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, color, 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, color, 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 the 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:

Target Domain/URL/Website for whois : https://www.sfit.ac.in			
Registrar:	ERNET India	Registration Expiry date:	2028-09-25
Registration Update date:	2018-11-24	Name Servers:	ns2.cp-34.webhostbox.net ns1.cp-34.webhostbox.net
Registrant Organization	ST FRANCIS INSTITUTE OF TECHNOLOGY	Registrant Country:	IN

Target Domain/URL/Website for netcraft : https://linkedin.com			
IPv4 address:	13.107.42.14	SSL/TLS certificate Issuing organization:	DigiCert Inc
Certificate Validity period:	From Sep 11 2024 to Mar 11 2025	Public key algorithm:	rsaEncryption
Public key length:	2048	Certificate Hash:	3SgvWiqHet1CrKPfC5FhP9G2FZE
Signature algorithm:	sha256WithRSAEncryption	Public Key Hash:	10749dee28bda4b982f2107eb01e786998e0df23d9cfabd111e3f414886396f0
Server-Side site technology:	Java Servlet , SSL	Client-Side site technology:	JavaScript and Asynchronous Javascript

Post Experimental Exercise Questions: *(to be handwritten on journal sheets)*

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

Conclusion:

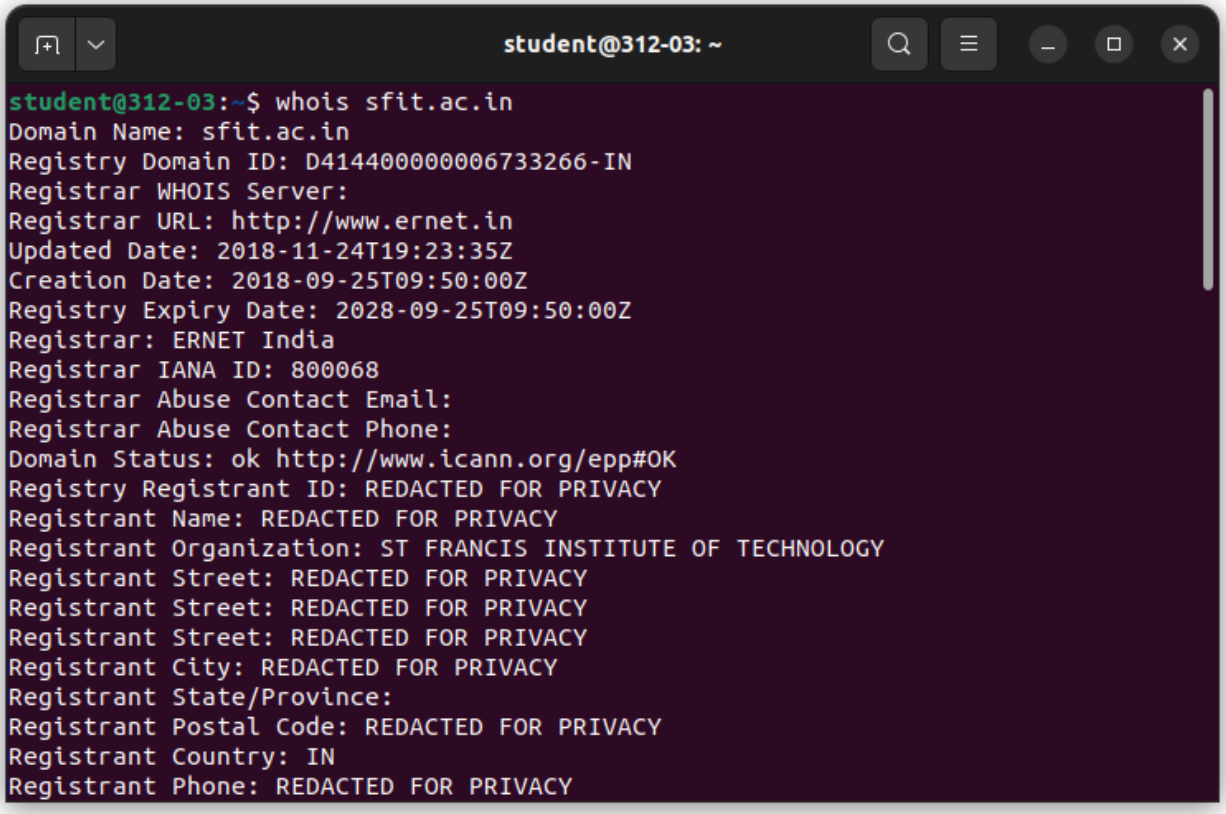
In this experiment we studied various reconnaissance tools that can be used to gather primary information about the target/victim before launching any cyber-attack.

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*

C. Passive Reconnaissance through network commands

1. Whois <Domain name>



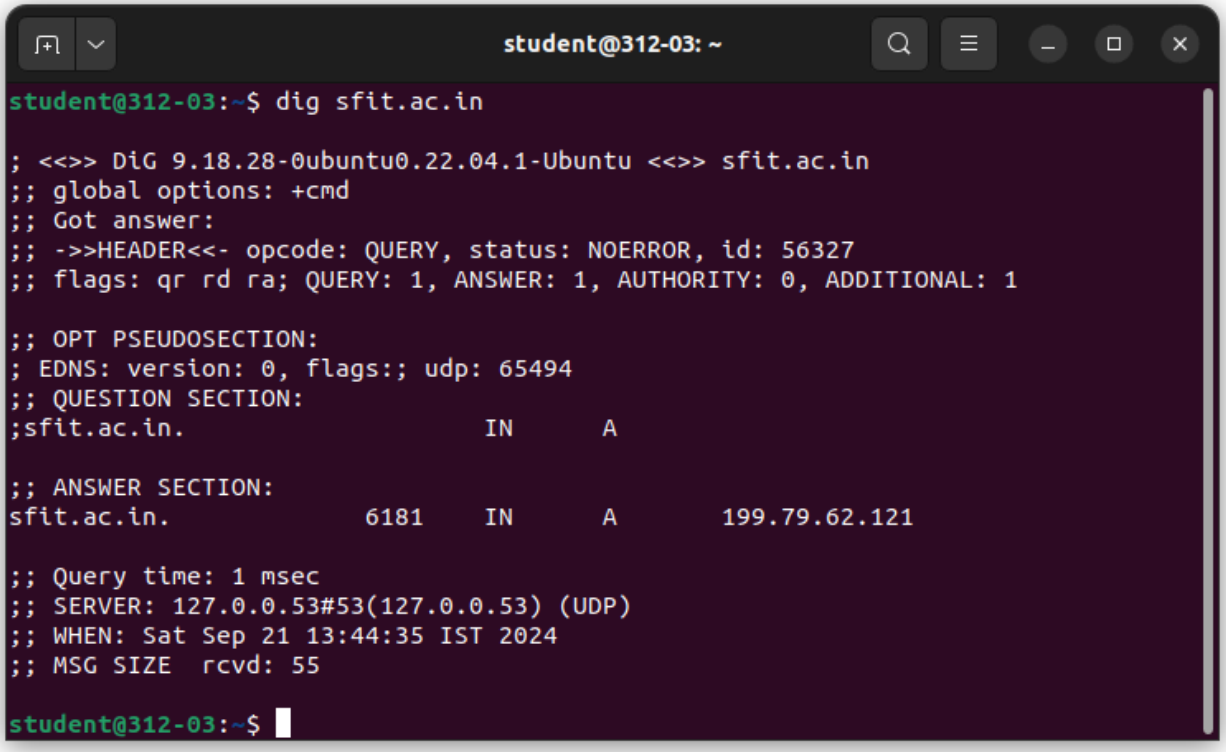
```
student@312-03: ~
student@312-03:~$ whois sfit.ac.in
Domain Name: sfit.ac.in
Registry Domain ID: D414400000006733266-IN
Registrar WHOIS Server:
Registrar URL: http://www.ernet.in
Updated Date: 2018-11-24T19:23:35Z
Creation Date: 2018-09-25T09:50:00Z
Registry Expiry Date: 2028-09-25T09:50:00Z
Registrar: 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: ST FRANCIS INSTITUTE OF TECHNOLOGY
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
Registrant Phone: REDACTED FOR PRIVACY
```

The **WHOIS command** provides essential registration details for the domain **sfit.ac.in**, owned by **St. Francis Institute of Technology**. Key information includes the **creation date** (September 25, 2018), **expiry date** (September 25, 2028), and its **active status** (ok). The **registrar**, ERNET India, manages the domain, while **privacy protections** redact specific registrant details, including contact information. Notable technical data includes the associated **name servers** (ns1.cp-34.webhostbox.net and ns2.cp-34.webhostbox.net) and an **unsigned DNSSEC** status, indicating that security extensions are not enabled. Additionally, users are directed to report inaccuracies through a link to the **ICANN compliance form**, reinforcing data integrity.

Key Points:

- **Domain Name**: sfit.ac.in
- **Registrar**: ERNET India
- **Creation Date**: September 25, 2018
- **Expiry Date**: September 25, 2028
- **Status**: Active (ok)
- **Name Servers**: ns1.cp-34.webhostbox.net, ns2.cp-34.webhostbox.net
- **DNSSEC**: Unsigned
- **Privacy Protections**: Registrant details redacted

2. dig <Domain name>



```
student@312-03: ~
student@312-03:~$ dig sfit.ac.in

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> sfit.ac.in
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56327
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;sfit.ac.in.                    IN      A

;; ANSWER SECTION:
sfit.ac.in.             6181    IN      A       199.79.62.121

;; Query time: 1 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Sep 21 13:44:35 IST 2024
;; MSG SIZE  rcvd: 55

student@312-03:~$
```

The **dig** command was executed for the domain **sfit.ac.in**, successfully resolving its address. The query returned a status of **NOERROR**, indicating a successful lookup. The domain's **A record** points to the IP address **199.79.62.121**, with a **time to live (TTL)** of **6181 seconds**. The query response time was a swift **1 ms**, and it utilized the local resolver at **127.0.0.53**.

Key Points:

- **Domain**: sfit.ac.in
- **Resolved IP Address**: 199.79.62.121
- **TTL**: 6181 seconds
- **Query Status**: NOERROR
- **Response Time**: 1 ms

3. **traceroute <Domain name>**

```
student@312-03: ~
student@312-03:~$ traceroute sfit.ac.in
traceroute to sfit.ac.in (199.79.62.121), 64 hops max
  1   192.168.7.254  0.545ms  0.700ms  0.734ms
  2   27.107.173.133  3.734ms  2.433ms  1.691ms
  3   10.118.143.1  2.342ms  2.949ms  *
  4   *  203.200.11.141  8.048ms  *
  5   172.31.180.57  25.378ms  24.934ms  25.144ms
  6   180.87.36.9  24.883ms  24.999ms  25.075ms
  7   180.87.36.139  57.415ms  57.070ms  56.519ms
  8   180.87.37.114  58.692ms  58.208ms  58.627ms
  9   180.87.37.99  58.971ms  59.192ms  58.294ms
 10   63.243.180.65  58.273ms  *  *
 11   129.250.66.9  57.583ms  57.649ms  57.598ms
 12   *  *  129.250.2.243  134.364ms
 13   *  *  *
 14   129.250.3.142  235.630ms  235.528ms  237.141ms
 15   168.143.228.173  245.798ms  245.920ms  245.833ms
 16   168.143.228.173  260.574ms  244.887ms  244.648ms
 17   162.215.195.141  260.681ms  257.744ms  270.810ms
 18   69.195.64.105  259.962ms  259.410ms  259.505ms
 19   69.195.64.105  257.681ms  257.220ms  258.482ms
 20   162.144.240.175  266.499ms  265.664ms  265.149ms
 21   199.79.62.121  261.953ms  262.222ms  262.203ms
student@312-03:~$
```

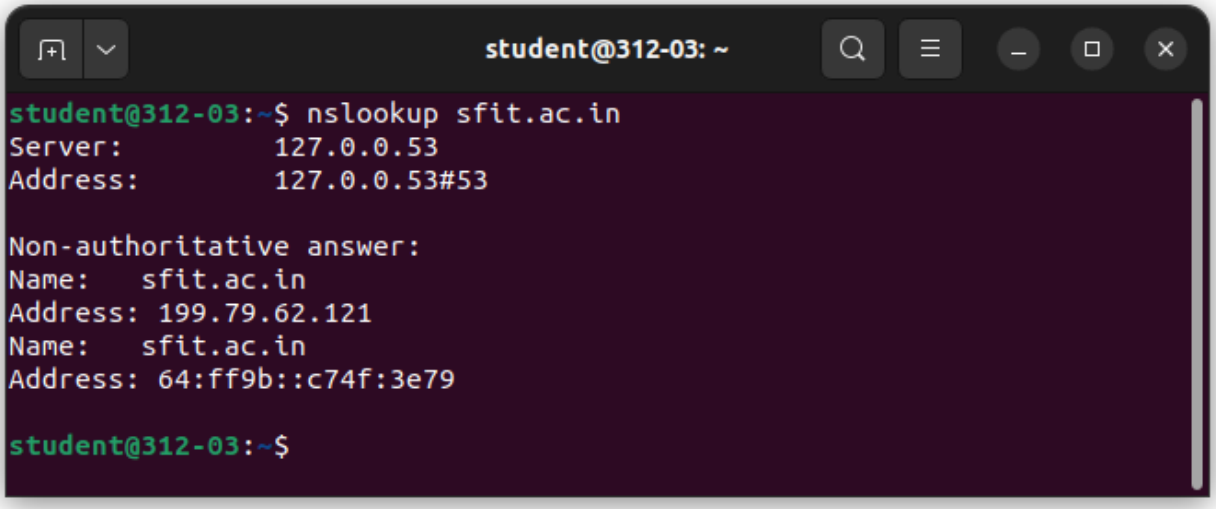
The **traceroute** command for **sfit.ac.in** successfully traced the path to the IP address **199.79.62.121**, allowing up to **64 hops**. The first hop, at **192.168.7.254**, recorded quick response times around **0.545 ms**. Several hops timed out, specifically the **4th**, **11th**, and **13th**. The longest response time noted was **134.364 ms** at the **12th hop**, indicating some latency as the route progressed. The final hop to the destination recorded response times of approximately **262 ms**.

Key Points:

- **Destination IP**: 199.79.62.121
- **First Hop**: 192.168.7.254 (0.545 ms)
- **Timed Out Hops**: 4th, 11th, and 13th
- **Longest Response Time**: 134.364 ms (12th hop)
- **Final Hop Response Time**: ~262 ms

This output provides insights into the routing and latency involved in reaching the specified domain.

4. **nslookup <Domain name>**



The DNS query for **sfit.ac.in** returned non-authoritative answers indicating its associated IP addresses. The server used for the query was **127.0.0.53**, and the results show two addresses linked to the domain: the IPv4 address **199.79.62.121** and the IPv6 address **64:ff9b::c74f:3e79**. This indicates that the domain is accessible via both IPv4 and IPv6 protocols.

Key Points:

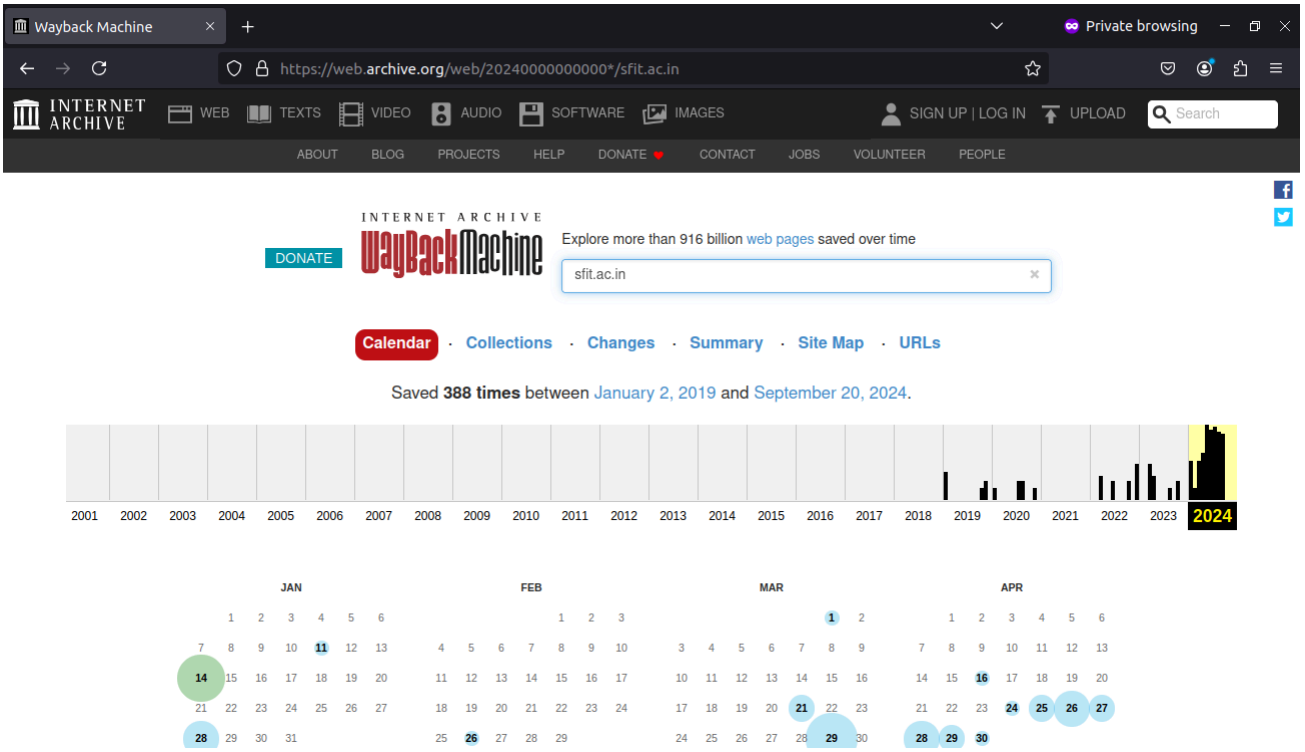
- **DNS Server**: 127.0.0.53
- **IPv4 Address**: 199.79.62.121
- **IPv6 Address**: 64:ff9b::c74f:3e79
- **Response Type**: Non-authoritative answer

This output highlights the domain's dual stack configuration, allowing it to support both address formats.

D. Passive Reconnaissance through publicly available tools

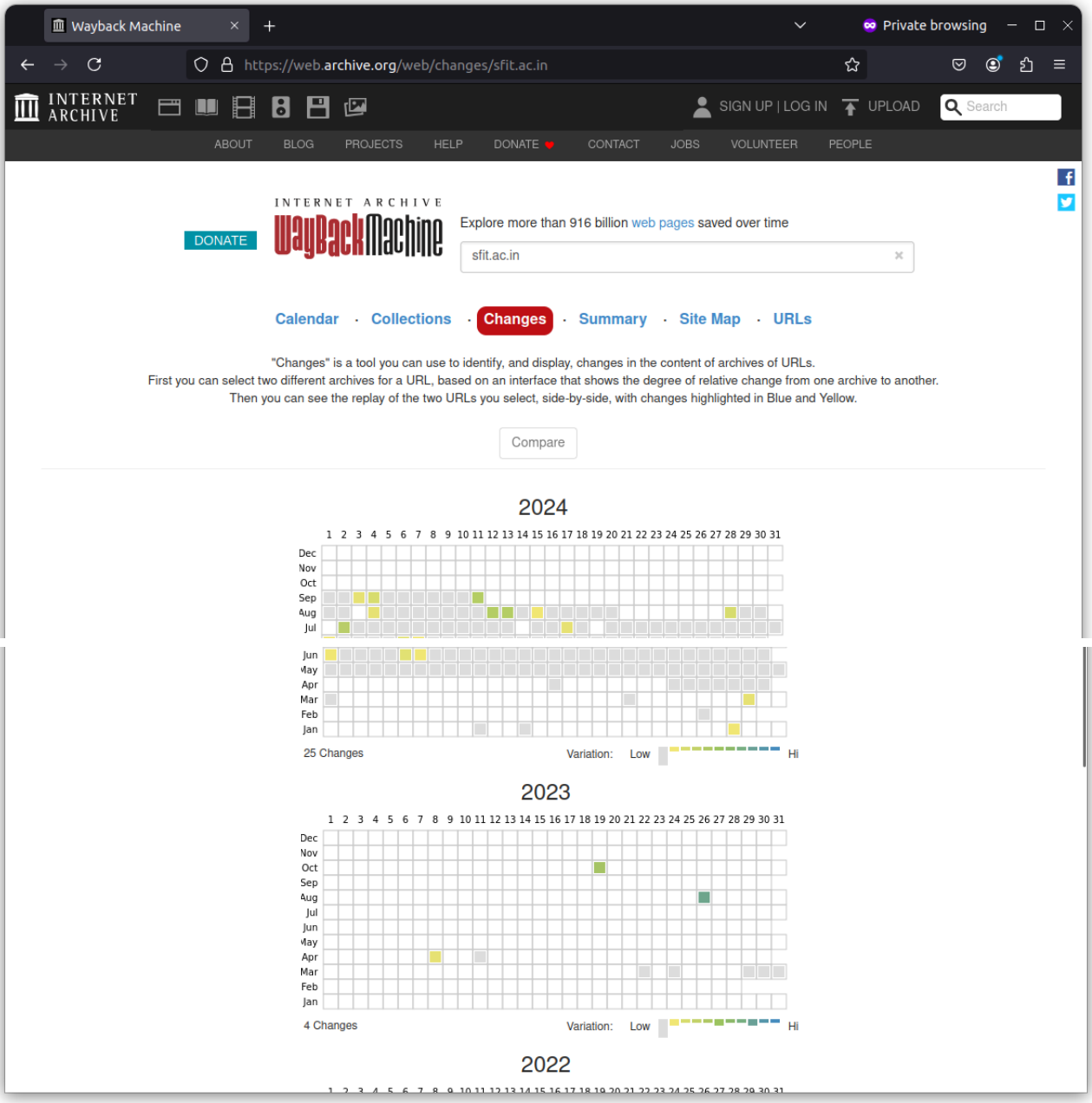
1. archive.org

- **Calendar**



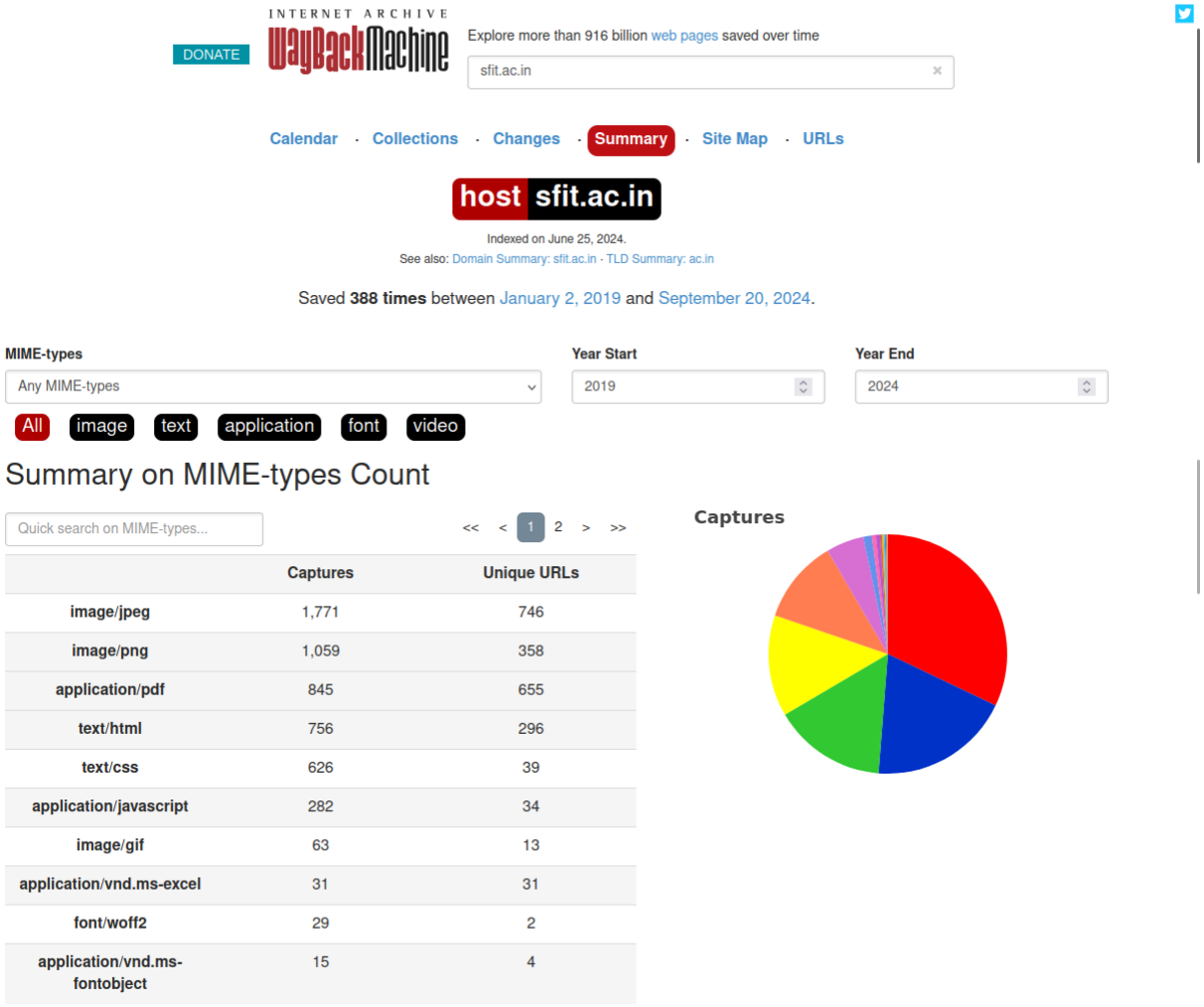
- The **Wayback Machine snapshot** reveals archival activity for the website "sfit.ac.in" between **January 2, 2019, and September 18, 2024.**
- A **timeline** at the top indicates increased **archival frequency** in 2023 and 2024, suggesting heightened web traffic or updates.
- **Calendar view** displays specific dates of captures in 2024, represented by **blue circles**—the size of the circle correlates with the **number of captures** on that day.
- The image highlights the **importance of web preservation** and how it provides insights into the **historical development** and changes in the website content over time.

- **Changes**



- The image showcases the **"Changes" tool** on the Wayback Machine, used to track **content modifications** in archived versions of the website "sfit.ac.in."
- The **grid visualization** represents **changes in 2024 & 2023**, with color coding to indicate the **degree of variation**. **Yellow** and **green** boxes suggest **higher variation**, while **gray** boxes represent little to no change.
- The tool allows for **comparative analysis** by selecting two archival versions to view **side-by-side**, highlighting the extent of change on the website between dates.
- This analysis aids in understanding the **evolution of web content**, useful for tracking updates, revisions, or content alterations over time.

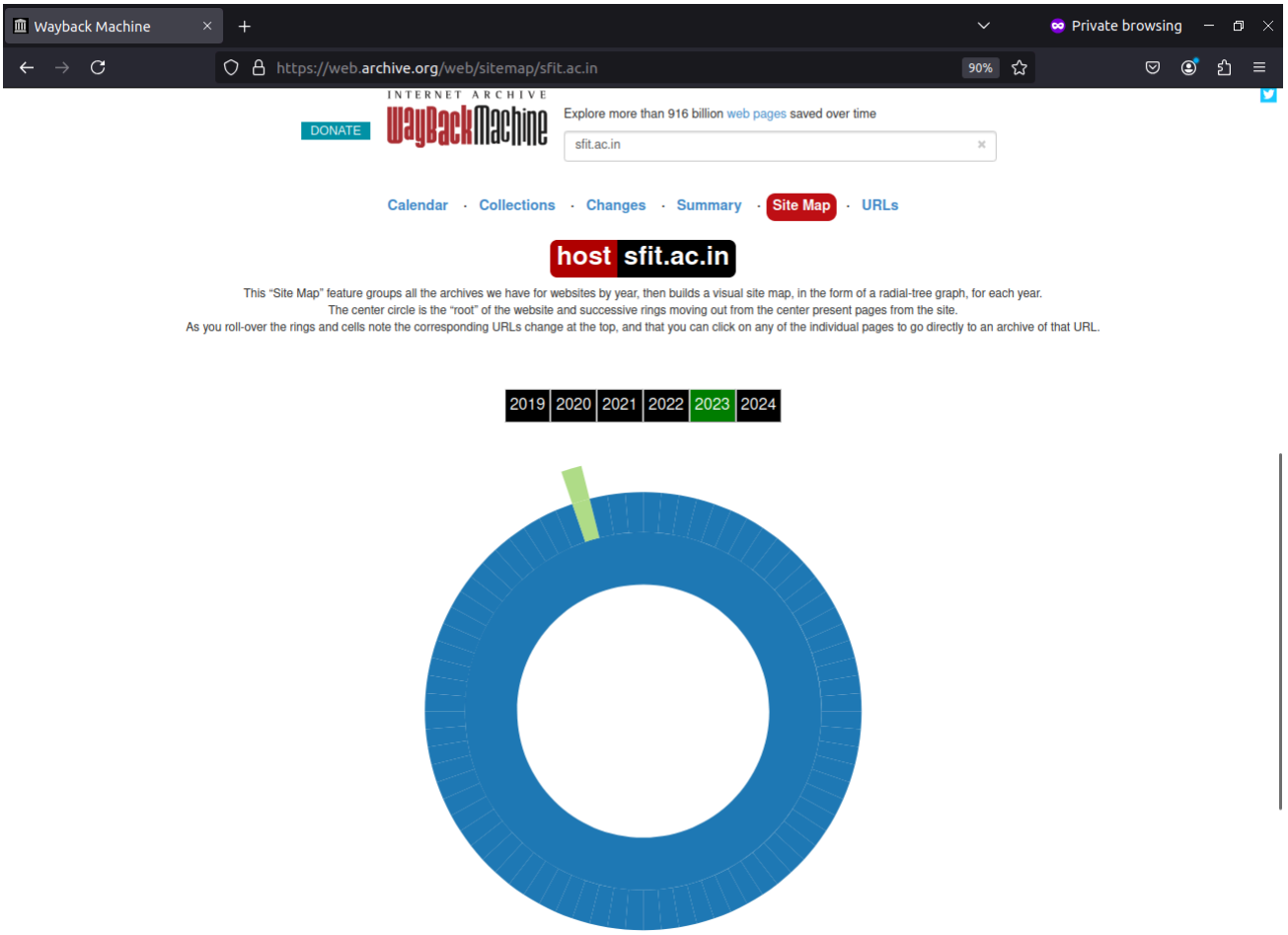
- **Summary**



	Captures	Unique URLs
image/jpeg	1,771	746
image/png	1,059	358
application/pdf	845	655
text/html	756	296
text/css	626	39
application/javascript	282	34
image/gif	63	13
application/vnd.ms-excel	31	31
font/woff2	29	2
application/vnd.ms-fontobject	15	4

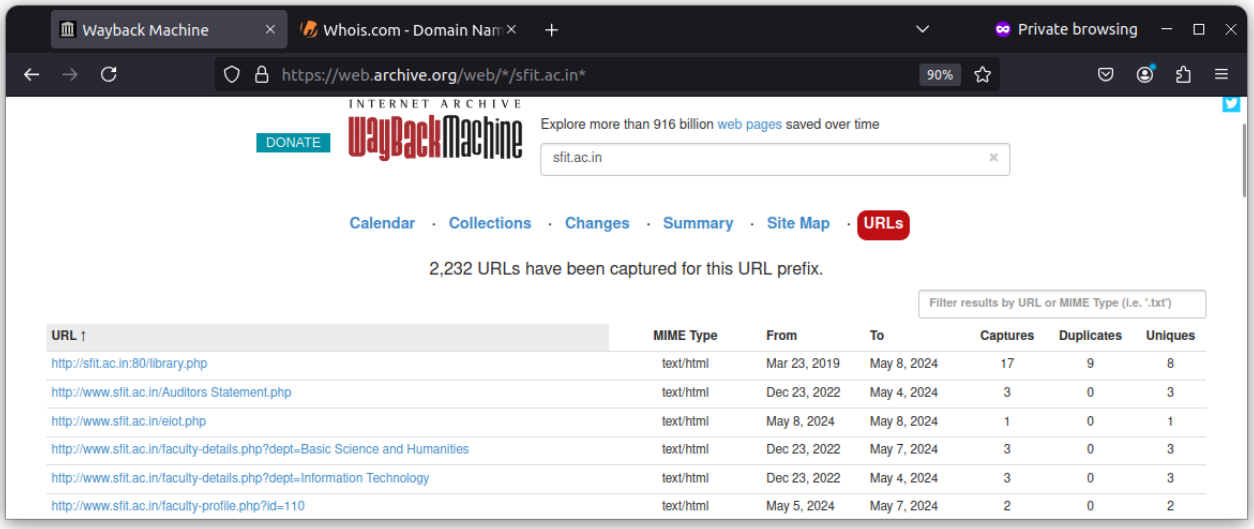
- The image presents a **summary of MIME-types** for "sfit.ac.in" from the Wayback Machine, showcasing the distribution of different file types archived between **2019 and 2024.**
- The **table** lists various MIME types, with **image/jpeg** and **image/png** leading in the number of captures, followed by **application/pdf** and **text/html**, indicating a high number of images and documents archived.
- The **pie chart** visualizes this data, with **red (image/jpeg)** and **blue (image/png)** sectors representing the largest shares, emphasizing the prevalence of image files in the site's content.
- This analysis helps to understand the **content composition** of the site, with a focus on **image-heavy** and **document-based** materials

- **Site Map**



- The image displays the **Site Map** feature from the Wayback Machine for the website "sfit.ac.in."
- It visualizes **archived URLs** over time using a **radial-tree graph**, where the **center circle** represents the **root** of the website, and successive **rings** represent pages from the site for each year.
- The **color-coded timeline** at the top shows archives from **2019 to 2024**, with most activity visualized in **2023**, indicated by a large blue outer ring.
- This diagram allows users to explore the **hierarchical structure** of the website and navigate through different years' archived content.

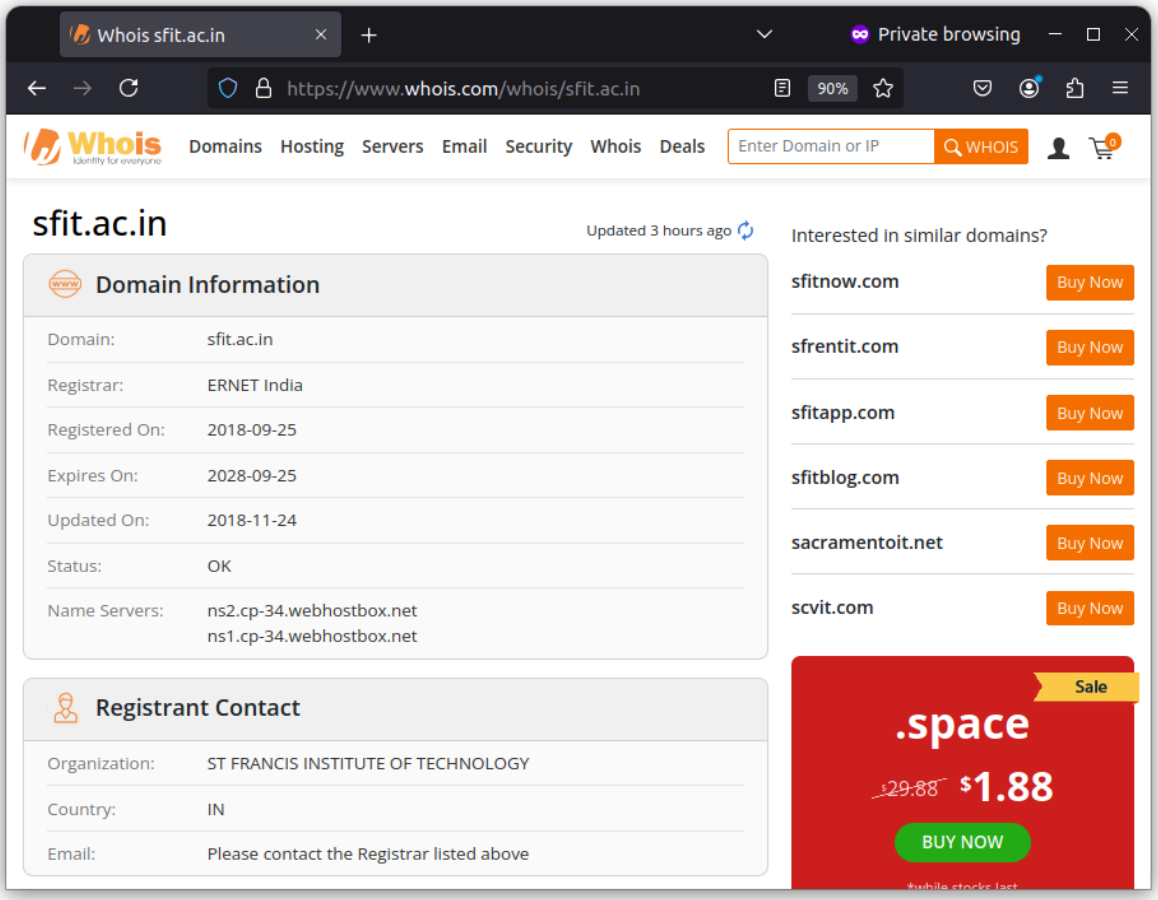
- **URL**



URL ↑	MIME Type	From	To	Captures	Duplicates	Uniques
http://sfit.ac.in:80/library.php	text/html	Mar 23, 2019	May 8, 2024	17	9	8
http://www.sfit.ac.in/Auditors Statement.php	text/html	Dec 23, 2022	May 4, 2024	3	0	3
http://www.sfit.ac.in/eiot.php	text/html	May 8, 2024	May 8, 2024	1	0	1
http://www.sfit.ac.in/faculty-details.php?dept=Basic Science and Humanities	text/html	Dec 23, 2022	May 7, 2024	3	0	3
http://www.sfit.ac.in/faculty-details.php?dept=Information Technology	text/html	Dec 23, 2022	May 4, 2024	3	0	3
http://www.sfit.ac.in/faculty-profile.php?id=110	text/html	May 5, 2024	May 7, 2024	2	0	2

- The image displays the **Wayback Machine's URL capture** log for "sfit.ac.in," listing **2,232 URLs** captured over time.
- Each **URL** has corresponding **MIME types**, the **date range** for when the page was archived, and the number of **captures, duplicates,** and **unique URLs.**
- For example, the page **"library.php"** has 17 captures from **March 23, 2019** to **May 8, 2024**, with 9 duplicates and 8 unique versions.
- The data shows consistent captures of specific pages, indicating regular updates or changes to those URLs.
- This observation reflects the **site's content evolution** over the years and the Wayback Machine's thorough archival process.

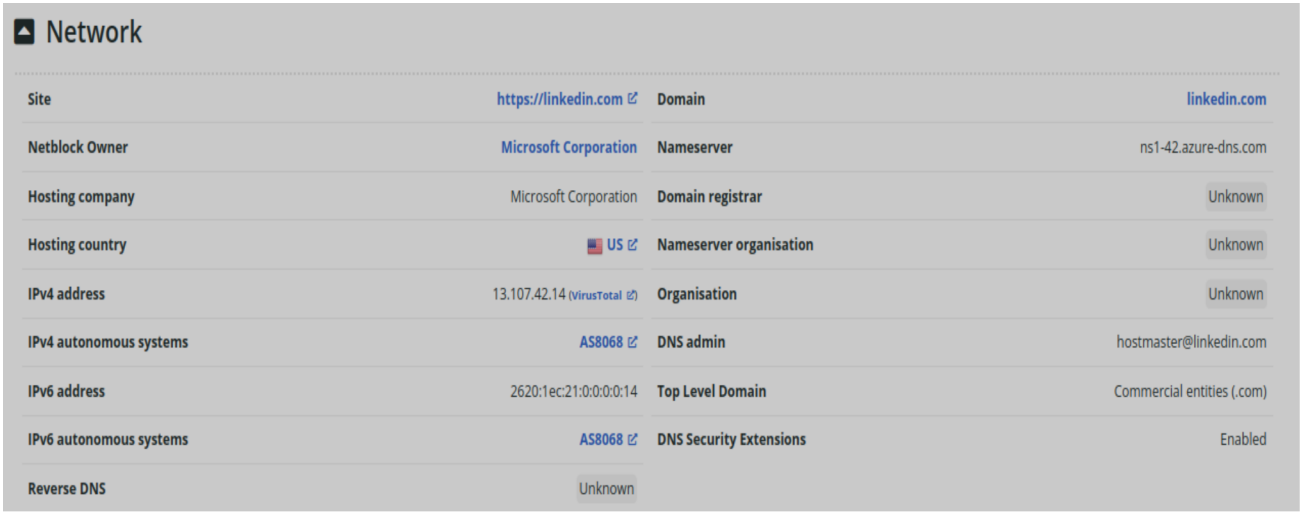
2. whois.com



WHOIS Lookup for Domain: sfit.ac.in

1. **Domain Registrar**: ERNET India
   The entity responsible for managing the domain name.
2. **Registered On**: September 25, 2018
   The date when the domain was first registered.
3. **Expires On**: September 25, 2028
   The expiration date of the domain's current registration. It is valid for 10 years.
4. **Updated On**: November 24, 2018
   The last date the domain's registration details were updated.
5. **Status**: OK
   Indicates the domain is active and functioning properly.
6. **Name Servers**:
   - ns2.cp-34.webhostbox.net
   - ns1.cp-34.webhostbox.net
     These are the servers responsible for translating the domain name into an IP address.
7. **Registrant Contact**:
   - **Organization**: St. Francis Institute of Technology
   - **Country**: IN (India)
     The contact details of the organization managing the domain.

3. netcraft.com



Network

Site	https://linkedin.com	Domain	linkedin.com
Netblock Owner	Microsoft Corporation	Nameserver	ns1-42.azure-dns.com
Hosting company	Microsoft Corporation	Domain registrar	Unknown
Hosting country	US	Nameserver organisation	Unknown
IPv4 address	13.107.42.14 (VirusTotal)	Organisation	Unknown
IPv4 autonomous systems	AS8068	DNS admin	hostmaster@linkedin.com
IPv6 address	2620:1ec:21:0:0:0:0:14	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	AS8068	DNS Security Extensions	Enabled
Reverse DNS	Unknown		

The image is a **Netcraft Network report** for **LinkedIn.com**, showing the following details:

- **Site**: The domain in focus is **linkedin.com**.
- **Netblock Owner**: The IP range hosting LinkedIn is owned by **Microsoft Corporation**.
- **Hosting Company**: The hosting services are also provided by **Microsoft Corporation**.
- **Hosting Country**: The website is hosted in the **United States**.
- **IPv4 Address**: LinkedIn's primary IPv4 address is **13.107.42.14**.
- **IPv6 Address**: The IPv6 address is **2620:1ec:21::14**.
- **Autonomous Systems**: The autonomous system for both IPv4 and IPv6 is **AS8068**, which is managed by Microsoft.
- **Nameserver**: LinkedIn uses the nameserver **ns1-42.azure-dns.com**, part of Microsoft Azure’s DNS.
- **DNSSEC**: DNS Security Extensions are **enabled** for LinkedIn’s domain, providing an extra layer of DNS security.
- **Reverse DNS**: The reverse DNS for the domain is **unknown**.

SSL/TLS

Assurance	Organisation validation	**Perfect Forward Secrecy**	Yes
Common name	www.linkedin.com	**Supported TLS Extensions**	RFC4366 status request, RFC5077 session ticket, RFC7301 application-layer protocol negotiation, RFC7627 extended master secret, RFC5746 renegotiation info
Organisation	LinkedIn Corporation	**Application-Layer Protocol Negotiation**	h2
State	California	**Next Protocol Negotiation**	Not Present
Country	US	**Issuing organisation**	DigiCert Inc
Organisational unit	Not Present	**Issuer common name**	DigiCert SHA2 Secure Server CA
Subject Alternative Name	▸ www.linkedin.com, linkedin.com, rum5.perf.linkedin.com, exp4.www.linkedin.com, exp3.www.linkedin.com, exp2.www.linkedin.com, exp1.www.linkedin.com, rum2.perf.linkedin.com, rum4.perf.linkedin.com, rum6.perf.linkedin.com, rum17.perf.linkedin.com and 21 more	**Issuer unit**	Not Present
Validity period	From Sep 11 2024 to Mar 11 2025 (6 months)	**Issuer location**	Not Present

The image shows an **SSL/TLS** report for **LinkedIn.com**, providing details about the website's security certificate. Here’s what it contains:

- **Assurance**: The SSL certificate provides **Organization Validation (OV)**, which verifies LinkedIn as a legitimate entity.
- **Perfect Forward Secrecy**: **Enabled**, ensuring session keys are not compromised even if the private key is.
- **Common Name**: The certificate is issued for www.linkedin.com, which is the domain name.
- **Organization**: The certificate is issued to **LinkedIn Corporation**.
- **State and Country**: The company is based in **California, US**.
- **Issuing Organization**: The certificate is issued by **DigiCert Inc**, a trusted certificate authority.
- **Supported TLS Extensions**: Includes several extensions like **RFC6066**, **RFC5077**, and **RFC5246**, which enhance security and session management.
- **Application-Layer Protocol Negotiation (ALPN)**: Supports **h2** (HTTP/2) protocol, providing faster data transfer.
- **Subject Alternative Name (SAN)**: The certificate covers several LinkedIn subdomains such as www.linkedin.com, **exp1.**www.linkedin.com, and others.
- **Validity Period**: The certificate is valid from **September 11, 2024**, to **March 11, 2025** (6 months).

Matches hostname	Yes	Issuer country	US
Server	Not Present	Issuer state	Not Present
Public key algorithm	rsaEncryption	Certificate Revocation Lists	http://crl3.digicert.com/DigicertSHA2SecureServerCA-1.crl http://crl4.digicert.com/DigicertSHA2SecureServerCA-1.crl
Protocol version	TLSv1.2	Certificate Hash	3SgvWiqHet1CrKPfC5FhP9G2FZE
Public key length	2048	Public Key Hash	10749dee28bda4b982f2107eb01e786998e0df23d9cfabd111e3f414886396f0
Certificate check	ok	OCSP servers	http://ocsp.digicert.com
Signature algorithm	sha256WithRSAEncryption	OCSP stapling response	Certificate valid
Serial number	0x0d42a363237bce4c2c938869dbceb39b	OCSP data generated	Sep 18 01:21:02 2024 GMT
Cipher	ECDHE-RSA-AES256-GCM-SHA384	OCSP data expires	Sep 25 00:21:02 2024 GMT
Version number	0x02		

The image shows the output from an SSL certificate inspection, likely from a security testing tool or a web server information tool. Here's a breakdown of the key information shown in the image:

1. **Matches hostname**: Indicates that the certificate matches the domain's hostname, marked as "Yes."
2. **Issuer country**: The issuer country of the SSL certificate is the **US**.
3. **Server**: Not present, meaning no server information is detected or not reported.
4. **Public Key Algorithm**: The public key algorithm used is **rsaEncryption.**
5. **Protocol Version**: The protocol version supported is **TLSv1.2**, which refers to Transport Layer Security version 1.2.
6. **Public Key Length**: The public key length is **2048** bits, which is standard for strong encryption.
7. **Certificate Hash**: The hash value of the certificate is provided as **35a9fbe6...** (truncated).
8. **Certificate Check**: An icon suggesting the certificate is valid, with a lock indicating a successful check.
9. **OCSP Servers**: The URL to the OCSP (Online Certificate Status Protocol) server is shown: **http://ocsp.digicert.com**.
10. **Signature Algorithm**: The algorithm used to sign the certificate is **sha256WithRSAEncryption**, which is commonly used for secure communication.
11. **Serial Number**: The serial number of the certificate is **0x6dd4a3231f...** (truncated).
12. **Cipher**: The cipher suite used is **ECDHE-RSA-AES256-GCM-SHA384**, indicating strong encryption with forward secrecy and AES 256-bit encryption.
13. **OCSP Stapling Response**: The certificate status is marked as valid.
14. **OCSP Data Generated**: The OCSP data was generated on **Sep 18, 2024, at 10:22:04 GMT.**
15. **OCSP Data Expires**: The OCSP data expires on **Sep 25, 2024, at 10:22:04 GMT.**
16. **Version Number**: The version of the certificate is **0x02**, indicating version 3.