**PRACTICAL NO 3**

**AIM:** Linux Network Analysis and ARP Poisoning

Linux Network Analysis:

* Execute the ifconfig command to retrieve network interface information.
* Use the ping command to test network connectivity and analyze the output.
* Analyze the netstat command output to view active network connections.
* Perform a traceroute to trace the route packets take to reach a target host.

ARP Poisoning:

* Use ARP poisoning techniques to redirect network traffic on a Windows system.
* Analyze the effects of ARP poisoning on network communication and security.

**SOLUTION:**

1) Linux Network Analysis:

* Execute the ifconfig command to retrieve network interface information.
* Use the ping command to test network connectivity and analyze the output.
* Analyze the netstat command output to view active network connections.
* Perform a traceroute to trace the route packets take to reach a target host.

**i) Execute the ifconfig command to retrieve network interface information.**

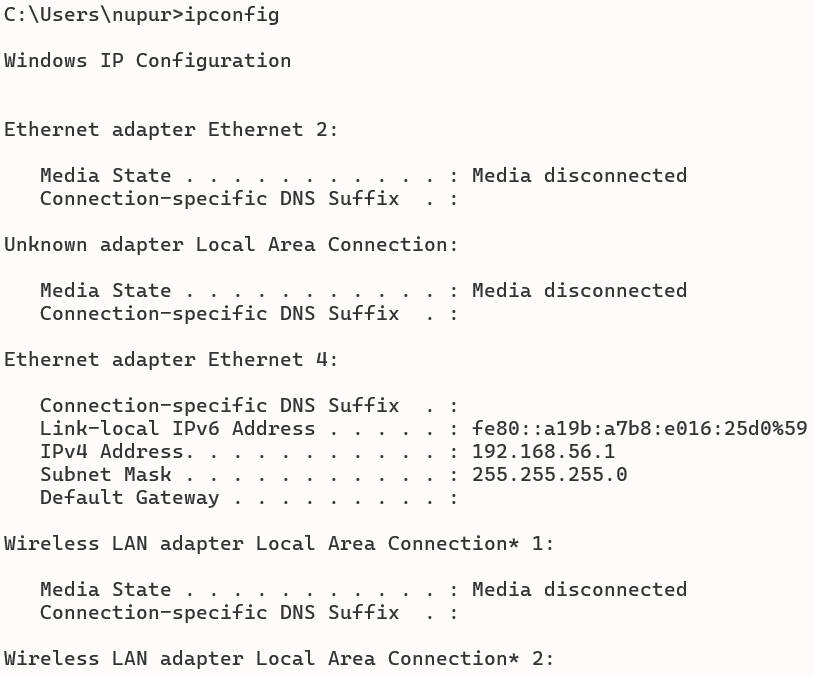
ifconfig (interface configuration) is a command-line utility in Unix-like operating systems used to configure, manage, and display network interfaces. It allows users to view network interface details, assign IP addresses, and enable or disable interfaces.

**UBUNTU**

A screenshot of a computer program

Description automatically generated

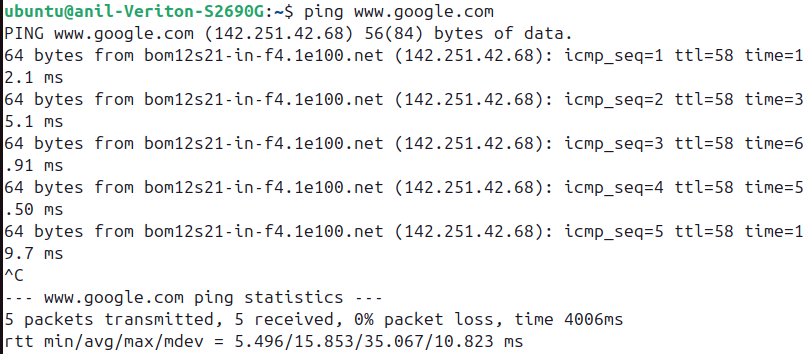
**WINDOWS**



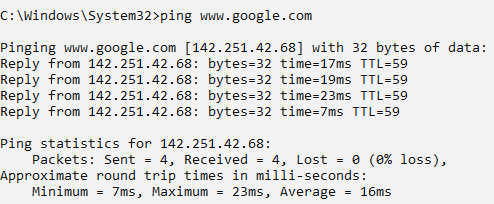
**ii) Use the ping command to test network connectivity and analyze the output.**

ping is a network diagnostic command used to test the connectivity between two devices on a network. It sends ICMP Echo Request packets to a target host and waits for Echo Reply packets, measuring the round-trip time and indicating whether the target is reachable.

**UBUNTU**



**WINDOWS**



**iii) Analyze the netstat command output to view active network connections.**

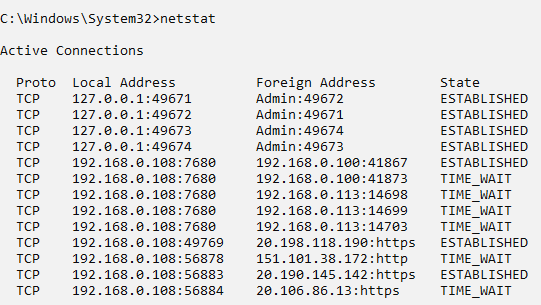
netstat (network statistics) is a command-line tool used to display network connections, routing tables, interface statistics, and other network-related information on a computer. It helps monitor active connections, open ports, and network interfaces in use.

**UBUNTU**

A screenshot of a computer

Description automatically generated

**WINDOWS**



**iv) Perform a traceroute to trace the route packets take to reach a target host.**

traceroute is a network diagnostic tool used to trace the path data packets take from one device to another across an IP network. It shows the sequence of routers (hops) the packets pass through, along with the time taken for each hop, helping identify network bottlenecks or failures.

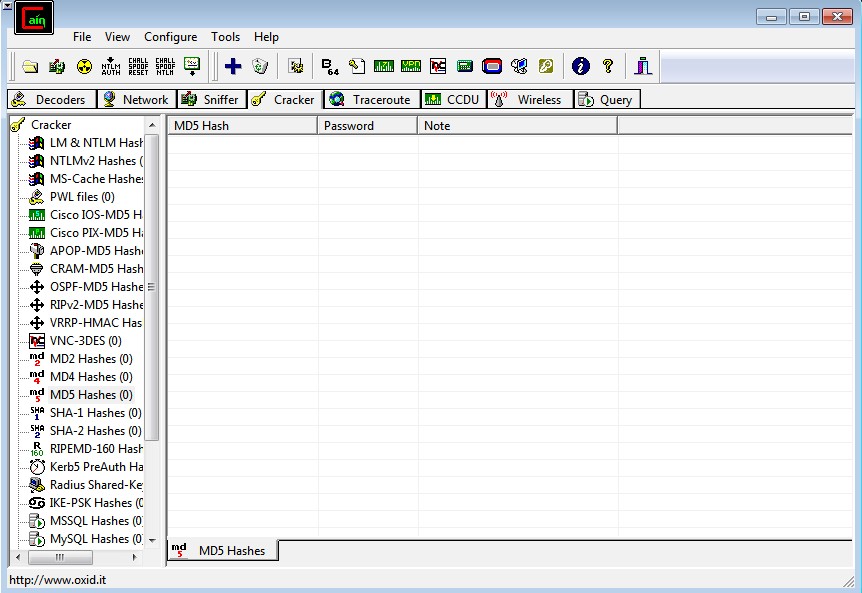
**WINDOWS**

****

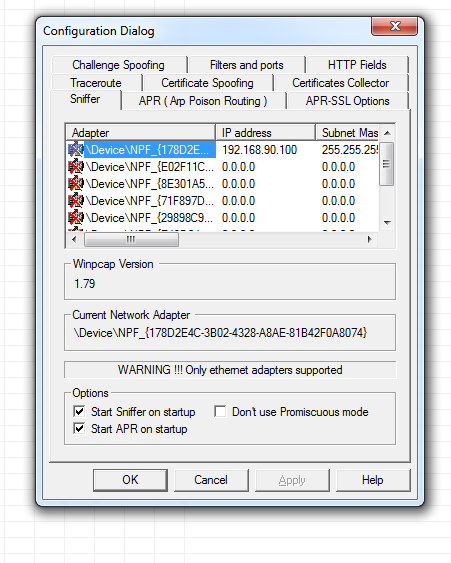
2) ARP Poisoning:

* Use ARP poisoning techniques to redirect network traffic on a Windows system.
* Analyze the effects of ARP poisoning on network communication and security.

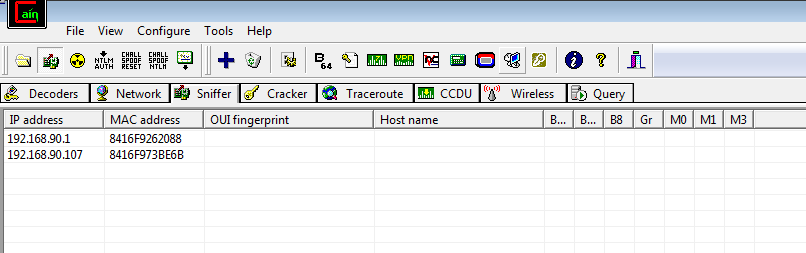
**Step 1 :** Download Install and then open the Cain & Abel Tool



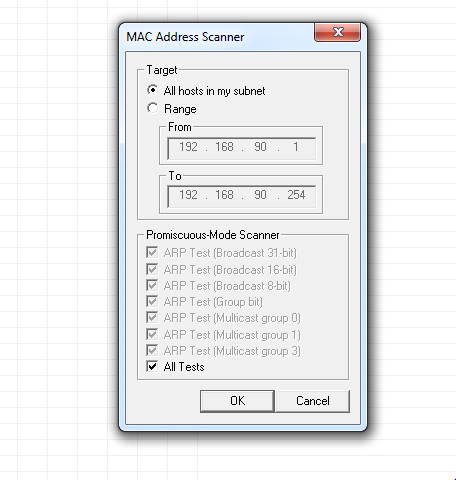
**Step 2 :** first go to sniffer and then click on configure , select the appropraite wireless adapter. Click on apply and then click on the ok button

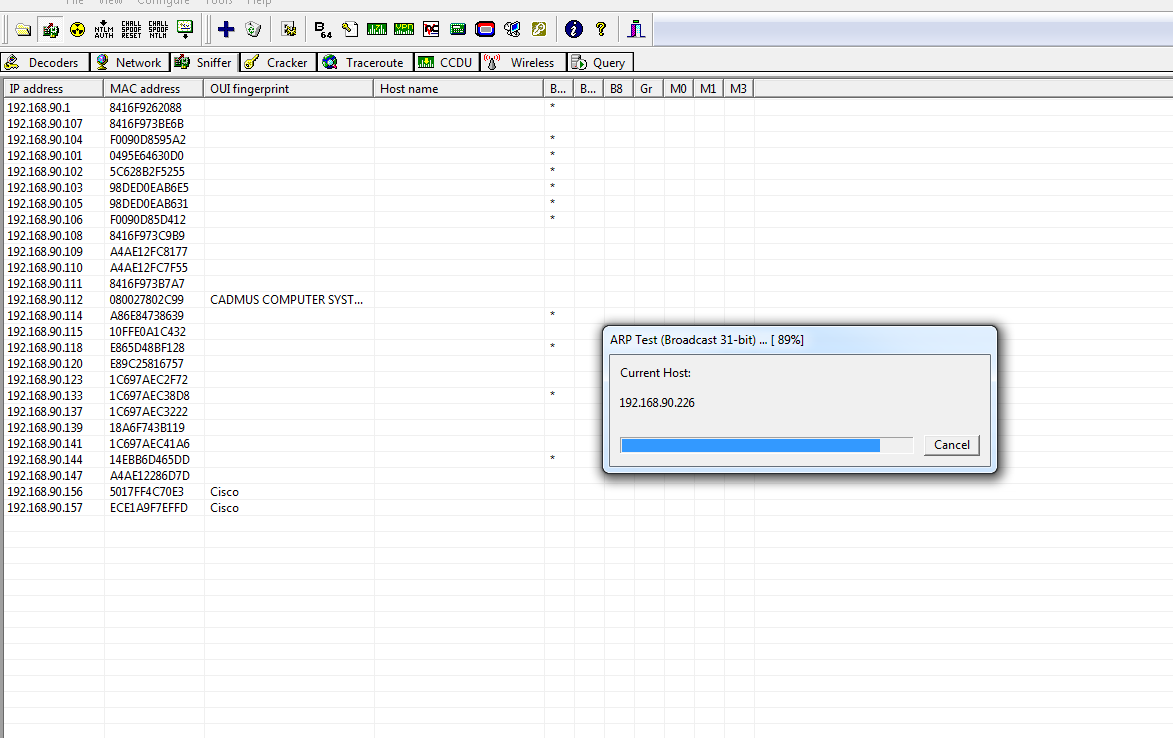


**Step 3 :** activate sniffer

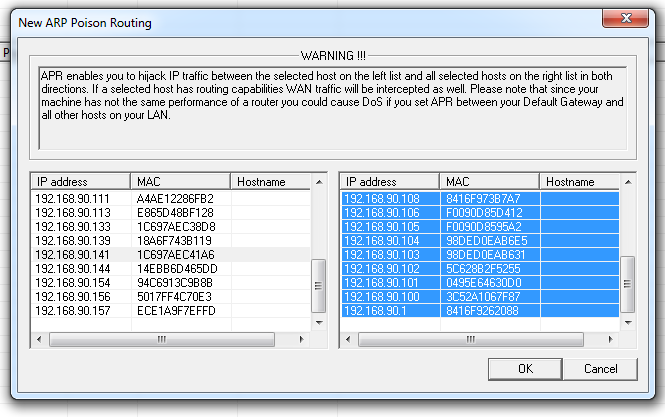


**Step 4 :** Click on + icon . check all tests checkbox and then click on OK





**Step 5 :**  click on APR then click on the blank screen and then on the + icon. select any ip address ( ipv4 address) form the left side and select all ip address and mac address from right side and then click on ok



**Step 6 :** Apply sniffer by click on the start /stop sniffer on the top. It gives the status of all the devices connected to wifi. also in the status tab you will see the status ‘poisoining’

