Information Security: Practical Notes

INSTRUCTOR

Prof. M. Iqbal Bhat

PHONE

01951295539

EMAIL

Iqbal.jkhed@jk.gov.in

OFFICE LOCATION

Department of Computer Sciences, Government Degree College Beerwah

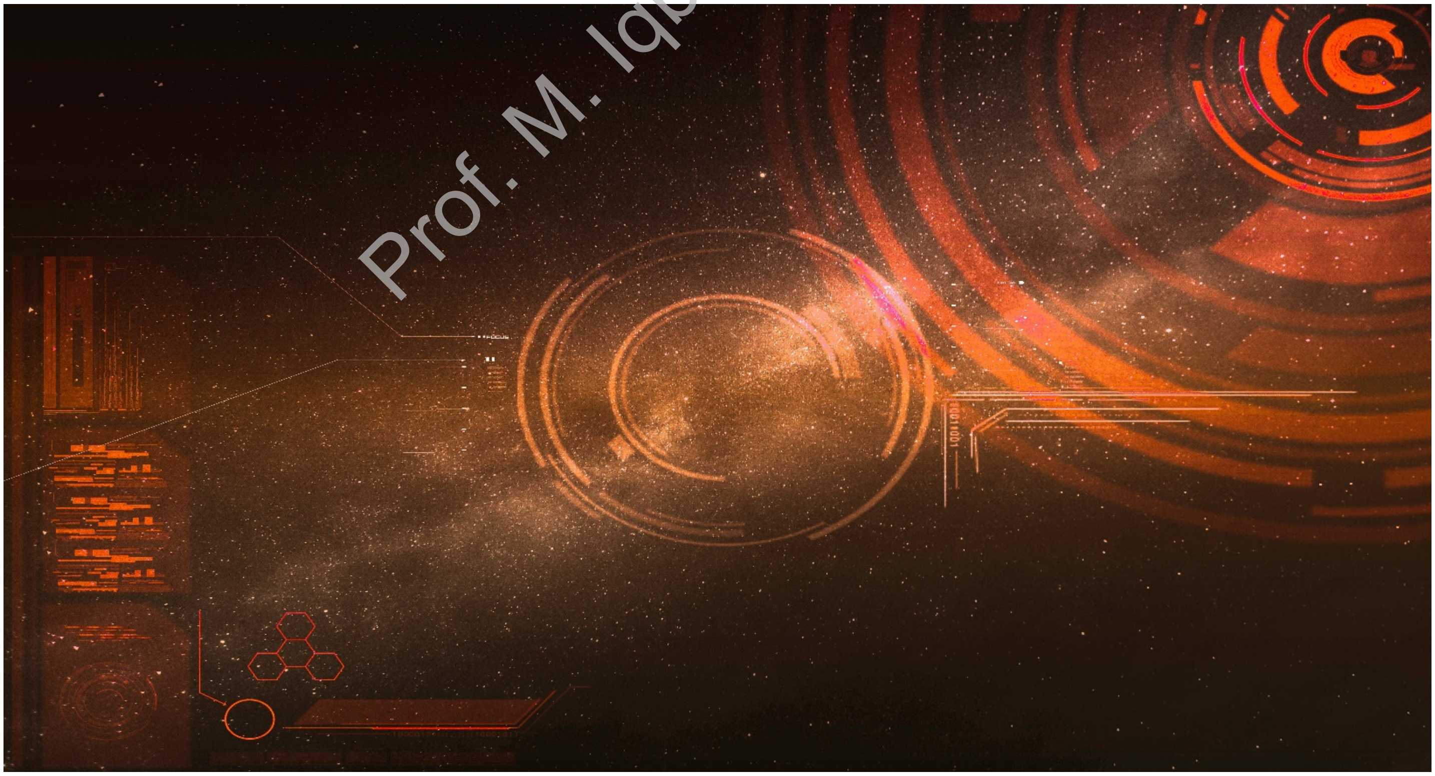
PRACTICAL OVERVIEW

DEMONSTRATE THE USE OF NETWORK TOOLS: PING, IPCONFIG, IFCONFIG, TRACERT, ARP, NETSTAT, WHOIS

REQUIRED TOOLS/SOFTWARE

Operating System:

1. Windows 7/10/11
2. Linux (preferably KALI Linux)



1. Ping:

Ping is a network tool used to test the connectivity between two devices on a network. It works by sending ICMP (Internet Control Message Protocol) packets to the destination device and waiting for a response. The time it takes for the packet to travel from the source device to the destination device and back is known as the round-trip time (RTT), and is measured in milliseconds.

Ping can be used to troubleshoot network connectivity issues, as it can help identify whether a device is connected to the network and whether it can communicate with other devices. If a ping request fails, it could indicate a problem with the network connection, the destination device, or the routing between the two devices.

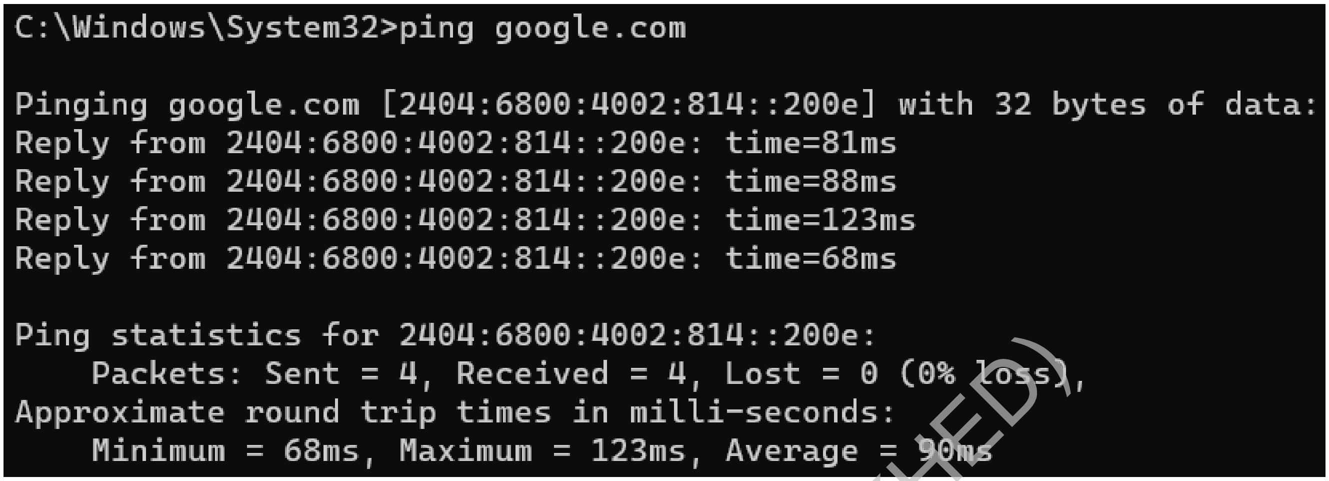
Ping can also be used to test the performance of a network connection, as the RTT can be used to calculate the latency, which is the time it takes for data to travel from the source device to the destination device and back. High latency can indicate a slow network connection, which can affect the performance of applications and services that rely on real-time data transmission.

Ping can be used in a variety of ways, including:

- Testing connectivity between two devices: `ping <destination IP>` or `ping <destination hostname>`
- Testing network performance: `ping -n <number of packets> <destination IP>`
- Testing packet loss: `ping -n <number of packets> -w <timeout in milliseconds> <destination IP>`

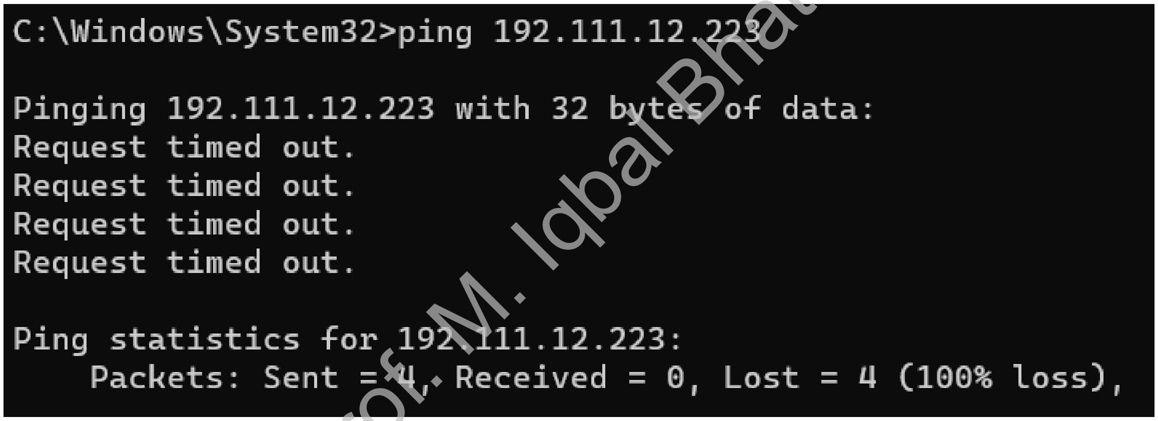
Ping is a simple yet powerful tool that is essential for network administrators and can help diagnose and troubleshoot network issues, monitor network performance, and ensure that network devices are functioning properly

Ping an address that is reachable:



```
C:\Windows\System32>ping google.com

Pinging google.com [2404:6800:4002:814::200e] with 32 bytes of data:
Reply from 2404:6800:4002:814::200e: time=81ms
Reply from 2404:6800:4002:814::200e: time=88ms
Reply from 2404:6800:4002:814::200e: time=123ms
Reply from 2404:6800:4002:814::200e: time=68ms

Ping statistics for 2404:6800:4002:814::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 68ms, Maximum = 123ms, Average = 90ms
```

Ping an address that is not reachable:



```
C:\Windows\System32>ping 192.111.12.223

Pinging 192.111.12.223 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.111.12.223:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

2. Ipconfig and Ifconfig:

Ipconfig and Ifconfig are network tools used to view and configure network interfaces on a device. They can display information such as IP address, subnet mask, and default gateway, and can also be used to release and renew IP addresses. Here are some details on how these tools work:

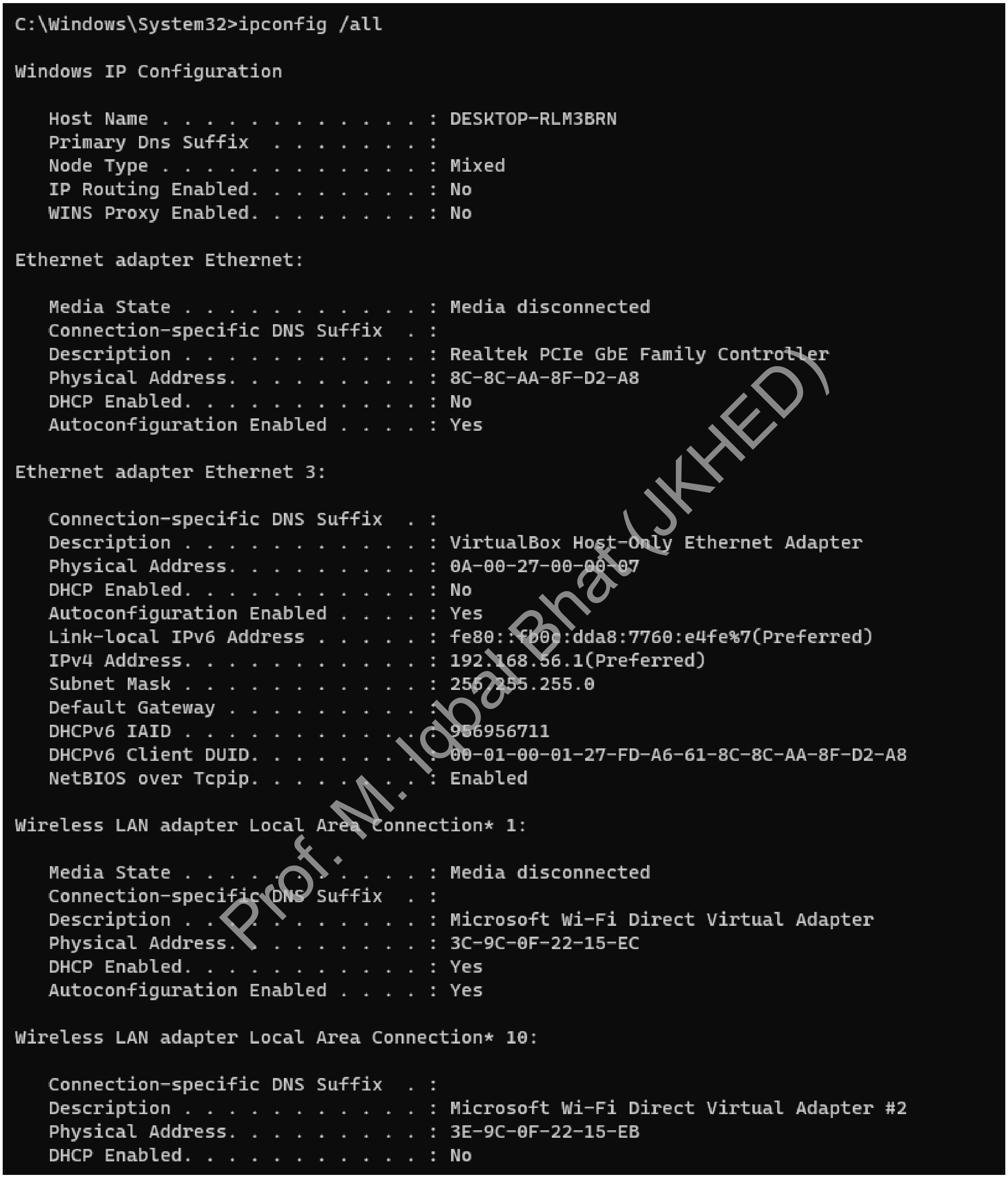
1. Ipconfig (Windows):

- Ipconfig is a command-line tool used to view and configure network interfaces on a Windows device.
- It can display information such as IP address, subnet mask, default gateway, DNS servers, and more.
- It can also be used to release and renew IP addresses, which can help troubleshoot connectivity issues.
- Example commands:
    - `ipconfig /all`: displays detailed information about all network interfaces on the device.
    - `ipconfig /release`: releases the currently assigned IP address for all network interfaces on the device.
    - `ipconfig /renew`: renews the IP address for all network interfaces on the device.

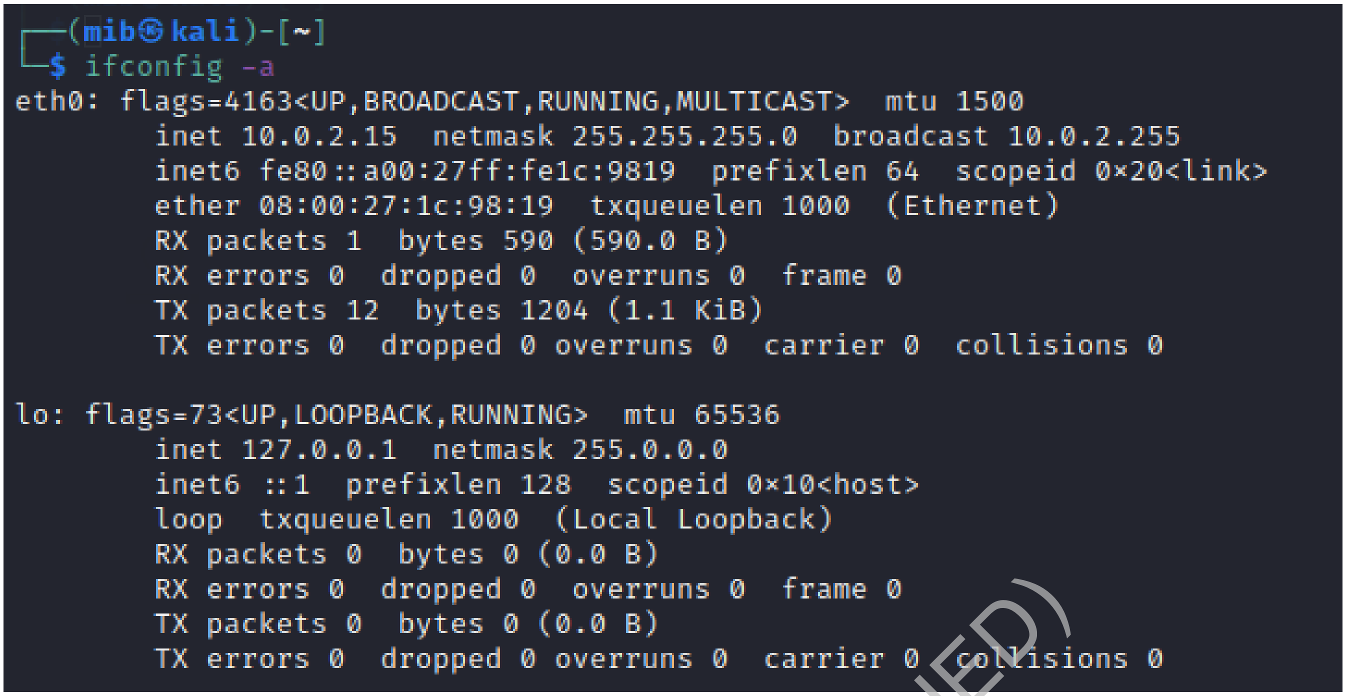
2. Ifconfig (Linux/Mac):

- Ifconfig is a command-line tool used to view and configure network interfaces on a Linux or Mac device.
- It can display information such as IP address, subnet mask, MAC address, and more.
- It can also be used to configure network interfaces, such as assigning IP addresses and enabling or disabling network interfaces.
- Example commands:
    - `ifconfig`: displays information about all network interfaces on the device.
    - `ifconfig eth0 up`: enables the eth0 network interface.
    - `ifconfig eth0 down`: disables the eth0 network interface.
    - `ifconfig eth0 192.168.0.1 netmask 255.255.255.0`: assigns the IP address 192.168.0.1 and subnet mask 255.255.255.0 to the eth0 network interface.

Ipconfig and Ifconfig are essential network tools for network administrators and can help diagnose and troubleshoot network connectivity issues, configure network interfaces, and gather information about network devices and connections.



```
C:\Windows\System32>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-RLM3BRN
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : 8C-8C-AA-8F-D2-A8
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-07
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::fb0c:dda8:7760:e4fe%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.56.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 956956711
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-FD-A6-61-8C-8C-AA-8F-D2-A8
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 3C-9C-0F-22-15-EC
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 10:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 3E-9C-0F-22-15-EB
   DHCP Enabled. . . . . . . . . . . : No
```



```
┌──(mib㉿kali)-[~]
└─$ ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe1c:9819  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:1c:98:19  txqueuelen 1000  (Ethernet)
        RX packets 1  bytes 590 (590.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12  bytes 1204 (1.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

3. Tracert/Traceroute:

Tracert (or "traceroute" in Linux) is a network tool used to trace the path that packets take from the source device to the destination device on a network. It works by sending packets with varying time-to-live (TTL) values to the destination device, and then analyzing the responses to determine the path that the packets took.

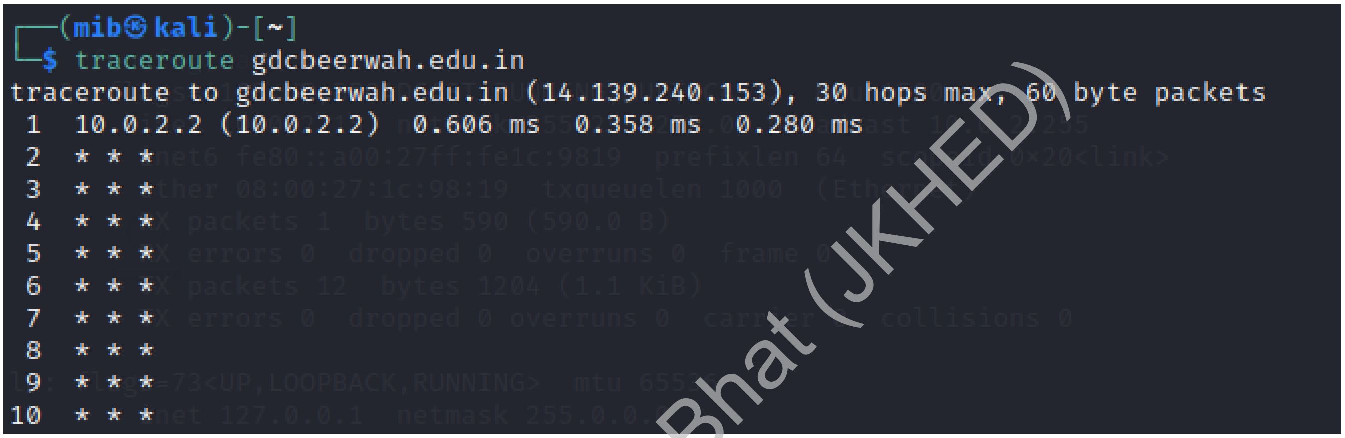
Tracert can be used to troubleshoot network connectivity issues, as it can help identify where packets are being dropped or delayed along the path between the source device and the destination device. If a tracert command fails to reach the destination device or shows high latency at a particular hop, it could indicate a problem with the network connection or the routing between the two devices.

Tracert can also be used to identify network performance issues, as it can help pinpoint bottlenecks or slow points along the path. By analyzing the round-trip time (RTT) of each hop in the path, network administrators can identify areas where latency is high and take steps to optimize the network.

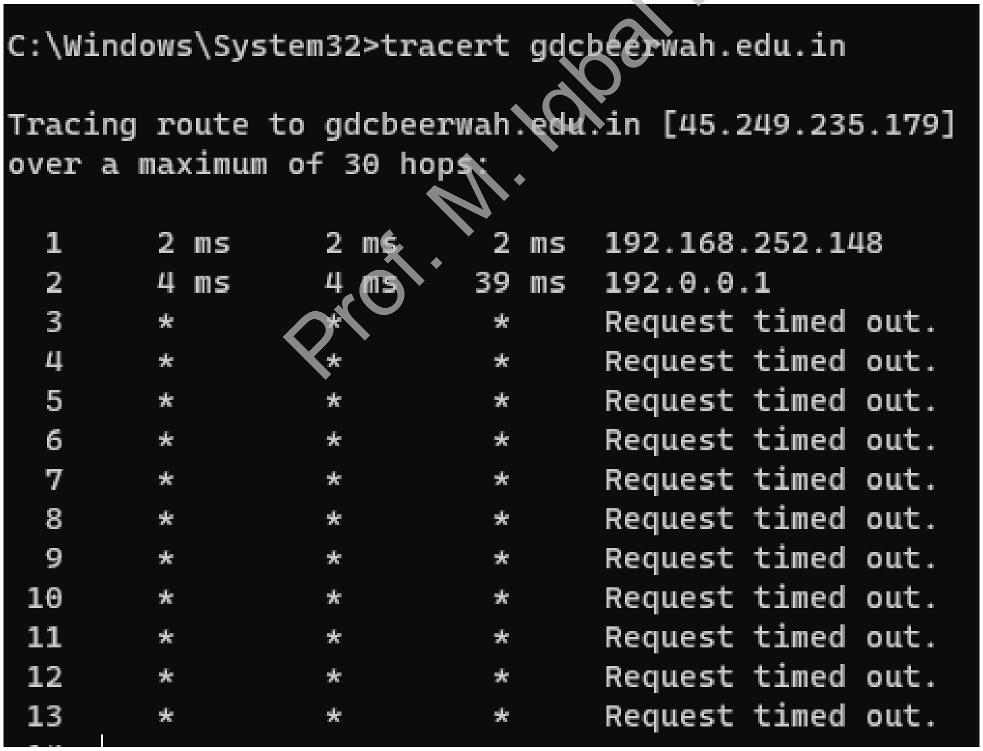
Here are some examples of how to use Tracert:

- Tracing the path to a destination device: `tracert <destination IP>` or `tracert <destination hostname>`
- Controlling the number of hops: `tracert -h <maximum number of hops> <destination IP>`
- Resolving hostnames to IP addresses: `tracert -d <destination hostname>`

Tracert is a powerful tool for network administrators and can help diagnose and troubleshoot network connectivity and performance issues. However, it's important to note that some networks may block or restrict the use of Tracert, so it may not always be a reliable tool in all situations



```
┌──(mib㉿kali)-[~]
└─$ traceroute gdcbeerwah.edu.in
traceroute to gdcbeerwah.edu.in (14.139.240.153), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  0.606 ms  0.358 ms  0.280 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
```



```
C:\Windows\System32>tracert gdcbeerwah.edu.in

Tracing route to gdcbeerwah.edu.in [45.249.235.179]
over a maximum of 30 hops:

  1     2 ms     2 ms     2 ms  192.168.252.148
  2     4 ms     4 ms    39 ms  192.0.0.1
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
```

4. ARP:

ARP (Address Resolution Protocol) is a network protocol used to map a device's MAC address to its IP address on a local network. When a device wants to communicate with another device on the same network, it needs to know the other device's MAC address in order to send packets directly to that device. However, the device only knows the other device's IP address. That's where ARP comes in.

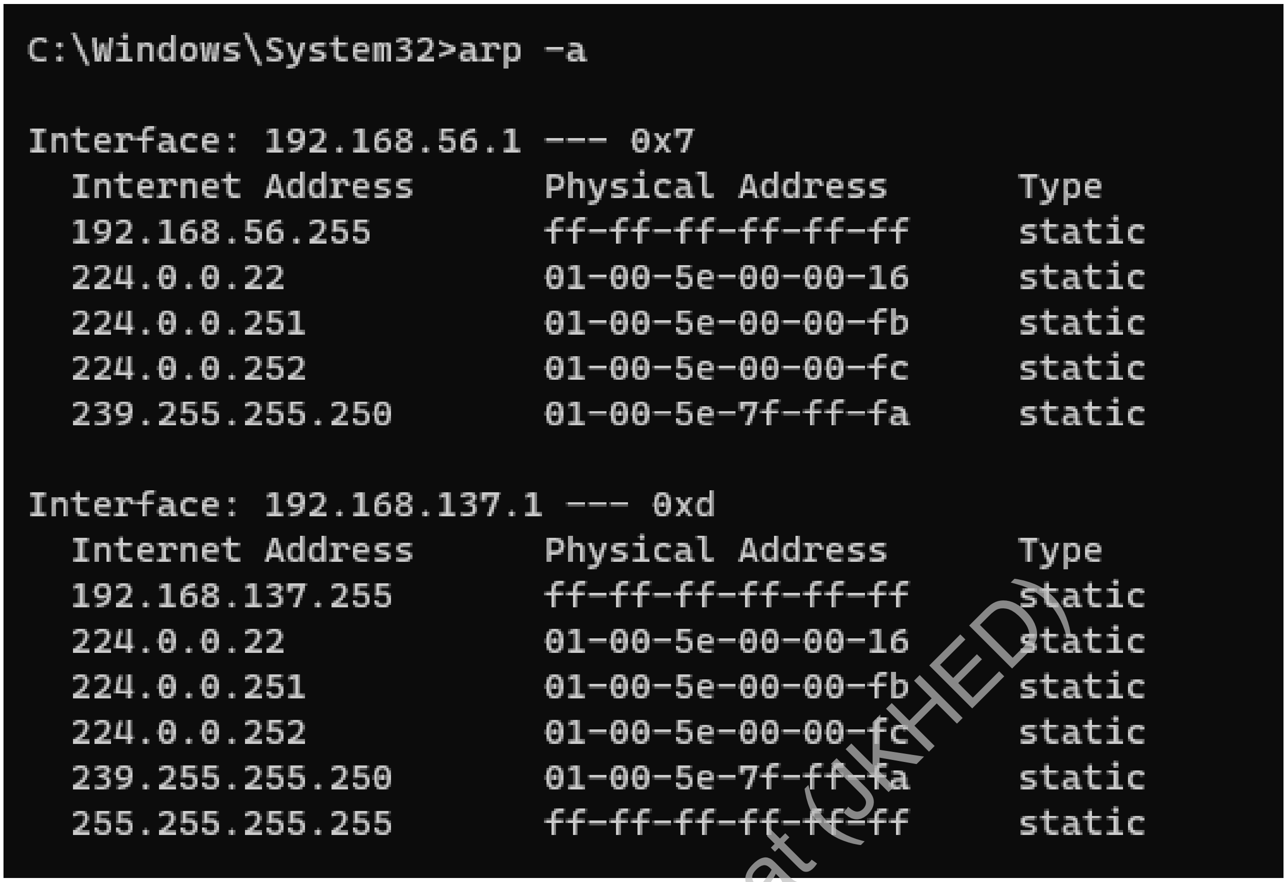
When a device needs to send packets to another device on the same network, it first checks its ARP cache to see if it already has the MAC address for that IP address. If the MAC address is not in the cache, the device sends an ARP request to the network asking for the MAC address corresponding to the IP address it wants to communicate with. The device with the corresponding IP address then responds with its MAC address, and the requesting device adds that information to its ARP cache.

ARP is a critical protocol for local network communication and is used by devices such as routers, switches, and computers. It helps ensure that packets are delivered directly to the intended recipient, improving network performance and reducing unnecessary traffic.

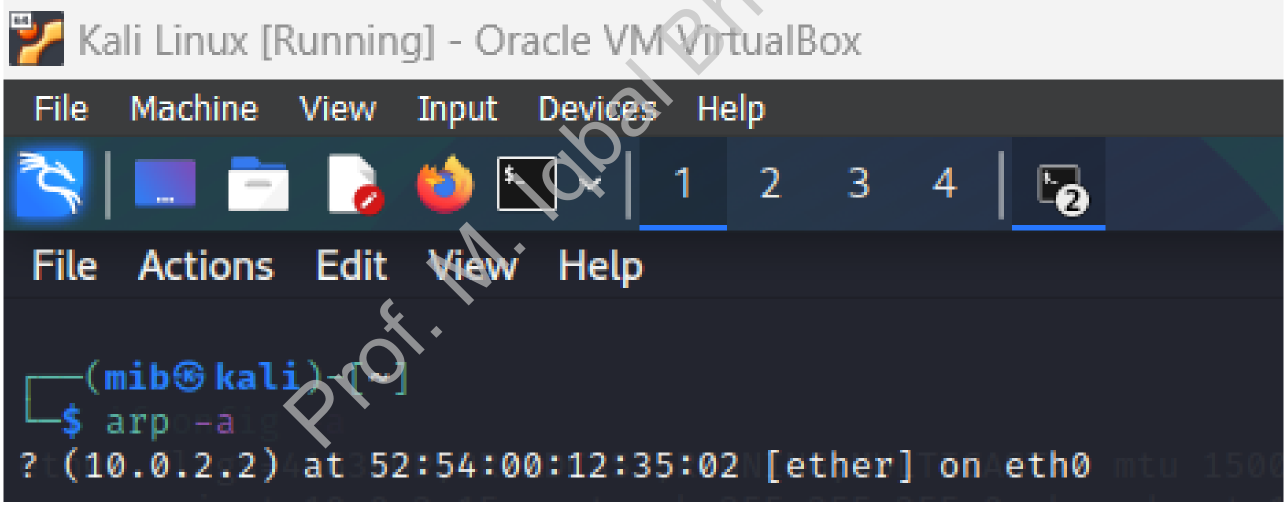
Here are some common ARP commands:

- Displaying the ARP cache: `arp -a` (Windows) or `arp -n` (Linux/Mac)
- Clearing the ARP cache: `arp -d <IP address>` (Windows) or `sudo arp -d <IP address>` (Linux/Mac)

While ARP is a useful protocol for local network communication, it's important to note that it can also be vulnerable to certain types of attacks, such as ARP spoofing. In an ARP spoofing attack, an attacker sends false ARP messages to the network, tricking devices into mapping the attacker's MAC address to the IP address of a legitimate device. This can allow the attacker to intercept and modify network traffic. To prevent ARP spoofing, network administrators can implement measures such as static ARP table entries, port security, and ARP monitoring tools.



```
C:\Windows\System32>arp -a

Interface: 192.168.56.1 --- 0x7
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.137.1 --- 0xd
  Internet Address      Physical Address      Type
  192.168.137.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
File Actions Edit View Help

```
┌──(mib㉿kali)-[~]
└─$ arp -a
? (10.0.2.2) at 52:54:00:12:35:02 [ether] on eth0
```

5. Netstat:

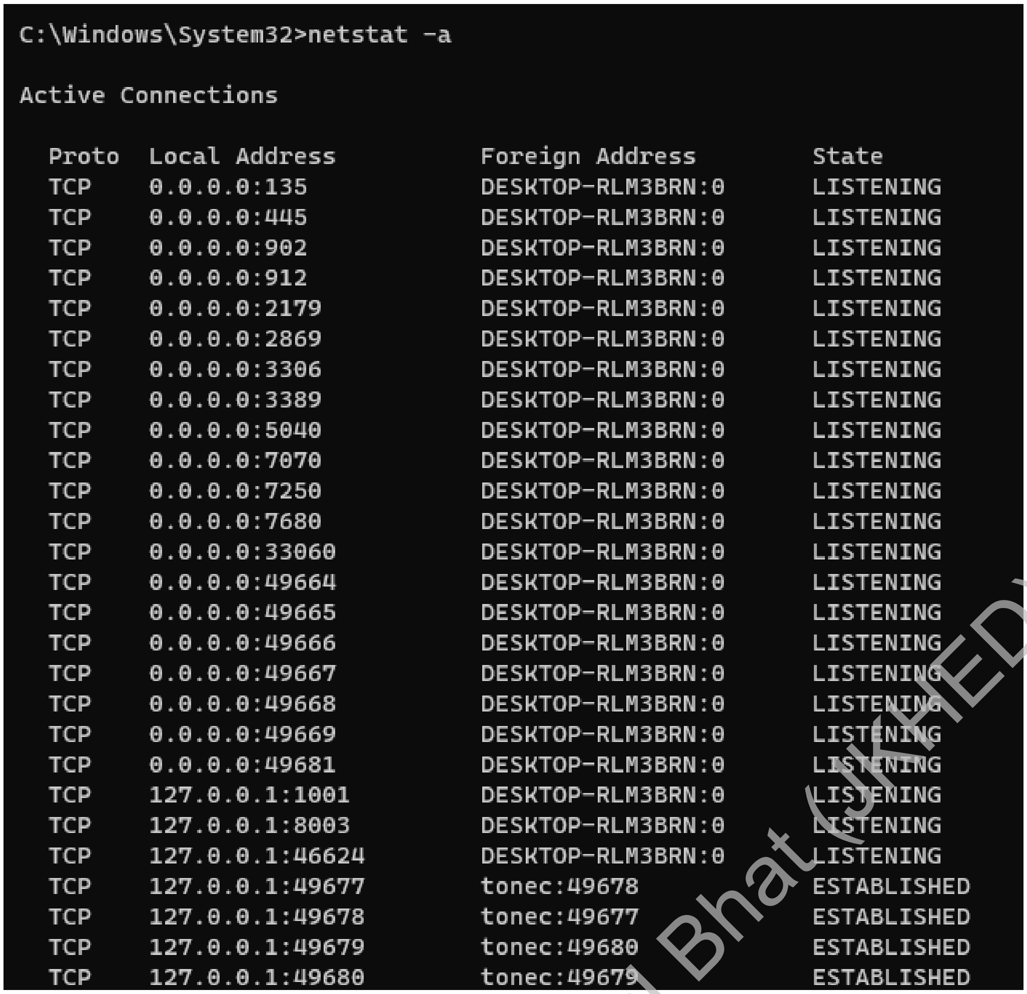
Netstat (short for "network statistics") is a command-line tool used to display network connections, routing tables, and network interface statistics on a device. It can be used to diagnose network connectivity issues, monitor network traffic, and identify network performance issues.

Here are some common Netstat commands:

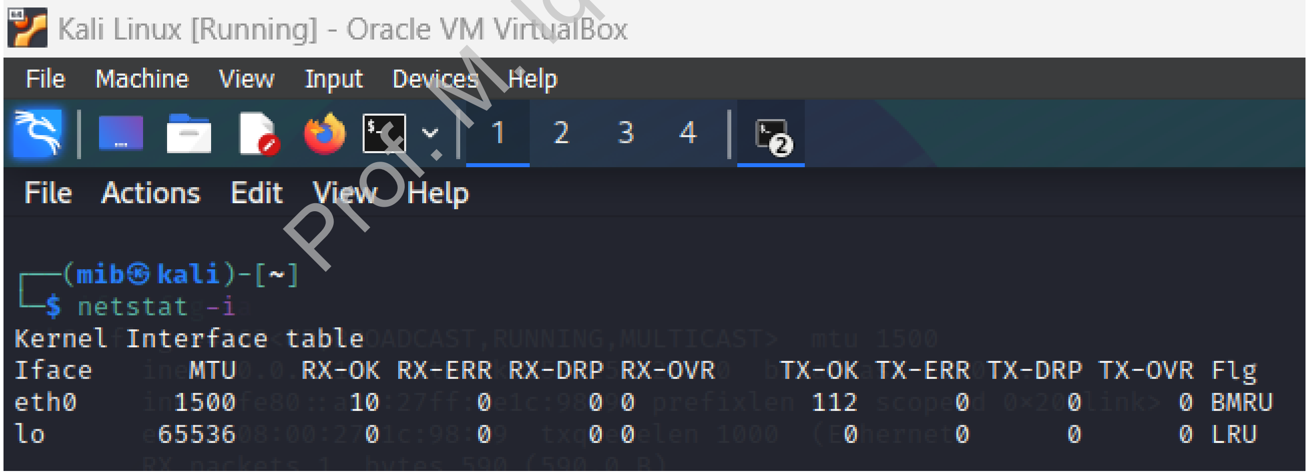
- Displaying active network connections: `netstat -a` (Windows) or `netstat -an` (Linux/Mac)
- Displaying network interface statistics: `netstat -i` (Windows) or `netstat -i` (Linux/Mac)
- Displaying routing table information: `netstat -r` (Windows) or `netstat -rn` (Linux/Mac)

Netstat can provide valuable information for network administrators, such as the source and destination IP addresses and ports of active network connections, the amount of data transmitted and received on each network interface, and the routing paths for packets sent on the network.

However, it's important to note that Netstat can also be used by attackers to gather information about a network or device. For example, an attacker might use Netstat to identify open ports on a device that can be exploited to gain unauthorized access. To mitigate these risks, network administrators should secure their devices and networks by implementing firewalls, access controls, and other security measures.



```
C:\Windows\System32>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            DESKTOP-RLM3BRN:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-RLM3BRN:0      LISTENING
  TCP    0.0.0.0:902            DESKTOP-RLM3BRN:0      LISTENING
  TCP    0.0.0.0:912            DESKTOP-RLM3BRN:0      LISTENING
  TCP    0.0.0.0:2179           DESKTOP-RLM3BRN:0      LISTENING
  TCP    0.0.0.0:2869           DESKTOP-RLM3BRN:0      LISTENING
  TCP    0.0.0.0:3306           DESKTOP-RLM3BRN:0      LISTENING
  TCP    0.0.0.0:3389           DESKTOP-RLM3BRN:0      LISTENING
  TCP    0.0.0.0:5040           DESKTOP-RLM3BRN:0      LISTENING
  TCP    0.0.0.0:7070           DESKTOP-RLM3BRN:0      LISTENING
  TCP    0.0.0.0:7250           DESKTOP-RLM3BRN:0      LISTENING
  TCP    0.0.0.0:7680           DESKTOP-RLM3BRN:0      LISTENING
  TCP    0.0.0.0:33060          DESKTOP-RLM3BRN:0      LISTENING
  TCP    0.0.0.0:49664          DESKTOP-RLM3BRN:0      LISTENING
  TCP    0.0.0.0:49665          DESKTOP-RLM3BRN:0      LISTENING
  TCP    0.0.0.0:49666          DESKTOP-RLM3BRN:0      LISTENING
  TCP    0.0.0.0:49667          DESKTOP-RLM3BRN:0      LISTENING
  TCP    0.0.0.0:49668          DESKTOP-RLM3BRN:0      LISTENING
  TCP    0.0.0.0:49669          DESKTOP-RLM3BRN:0      LISTENING
  TCP    0.0.0.0:49681          DESKTOP-RLM3BRN:0      LISTENING
  TCP    127.0.0.1:1001         DESKTOP-RLM3BRN:0      LISTENING
  TCP    127.0.0.1:8003         DESKTOP-RLM3BRN:0      LISTENING
  TCP    127.0.0.1:46624        DESKTOP-RLM3BRN:0      LISTENING
  TCP    127.0.0.1:49677        tonec:49678            ESTABLISHED
  TCP    127.0.0.1:49678        tonec:49677            ESTABLISHED
  TCP    127.0.0.1:49679        tonec:49680            ESTABLISHED
  TCP    127.0.0.1:49680        tonec:49679            ESTABLISHED
```


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
File Actions Edit View Help

```
┌──(mib㉿kali)-[~]
└─$ netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0      1500       10      0      0 0           112      0      0      0 BMRU
lo       65536        0      0      0 0             0      0      0      0 LRU
```

6. Whois:

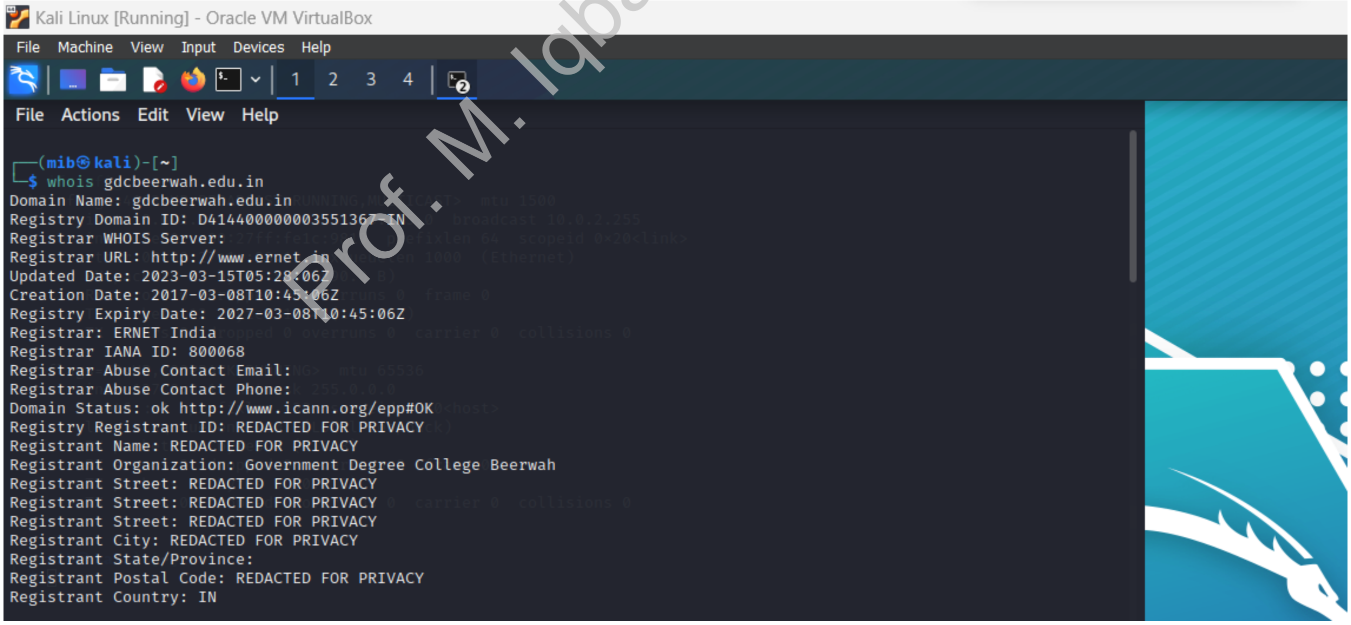
Whois is a command-line tool used to query the public database of domain name registrations and IP address allocations. It can be used to retrieve information about the owner of a domain name or IP address, such as the registrar, contact details, and administrative and technical information.

Here are some common Whois commands:

- Querying the Whois database for a domain name: `whois example.com`
- Querying the Whois database for an IP address: `whois 192.0.2.1`

Whois can provide valuable information for network administrators, such as the owner of a domain name or IP address, the date of registration, and the expiry date. It can also be used to identify potential security threats, such as domains associated with spam or phishing activities.

However, it's important to note that Whois information is publicly available, which can also make it accessible to attackers. Attackers may use Whois to gather information about an organization's network infrastructure or to perform reconnaissance for targeted attacks. To mitigate these risks, network administrators should take steps to protect their domains and IP addresses, such as enabling privacy protection services or limiting the amount of information available in the Whois database.


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
File Actions Edit View Help

```
┌──(mib㉿kali)-[~]
└─$ whois gdcbeerwah.edu.in
Domain Name: gdcbeerwah.edu.in
Registry Domain ID: D414400000003551367-IN
Registrar WHOIS Server:
Registrar URL: http://www.ernet.in
Updated Date: 2023-03-15T05:28:06Z
Creation Date: 2017-03-08T10:45:06Z
Registry Expiry Date: 2027-03-08T10:45:06Z
Registrar: ERNET India
Registrar IANA ID: 800068
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: ok http://www.icann.org/epp#OK
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Government Degree College Beerwah
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province:
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
```

END