**AIM:** Study the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registrars.

Commands:

1. whois:

* Description:

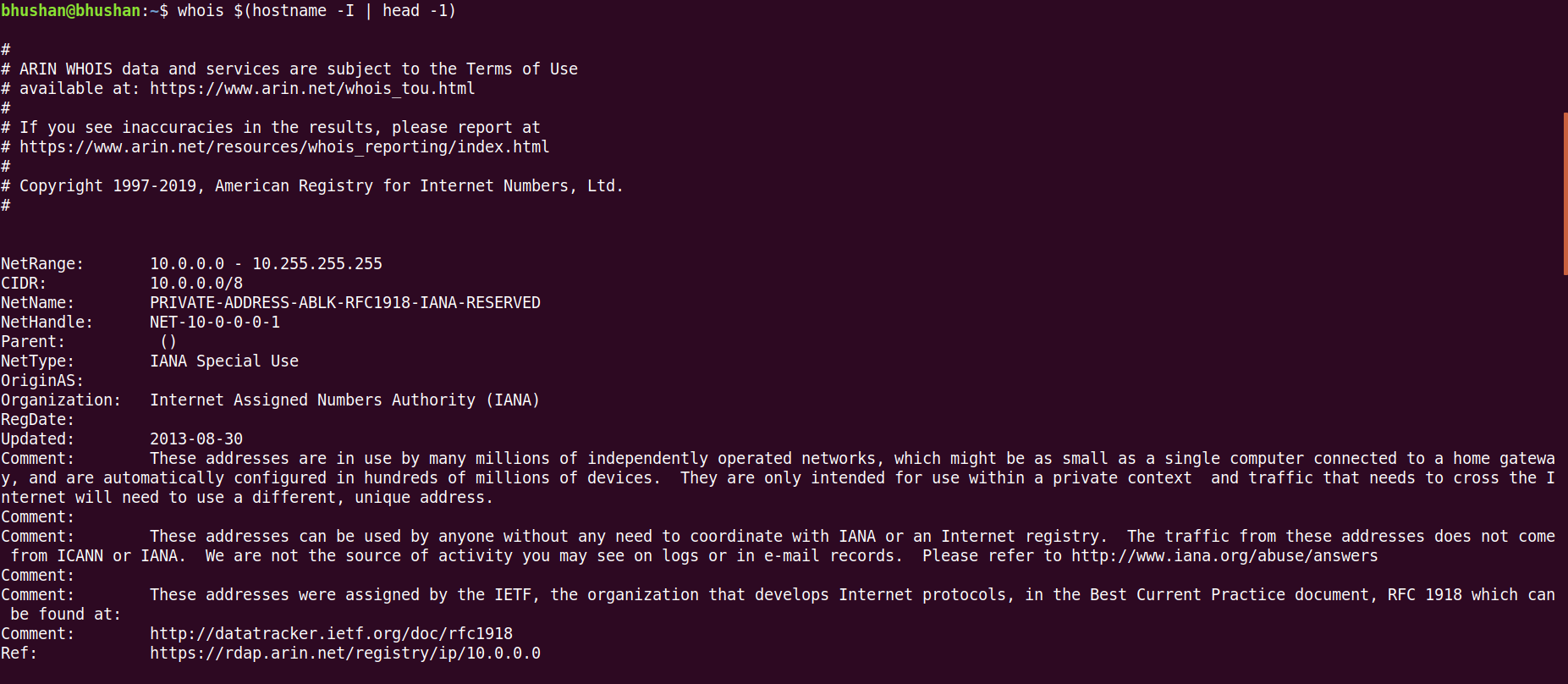
1. whois client tries to guess the right server to ask for the specified object.
2. If no guess can be made it will connect to whois.networksolutions.com for NIC handles or whois.arin.net for IPv4 addresses and network names.

* Parameters:

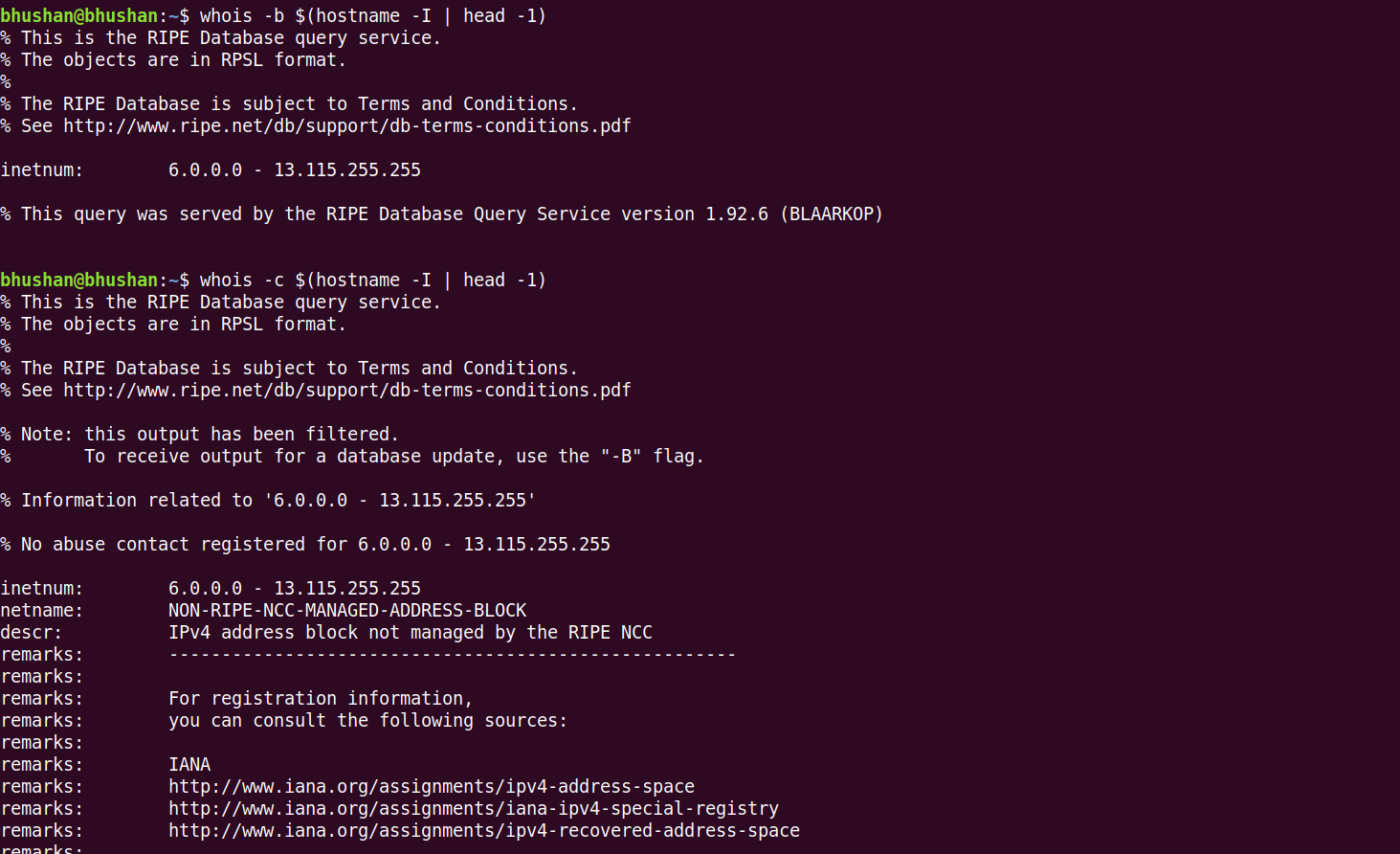
1. The only required parameter is the object which is to be searched for in the database.
2. Object can be ip address or the link to any website.

* Some options:

1. -b : returns the range of the addresses within the given objects range alongwith the abuse contact.
2. -c : Return the smallest IP address range with a reference to an irt object.



1.a) Unfiltered output of whois command



1.b) Outputs of -b and -c options.

1. **traceroute**:

* Description:

1. *traceroute* command tracks the route packet taken from an IP network on their way to the given host.
2. The default timeout time is 5.0 seconds. That is, if there is no response from the probe sent, asterisk will be printed for that probe.

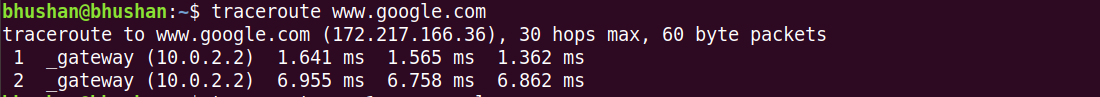
* Parameters:

1. The only required parameter is the name or the IP address of the destination of the host.

* Options:

1. -4, -6 : Specifies which ip version should be used for tracerouting. By default, program will try to resolve the name given and choose the appropriate protocol automatically.
2. -q : Specifies the number of probes that should be sent per hop. This parameter defaults to 3.
3. -m : Specifies the max number of hops that can be taken. It defaults to 30. Max number of hops is 255.
4. -z: Specifices the time delay between two probes that are being sent. It defaults to 0. When value is more than 10, it states that, the time is in milliseconds, else, time is considered in seconds.

Output:



2.a) Outputs of traceroute

1. dig:

* Description:

1. It is a tool used for interrogating DNS name servers.
2. Unless specified, dig will try each of the servers in */etc/resolv.conf*. If no servers are found, dig will query the localhost.

* Usage:

1. Typical invocation of dig command is given as:

dig @server name type

* Parameters:

1. dig works with no parameters as well. That is, it has no mandatory examples.
2. name : name of the required resource.
3. type: indicates what type of query is required. For example: A, MX, SIG, etc.

This defaults to A.

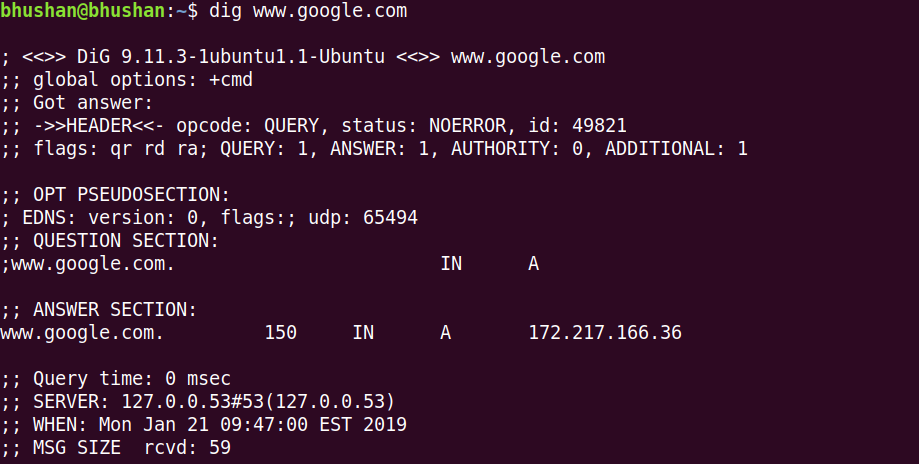
* Options:

1. -4, -6 : Specifies which ip version should be used.
2. -q: This is used to specify the name of the resource given in the usage section.
3. -t: Specifies which type of query is required. type of usage is followed after this flag. Use ANY as succeding word for this parameter and all the types of queries will be returned.
4. +[no]all: specifies whether user wants to display all the fields which dig command returns.

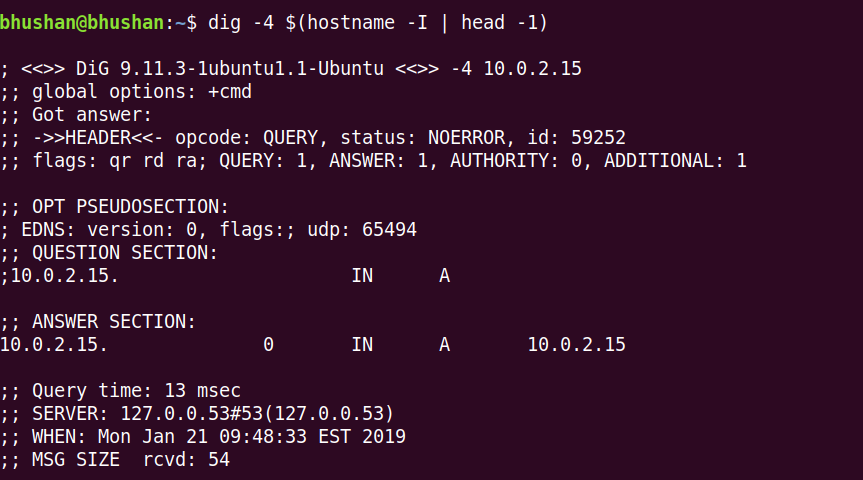
*dig* address +noall

Will return only initial comments.

* Commands can be used to add section according to our wish.



3.a) dig command querying google website.



3.b) digging for local machine’s address using -4 option

1. **nslookup:**

* Description:

1. Nslookup is a program to query Internet domain name servers.
2. Nslookup has two modes: interactive and non-interactive.
3. Interactive mode allows the user to query name servers for information about various hosts and domains or to print a list of hosts in a domain.
4. Non-interactive mode is used to print just the name and requested information for a host or domain.

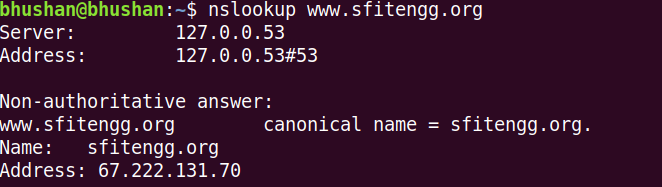
* Usage:

1. Interactive mode can be invoked in two ways:
2. Invoking nslookup command without any arguments.
3. Command along with first parameter as hyphen and second parameter as internet address of a name server.
4. Non interactive mode:

This is the default mode of nslookup command that requires the name of the object you are looking for alongwith the command as the first argument.

Non-interactive mode is used when the name or Internet address of the host to be looked up is given as the first argument. The optional second argument specifies the host name or address of a name server.

* Output:



4.a) Searching for server and address stored by it.

**AIM:** Study of packet sniffer tools : wireshark, :

1. Download and install wireshark and capture icmp, tcp, and http packets in

promiscuous mode.

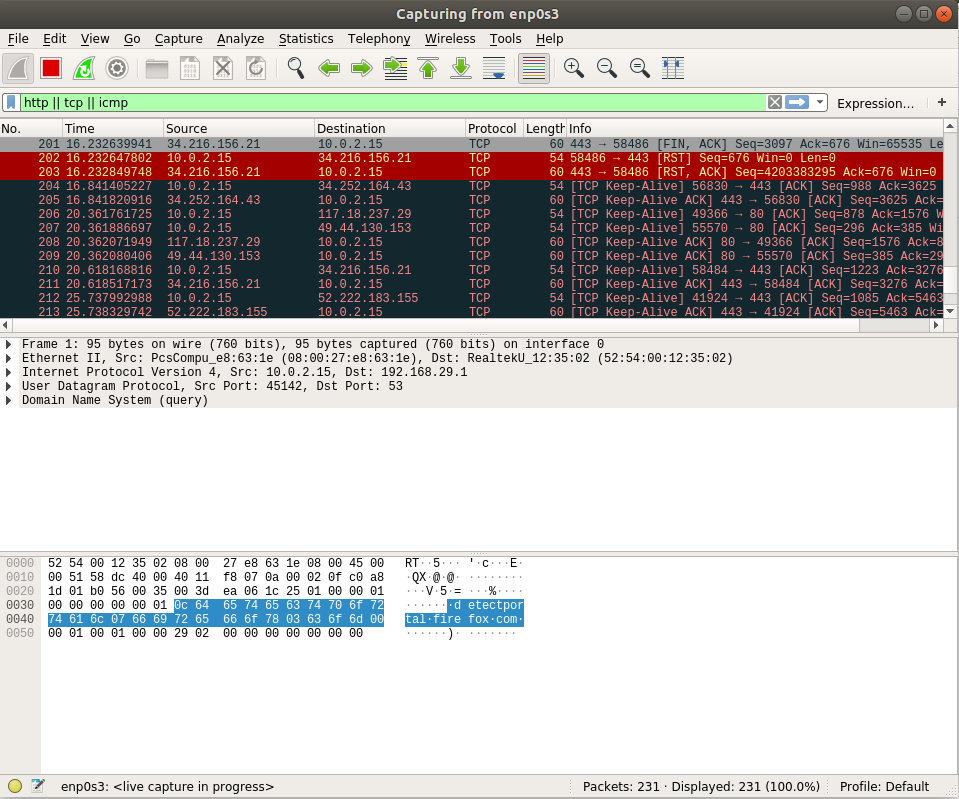
2. Explore how the packets can be traced based on different filters.

**Part 1**

Downloading and installing of wireshark:

**Steps:**

1. Removing previous installations:
2. sudo apt-get autoremove wireshark
3. sudo apt autoremove wireshark
4. sudo apt-get autoclean
5. sudo apt-get autoremove
6. Installing wireshark package:
7. sudo apt-get install wireshark



1.a) Capturing of tcp, http, icmp packets