

**ST. FRANCIS INSTITUTE OF TECHNOLOGY**  
**DEPARTMENT OF INFORMATION TECHNOLOGY**  
**SECURITY LAB**

**Experiment – 7: Study the use of Passive Network Reconnaissance tools**

**Aim:** To study the use of passive network reconnaissance tools, such as WHOIS, dig, traceroute, nslookup, etc. to gather information about networks and domain registrars.

**Objective:** After performing the experiment, the students will be able to apply basic network commands to gather network information.

**Lab objective mapped:** L502.6: Students should be able to apply network security basics, analyse different attacks on networks and evaluate the performance of firewalls and security protocols, such as SSL, IPSEC, and PGP, and authentication mechanisms to design secure applications.

**Prerequisite:** Basic knowledge of passive attack.

**Requirements:** Ubuntu/Unix/Linux Operating system

**Pre-Experiment Theory:**

**A. Passive Reconnaissance through network commands**

1. **WHOIS:** WHOIS is the Linux utility for searching an object in a WHOIS database. WHOIS is a database of domains, which includes a publicly displayed information about domains ownership, billing, technical, administrative, and nameserver information.

Running a WHOIS on your domain will look the domain up at the registrar for the domain information. All domains have WHOIS information. WHOIS database can be queried to obtain the following information,

- Administrative contact details, including names, email addresses, and telephone numbers.
- Mailing addresses for office locations relating to the target organization.
- Details of authoritative name servers for each given domain.

**Example:** `$ whois example.com` (*Use any URL of your choice*)

2. **Dig (Domain Information Groper):** Dig is a networking tool that can query DNS servers for information. It is very helpful for diagnosing problems with domain pointing and is a good way to verify that your configuration is working. The most basic way to use dig is to specify the domain you wish to query.

**Example:** `$ dig www.example.com` (*Use any URL of your choice*)

3. **Traceroute** - traceroute prints the route that packets take to a network host. Traceroute utility uses the TTL field in the IP header to achieve its operation. For users who are new to TTL field, this field describes how much hops a particular packet will take while traveling on network. So, this effectively outlines the lifetime of the packet on network. This field is usually set to 32 or 64. Each time the packet is held on an intermediate router, it decreases the TTL value by 1. When a router finds the TTL value of 1 in a received packet then that packet is not forwarded but instead discarded. After discarding the packet, router sends an ICMP error message of —Time exceeded back to the source from where packet generated. The ICMP packet that is sent back contains the IP address of the router. So now it can be easily understood that traceroute operates by sending packets with TTL value starting from 1 and then incrementing by one each time. Each time a router receives the

packet, it checks the TTL field, if TTL field is 1 then it discards the packet and sends the ICMP error packet containing its IP address and this is what traceroute requires. So traceroute incrementally fetches the IP of all the routers between the source and the destination.

**Example:** `$ traceroute example.com` *(Use any URL of your choice)*

4. **Nslookup** - The nslookup command is used to query internet name servers interactively for information. nslookup, which stands for "name server lookup", is a useful tool for finding out information about a named domain. By default, nslookup will translate a domain name to an IP address (or vice versa).

**Example:** `$ nslookup example.com` *(Use any URL of your choice)*

## **B. Passive Reconnaissance through publicly available tools**

1. **archive.org** (<https://archive.org/>)

In the archive.org website we can get the complete history of any website like when it was last updated. We can go back to a particular date and observe the webpage. We can mirror the website which will load all the files locally, such as HTML codes, images etc. that can be used to observe the directories used.

2. **Whois** (<https://www.whois.com/>)

Whois database lookup allows us to access many useful information about target such as:

- Registration details
- IP address
- Contact number and Email ID
- Domain owner
- Name servers
- Regional Internet Registries

3. **Netcraft** (<https://www.netcraft.com/>)

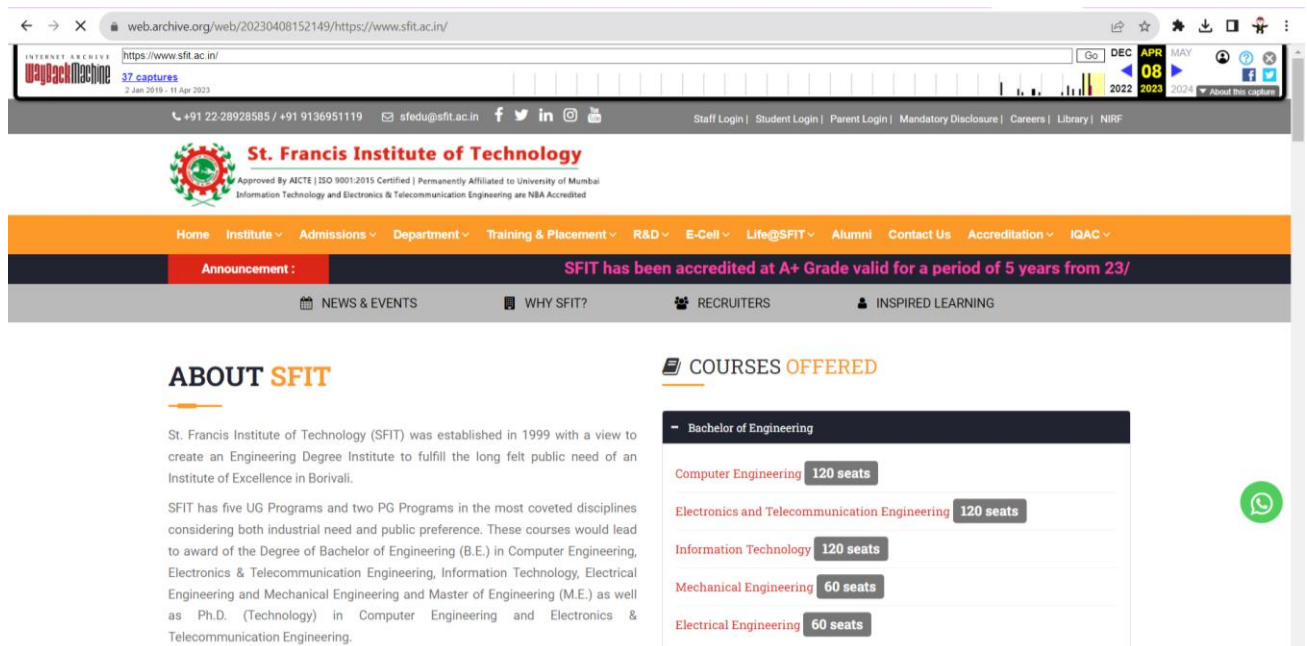
Netcraft is an internet service organization, used to collect information such as IP address, services running on systems, operating systems, name servers, technologies used by websites.

### **Procedure & Outputs:**

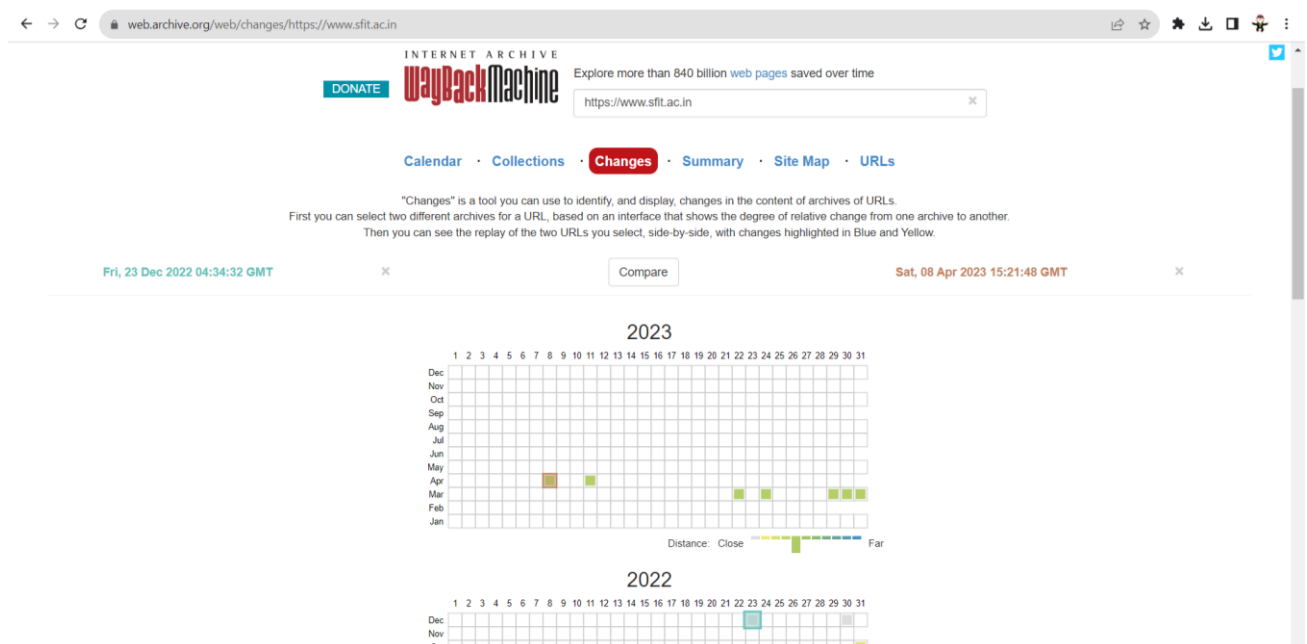
1. With Linux/Ubuntu/Unix operating systems run the commands discussed in part A of theory section. Analyze the output. Take screenshots (SS). Describe your observations under each SS in detail. Use indicators such as highlight, colour, and box for this purpose.
2. Browse the web tools discussed in part B of the theory section. Identify following:
  - a. Using 'archive.org' find the update history of 'sfit.ac.in' domain.
  - b. Perform a passive reconnaissance using the Calendar, Changes, Summary, Site Map, URL tabs. Take appropriate screenshots. Describe your observations under each SS in detail. Use indicators such as highlight, colour, and box for this purpose.
  - c. Using 'whois.com' find the domain information of 'facebook.com'. Take appropriate screenshots. Indicate the following information in your screenshots and complete the observation table given in observation section.
  - d. Using 'netcraft.com' find the site report of 'microsoft.com'. Perform passive reconnaissance for useful information. Take appropriate screenshots. Describe your observations under each SS in detail. Use indicators such as highlight, colour, and box for this purpose. Complete the observation table given in observation section.

## Observations:

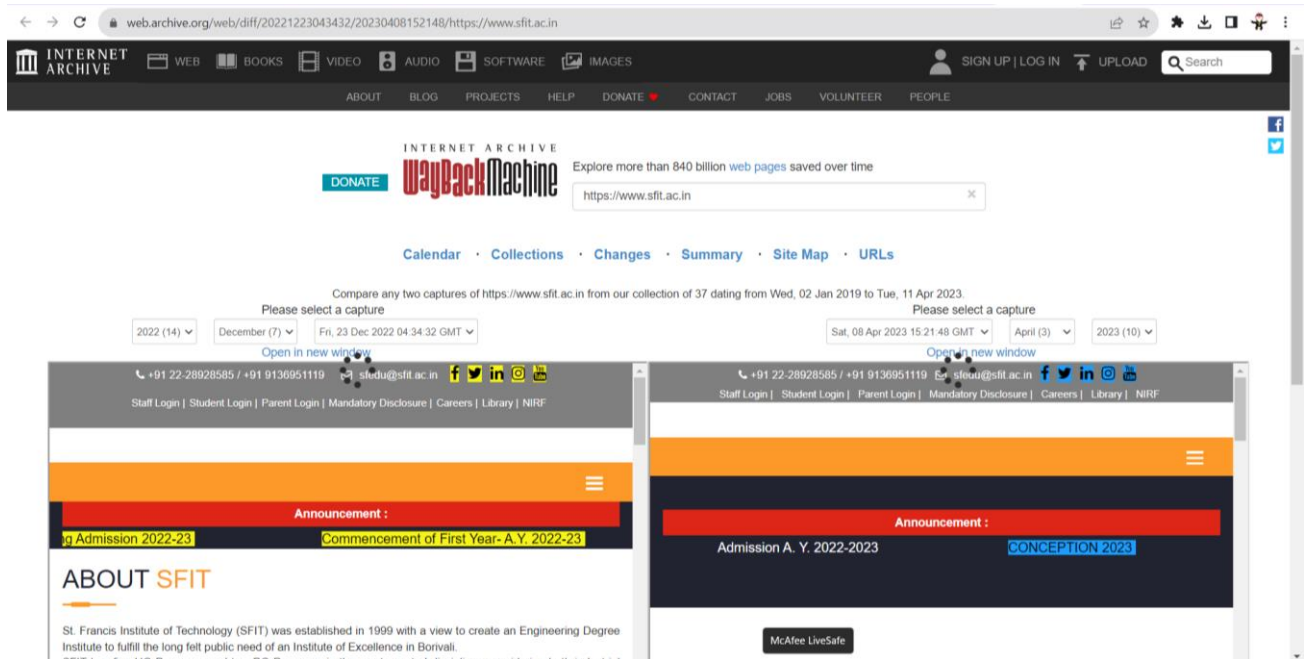
## Archive.org:



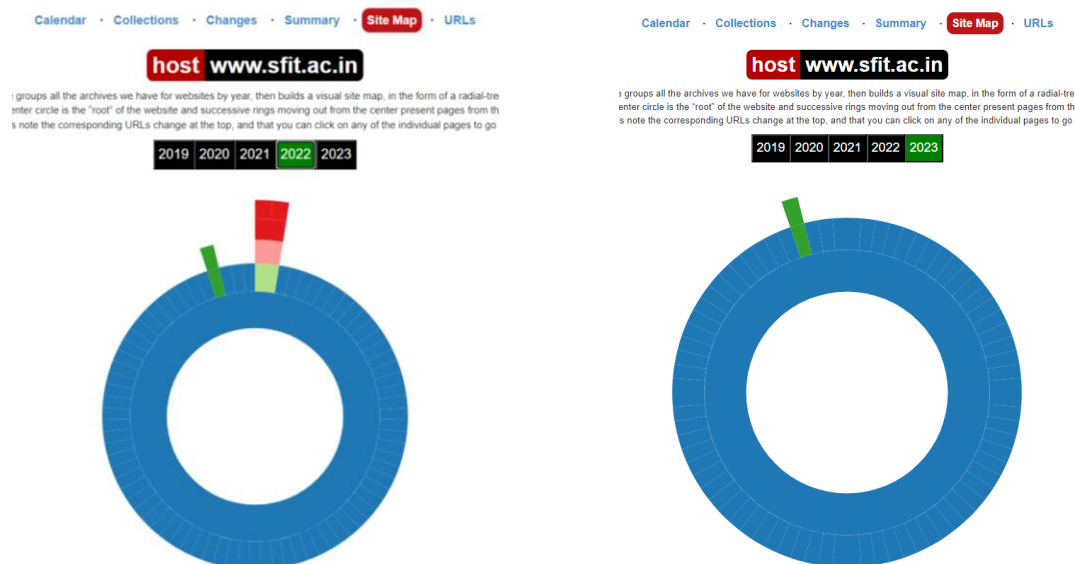
In the above screenshot, we have searched our sfit website through the publically available tool archive.org. We can see our website through the calendar and how our website looks at particular dates of a calendar.



In the above screenshot, we see our sfit website changes before and after by choosing the date of change and comparing both of them and easily we can see what changes had been done before and after. But in the above screenshot, we only can see the selected dates.



In the above screenshot, as in the previous screenshot, we discussed the changes between the duration, over here we can observe the changes made in the duration, where the yellow color indicates the deletion of content whereas the blue color indicates the addition of content on the sfit website.



In the above screenshot, we can see the sitemap of the sfit website for the years 2022 and 2023 and see the difference between them easily.

Target Domain/URL/Website for whois : facebook.com			
Registrar:	RegistrarSafe, LLC	Registration Expiry date:	2032-03-30
Registration Update date:	2023-04-26	Name Servers:	a.ns.facebook.com b.ns.facebook.com c.ns.facebook.com d.ns.facebook.com
Registrant Organization	Meta Platforms, Inc.	Registrant City:	Menlo Park



## Domain Information

Domain: facebook.com

Registrar: RegistrarSafe, LLC

Registered On: 1997-03-29

Expires On: 2032-03-30

Updated On: 2023-04-26

Status: clientDeleteProhibited  
clientTransferProhibited  
clientUpdateProhibited  
serverDeleteProhibited  
serverTransferProhibited  
serverUpdateProhibited

Name Servers: a.ns.facebook.com  
b.ns.facebook.com  
c.ns.facebook.com  
d.ns.facebook.com



## Registrant Contact

Name: Domain Admin

Organization: Meta Platforms, Inc.

Street: 1601 Willow Rd

City: Menlo Park

Target Domain/URL/Website for netcraft : <b>google.com</b>			
IPv4 address:	74.125.193.139	SSL/TLS certificate Issuing organization:	Google Trust Services LLC
Certificate Validity period:	From Aug 14 2023 to Nov 6 2023	Public key algorithm:	id-ecPublicKey
Public key length:	256	Certificate Hash:	WBEMOJyH7FIK5KKHa4lrTFR2nEg
Signature algorithm:	sha256WithRSAEncryption	Public Key Hash:	ef9e8165f3190e018aae496fef88b248fcace60334ab797e9b1a0e266783411c
Server-Side site technology:	SSL	Client-Side site technology:	JavaScript

**Site** <http://google.com> 

**Netblock Owner** [Google LLC](#)

**Hosting company** [Google](#)

**Hosting country**  [US](#) 

**IPv4 address** [74.125.193.139](#) ([VirusTotal](#) )

**IPv4 autonomous systems** [AS15169](#) 

**IPv6 address** [2a00:1450:400b:c01:0:0:66](#)

**IPv6 autonomous systems** [AS15169](#) 

**Reverse DNS** [di-in-f139.1e100.net](#)


## Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description
<a href="#">SSL</a> 	A cryptographic protocol providing com Internet

## Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash

Technology	Description
Local Storage	<i>No description</i>
<a href="#">JavaScript</a> 	Widely-supported programming language side dynamic content on websites

Validity period	From Aug 14 2023 to Nov 6 2023 (2 months, 3 weeks, 1 day)
Matches hostname	Yes
Server	gws
Public key algorithm	id-ecPublicKey
Protocol version	TLSv1.3
Public key length	256
Certificate check	ok
Signature algorithm	sha256WithRSAEncryption
Certificate Revocation Lists	<a href="http://crls.pki.goog/gts1c3/zdATt0Ex_Fk.crl">http://crls.pki.goog/gts1c3/zdATt0Ex_Fk.crl</a>
Certificate Hash	WBEMOJyH7FIK5KKHa4lrTFR2nEg
Public Key Hash	ef9e8165f3190e018aae496fef88b248fcace60334ab797e9b1a0e266783411c

### Post Experimental Exercise Questions:

1. What is network reconnaissance?
2. What is passive reconnaissance? Give some examples.
3. What is active reconnaissance? Give some examples.

### Conclusion:

In this experiment we studied various reconnaissance tools that can be used to gather primary information about the target/victim before launching any cyber-attack.

### References:

1. "How to Use Linux dig Command", <https://phoenixnap.com/kb/linux-dig-command-examples>
2. "Lecture 17: Information Gathering (Part 1)", <https://youtu.be/mLvwpiR4dG4>



## Screenshots:

Command: whois

```
File Edit View Search Terminal Help
student@Atharva:~$ whois google.com
Domain Name: GOOGLE.COM
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T15:39:04Z
Creation Date: 1997-09-15T04:00:00Z
Registry Expiry Date: 2028-09-14T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
```

In the above screenshot, we have highlighted the part where the website info is shown, and this info can be useful for hacking purpose.

Command: dig

```
File Edit View Search Terminal Help
student@Atharva:~$ dig www.google.com

; <<>> DiG 9.11.3-1ubuntu1.18-Ubuntu <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55965
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;, udp: 65494
;; QUESTION SECTION:
;www.google.com.                IN      A

;; ANSWER SECTION:
www.google.com.                 52      IN      A      142.250.192.36

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sat Sep 09 10:56:00 IST 2023
;; MSG SIZE rcvd: 59
```

In the above Screenshot, the most important section is the ANSWER section:

The first column lists the name of the server that was queried

The second column is the Time to Live, a set timeframe after which the record is refreshed

The third column shows the class of query – in this case, “IN” stands for Internet

The fourth column displays the type of query – in this case, “A” stands for an A (address) record

The final column displays the IP address associated with the domain name



Command: traceroute

```
File Edit View Search Terminal Help
student@Atharva:~$ traceroute example.com
traceroute to example.com (93.184.216.34), 64 hops max
 1  192.168.7.254  0.470ms  0.382ms  0.466ms
 2  139.5.239.161  1.161ms  1.039ms  0.877ms
 3  172.169.3.185  1.955ms  *  *
 4  122.187.212.149  2.293ms  1.962ms  2.233ms
 5  116.119.57.84  101.913ms  100.385ms  112.217ms
 6  62.115.42.118  187.271ms  193.086ms  187.328ms
 7  62.115.124.54  197.970ms  189.112ms  188.924ms
 8  62.115.112.242  207.457ms  207.223ms  207.312ms
 9  62.115.123.125  205.721ms  205.912ms  205.883ms
10  62.115.175.71  197.815ms  198.076ms  197.544ms
11  152.195.64.129  187.416ms  187.263ms  187.435ms
12  93.184.216.34  193.181ms  193.095ms  193.101ms
13  93.184.216.34  193.548ms  193.611ms  193.536ms
student@Atharva:~$
```

As you can see in the above screenshot, there are several rows divided into columns on the report. Each row represents a "hop" along the route. Think of it as a check-in point where the signal gets its next set of directions. Each row is divided into five columns. Let's break this particular hop down into its parts. **Hop Number** - This is the first column and is simply the number of the hop along the route. In this case, it is the tenth hop. **RTT Columns** - The next three columns display the round trip time (RTT) for your packet to reach that point and return to your computer. This is listed in milliseconds. There are three columns because the traceroute sends three separate signal packets. This is to display consistency, or a lack thereof, in the route. **Domain/IP column** - The last column has the IP address of the router. If it is available, the domain name will also be listed.

Command: nslookup

```
File Edit View Search Terminal Help
student@Atharva:~$ nslookup example.com
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   example.com
Address: 93.184.216.34
Name:   example.com
Address: 2606:2800:220:1:248:1893:25c8:1946

student@Atharva:~$
```

In the above screenshot, the DNS server used was 127.0.0.53. As mentioned earlier, basic nslookup commands pull data from the DNS server cache. The message non-authoritative answer proves this, as the data was not taken directly from the server that actually hosts the data. Next, we have the website URL which we typed earlier. You can see that the Google server IPv4 address was 93.184.216.34, and the IPv6 address was 2606:2800:220:1:248:1893:25c8:1946.