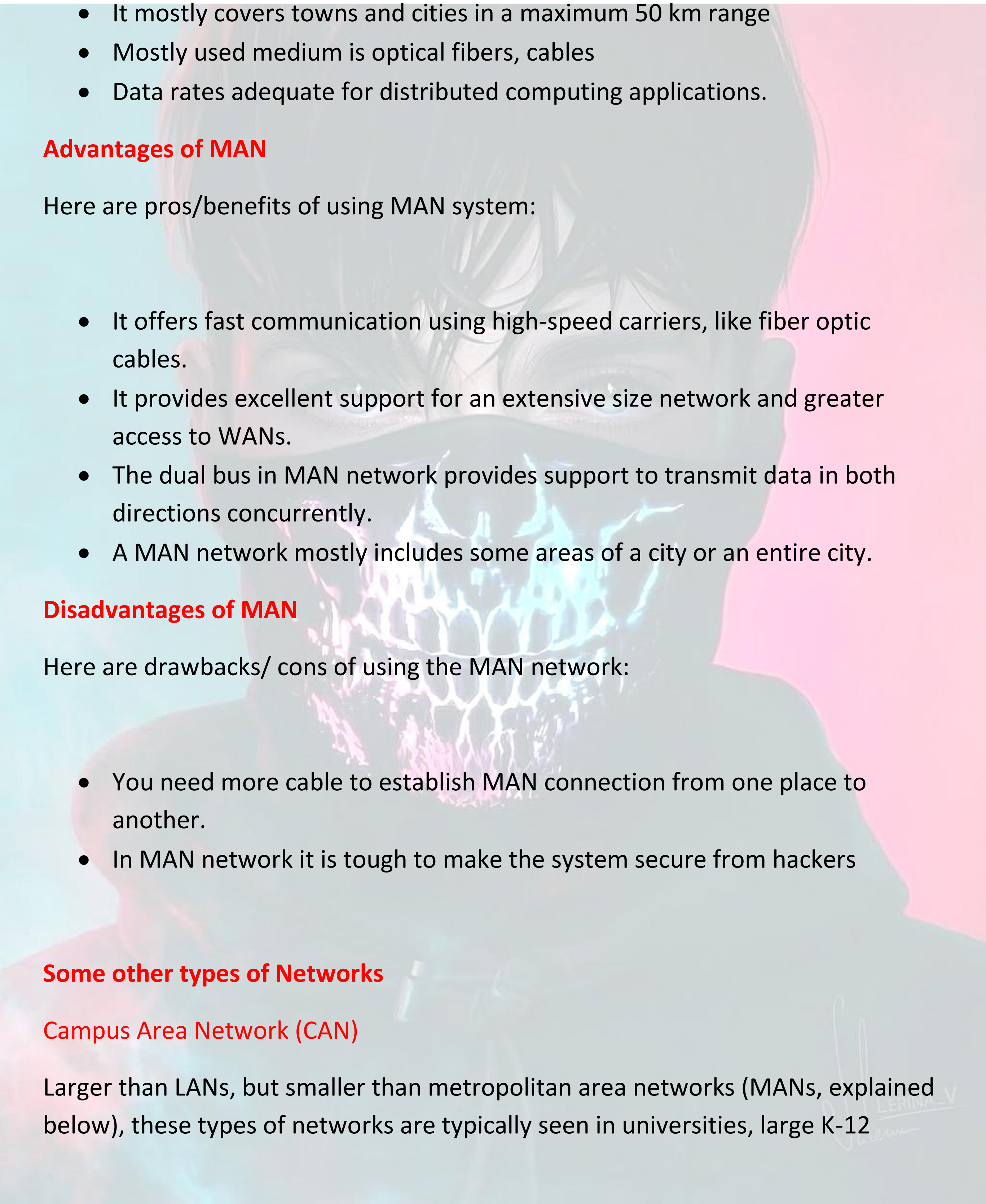
4. Metropolitan Area Network (MAN)

These types of networks are larger than LANs but smaller than WANs – and incorporate elements from both types of networks. MANs span an entire geographic area (typically a town or city, but sometimes a campus). Ownership and maintenance is handled by either a single person or company (a local council, a large company, etc.).



Characteristics of MAN

Here are important characteristics of the MAN network:



- It mostly covers towns and cities in a maximum 50 km range
- Mostly used medium is optical fibers, cables
- Data rates adequate for distributed computing applications.

Advantages of MAN

Here are pros/benefits of using MAN system:

- It offers fast communication using high-speed carriers, like fiber optic cables.
- It provides excellent support for an extensive size network and greater access to WANs.
- The dual bus in MAN network provides support to transmit data in both directions concurrently.
- A MAN network mostly includes some areas of a city or an entire city.

Disadvantages of MAN

Here are drawbacks/ cons of using the MAN network:

- You need more cable to establish MAN connection from one place to another.
- In MAN network it is tough to make the system secure from hackers

Some other types of Networks

Campus Area Network (CAN)

Larger than LANs, but smaller than metropolitan area networks (MANs, explained below), these types of networks are typically seen in universities, large K-12 school districts or small businesses. They can be spread across several buildings that are fairly close to each other so users can share resources.

Wide Area Network (WAN)

Slightly more complex than a LAN, a WAN connects computers together across longer physical distances. This allows computers and low-voltage devices to be remotely connected to each other over one large network to communicate even when they're miles apart

The Internet is the most basic example of a WAN, connecting all computers together around the world. Because of a WAN's vast reach, it is typically owned and maintained by multiple administrators or the public

Storage-Area Network (SAN)

As a dedicated high-speed network that connects shared pools of storage devices to several servers, these types of networks don't rely on a LAN or WAN. Instead, they move storage resources away from the network and place them into their own high-performance network. SANs can be accessed in the same fashion as a drive attached to a server. Types of storage-area networks include converged, virtual and unified SANs.

System-Area Network (also known as SAN)

This term is fairly new within the past two decades. It is used to explain a relatively local network that is designed to provide high-speed connection in server-to-server applications (cluster environments), storage area networks (called "SANs" as well) and processor-to-processor applications. The computers connected on a SAN operate as a single system at very high speeds.

Passive Optical Local Area Network (POLAN)

As an alternative to traditional switch-based Ethernet LANs, POLAN technology can be integrated into structured cabling to overcome concerns about supporting traditional Ethernet protocols and network applications such as PoE (Power over Ethernet). A point-to-multipoint LAN architecture, POLAN uses optical splitters to split an optical signal from one strand of singlemode optical fiber into multiple signals to serve users and devices.

Enterprise Private Network (EPN)

These types of networks are built and owned by businesses that want to securely connect its various locations to share computer resources.

Virtual Private Network (VPN)

By extending a private network across the Internet, a VPN lets its users send and receive data as if their devices were connected to the private network – even if they're not. Through a virtual point-to-point connection, users can access a private network remotely.

IP Address

- A unique Identification number to each Device connected to the Internet
- Internet – Interconnection of Devices to Share Data and Services.
  Eg. 192.168.0.1
- 32 Bit IP Address
- Each Octet Carries 8 Bit
- Totally there are 4,294,967,296
  0.0.0.0-255.255.255.255

DNS: Matching domain names to IP addresses

Many (though not all) internet-connected computers also have human-readable addresses that may include words and are known as domain names such as networkworld.com, for example. The Domain Name System, or DNS, is another part of the Internet protocol suite, and it makes sure that requests made using domain names reach the correct IP address. You can think of DNS as representing a more user-friendly layer on top of the IP-address infrastructure.

However, the IP address remains the fundamental way that internet-connected devices are found, and in some circumstances a domain name can correspond to multiple servers with different IP addresses

IP address versions: IPv4 and IPv6

There are two versions of IP addresses: IPv4 and IPv6, and they have different formats, the major difference between them being that it’s possible to create vastly more unique IPv6 addresses (2128) than IPv4 addresses (232).

That’s thanks to the format they use. IPv4 addresses are written in four parts separated by dots like this:

45.48.241.198

Each part written in conventional Base 10 numerals represents an eight-bit binary number from 0 to 255.

Each of these four numbers separated by dots is written in standard decimal notation. But computers fundamentally deal with numbers in binary (using just zeroes and ones, and each of the numbers in an IPv4 address represents an 8-bit binary number, which means that none of them can be higher than 255 (111111 in binary).

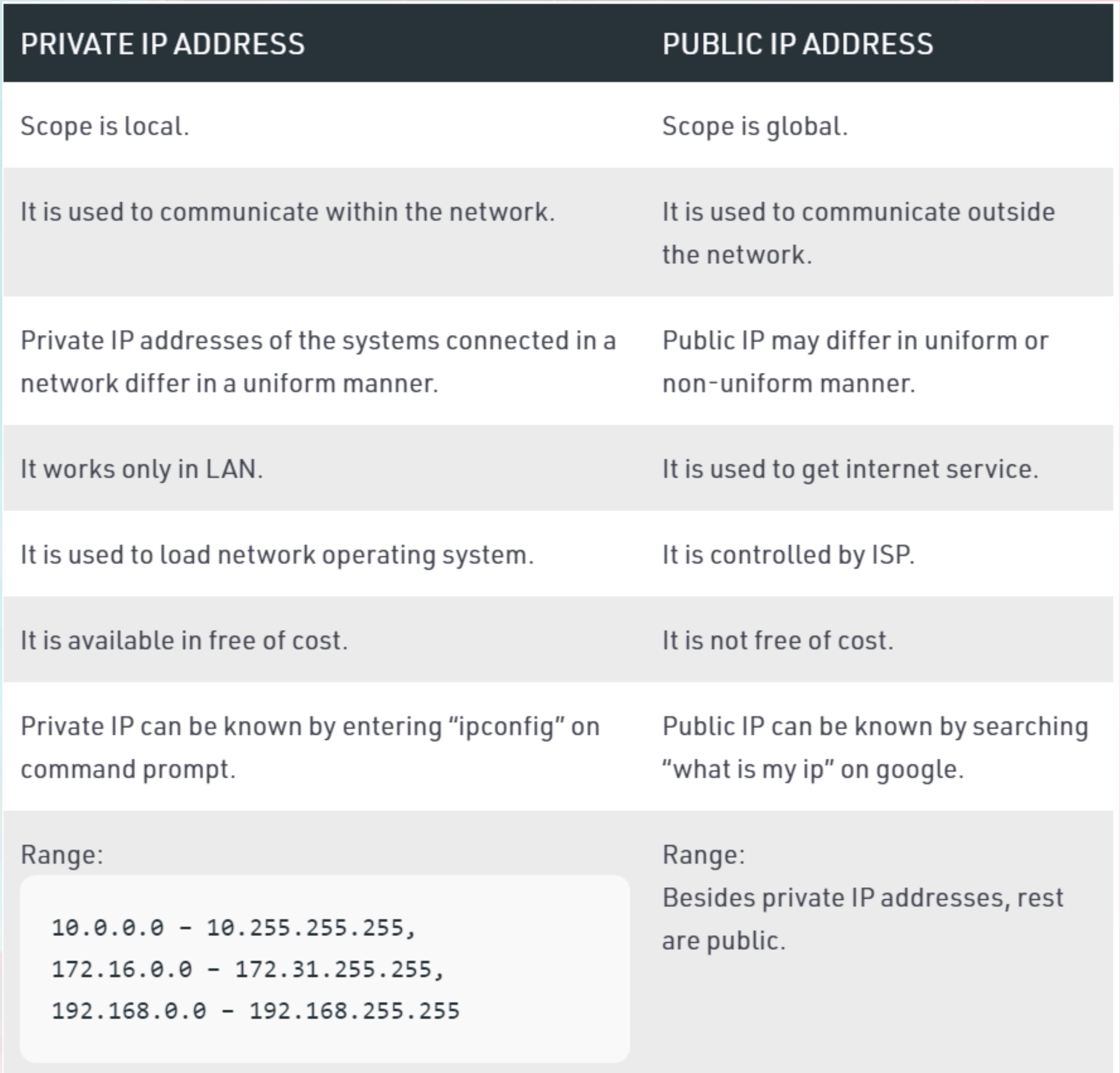
It’s quite likely that you’ve seen IP addresses like that one before since they’ve been around since 1983. The newer version of the protocol, IPv6, is slowly displacing IPv4, and its addressing looks like this:

2620:cc:8000:1c82:544c:cc2e:f2fa:5a9b

Note that instead of four numbers, there are eight, and they’re separated by colons rather than commas. And yes, they are all numbers. There are letters in there because IPv6 addresses are written in hexadecimal (Base 16) notation, which means 16 different symbols are required to uniquely represent Base 10 numbers 1-16. The ones used are numerals 0-9 plus letters A-F. Each of these numbers represents a 16-bit binary number, and the difference between that the 8-bit components of an IPv4 address is the main reason for IPv6’s existence.

IPv4 addresses are 32-bit numbers, and the total number of possible addresses of that length is the 232 mentioned above—about 4.3 billion. That’s number that seemed ample in the early days of the internet but began to loom as a potential crisis as internet-connected devices multiplied. IPv6 addresses are 128-bit numbers, which means that there are 2128 possible addresses, a number that we’re not going to bother writing out because it’s 39 digits long, but it's called 340 undecillion.

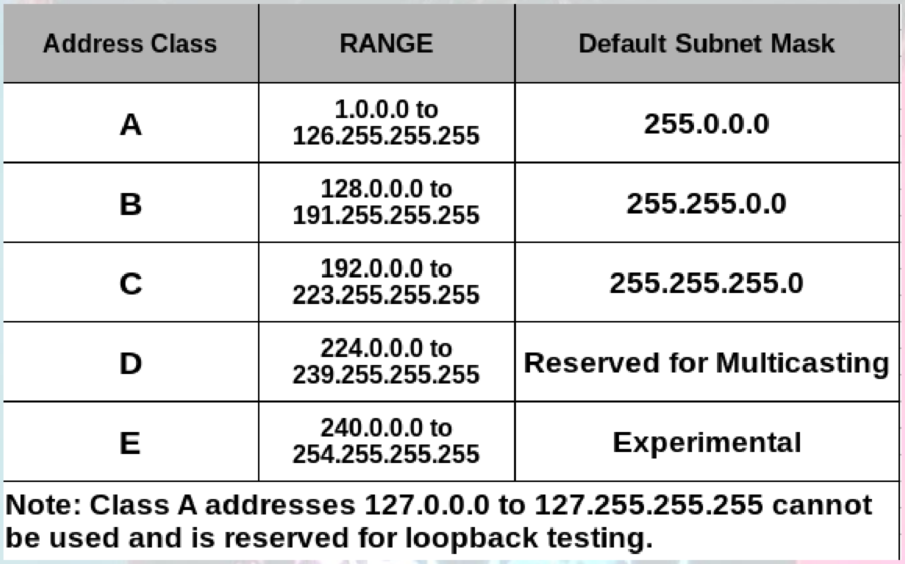
Public IP vs Private IP



PRIVATE IP ADDRESS	PUBLIC IP ADDRESS
Scope is local.	Scope is global.
It is used to communicate within the network.	It is used to communicate outside the network.
Private IP addresses of the systems connected in a network differ in a uniform manner.	Public IP may differ in uniform or non-uniform manner.
It works only in LAN.	It is used to get internet service.
It is used to load network operating system.	It is controlled by ISP.
It is available in free of cost.	It is not free of cost.
Private IP can be known by entering “ipconfig” on command prompt.	Public IP can be known by searching “what is my ip” on google.

Range:
`10.0.0.0 - 10.255.255.255,`
`172.16.0.0 - 172.31.255.255,`
`192.168.0.0 - 192.168.255.255`
	Range:
	Besides private IP addresses, rest are public.

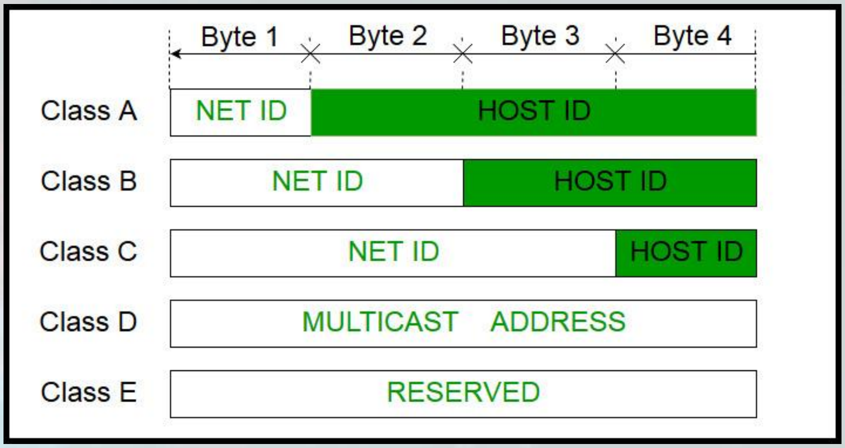
IP Address Classification



Address Class	RANGE	Default Subnet Mask
A	1.0.0.0 to 126.255.255.255	255.0.0.0
B	128.0.0.0 to 191.255.255.255	255.255.0.0
C	192.0.0.0 to 223.255.255.255	255.255.255.0
D	224.0.0.0 to 239.255.255.255	Reserved for Multicasting
E	240.0.0.0 to 254.255.255.255	Experimental

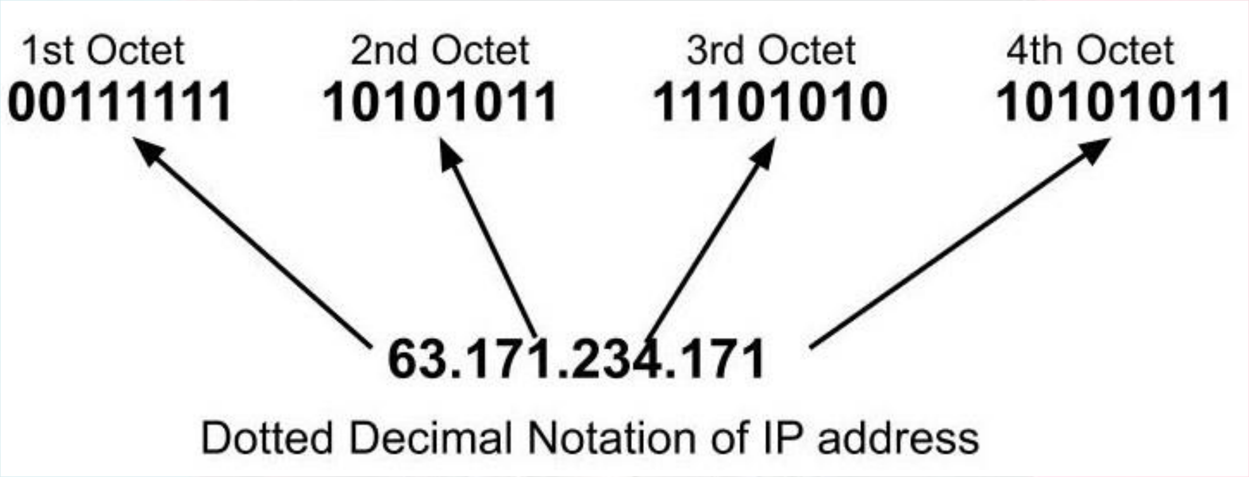
Note: Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and is reserved for loopback testing.

Subnet mask



By Sandeep Kumar

Insta @admirerr_20



DHCP

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway**.**

Why use DHCP?

Every device on a TCP/IP-based network must have a unique unicast IP address to access the network and its resources. Without DHCP, IP addresses for new computers or computers that are moved from one subnet to another must be configured manually; IP addresses for computers that are removed from the network must be manually reclaimed.

With DHCP, this entire process is automated and managed centrally. The DHCP server maintains a pool of IP addresses and leases an address to any DHCP-enabled client when it starts up on the network. Because the IP addresses are dynamic (leased) rather than static (permanently assigned), addresses no longer in use are automatically returned to the pool for reallocation

By Sandeep Kumar
Insta @admirerr_20

What is NAT vs. Bridged vs. Host-Only?

Host-Only: It can be thought of as a hybrid between the bridged and internal networking modes: as with bridged networking, the virtual machines can talk to each other and the host as if they were connected through a physical Ethernet switch. Similarly, as with internal networking however, a physical networking interface need not be present, and the virtual machines cannot talk to the world outside the host since they are not connected to a physical networking interface.

Instead, when host-only networking is used, VirtualBox creates a new software interface on the host which then appears next to your existing network interfaces. In other words, whereas with bridged networking an existing physical interface is used to attach virtual machines to, with host-only networking a new “loopback” interface is created on the host. And whereas with internal networking, the traffic between the virtual machines cannot be seen, the traffic on the “loopback” interface on the host can be intercepted.

Host-only networking is particularly useful for preconfigured virtual appliances, where multiple virtual machines are shipped together and designed to cooperate. For example, one virtual machine may contain a web server and a second one a database, and since they are intended to talk to each other, the appliance can instruct VirtualBox to set up a host-only network for the two. A second (bridged) network would then connect the web server to the outside world to serve data to, but the outside world cannot connect to the database.

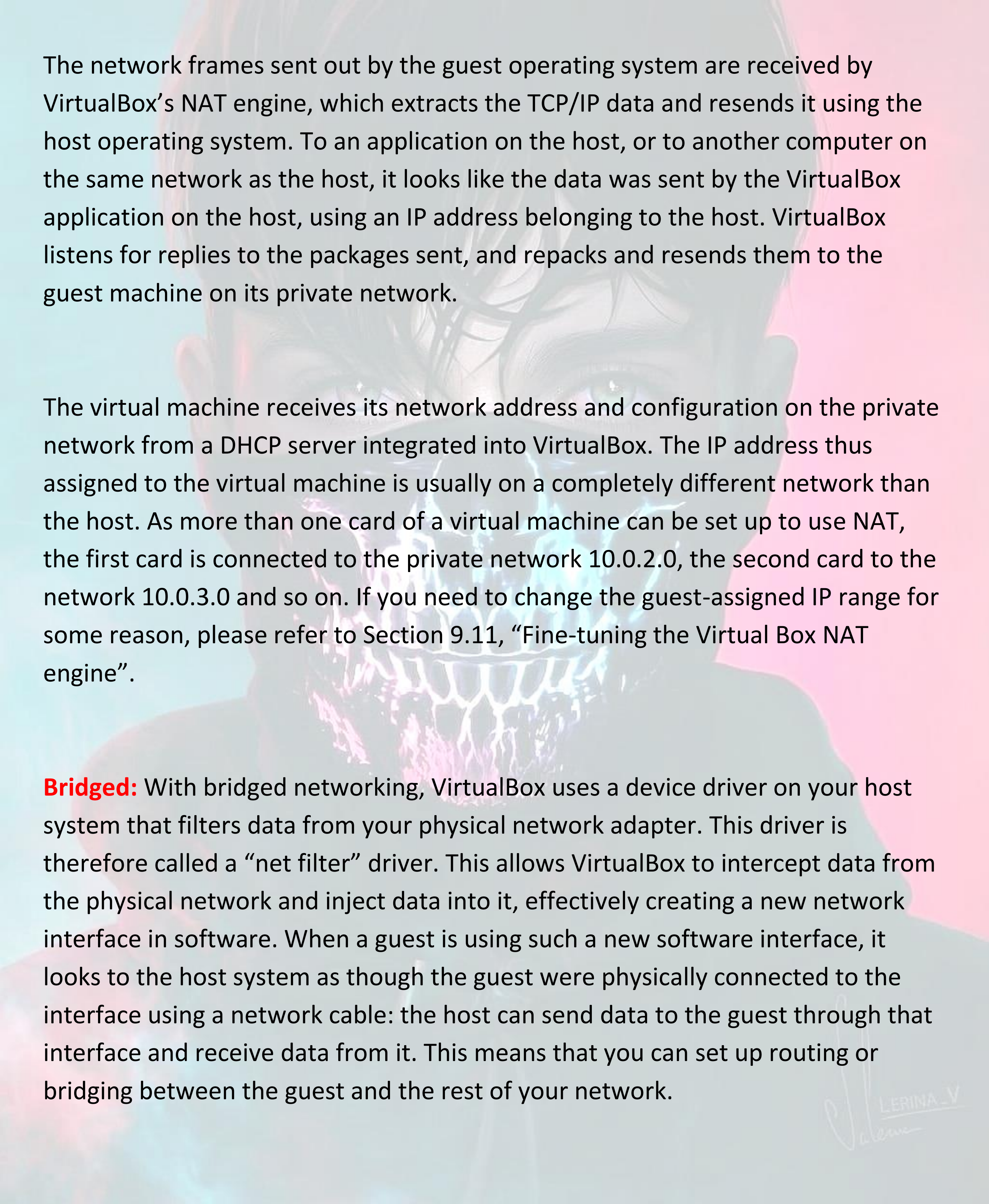
To change a virtual machine's virtual network interface to "host only" mode:

- either go to the "Network" page in the virtual machine's settings notebook in the graphical user interface and select "Host-only networking", or
- on the command line, type VBoxManage modifyvm "VM name" –nic hostonly; see Section 8.8, "VBoxManage modifyvm" for details.

NAT: Network Address Translation (NAT) is the simplest way of accessing an external network from a virtual machine. Usually, it does not require any configuration on the host network and guest system. For this reason, it is the default networking mode in VirtualBox.

A virtual machine with NAT enabled acts much like a real computer that connects to the Internet through a router. The "router", in this case, is the VirtualBox networking engine, which maps traffic from and to the virtual machine transparently. In VirtualBox this router is placed between each virtual machine and the host. This separation maximizes security since by default virtual machines cannot talk to each other.

The disadvantage of NAT mode is that, much like a private network behind a router, the virtual machine is invisible and unreachable from the outside internet; you cannot run a server this way unless you set up port forwarding (described below).



The network frames sent out by the guest operating system are received by VirtualBox's NAT engine, which extracts the TCP/IP data and resends it using the host operating system. To an application on the host, or to another computer on the same network as the host, it looks like the data was sent by the VirtualBox application on the host, using an IP address belonging to the host. VirtualBox listens for replies to the packages sent, and repacks and resends them to the guest machine on its private network.

The virtual machine receives its network address and configuration on the private network from a DHCP server integrated into VirtualBox. The IP address thus assigned to the virtual machine is usually on a completely different network than the host. As more than one card of a virtual machine can be set up to use NAT, the first card is connected to the private network 10.0.2.0, the second card to the network 10.0.3.0 and so on. If you need to change the guest-assigned IP range for some reason, please refer to Section 9.11, "Fine-tuning the Virtual Box NAT engine".

Bridged: With bridged networking, VirtualBox uses a device driver on your host system that filters data from your physical network adapter. This driver is therefore called a "net filter" driver. This allows VirtualBox to intercept data from the physical network and inject data into it, effectively creating a new network interface in software. When a guest is using such a new software interface, it looks to the host system as though the guest were physically connected to the interface using a network cable: the host can send data to the guest through that interface and receive data from it. This means that you can set up routing or bridging between the guest and the rest of your network.

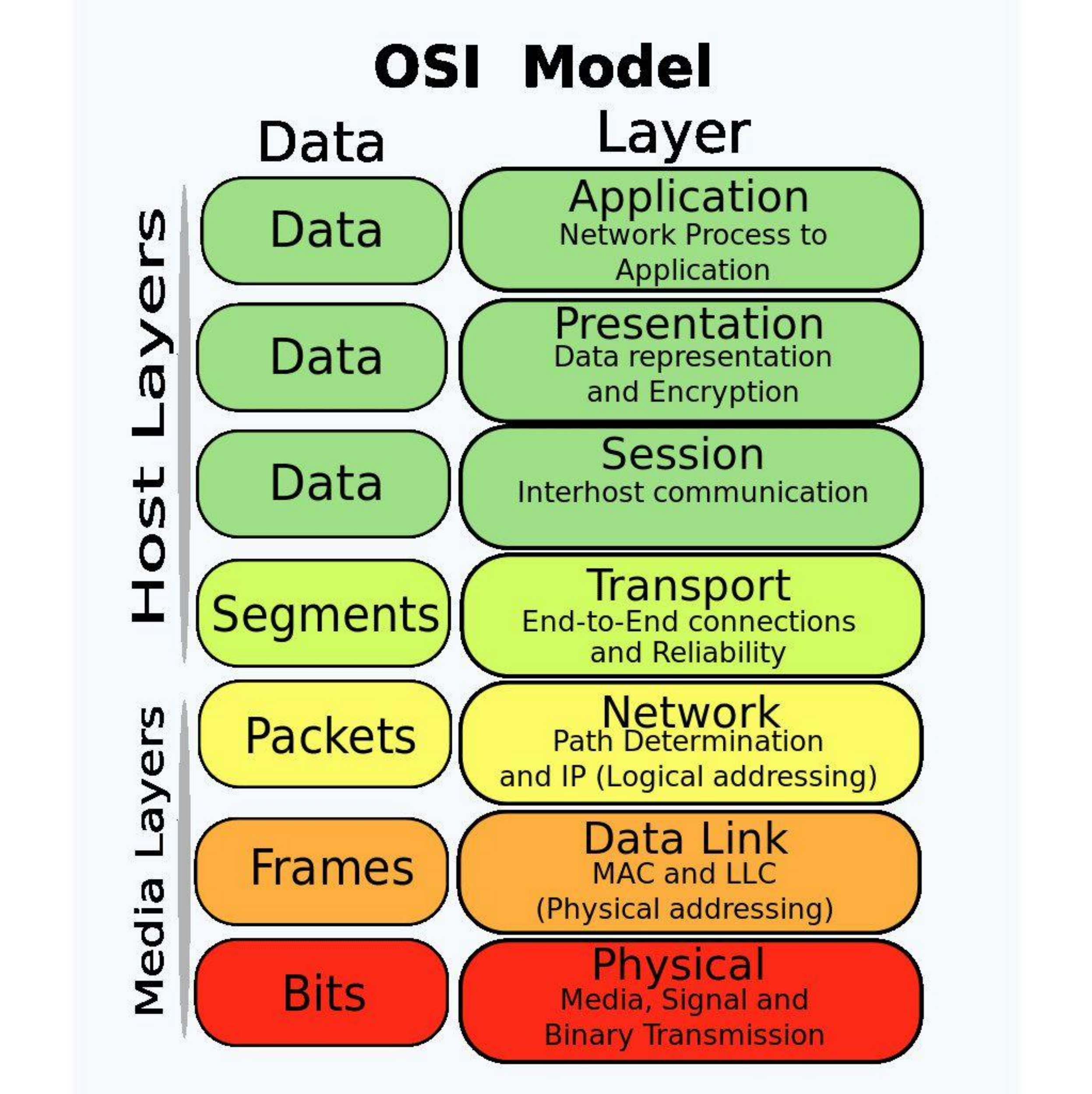
For this to work, VirtualBox needs a device driver on your host system. The way bridged networking works has been completely rewritten with VirtualBox depending on the host operating system. From the user perspective, the main difference is that complex configuration is no longer necessary on any of the supported host operating systems.

Note Even though TAP is no longer necessary on Linux with bridged networking, you can still use TAP interfaces for certain advanced setups, since you can connect a VM to any host interface — which could also be a TAP interface.

To enable bridged networking, all you need to do is to open the Settings dialog of a virtual machine, go to the “Network” page and select “Bridged network” in the drop down list for the “Attached to” field. Finally, select desired host interface from the list at the bottom of the page, which contains the physical network interfaces of your systems. On a typical MacBook, for example, this will allow you to select between “en1: AirPort” (which is the wireless interface) and “en0: Ethernet”, which represents the interface with a network cable.

Note Bridging to a wireless interface is done differently from bridging to a wired interface, because most wireless adapters do not support promiscuous mode. All traffic has to use the MAC address of the host’s wireless adapter, and therefore VirtualBox needs to replace the source MAC address in the Ethernet header of an outgoing packet to make sure the reply will be sent to the host interface. When VirtualBox sees an incoming packet with a destination IP address that belongs to one of the virtual machine adapters it replaces the destination MAC address in the Ethernet header with the VM adapter’s MAC address and passes it on. VirtualBox examines ARP and DHCP packets in order to learn the IP addresses of virtual machines.

OSI MODEL



OSI Model

	Data	Layer
Host Layers	Data	**Application** Network Process to Application
	Data	**Presentation** Data representation and Encryption
	Data	**Session** Interhost communication
	Segments	**Transport** End-to-End connections and Reliability
Media Layers	Packets	**Network** Path Determination and IP (Logical addressing)
	Frames	**Data Link** MAC and LLC (Physical addressing)
	Bits	**Physical** Media, Signal and Binary Transmission

By Sandeep Kumar
Insta @admirerr_20

7. Application Layer

The application layer is used by end-user software such as web browsers and email clients. It provides protocols that allow software to send and receive information and present meaningful data to users. A few examples of application layer protocols are the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).

6. Presentation Layer

The presentation layer prepares data for the application layer. It defines how two devices should encode, encrypt, and compress data so it is received correctly on the other end. The presentation layer takes any data transmitted by the application layer and prepares it for transmission over the session layer**.**

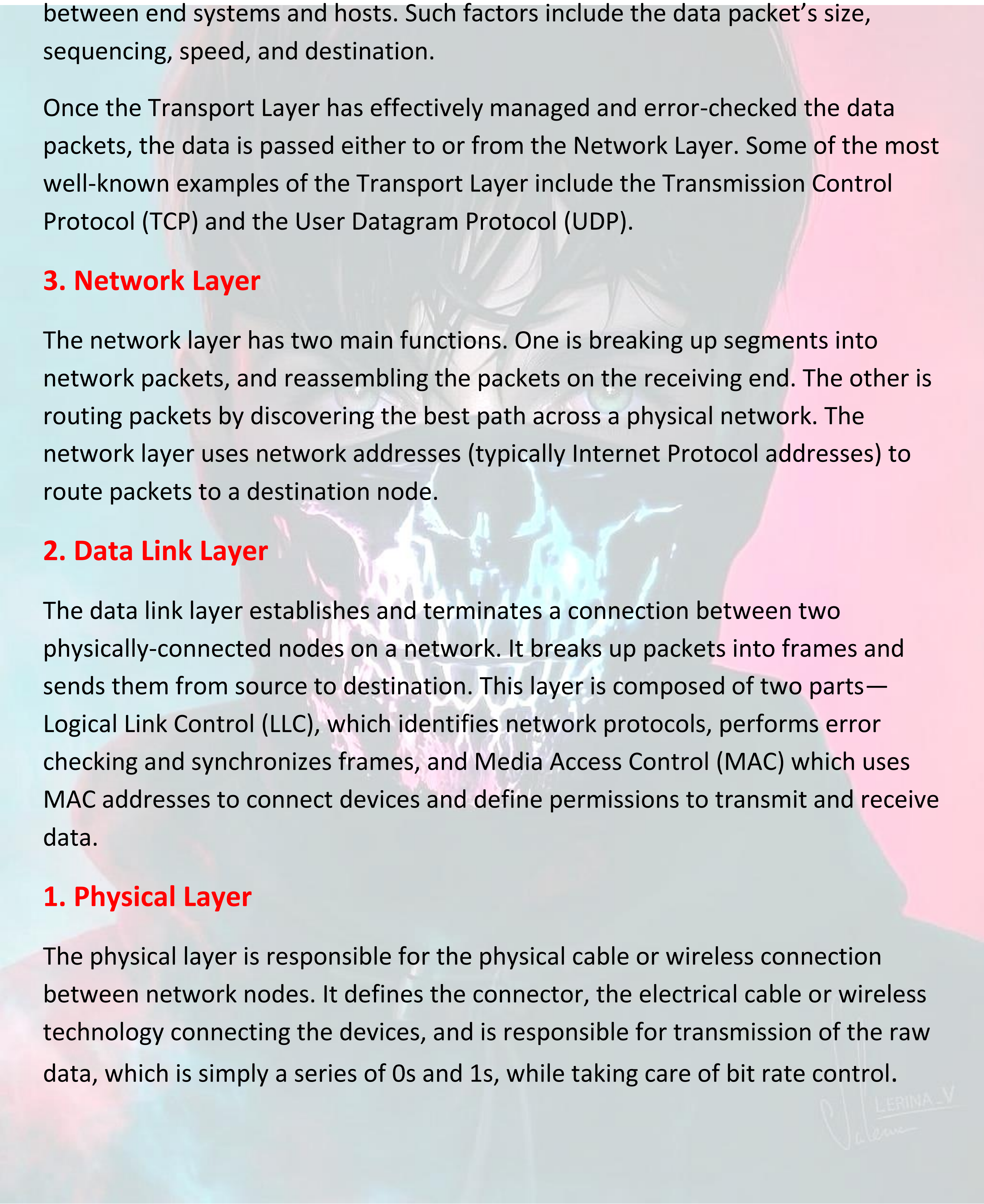
Layer 5: The Session Layer

The Session Layer is responsible for creating a session or connection that allows two devices, computers, or servers to communicate with one another. Once the session has been formed, the data is then passed either to or from the Transport Layer.

In addition to setting up a session, the resulting connection between the machines is also managed and terminated once the session ends at Layer 5. The Session Layer is also responsible for authentication and reconnection in the case that a network interruption occurs.

Layer 4: The Transport Layer

The Transport Layer is responsible for coordinating data transfer across network connections. It helps regulate various elements involved in data transmission



between end systems and hosts. Such factors include the data packet’s size, sequencing, speed, and destination.

Once the Transport Layer has effectively managed and error-checked the data packets, the data is passed either to or from the Network Layer. Some of the most well-known examples of the Transport Layer include the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

3. Network Layer

The network layer has two main functions. One is breaking up segments into network packets, and reassembling the packets on the receiving end. The other is routing packets by discovering the best path across a physical network. The network layer uses network addresses (typically Internet Protocol addresses) to route packets to a destination node.

2. Data Link Layer

The data link layer establishes and terminates a connection between two physically-connected nodes on a network. It breaks up packets into frames and sends them from source to destination. This layer is composed of two parts—Logical Link Control (LLC), which identifies network protocols, performs error checking and synchronizes frames, and Media Access Control (MAC) which uses MAC addresses to connect devices and define permissions to transmit and receive data.

1. Physical Layer

The physical layer is responsible for the physical cable or wireless connection between network nodes. It defines the connector, the electrical cable or wireless technology connecting the devices, and is responsible for transmission of the raw data, which is simply a series of 0s and 1s, while taking care of bit rate control.

Advantages of OSI Model

The OSI model helps users and operators of computer networks:

- Determine the required hardware and software to build their network.
- Understand and communicate the process followed by components communicating across a network.
- Perform troubleshooting, by identifying which network layer is causing an issue and focusing efforts on that layer.

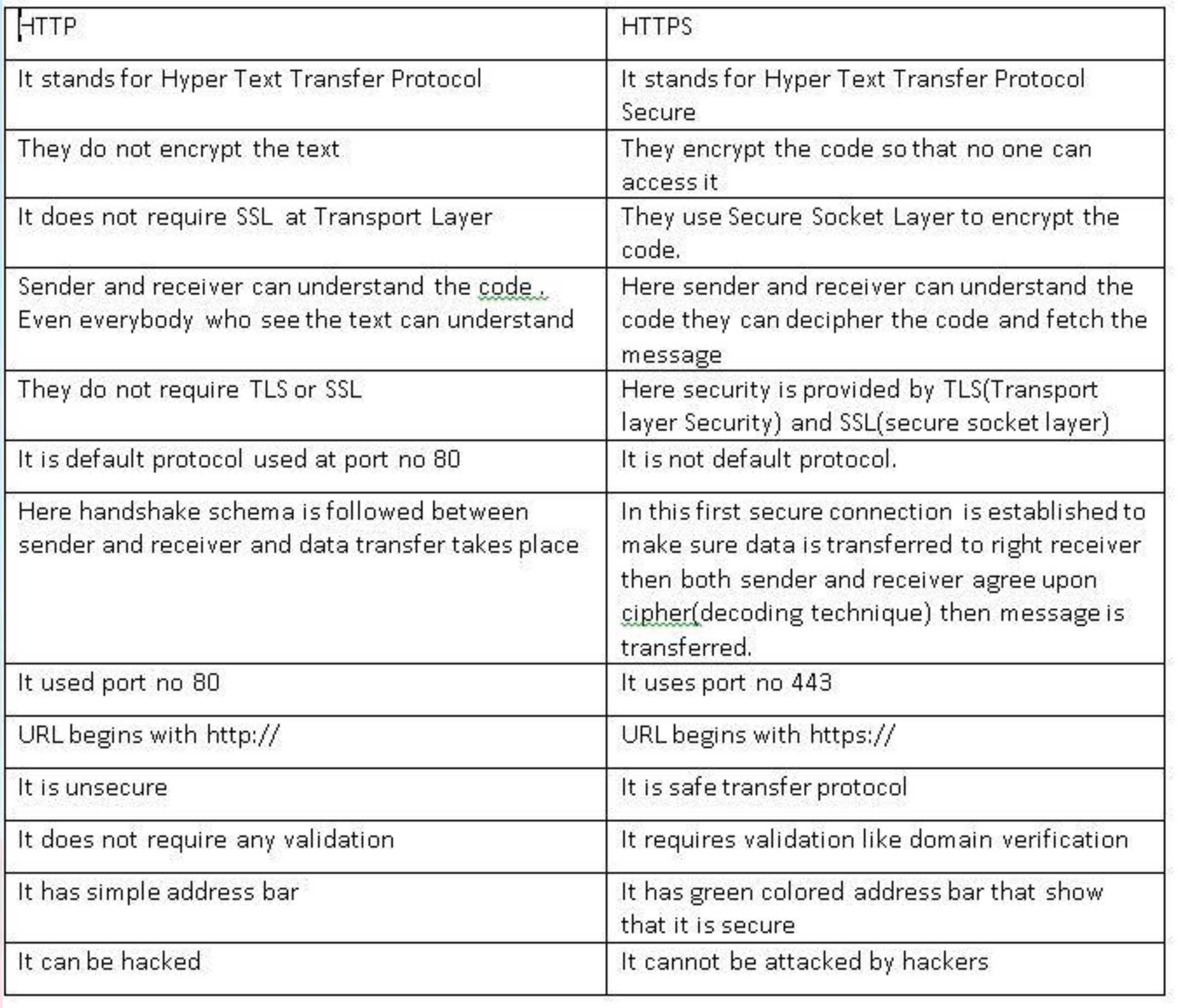
Why we use OSI model?

To establish communication between two different vendors.

Protocols

Protocol, a set of rules or procedures for transmitting data between electronic devices, such as computers. In order for computers to exchange information.

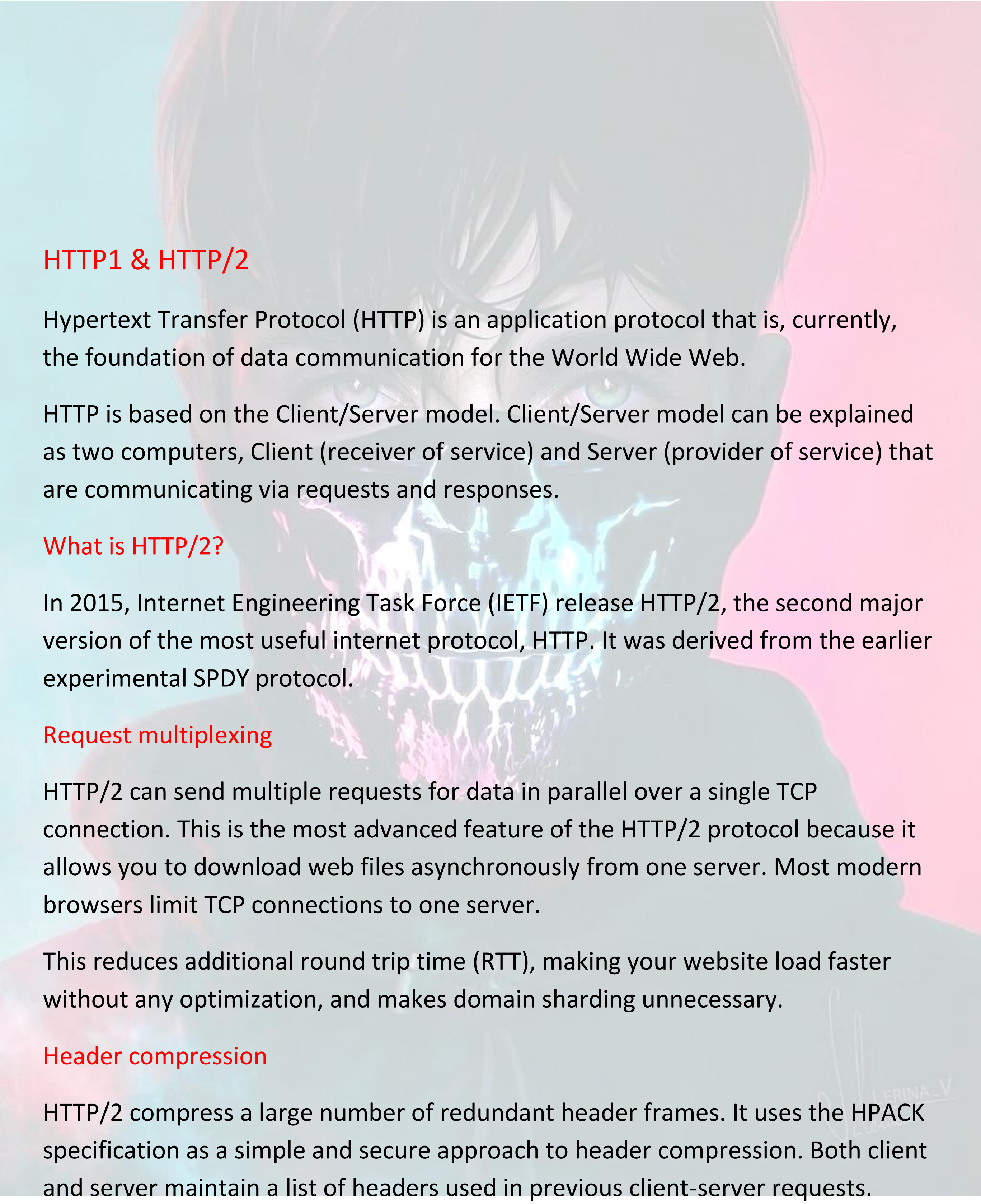
HTTP vs HTTPS



HTTP	HTTPS
It stands for Hyper Text Transfer Protocol	It stands for Hyper Text Transfer Protocol Secure
They do not encrypt the text	They encrypt the code so that no one can access it
It does not require SSL at Transport Layer	They use Secure Socket Layer to encrypt the code.
Sender and receiver can understand the code . Even everybody who see the text can understand	Here sender and receiver can understand the code they can decipher the code and fetch the message
They do not require TLS or SSL	Here security is provided by TLS(Transport layer Security) and SSL(secure socket layer)
It is default protocol used at port no 80	It is not default protocol.
Here handshake schema is followed between sender and receiver and data transfer takes place	In this first secure connection is established to make sure data is transferred to right receiver then both sender and receiver agree upon cipher(decoding technique) then message is transferred.
It used port no 80	It uses port no 443
URL begins with http://	URL begins with https://
It is unsecure	It is safe transfer protocol
It does not require any validation	It requires validation like domain verification
It has simple address bar	It has green colored address bar that show that it is secure
It can be hacked	It cannot be attacked by hackers

By Sandeep Kumar

Insta @admirerr_20



HTTP1 & HTTP/2

Hypertext Transfer Protocol (HTTP) is an application protocol that is, currently, the foundation of data communication for the World Wide Web.

HTTP is based on the Client/Server model. Client/Server model can be explained as two computers, Client (receiver of service) and Server (provider of service) that are communicating via requests and responses.

What is HTTP/2?

In 2015, Internet Engineering Task Force (IETF) release HTTP/2, the second major version of the most useful internet protocol, HTTP. It was derived from the earlier experimental SPDY protocol.

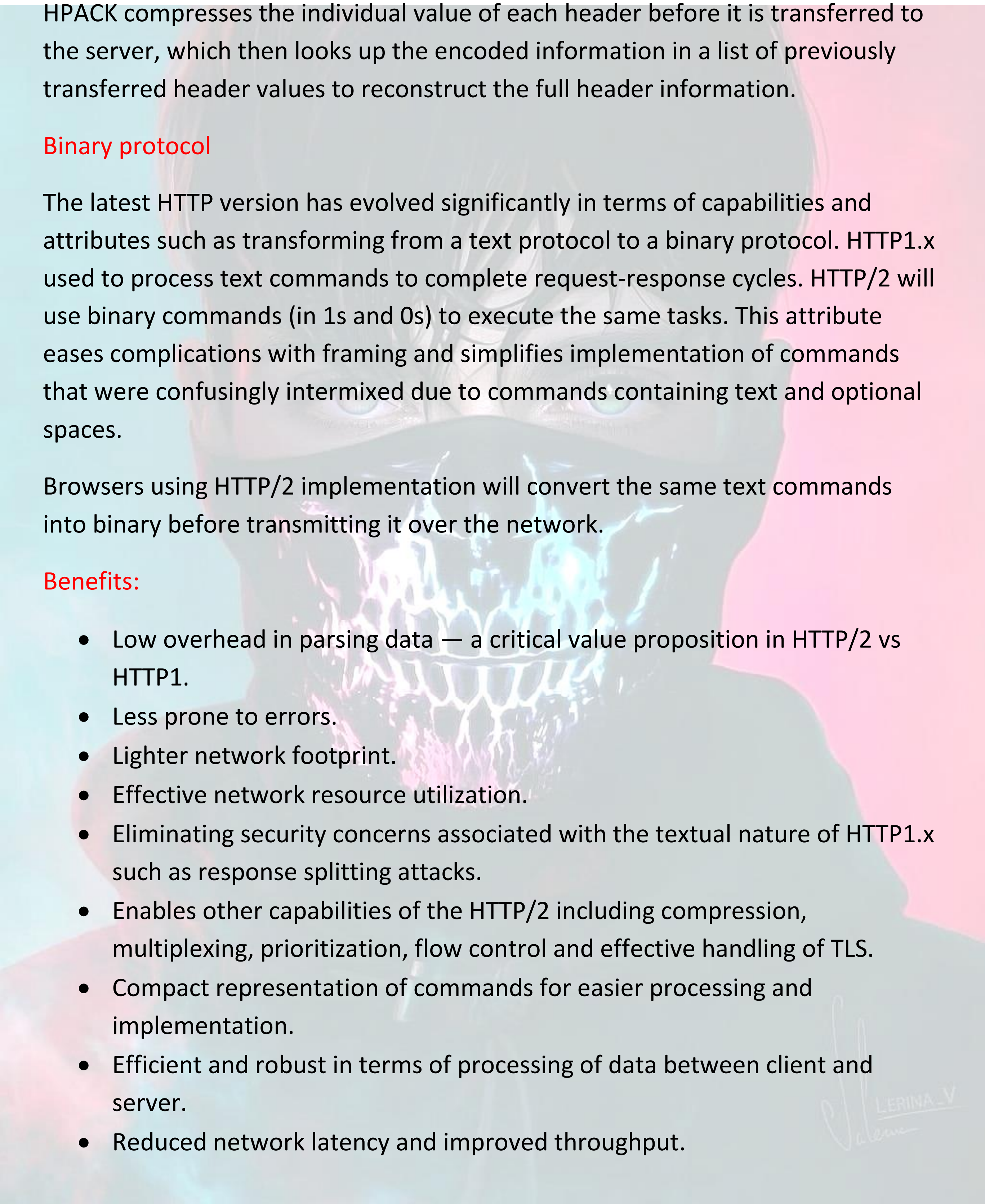
Request multiplexing

HTTP/2 can send multiple requests for data in parallel over a single TCP connection. This is the most advanced feature of the HTTP/2 protocol because it allows you to download web files asynchronously from one server. Most modern browsers limit TCP connections to one server.

This reduces additional round trip time (RTT), making your website load faster without any optimization, and makes domain sharding unnecessary.

Header compression

HTTP/2 compress a large number of redundant header frames. It uses the HPACK specification as a simple and secure approach to header compression. Both client and server maintain a list of headers used in previous client-server requests.



HPACK compresses the individual value of each header before it is transferred to the server, which then looks up the encoded information in a list of previously transferred header values to reconstruct the full header information.

Binary protocol

The latest HTTP version has evolved significantly in terms of capabilities and attributes such as transforming from a text protocol to a binary protocol. HTTP1.x used to process text commands to complete request-response cycles. HTTP/2 will use binary commands (in 1s and 0s) to execute the same tasks. This attribute eases complications with framing and simplifies implementation of commands that were confusingly intermixed due to commands containing text and optional spaces.

Browsers using HTTP/2 implementation will convert the same text commands into binary before transmitting it over the network.

Benefits:

- Low overhead in parsing data — a critical value proposition in HTTP/2 vs HTTP1.
- Less prone to errors.
- Lighter network footprint.
- Effective network resource utilization.
- Eliminating security concerns associated with the textual nature of HTTP1.x such as response splitting attacks.
- Enables other capabilities of the HTTP/2 including compression, multiplexing, prioritization, flow control and effective handling of TLS.
- Compact representation of commands for easier processing and implementation.
- Efficient and robust in terms of processing of data between client and server.
- Reduced network latency and improved throughput.

HTTP/3

HTTP/3 runs over QUIC – an encrypted general-purpose transport protocol that multiplexes multiple streams of data on a single connection.

QUIC was initially developed by Google. The protocol utilizes space congestion control over User Datagram Protocol (UDP).

HTTP/3 is largely similar to HTTP/2 in high-level features,

Benifits --

- The practical effect of the upgrade to HTTP/3 is to reduce the latency of poor or lossy internet connections.
- QUIC is almost entirely encrypted, meaning security should also be significantly improved with HTTP/3.
- This built-in encryption means fewer opportunities for manipulator-in-the-middle (MitM) attacks, while QUIC also includes other features that help protect against denial of service exploits
- QUIC combines its cryptographic and transport handshakes in a way that allows connection to a new server in a single round trip.

What is HSTS?

HTTP Strict Transport Security (HSTS) is a web server directive that informs user agents and web browsers how to handle its connection through a response header sent at the very beginning and back to the browser.

This sets the Strict-Transport-Security policy field parameter. It forces those connections over HTTPS encryption.

Setting up our Ethical Hacking Environment

Introduction

Kali Linux is a Debian-derived Linux distribution designed for penetration testing. With over 600+ preinstalled penetration-testing programs, it earned a reputation as one of the best-operating systems used for security testing. As a security-testing platform, it is best to install Kali as a VM on VirtualBox.

Virtual box --

Oracle VM VirtualBox is a free and open-source hosted hypervisor for x86 virtualization, developed by Oracle Corporation.Used for running multiple OS in single operating system

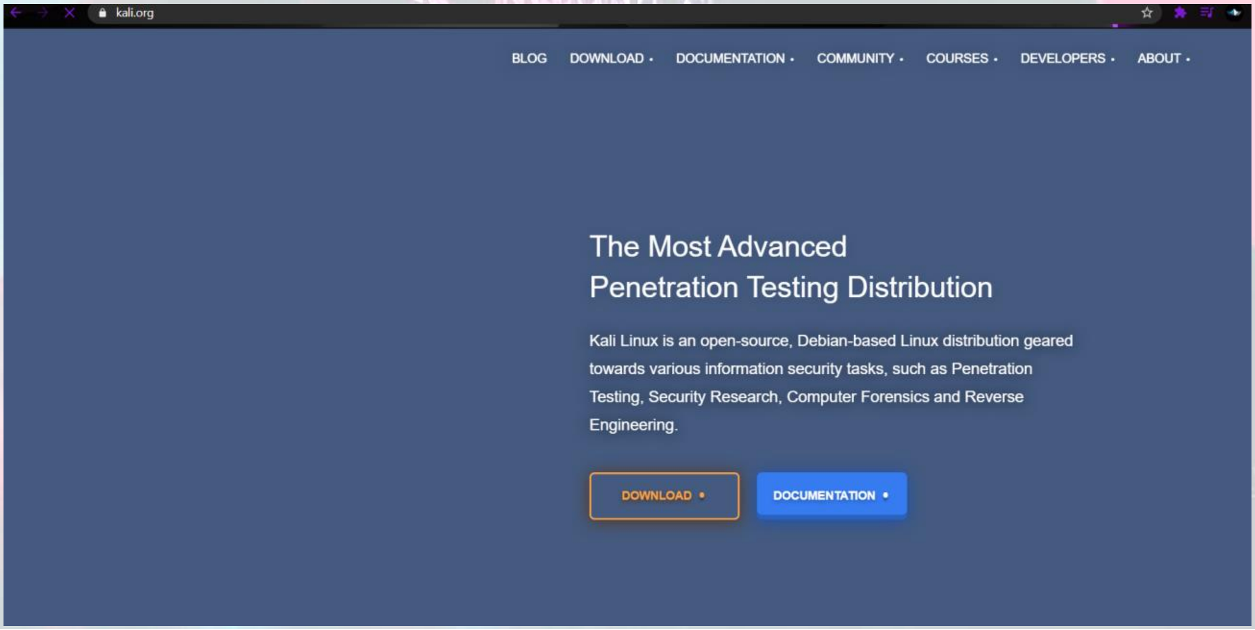
Prerequisites

At least 20 GB of disk space

At least 2 GB of RAM for i386 and amd64 architectures

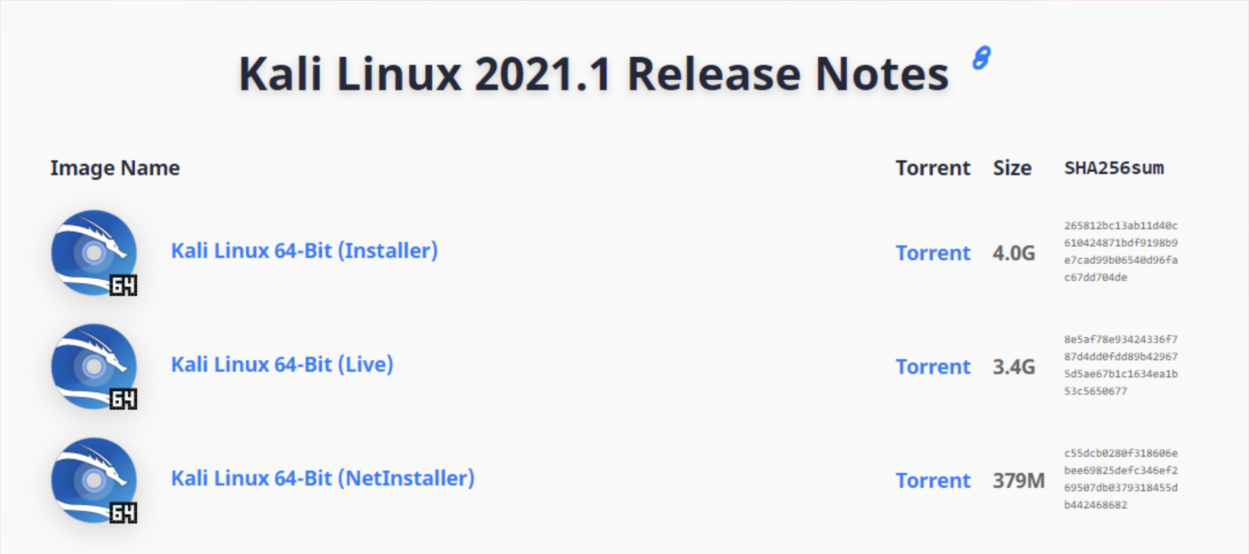
VirtualBox (or alternative virtualization software)

Step 1: Download Kali Linux ISO Image from kali.org



The Most Advanced
Penetration Testing Distribution

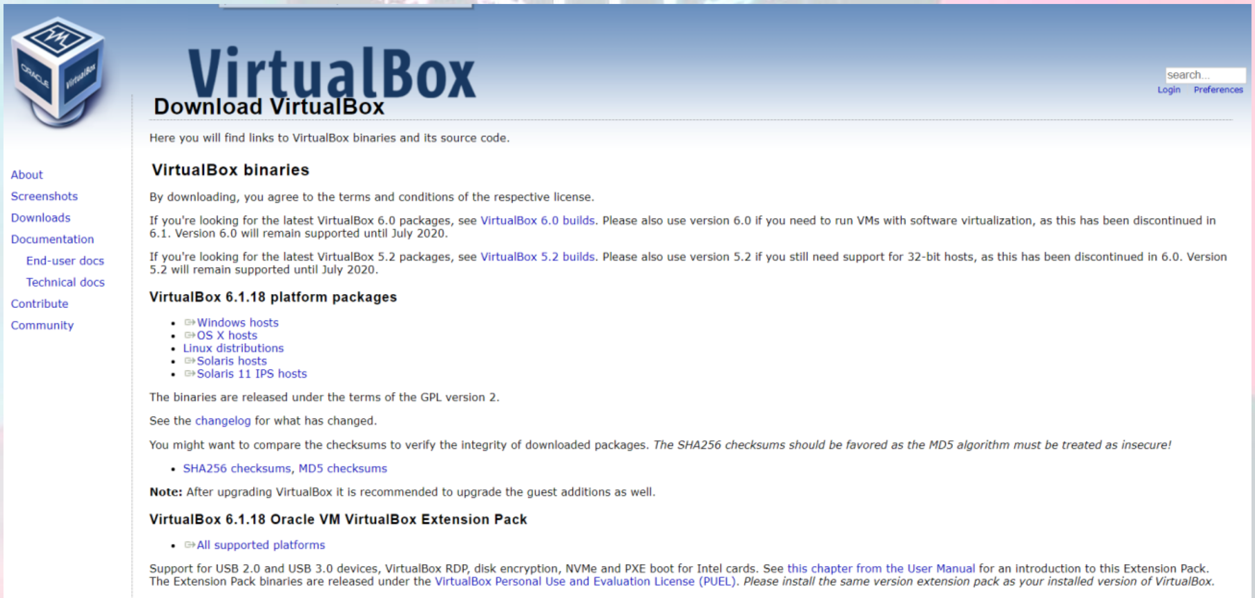
Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.



Kali Linux 2021.1 Release Notes

Image Name	Torrent	Size	SHA256sum
Kali Linux 64-Bit (Installer)	Torrent	4.0G	265812bc13ab11d40c610424871bdf9198b9e7cad99b06540d96fac67dd704de
Kali Linux 64-Bit (Live)	Torrent	3.4G	8e5af78e93424336f787d4dd0fdd89b429675d5ae67b1c1634ea1b53c5650677
Kali Linux 64-Bit (NetInstaller)	Torrent	379M	c55dcb0280f318606ebee69825defc346ef269507db0379318455db442468682

2) now download virtual box https://www.virtualbox.org/



Download VirtualBox

Here you will find links to VirtualBox binaries and its source code.

VirtualBox binaries

By downloading, you agree to the terms and conditions of the respective license.

If you're looking for the latest VirtualBox 6.0 packages, see VirtualBox 6.0 builds. Please also use version 6.0 if you need to run VMs with software virtualization, as this has been discontinued in 6.1. Version 6.0 will remain supported until July 2020.

If you're looking for the latest VirtualBox 5.2 packages, see VirtualBox 5.2 builds. Please also use version 5.2 if you still need support for 32-bit hosts, as this has been discontinued in 6.0. Version 5.2 will remain supported until July 2020.

VirtualBox 6.1.18 platform packages

- Windows hosts
- OS X hosts
- Linux distributions
- Solaris hosts
- Solaris 11 IPS hosts

The binaries are released under the terms of the GPL version 2.

See the changelog for what has changed.

You might want to compare the checksums to verify the integrity of downloaded packages. *The SHA256 checksums should be favored as the MD5 algorithm must be treated as insecure!*

- SHA256 checksums, MD5 checksums

Note: After upgrading VirtualBox it is recommended to upgrade the guest additions as well.

VirtualBox 6.1.18 Oracle VM VirtualBox Extension Pack

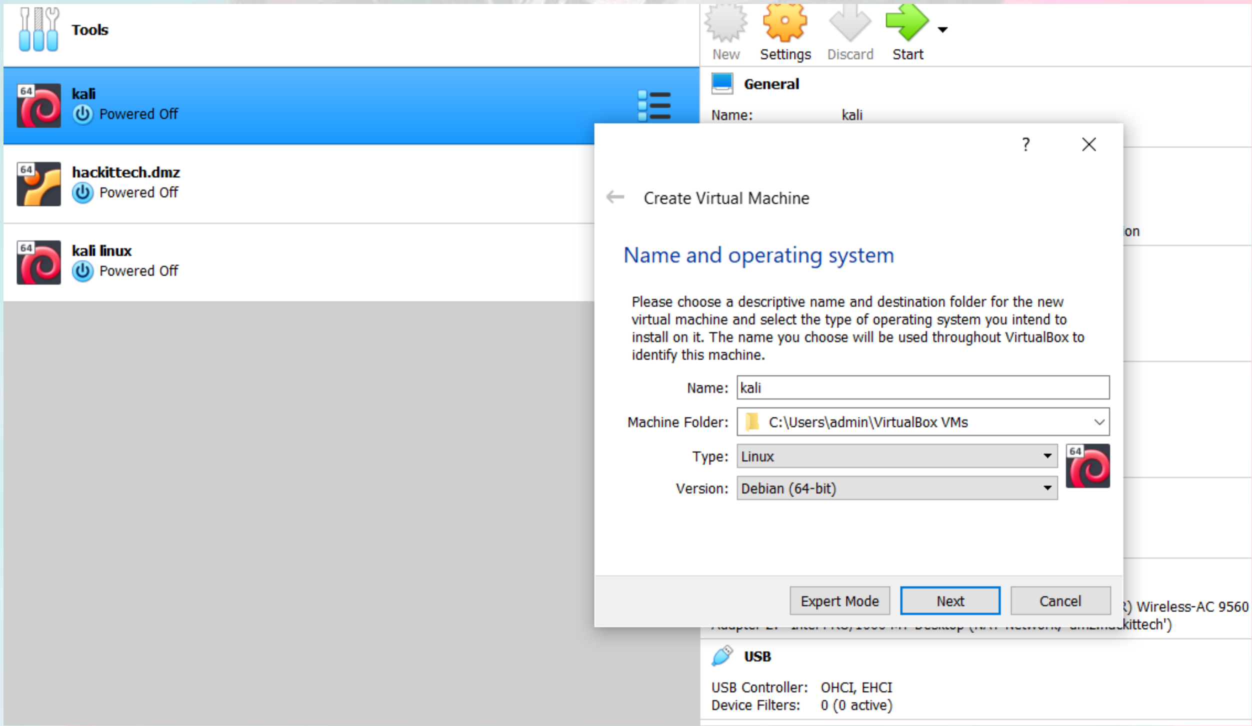
- All supported platforms

Support for USB 2.0 and USB 3.0 devices, VirtualBox RDP, disk encryption, NVMe and PXE boot for Intel cards. See this chapter from the User Manual for an introduction to this Extension Pack. The Extension Pack binaries are released under the VirtualBox Personal Use and Evaluation License (PUEL). *Please install the same version extension pack as your installed version of VirtualBox.*

3) install virtual box in your host machine

4) Launch VirtualBox Manager and click the New icon.

5) Name and operating system. A pop-up window for creating a new VM appears. Specify a name and a destination folder. The Type and Version change automatically, based on the name you provide. Make sure the information matches the package you downloaded and click Next.



Name: kali

Create Virtual Machine

Name and operating system

Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: kali

Machine Folder: C:\Users\admin\VirtualBox VMs

Type: Linux

Version: Debian (64-bit)

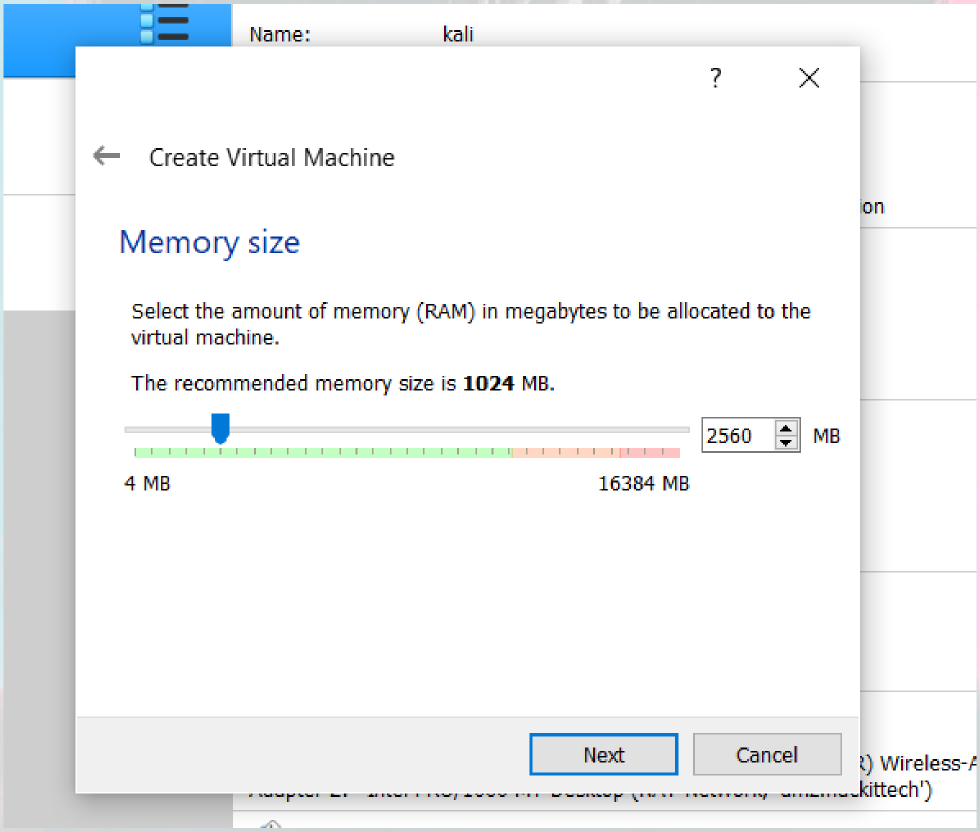
USB Controller: OHCI, EHCI

Device Filters: 0 (0 active)

3. Memory size. Choose how much memory to allocate to the virtual machine and click Next. The default setting for Linux is 1024 MB. However, this varies depending on your individual needs.

4. Hard disk. The default option is to create a virtual hard disk for the new VM. Click Create to continue. Alternatively, you can use an existing virtual hard disk file or decide not to add one at all.

create a virtual machine



Name: kali

Create Virtual Machine

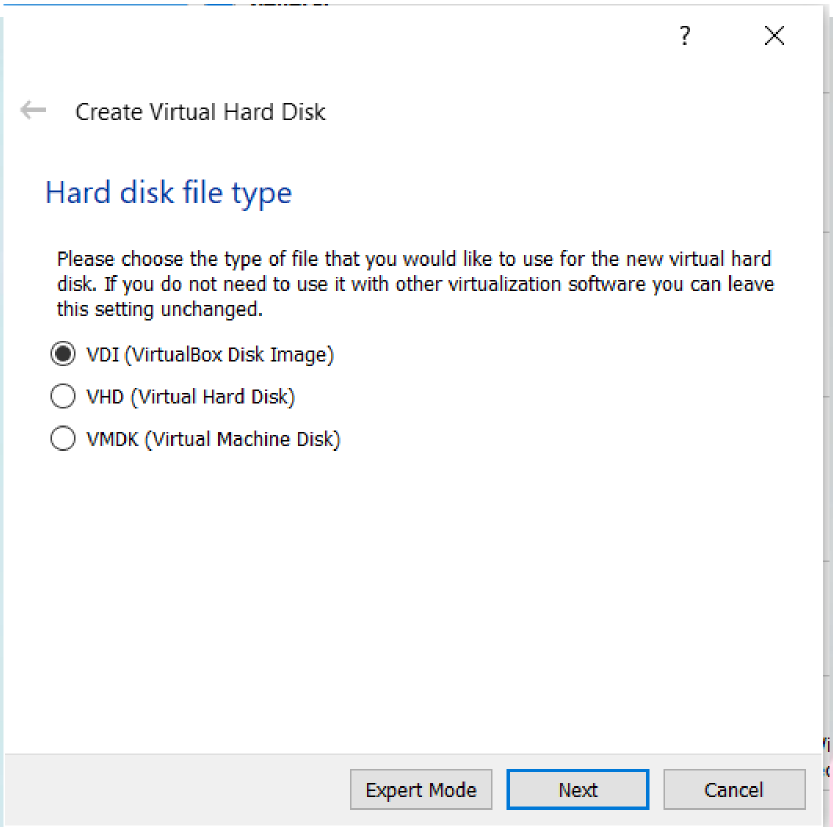
Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **1024** MB.

2560 MB

3. Memory size. Choose how much memory to allocate to the virtual machine and click Next. The default setting for Linux is 1024 MB. However, this varies depending on your individual needs.



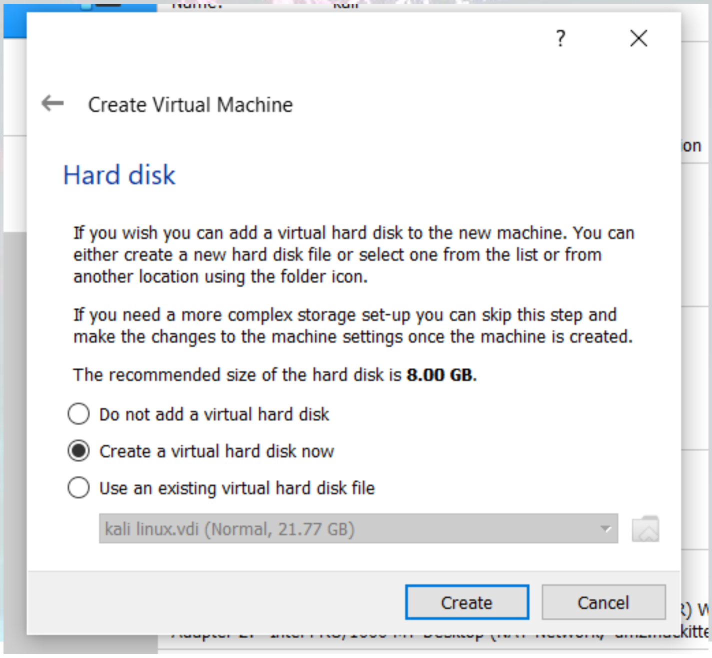
Create Virtual Hard Disk

Hard disk file type

Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.

● VDI (VirtualBox Disk Image)
○ VHD (Virtual Hard Disk)
○ VMDK (Virtual Machine Disk)

4. Hard disk. The default option is to create a virtual hard disk for the new VM. Click Create to continue. Alternatively, you can use an existing virtual hard disk file or decide not to add one at all.



Create Virtual Machine

Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **8.00 GB**.

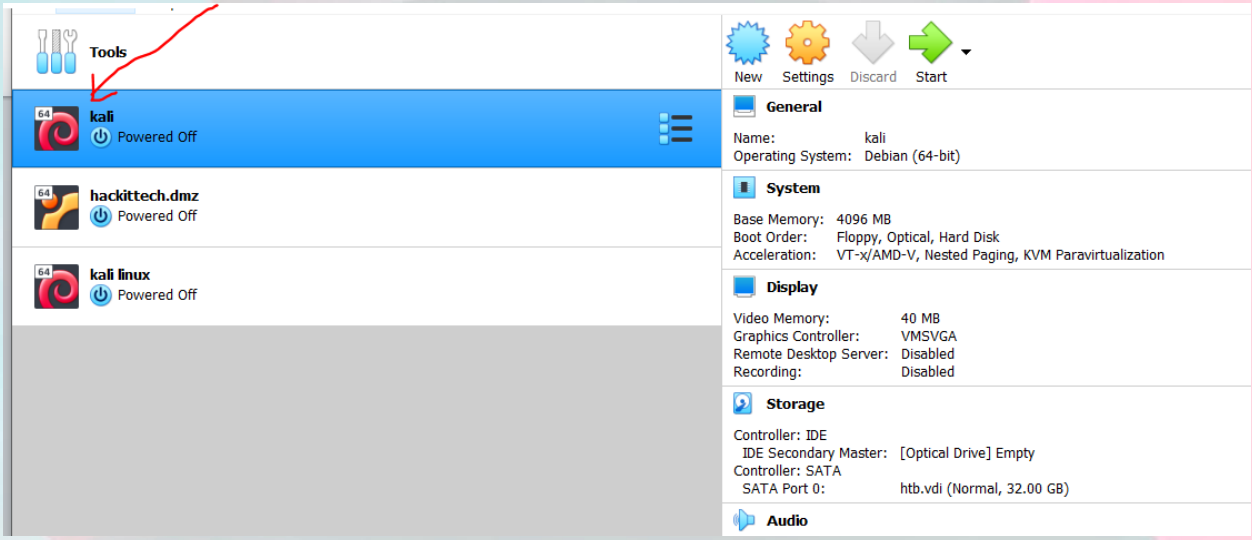
○ Do not add a virtual hard disk
● Create a virtual hard disk now
○ Use an existing virtual hard disk file

kali linux.vdi (Normal, 21.77 GB)

5. Storage on a physical hard disk. Decide between Dynamically allocated and Fixed size. The first choice allows the new hard disk to grow and fill up space dedicated to it. The second, fixed size, uses the maximum capacity from the start. Click Next.

6. File location and size. Specify the name and where you want to store the virtual hard disk. Choose the amount of file data the VM is allowed to store on the hard disk. We advise giving it at least 8 GB. Click Create to finish.

Now you created a new VM. The VM appears on the list in the VirtualBox Manager



kali
Powered Off

hackittech.dmz
Powered Off

kali linux
Powered Off

General

Name: kali
Operating System: Debian (64-bit)

System

Base Memory: 4096 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization

Display

Video Memory: 40 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Master: [Optical Drive] Empty
Controller: SATA
SATA Port 0: htb.vdi (Normal, 32.00 GB)

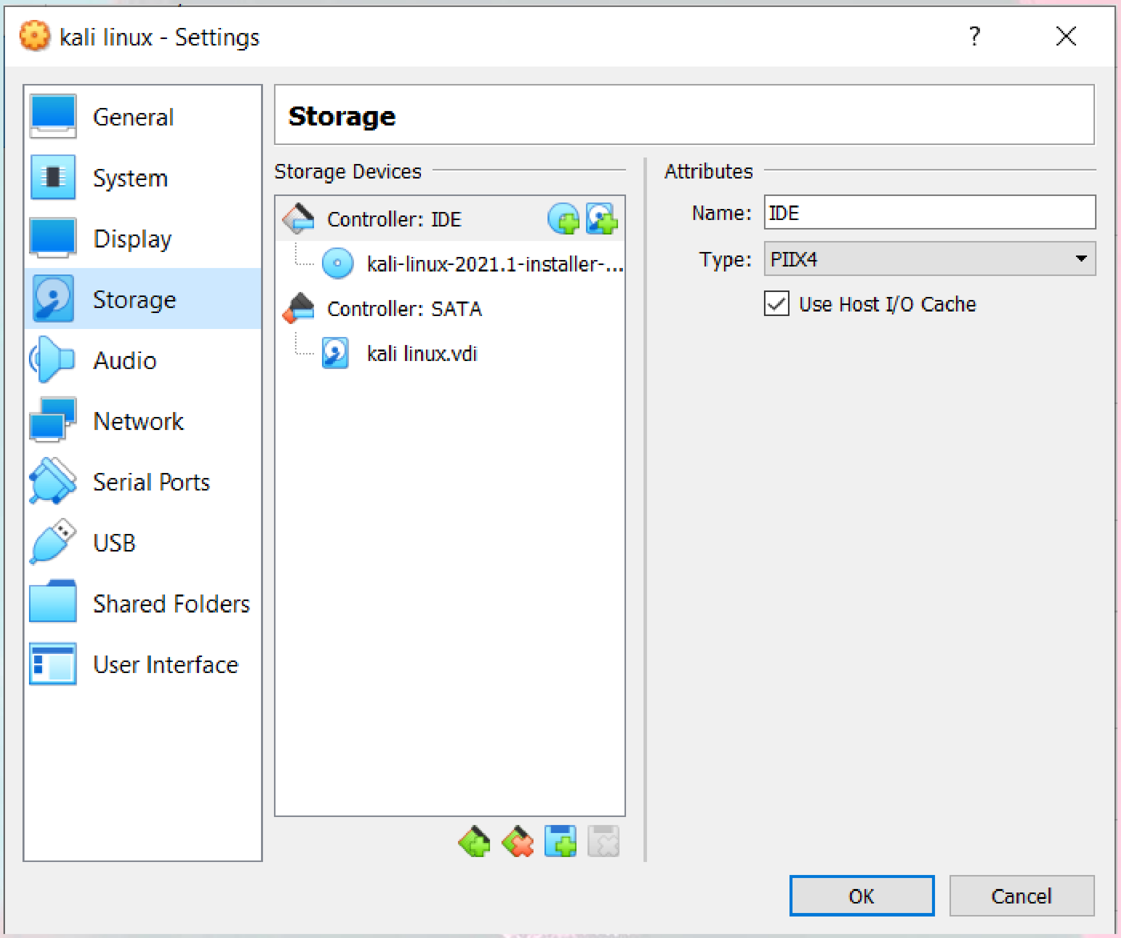
Audio

Configure Virtual Machine Settings

The next step is adjusting the default virtual machine settings.

1. Select a virtual machine and click the Settings icon. Make sure you marked the correct VM and that the right-hand side is displaying details for Kali Linux.

2)navigate to Storage settings. Add the downloaded Kali image to a storage device under Controller: IDE. Click the disk icon to search for the image. Once finished, close the Settings window.



kali linux - Settings

Storage

Storage Devices

Controller: IDE
- kali-linux-2021.1-installer-...

Controller: SATA
- kali linux.vdi

Attributes

Name: IDE

Type: PIIX4

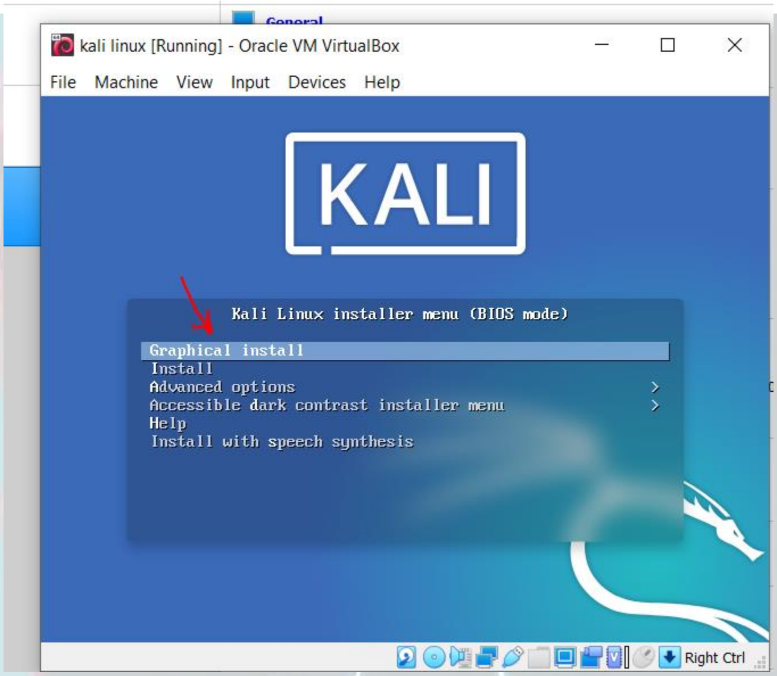
☑ Use Host I/O Cache

Click the Start icon to begin installing Kali.

Installing and Setting Up Kali Linux

After you booted the installation menu by clicking Start, a new VM VirtualBox window appears with the Kali welcome screen.

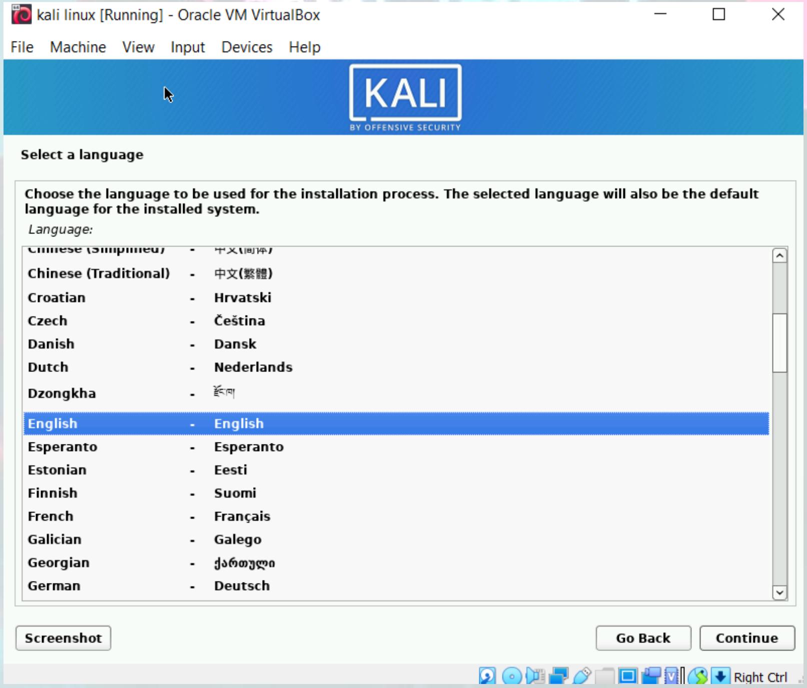
Select the Graphical install option and go through the following installation steps for setting up Kali Linux in VirtualBox


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
Right Ctrl

```
Kali Linux installer menu (BIOS mode)

Graphical install
Install
Advanced options                                  >
Accessible dark contrast installer menu           >
Help
Install with speech synthesis
```

1. Select a language. Choose the default language for the system (which will also be the language used during the installation process).


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
BY OFFENSIVE SECURITY
Screenshot
Go Back
Continue
Right Ctrl

Select a language

Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.

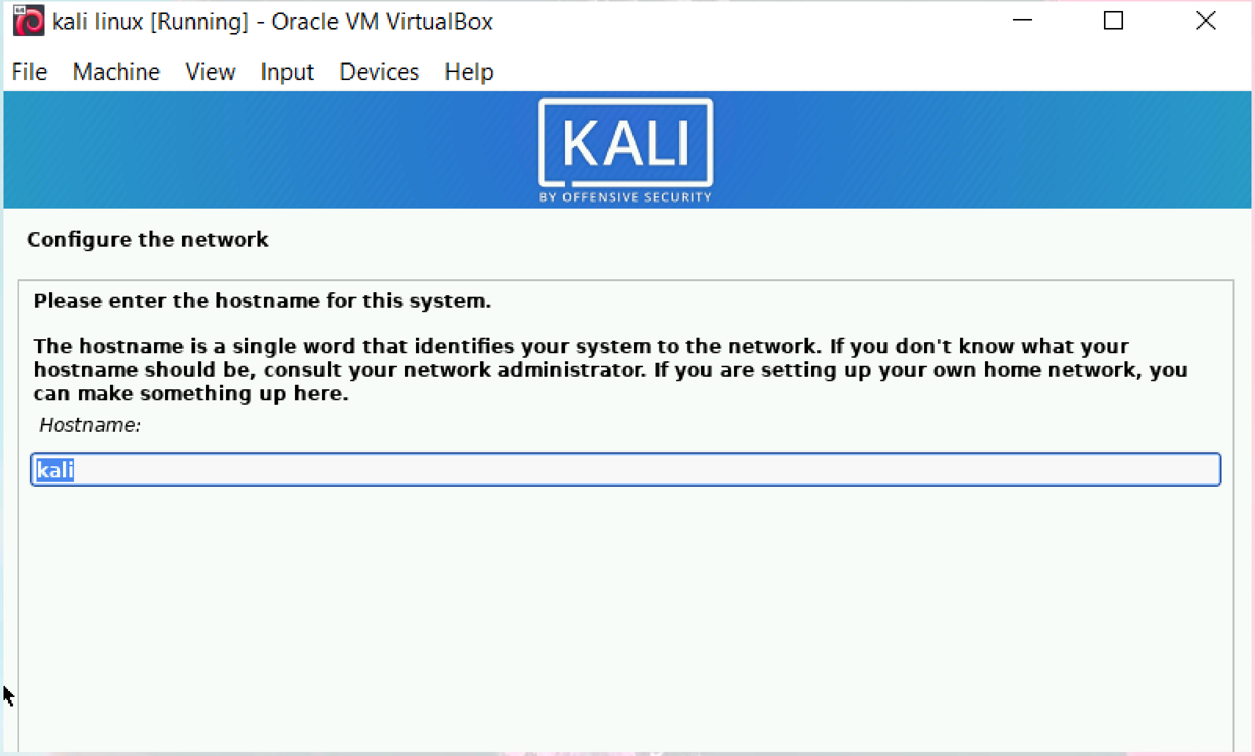
Language:

Chinese (Simplified)	-	中文(简体)
Chinese (Traditional)	-	中文(繁體)
Croatian	-	Hrvatski
Czech	-	Čeština
Danish	-	Dansk
Dutch	-	Nederlands
Dzongkha	-	རྫོང་ཁ
English	-	English
Esperanto	-	Esperanto
Estonian	-	Eesti
Finnish	-	Suomi
French	-	Français
Galician	-	Galego
Georgian	-	ქართული
German	-	Deutsch

2. Select your location. Find and select your country from the list (or choose “other”).

3. Configure the keyboard. Decide which keymap to use. In most cases, the best option is to select American English.

4. Configure the network. First, enter a hostname for the system and click Continue.


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
BY OFFENSIVE SECURITY

Configure the network

Please enter the hostname for this system.

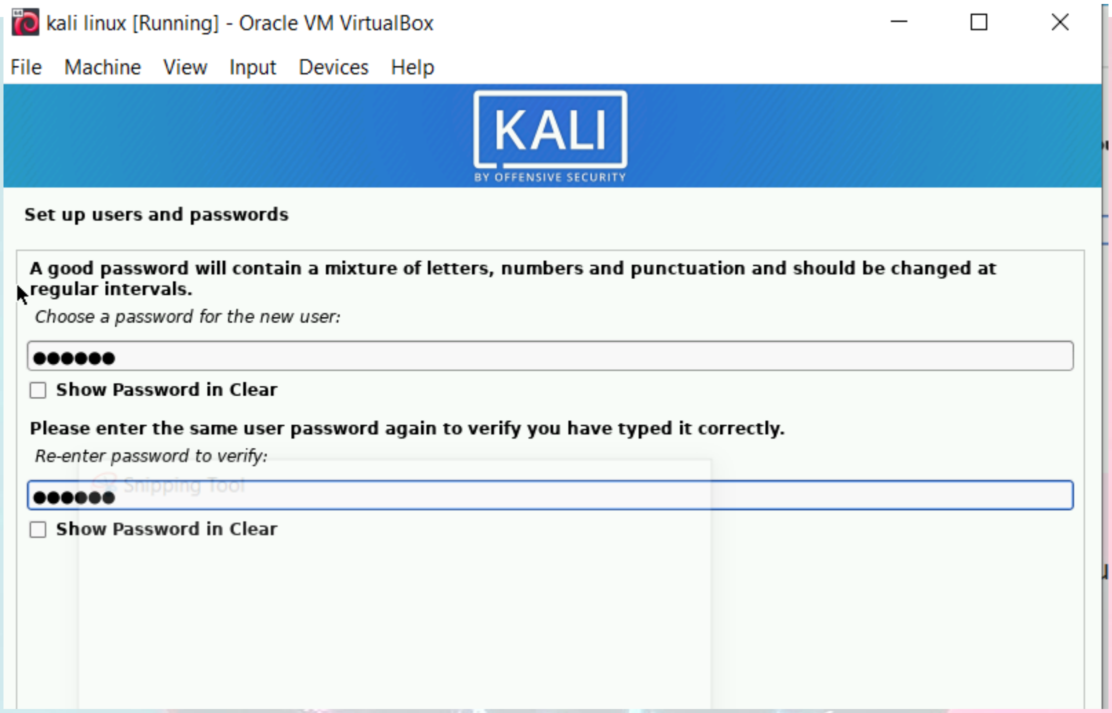
The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.

Hostname:

kali

5. Next, create a domain name (the part of your internet address after your hostname). Domain names usually end in .com, .net, .edu, etc. Make sure you use the same domain name on all your machines or you can simply skip this one.

6. Set up users and passwords. Create a strong root password for the system administrator account.



kali linux [Running] - Oracle VM VirtualBox

Set up users and passwords

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

Choose a password for the new user:

●●●●●●

□ Show Password in Clear

Please enter the same user password again to verify you have typed it correctly.

Re-enter password to verify:

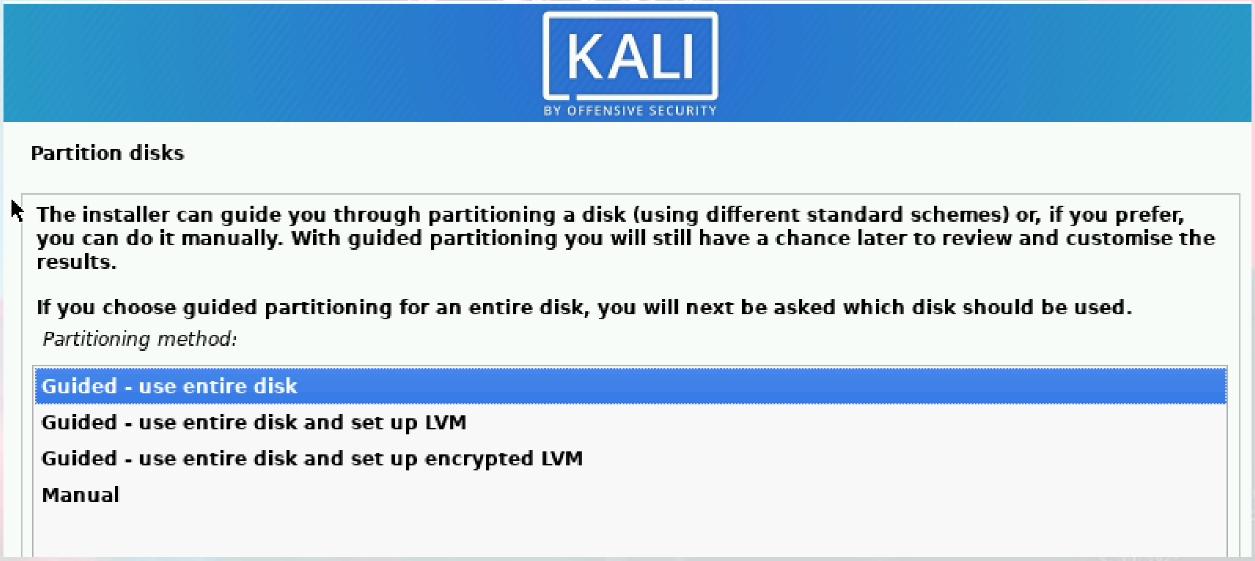
●●●●●●

□ Show Password in Clear

7. Configure the clock. Select your time zone from the available options.

8. Partition disks. Select how you would like to partition the hard disk. Unless you have a good reason to do it manually, go for the Guided –use entire disk option.

partition disk for kali virtual machine



Partition disks

The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.

If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.

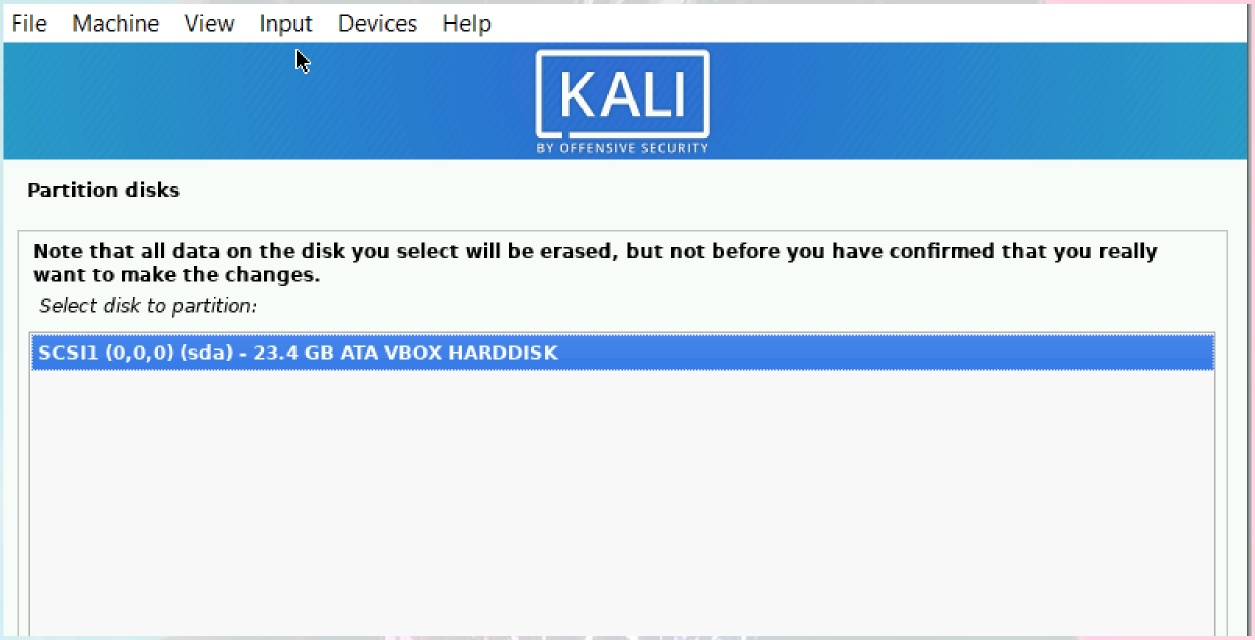
Partitioning method:

Guided - use entire disk
Guided - use entire disk and set up LVM
Guided - use entire disk and set up encrypted LVM
Manual

By Sandeep Kumar

Insta @admirerr_20

9. Then, select which disk you want to use for partitioning. As you created a single virtual hard disk in Step 3: Adjust VM Settings, you do not have to worry about data loss. Select the only available option – SCSI3 (0,0,0) (sda) – 68.7 GB ATA VBOK HARDDISK (the details after the dash vary depending on your virtualization software).



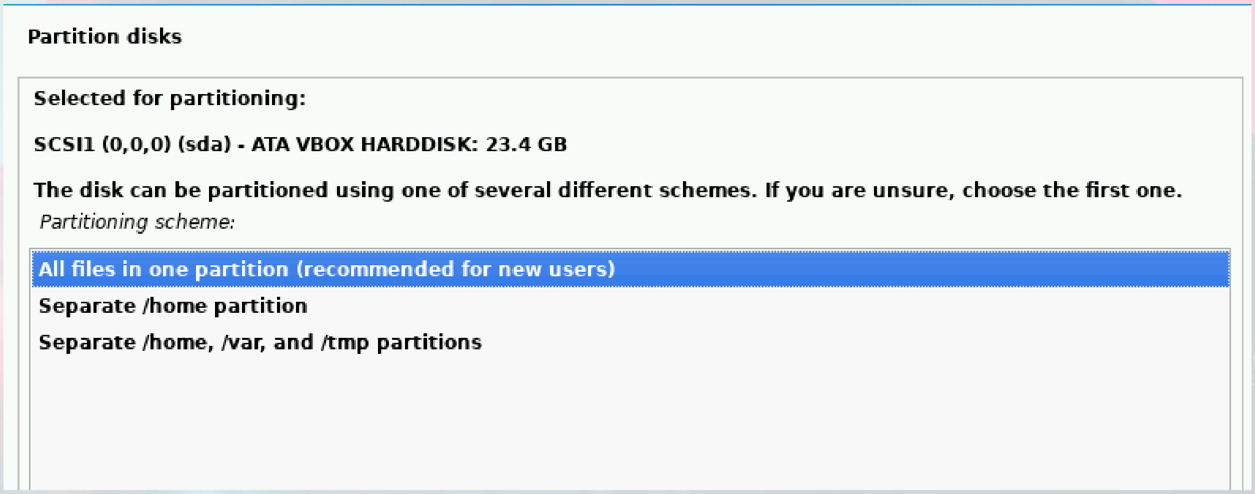
Partition disks

Note that all data on the disk you select will be erased, but not before you have confirmed that you really want to make the changes.

Select disk to partition:

SCSI1 (0,0,0) (sda) - 23.4 GB ATA VBOX HARDDISK

10. Next, select the scheme for partitioning. If you are a new user, go for All files in one partition.



Partition disks

Selected for partitioning:

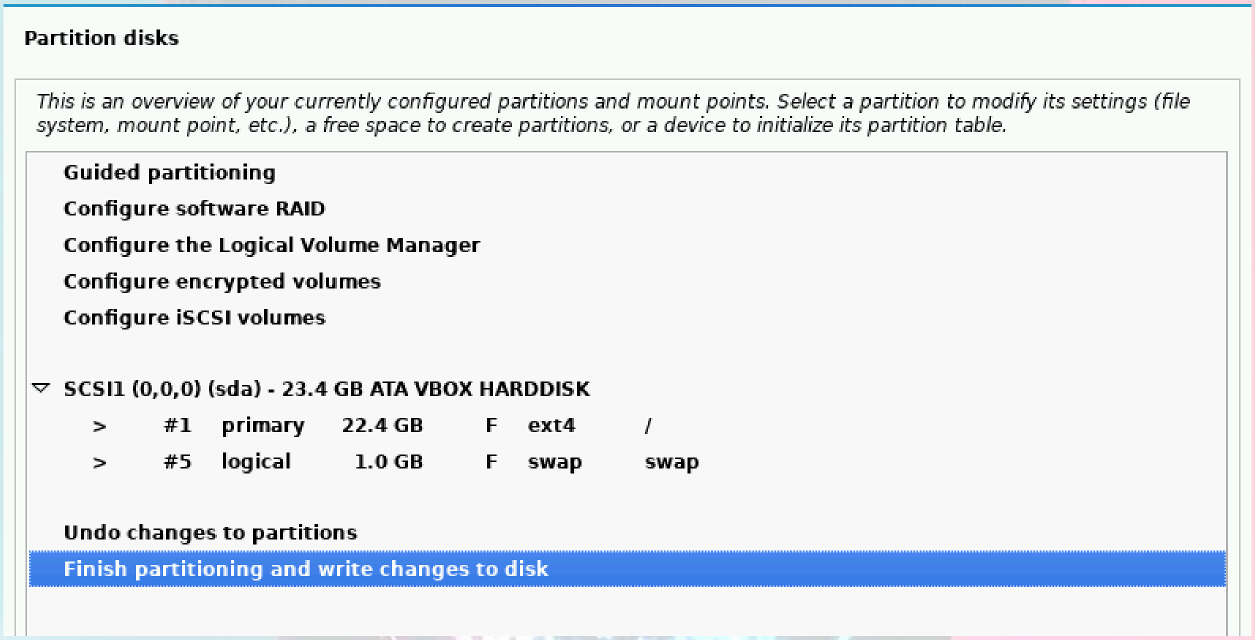
SCSI1 (0,0,0) (sda) - ATA VBOX HARDDISK: 23.4 GB

The disk can be partitioned using one of several different schemes. If you are unsure, choose the first one.

Partitioning scheme:

All files in one partition (recommended for new users)
Separate /home partition
Separate /home, /var, and /tmp partitions

11. The wizard gives you an overview of the configured partitions. Continue by navigating to Finish partitioning and write changes to disk. Click Continue and confirm with Yes.



Partition disks

This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.

```
Guided partitioning
Configure software RAID
Configure the Logical Volume Manager
Configure encrypted volumes
Configure iSCSI volumes

▽ SCSI1 (0,0,0) (sda) - 23.4 GB ATA VBOX HARDDISK
     >     #1   primary    22.4 GB     F   ext4       /
     >     #5   logical     1.0 GB     F   swap       swap

Undo changes to partitions
Finish partitioning and write changes to disk
```

12. The wizard starts installing Kali. While the installation bar loads, additional configuration settings appear.

13. Configure the package manager. Select whether you want to use a network mirror and click Continue. Enter the HTTP proxy information if you are using one. Otherwise, leave the field blank and click Continue again.

14. Install the GRUB boot loader on a hard disk. Select Yes and Continue. Then, select a boot loader device to ensure the newly installed system is bootable.

15. Once you receive the message Installation is complete, click Continue to reboot your VM.

With this, you have successfully installed Kali Linux on VirtualBox. After rebooting, the Kali login screen appears. Type in a username (root) and password you entered in the previous steps.

Finally, the interface of Kali Linux appears on your screen.

Linux Commands

1. pwd command

Use the pwd command to find out the path of the current working directory

2. cd command

To navigate through the Linux files and directories, use the cd command. It requires either the full path or the name of the directory, depending on the current working directory that you're in.

Let's say you're in /home/username/Documents and you want to go to Photos, a subdirectory of Documents. To do so, simply type the following command: cd Photos.

There are some shortcuts to help you navigate quickly:

cd .. (with two dots) to move one directory up

cd to go straight to the home folder

cd- (with a hyphen) to move to your previous directory

3. ls command

The ls command is used to view the contents of a directory. By default, this command will display the contents of your current working directory.

4. cat command

cat (short for concatenate) is one of the most frequently used commands in Linux. It is used to list the contents of a file on the standard output (sdout). To run this command, type cat followed by the file's name and its extension. For instance: cat file.txt.

5. cp command

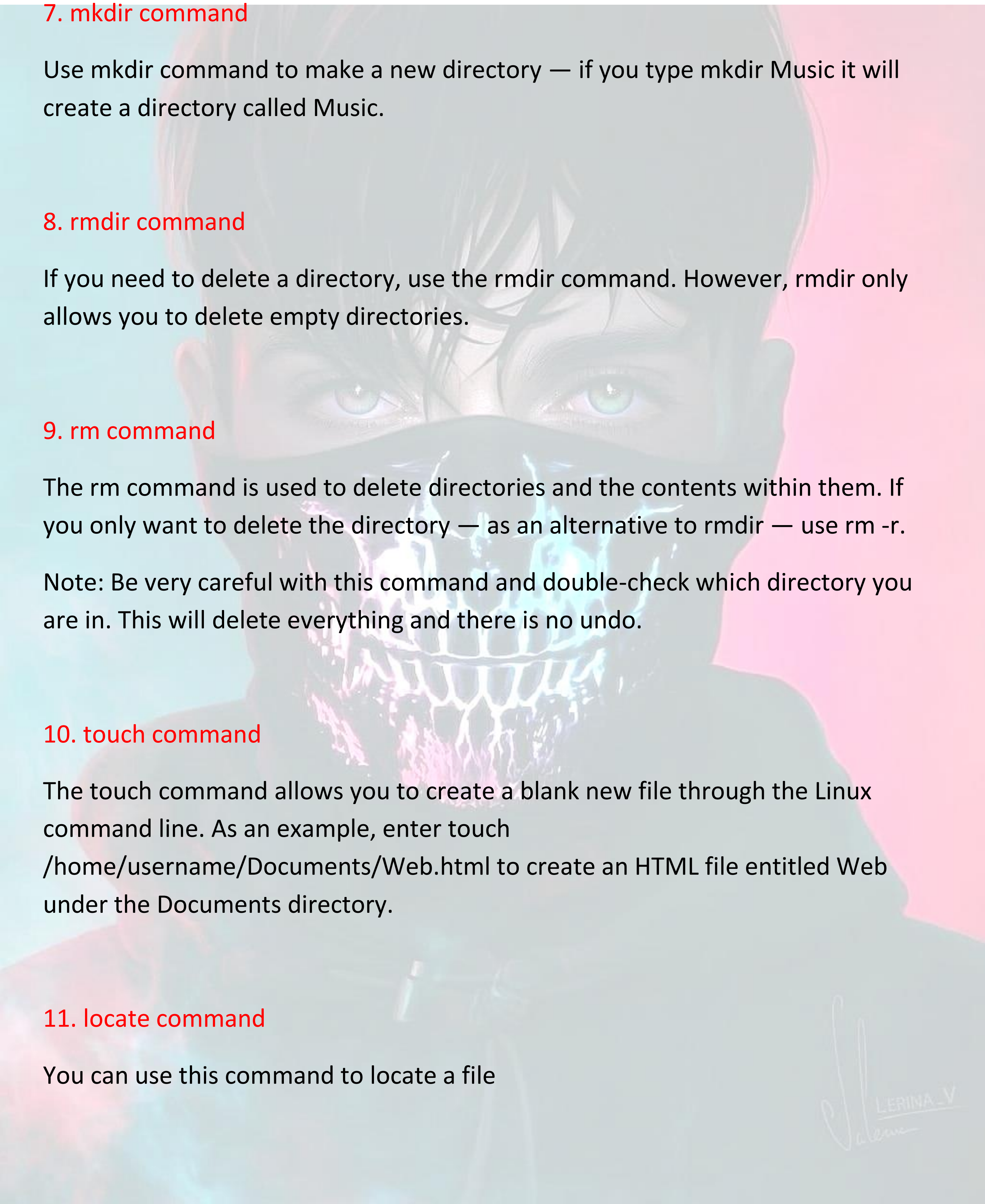
Use the cp command to copy files from the current directory to a different directory. For instance, the command cp scenery.jpg /home/username/Pictures would create a copy of scenery.jpg (from your current directory) into the Pictures directory.

6. mv command

The primary use of the mv command is to move files, although it can also be used to rename files.

The arguments in mv are similar to the cp command. You need to type mv, the file's name, and the destination's directory. For example: mv file.txt /home/username/Documents.

To rename files, the Linux command is mv oldname.ext newname.ext



7. mkdir command

Use mkdir command to make a new directory — if you type mkdir Music it will create a directory called Music.

8. rmdir command

If you need to delete a directory, use the rmdir command. However, rmdir only allows you to delete empty directories.

9. rm command

The rm command is used to delete directories and the contents within them. If you only want to delete the directory — as an alternative to rmdir — use rm -r.

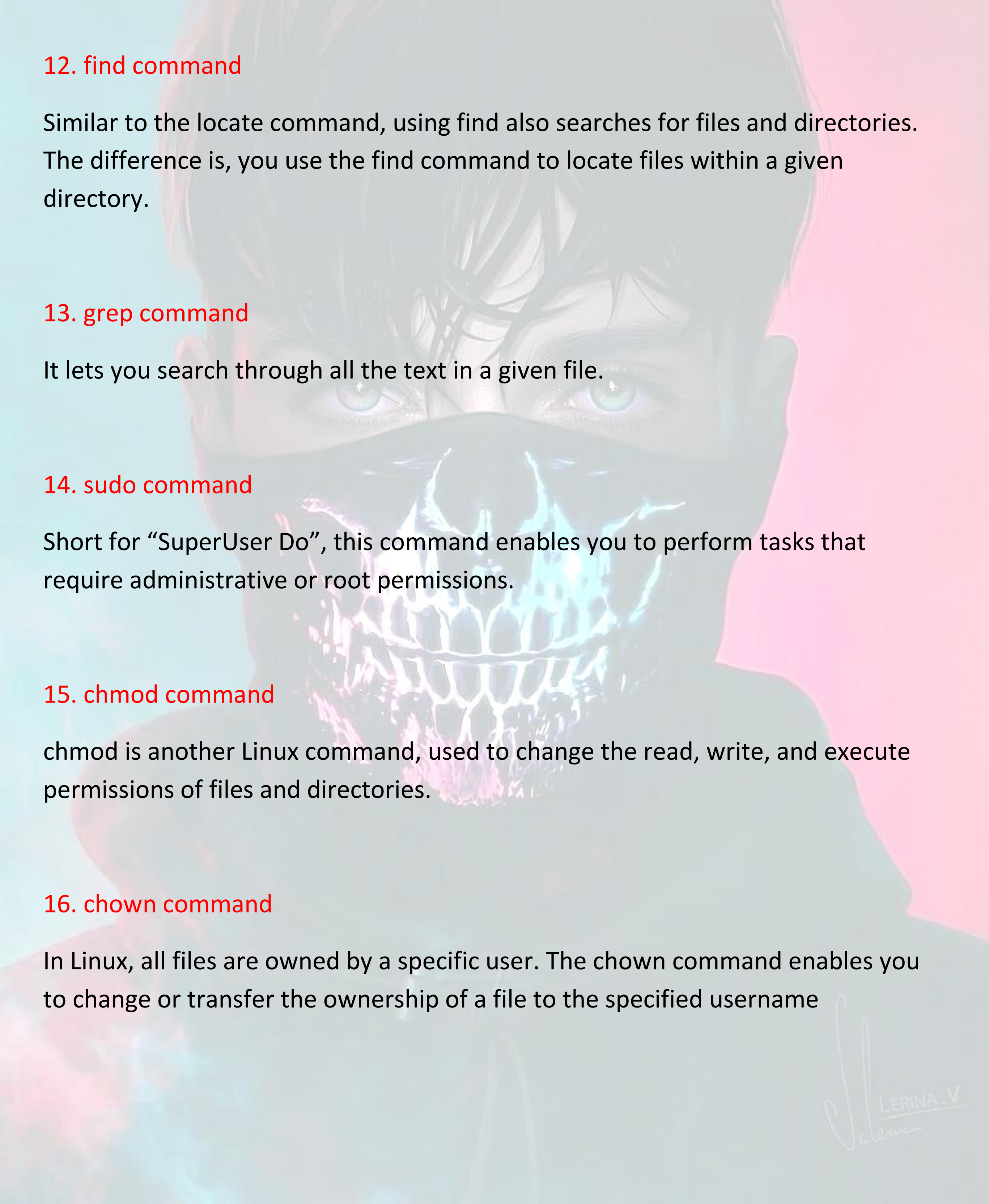
Note: Be very careful with this command and double-check which directory you are in. This will delete everything and there is no undo.

10. touch command

The touch command allows you to create a blank new file through the Linux command line. As an example, enter touch /home/username/Documents/Web.html to create an HTML file entitled Web under the Documents directory.

11. locate command

You can use this command to locate a file



12. find command

Similar to the locate command, using find also searches for files and directories. The difference is, you use the find command to locate files within a given directory.

13. grep command

It lets you search through all the text in a given file.

14. sudo command

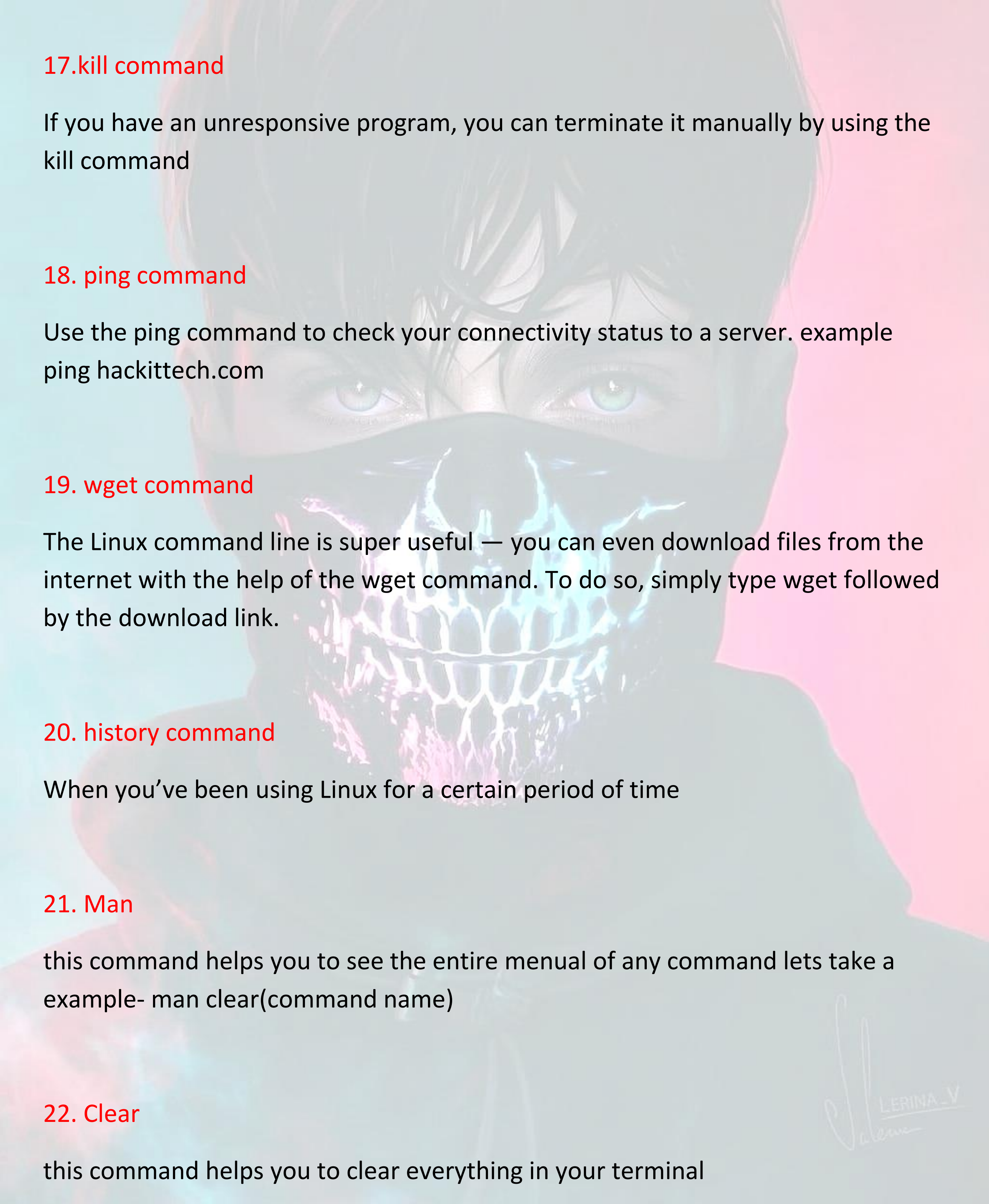
Short for “SuperUser Do”, this command enables you to perform tasks that require administrative or root permissions.

15. chmod command

chmod is another Linux command, used to change the read, write, and execute permissions of files and directories.

16. chown command

In Linux, all files are owned by a specific user. The chown command enables you to change or transfer the ownership of a file to the specified username



17.kill command

If you have an unresponsive program, you can terminate it manually by using the kill command

18. ping command

Use the ping command to check your connectivity status to a server. example ping hackittech.com

19. wget command

The Linux command line is super useful — you can even download files from the internet with the help of the wget command. To do so, simply type wget followed by the download link.

20. history command

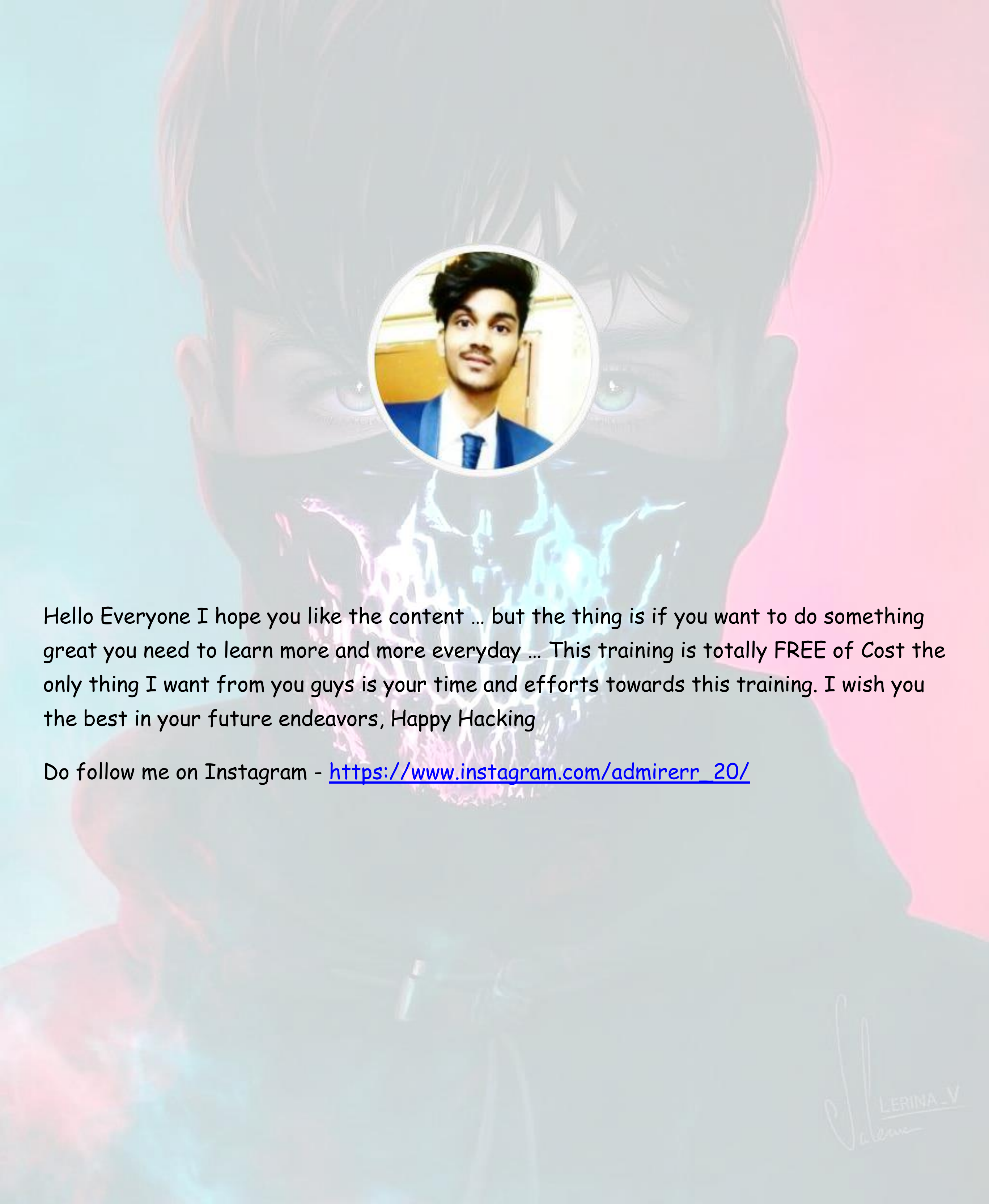
When you've been using Linux for a certain period of time

21. Man

this command helps you to see the entire menual of any command lets take a example- man clear(command name)

22. Clear

this command helps you to clear everything in your terminal



Hello Everyone I hope you like the content … but the thing is if you want to do something great you need to learn more and more everyday … This training is totally FREE of Cost the only thing I want from you guys is your time and efforts towards this training. I wish you the best in your future endeavors, Happy Hacking

Do follow me on Instagram - https://www.instagram.com/admirerr_20/

By Sandeep Kumar

Insta [@admirerr_20](https://www.instagram.com/admirerr_20/)