**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:**

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 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)*

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. 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)*

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. 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)*

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 :** [**http://youtube.com**](http://youtube.com/) | | | |
| --- | --- | --- | --- |
| Registrar: | MarkMonitor Inc. | Registration Expiry date: | 2025-02-15 |
| Registration Update date: | 2024-01-14 | Name Servers: | ns1.google.com  ns2.google.com  ns3.google.com  ns4.google.com |
| Registrant Organization | Google LLC | Registrant City: | CA |

| **Target Domain/URL/Website for netcraft :** [**https://microsoft.com**](https://microsoft.com/) | | | |
| --- | --- | --- | --- |
| IPv4 address: | 20.76.201.171 | SSL/TLS certificate Issuing organization: | Microsoft Corporation |
| Certificate Validity period: | From Sep 10 2024 to Sep 5 2025 (11 months, 3 weeks, 4 days) | Public key algorithm: | rsaEncryption |
| Public key length: | 2048 | Certificate Hash: | PCxRWeO0Jt29g6/RdCjP4XNSQh0 |
| Signature algorithm: | sha384WithRSAEncryption | Public Key Hash: | 2c275a27f652171152cee5e55be052a0e9f603df594fb9f1270e4ec6391d900e |
| Server-Side site technology: | ASP.NET  SSL | Client-Side site technology: | Javascript  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.

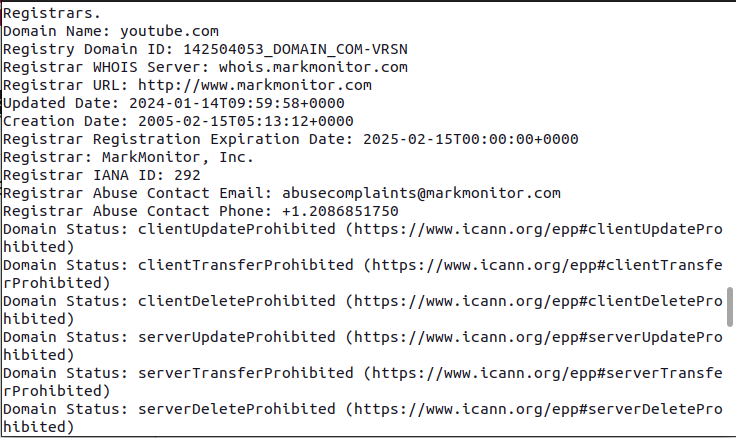
**Conclusion:**

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*

**WHOIS command:**



WHOIS is a protocol that is used to find the details of an internet resource such as a domain name, an IP address block or an autonomous system.This protocol is used to store the details in a database and deliver the details the database in a human readable formats.This type of information contains the general details about the domain. It will consist of the following fields:

**Domain:** This field will give you the domain name which we are querying the WHOIS details.

**Registrar:** This is the details of the registrar with whom the domain name is registered.

**Registration Date:** This is the date when the domain name was first registered. With some WHOIS lookup tools, it will be displayed as “Creation Date”.

**Expiration Date:** This is the date when the domain will expire.

**Updated Date:** This is the date when the WHOIS details last updated.

**Status:** This is the registrar status of the domain. This will be “OK” if there is no restriction and the domain is free to transfer from one registrar to another.

**Name Servers:** This field will provide the details of the nameservers used by the domain in the meantime.

**Registrant Contact**

As the name indicates, this area will provide you with details of the registrant of a domain ie,name,organization,street,city,state,postal code, phone number,etc.

**DIG Command:**

The dig command in [Linux](https://phoenixnap.com/kb/what-is-linux) is used to gather [Domain Name System (DNS)](https://phoenixnap.com/kb/what-is-domain-name-system) information. It stands for domain information groper and helps [troubleshoot DNS problems](https://phoenixnap.com/kb/dns-troubleshooting).

* The first line displays the dig command version.

The HEADER section in the dig output summarizes the DNS query and response details. It includes information about the query type (e.g., standard query), the response status (e.g., NOERROR for a successful response), and flags indicating key attributes like recursion.

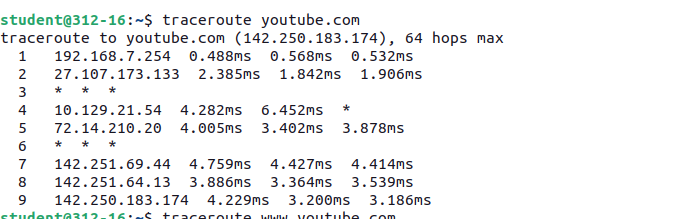
* The OPT PSEUDOSECTION displays advanced data:
  + EDNS. Extension system for DNS, if used.
  + flags. Specified flags. In this case, it's blank because no flags were specified.
  + udp. udp packet size.

The QUESTION SECTION displays the query data that was sent

The statistics section shows metadata about the query

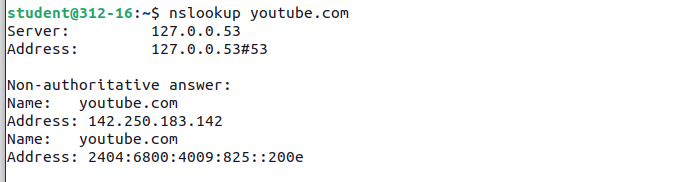
The most important section is the ANSWER SECTION:

* 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 query class. In this case, IN stands for Internet.
* The fourth column displays the query type. In this case, Astands for an A (address) record.
* The final column displays the IP address associated with the domain name.

**Traceroute command:**

The Traceroute command (Tracert on Windows) is a small network diagnostic software that you have built-in on your device and servers for tracing the route, hop by hop to a target. Apart from full route that the packets take to their destination (domain or IP address) we see the hostnames and IPs of the routers on the way and the latency, the time it takes for each device to receive and resend the data.

How does traceroute works?

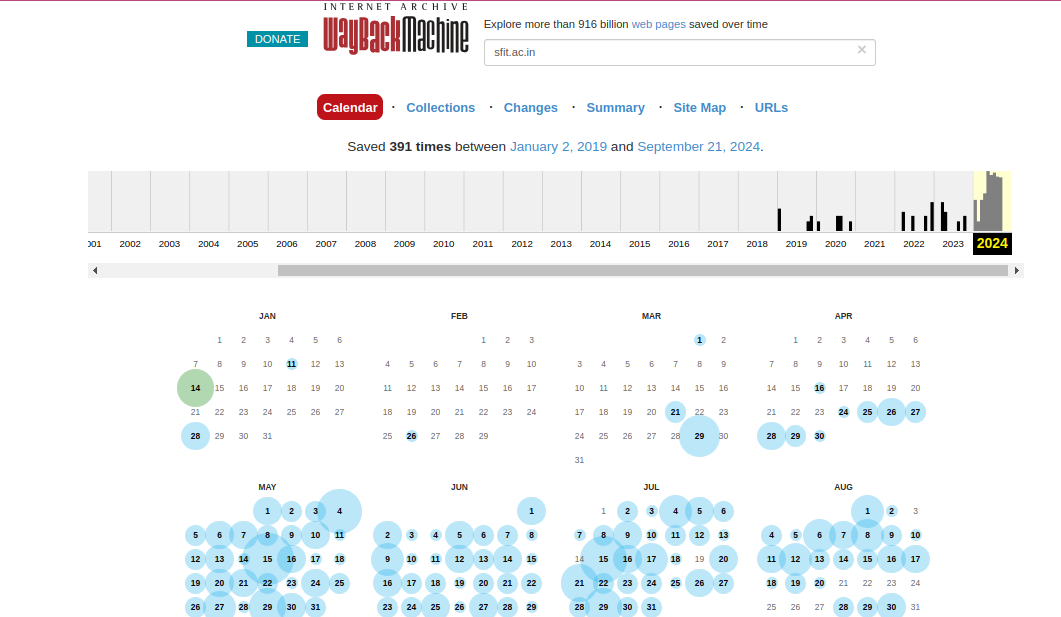
When you run a traceroute, you send an IP packet containing the source and destination addresses and the time to live (TTL) for each hop. TTL in packets decreases with each hop. This is to avoid server looping issues. Furthermore, when the TTL is reached, the packet expires and is discarded. When this occurs, Traceroute returns to the sender ICMP Time Exceeded messages (RFC 792). Because small TTL settings cause packets to expire quickly, traceroute forces all routers in a packet’s path to produce the [ICMP](https://www.cloudns.net/blog/what-is-icmp-internet-service-message-protocol/) messages that identify the router.

NSLOOKUP command:

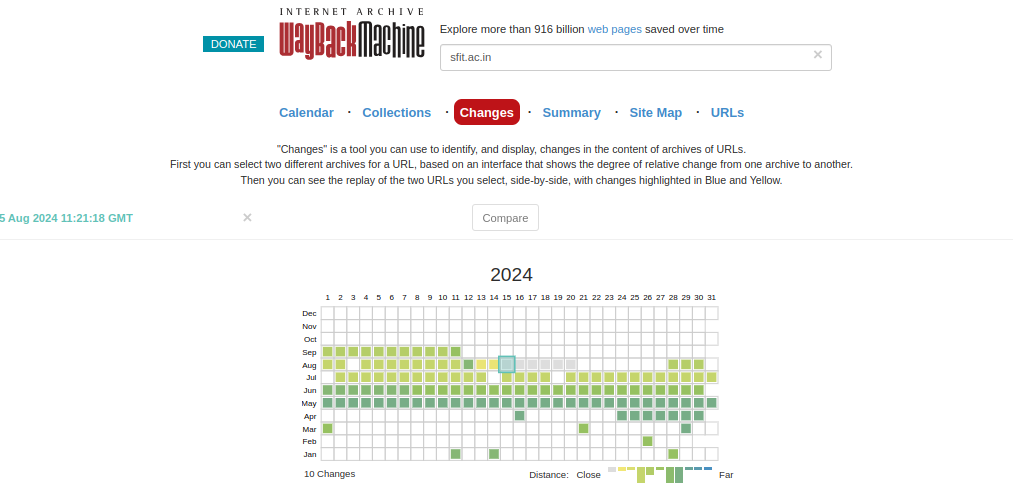
nslookup is an abbreviation of name server lookup and allows you to query your DNS service. The tool is typically used to obtain a domain name via your command line interface (CLI), receive IP address mapping details, and lookup DNS records. This information is retrieved from the DNS cache of your chosen DNS server.There are two primary functions included with nslookup. The first is DNS lookup, whereby you enter a domain URL and retrieve the corresponding server IP address. You can also reverse this process and enter an IP address to retrieve the corresponding domain URL.The nslookup tool can be used for DNS-related tasks like server testing and troubleshooting.

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

**calendar page:**

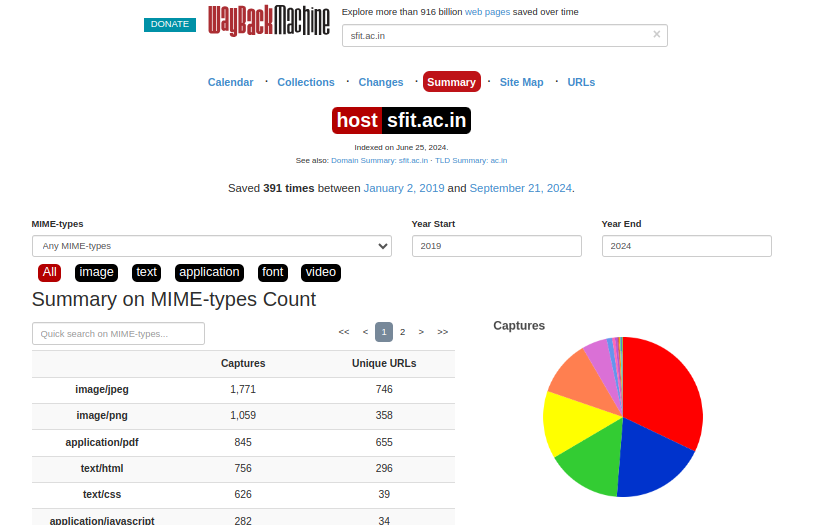


The Calendar page of the Internet Archive creates a visual timeline where you can browse archived website snapshots. You could click on the highlighted dates to view how the site has evolved over time with historical versions of that site. It's useful for researchers, specifically for people interested in digital history-the preservation of past versions of websites.



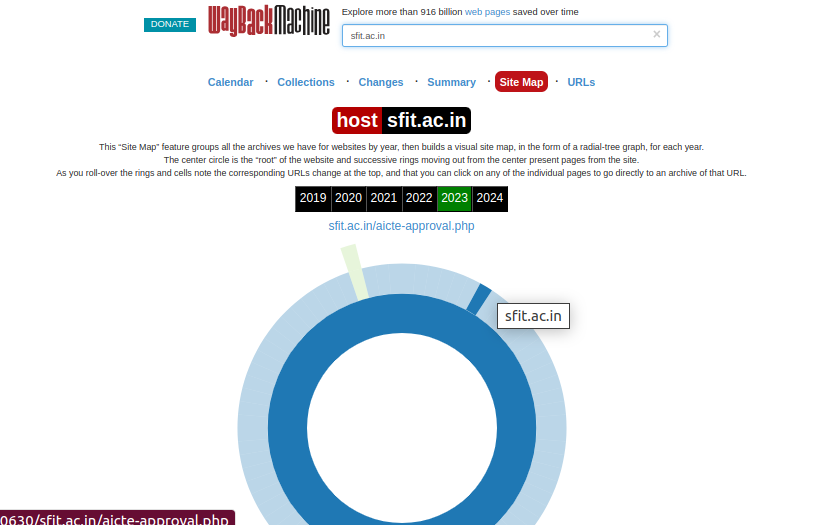
**Changes Page:**

The Changes page of Internet Archive provides a log of updates applied to archived websites; changes are easy to see over the passage of time. There is also a view showing side-by-side comparison of differences between snapshots for tracing what has evolved in the website as well as in its content. This is particularly helpful for researchers studying the evolution of web development.



**Summary Page:**

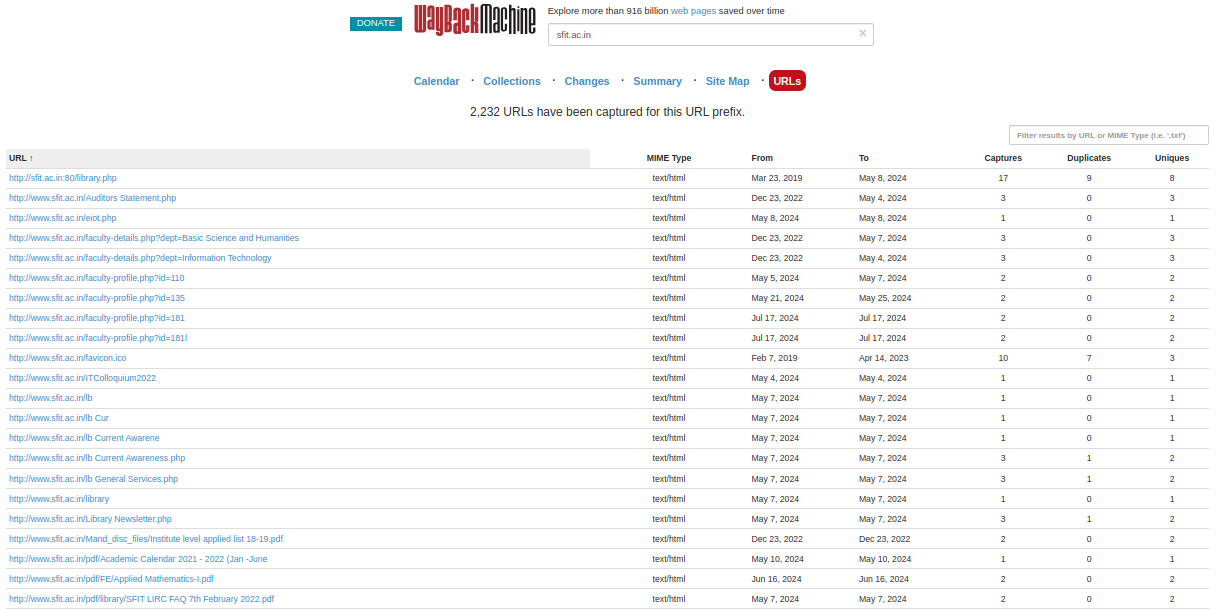
The Summary page of an archived website on Internet Archive features an overview of the particular archived website, including essential details such as the number of snapshots taken, the range of dates covered, and the timeline of major changes. In a nutshell, it helps users get an idea of the site's history and evolution at a glance.This page makes use of piechart,bar-grpahs,etc for visualization of data.



**Site Map page:**

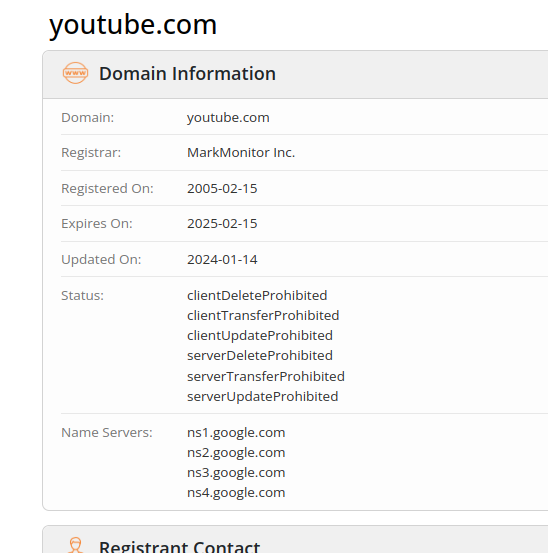
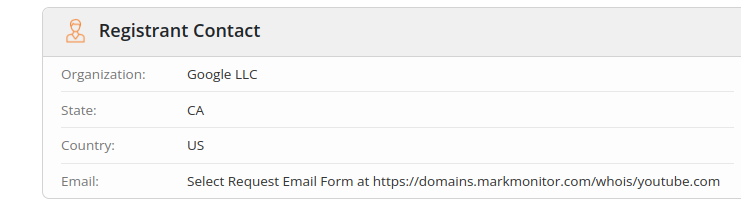
The Internet Archive uses a Site Map page for a given archived site; it defines the layout of the specific archived website and visually displays its pages and hyperlinks. It is somewhat more accessible to navigate archived content this way-by making it easier to find a desired section or piece of information within the site.

URLs page:



The URL page from Internet Archive would have information regarding a particular address on the web, for example: archive snapshots list of that URL, captures time line, access to other versions, and how the history of the site at that address has actually changed over time.

* [**https://www.whois.com**](https://www.whois.com) (for youtube.com)



The whois.com page does similar work of whois command i.e. giving registrant,domain,administrative contact,technical contact and raw data but Whois.com is an easy interface through which one can search for domain registration information from a web interface. The whois command, however, is a command-line tool that retrieves the same data but in raw text format. Whois.com comes with more features such as providing domain registration services. The whois command, however, is technical and demands knowledge of a command line.The attached screenshots focuses on the data that includes:

• Registration details

• IP address

• Contact number and Email ID

• Domain owner

• Name servers

• Regional Internet Registries

* **https://www.netcraft.com/**

Netfcraft is another tool like others that give information related to IP addresses,services running,operating system being used, name servers, technologies being used but following points makes it to stand out:

Comprehensive Web Survey Data: Offers detailed insights into hosting, technologies, and SSL certificates.

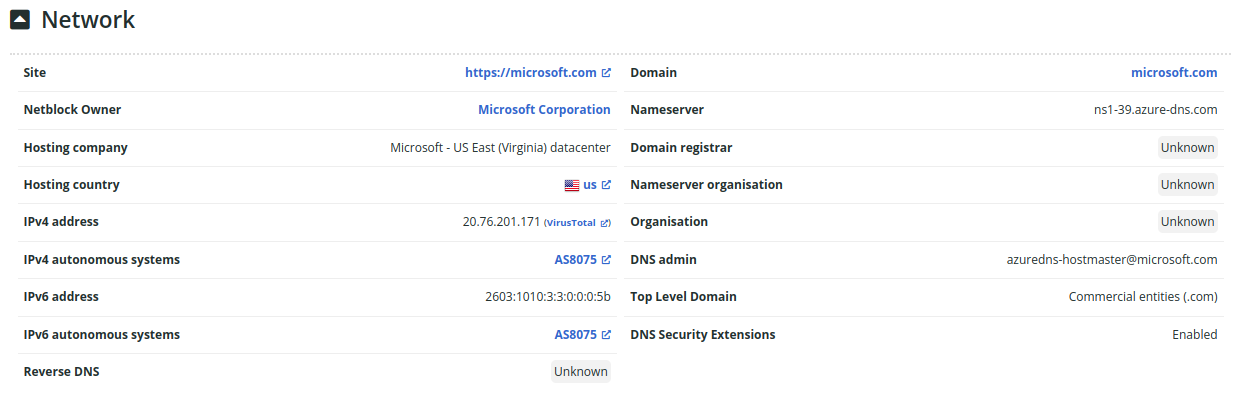
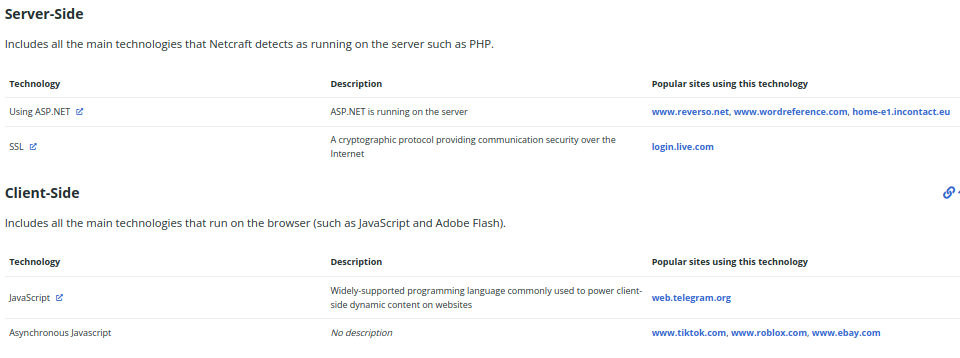
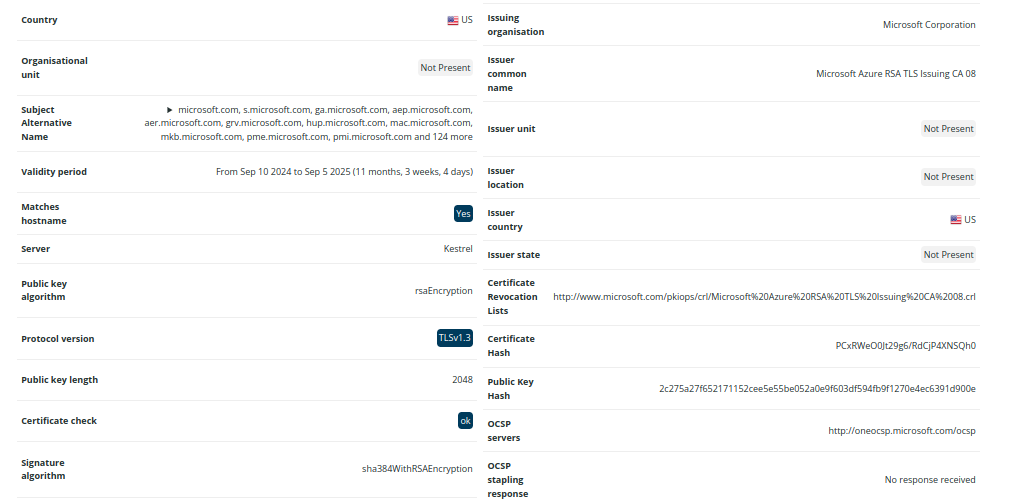
Anti-Phishing Services: Actively detects and helps take down phishing sites.

Historical Data: Tracks changes in website infrastructure over time.

Detailed SSL Information: Provides insights into SSL configurations and expiration.

Unique Web Application Fingerprinting: Accurately identifies server technologies and frameworks.

Cybersecurity Focus: Combines information gathering with threat detection and analysis.

 The attached screenshot includes the information related to the IPV4 address, SSL/TLS certificate issuing organization, certificate validity period, public key length, signature algorithm, server-side site technology, public key algorithm, certificate hash, public key hash,client-side site technology,etc.