**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.

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

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

**Pre-Experiment Theory:**

1. **Passive Reconnaissance through network commands**
2. **WHOIS:** WHOIS is the Linux utility for searching an object in a WHOIS database. WHOIS is a database of domains, which includes publicly displayed information about domain 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)*

1. **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)*

1. **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. 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.

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

1. **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.

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

1. **Passive Reconnaissance through publicly available tools**
2. **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.

1. **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

1. **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:
     1. Using ‘archive.org’ find the update history of ‘sfit.ac.in’ domain.
     2. 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.
     3. 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.
     4. 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 : www.yahoo.com** | | | |
| --- | --- | --- | --- |
| Registrar: | MarkMonitor Inc. | Registration Expiry date: | 2025-01-28 |
| Registration Update date: | 2023-12-27 | Name Servers: | ns1.yahoo.com  ns2.yahoo.com  ns3.yahoo.com  ns4.yahoo.com  ns5.yahoo.com |
| Registrant Organization | Yahoo Assets LLC | Registrant City: | VA |

| **Target Domain/URL/Website for netcraft : facebook.com** | | | |
| --- | --- | --- | --- |
| IPv4 address: | 157.240.221.35 | SSL/TLS certificate Issuing organization: | Meta Platforms, Inc. |
| Certificate Validity period: | From July 2 2024 to Sep 30 2024 (2 months, 4 weeks) | Public key algorithm: | id-ecPublicKey |
| Public key length: | 256 | Certificate Hash: | /AWr/tfducbbiz6i8RfS8EMpmAg |
| Signature algorithm: | sha256WithRSAEncryption | Public Key Hash: | a998f759ba0604cbc3ed9b598c3f9bca3f7c53ac5f6aa34504f8a6cec00d5521 |
| Server-Side site technology: | **SSL :** A cryptographic protocol providing communication security over the Internet  **PHP:** PHP is supported and/or running | Client-Side site technology: | **Client Pull**  **JavaScript:** Widely-supported programming language commonly used to power client-side dynamic content on websites |

**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.

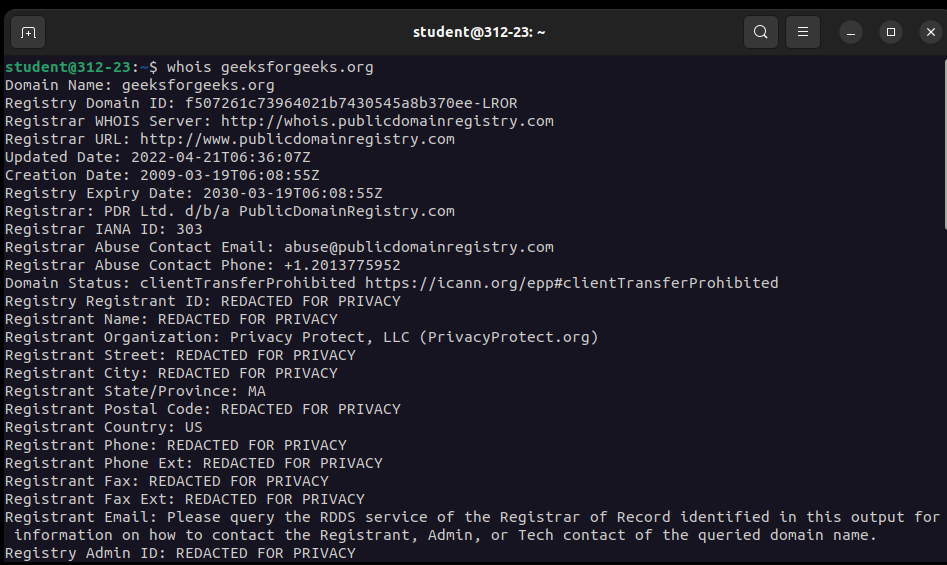
**References:**

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*

**A. Passive Reconnaissance through network commands**

**WHOIS COMMAND:**

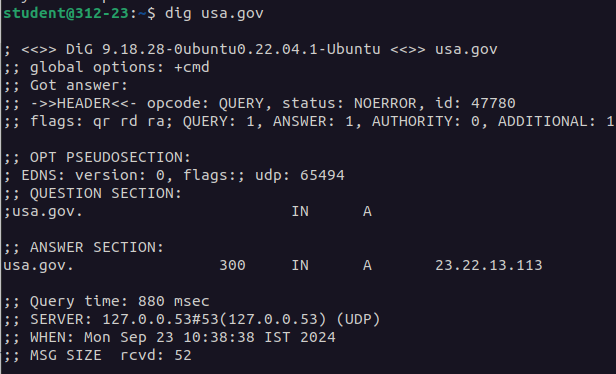
The whois command helps us to find information about that domain name or ip address. The output includes details such as the domain’s registrar, the creation date, and the expiration date, etc. It also provides information about the administrative and technical contacts responsible for managing the domain or IP address.



**DIG COMMAND:**

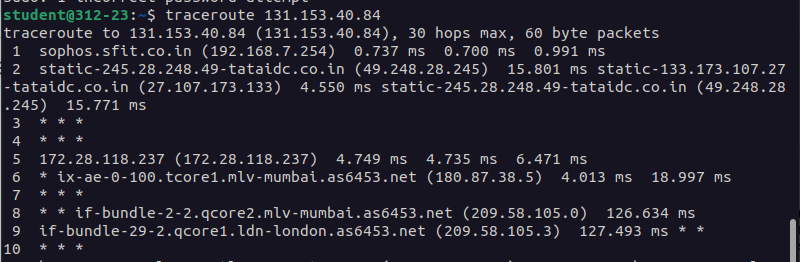
The dig command, short for domain information groper, is a powerful network tool for querying domain name system (DNS) servers. Querying a specific DNS record type lets you obtain particular information about a domain, such as its IP address, mail servers, or name servers.

It is popular due to its flexibility and crystal clear output over [host command](https://www.cyberciti.biz/faq/linux-unix-host-command-examples-usage-syntax/).



**TRACEROUTE:**

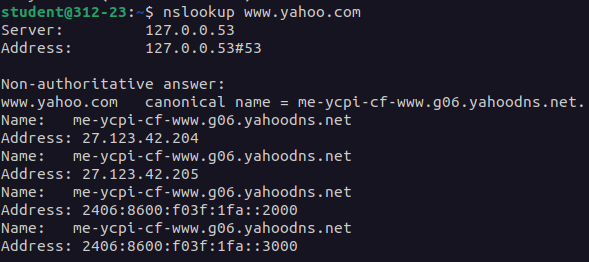
The traceroute command is a network diagnostic tool that allows users to track the route that a packet takes from the source computer to the destination. The traceroute command uses UDP packets by default. The output shows the IP addresses and hostnames of the routers that handle the packets, as well as the time taken for each hop and return.



**NSLOOKUP:**

Nslookup is a command-line tool used for querying the Domain Name System (DNS) to obtain domain name or IP address mapping information. It’s essential for troubleshooting DNS issues and verifying domain records. It lets users enter a [host](https://www.techtarget.com/searchnetworking/definition/host) name and find out the corresponding [IP address](https://www.techtarget.com/whatis/definition/IP-address) or domain name system DNS record.

nslookup has **two modes**: **interactive** and **non-interactive**. Interactive mode allows the user to query name servers for information about various hosts and domains. Non-interactive mode prints just the name and requested information for a host or domain.

****

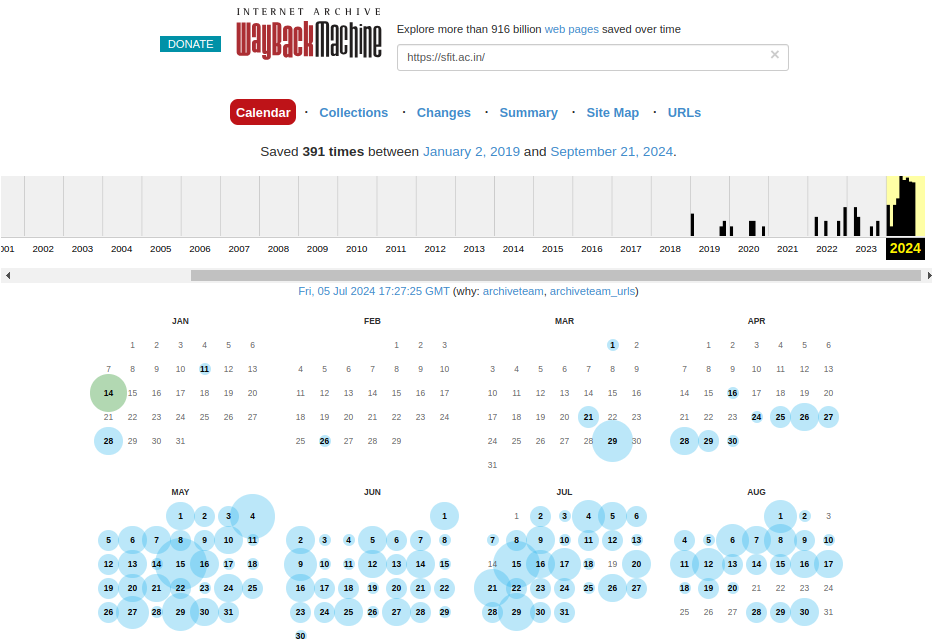
**B. Passive Reconnaissance through publicly available tools**

**1. archive.org (**[**https://archive.org/**](https://archive.org/)**):**

This machine allows passive reconnaissance of websites by providing access to historical snapshots of web pages. This tool can be used to gather various types of information without interacting directly with the target website, which makes it ideal for passive information gathering.

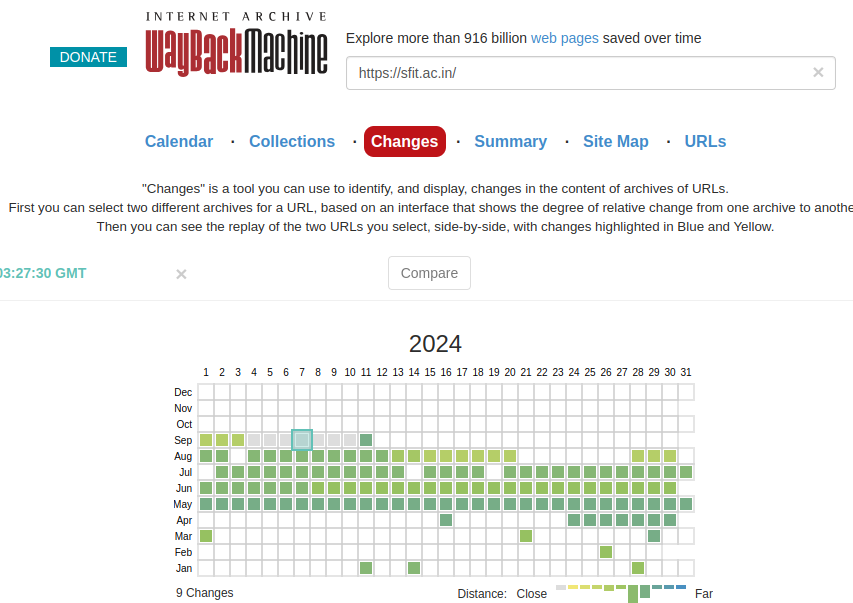
### Passive Reconnaissance Using Archive.org:

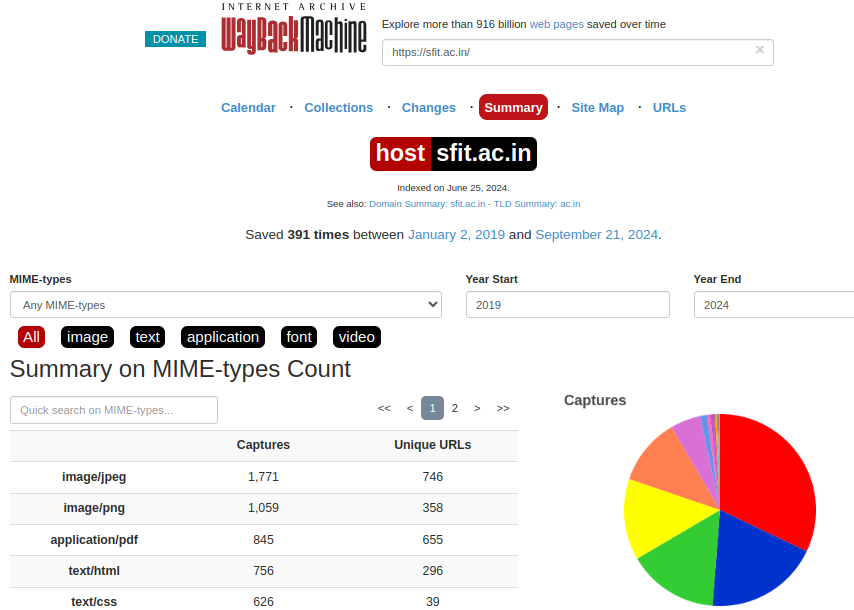
1. **Calendar:** The Wayback Machine provides a calendar view, which shows the dates when the website was crawled and archived. This helps in identifying key points in time when significant changes might have occurred on the site.

****

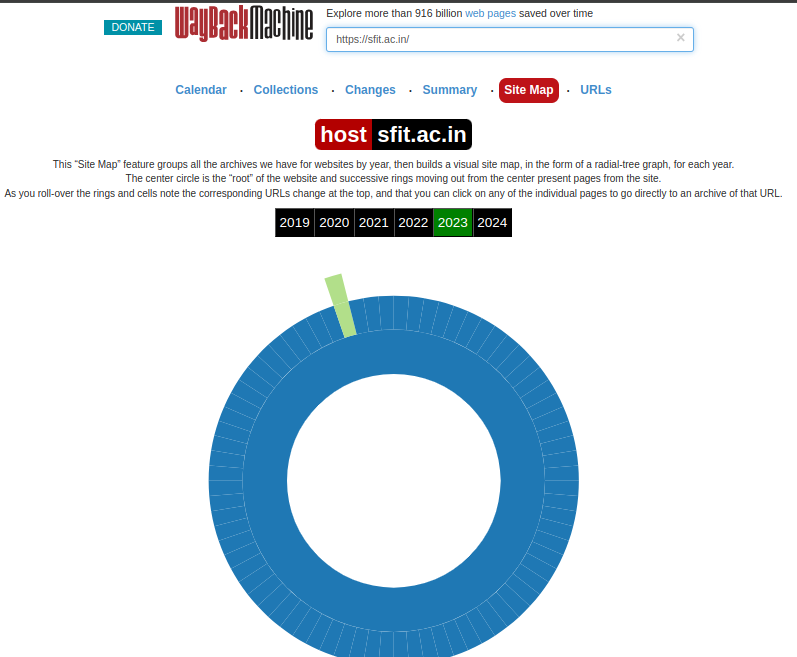
**2. Changes:** We can compare archived versions of the site from different points in time to see what has changed. This includes changes in content, layout, and even the removal or addition of pages.

It displays the changes throughout various years.

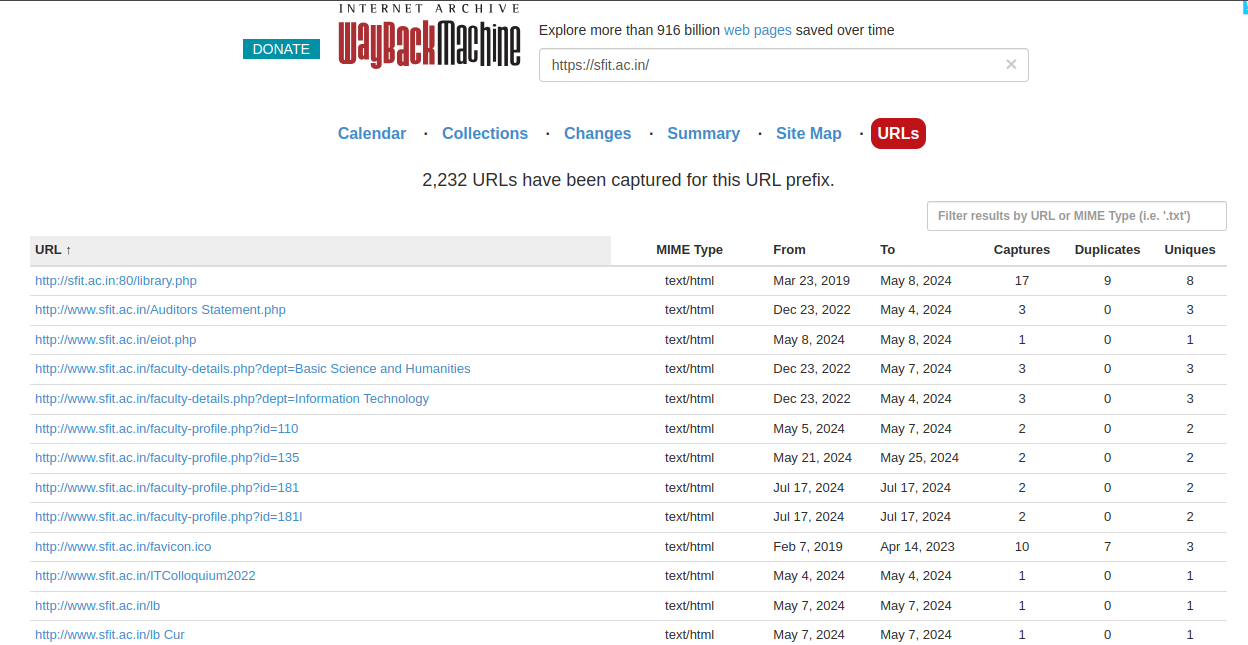
****

**3.** **Summary:** By reviewing archived pages, we seea general summary of the website's history, including changes in its structure, services, or content focus overtime.****

**4. Site Map:** While archive.org does not provide a direct site map feature, you can often reconstruct a historical site map by analyzing the structure of archived URLs and internal links from various snapshots.

****

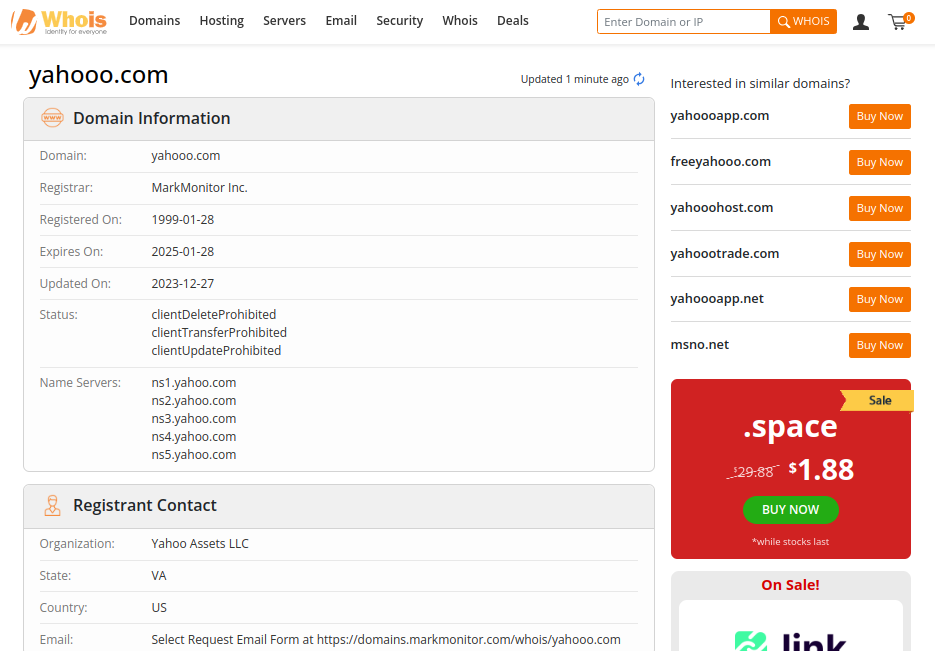
**5. URL**: Each archived version of a website has its own unique URL, allowing you to access specific snapshots from particular points in time for detailed analysis.

****

**2. Whois (**[**https://www.whois.com/**](https://www.whois.com/)**):**

**Whois** is a publicly available tool for passive reconnaissance that provides detailed domain registration information. It allows us to gather information about a website's domain, its owner, and other technical details without interacting with the target website directly.

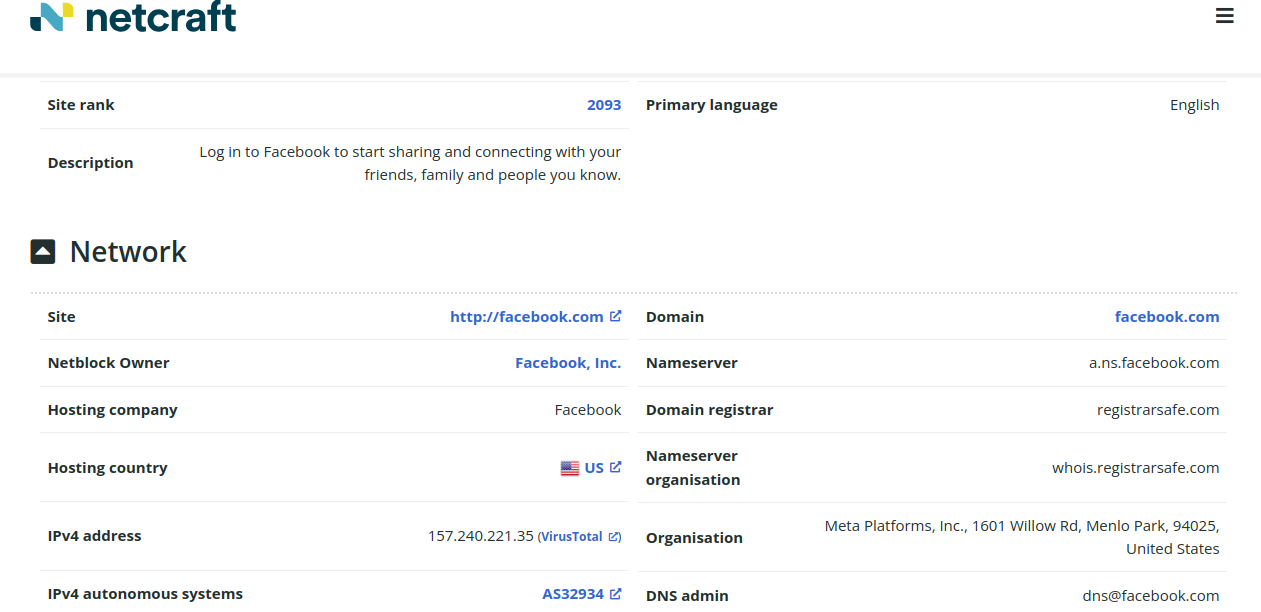
1. We see that the **yahoo.com** domain was originally registered on January 18, 1995, and this information is publicly available through Whois.
2. Whois provides details about the registrar and the registrant organization. In the case of yahoo.com, the domain is registered through MarkMonitor Inc., a domain management company, while the registrant organization is Yahoo Inc.

****

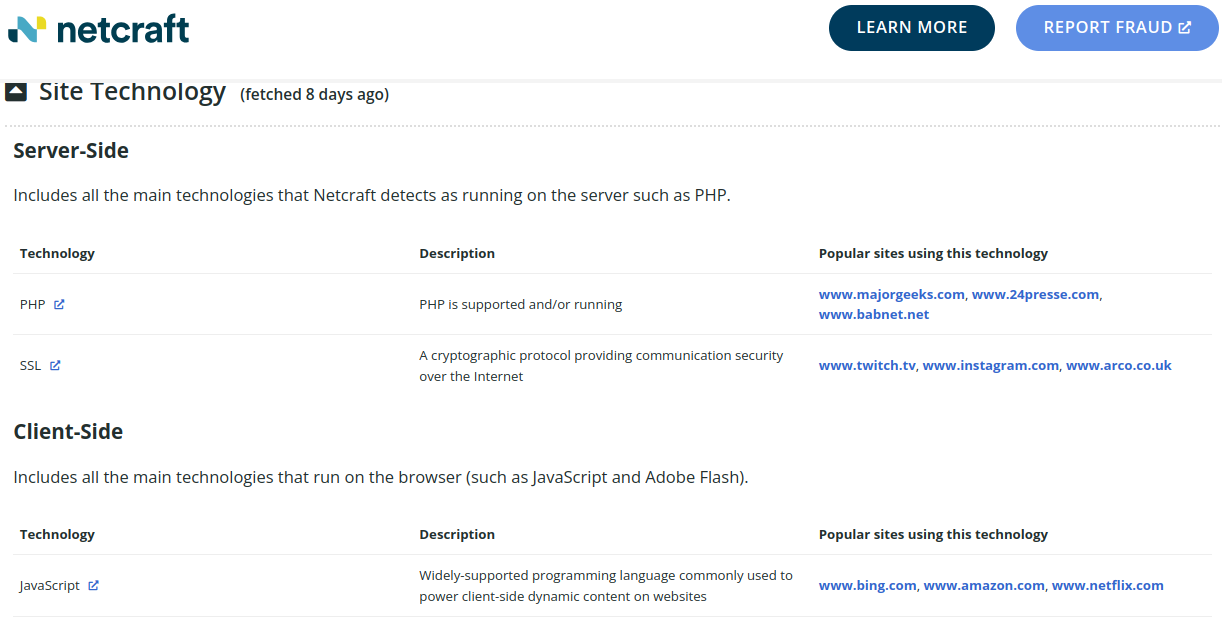
**4. Netcraft (**[**https://www.netcraft.com/**](https://www.netcraft.com/)**):**

NetCraft is a tool providing detailed technical and security-related information about a website. Netcraft reveals key insights about the site's infrastructure, server technologies, SSL/TLS certificate details, and more, allowing users to passively gather information without directly interacting with the site.

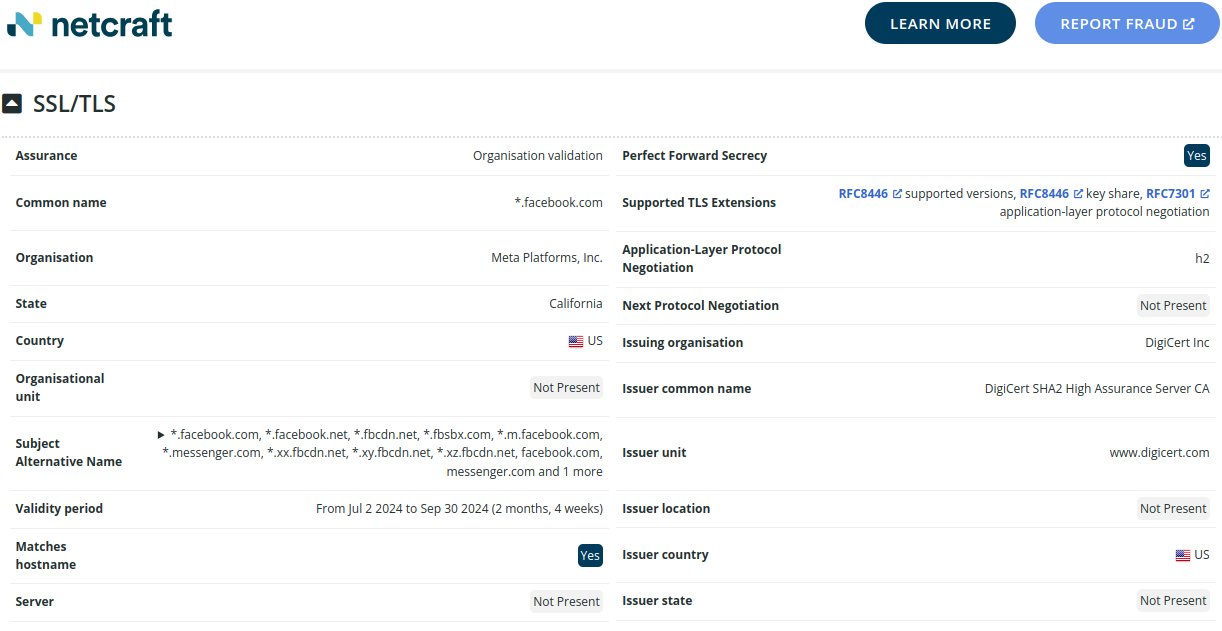
* **Network Section (IPv4 Address)**: Netcraft identifies the server's IP address, revealing its location and hosting provider, offering insight into the website's network infrastructure.

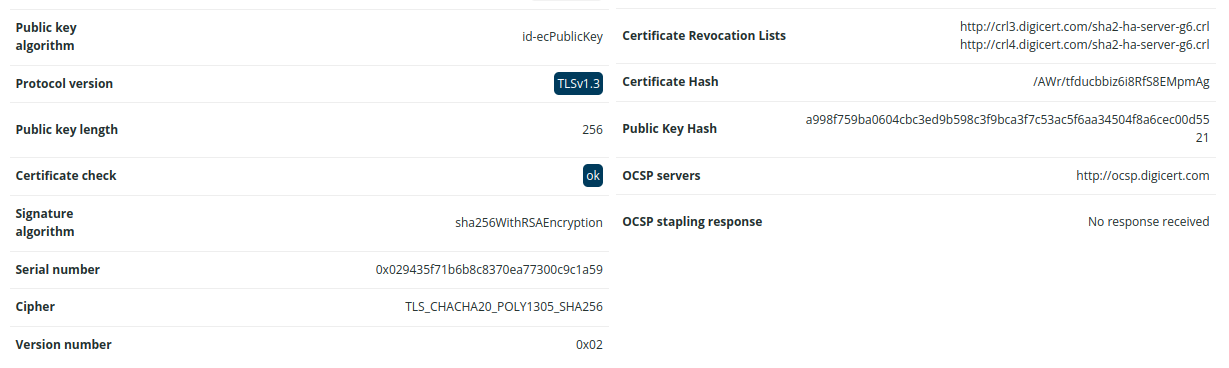
****

* **Client-Side and Server-Side Technologies**: It shows the technologies used for both client-side and server-side operations, detailing the web server, programming languages, and frameworks in use.

****

* **SSL/TLS Certificate**: Netcraft provides details on the SSL/TLS certificate, including validity, encryption strength, signing method, and the issuing organization, ensuring secure communication.

****

****