**EXPERIMENT NO - 04**

**Name: Kale Komal Janardan**

**Div: TE IT – A**

**Roll No.: ITA539 Batch: A2**

**DOP: Sign:**

**DOS: Grade:**

**---------------------------------------------------------------------------------------------------------**

**Aim:** To study the use of network reconnaissance tools like **whois, dig, traceroute and nslookup** to gather information about networks and domain registrars.

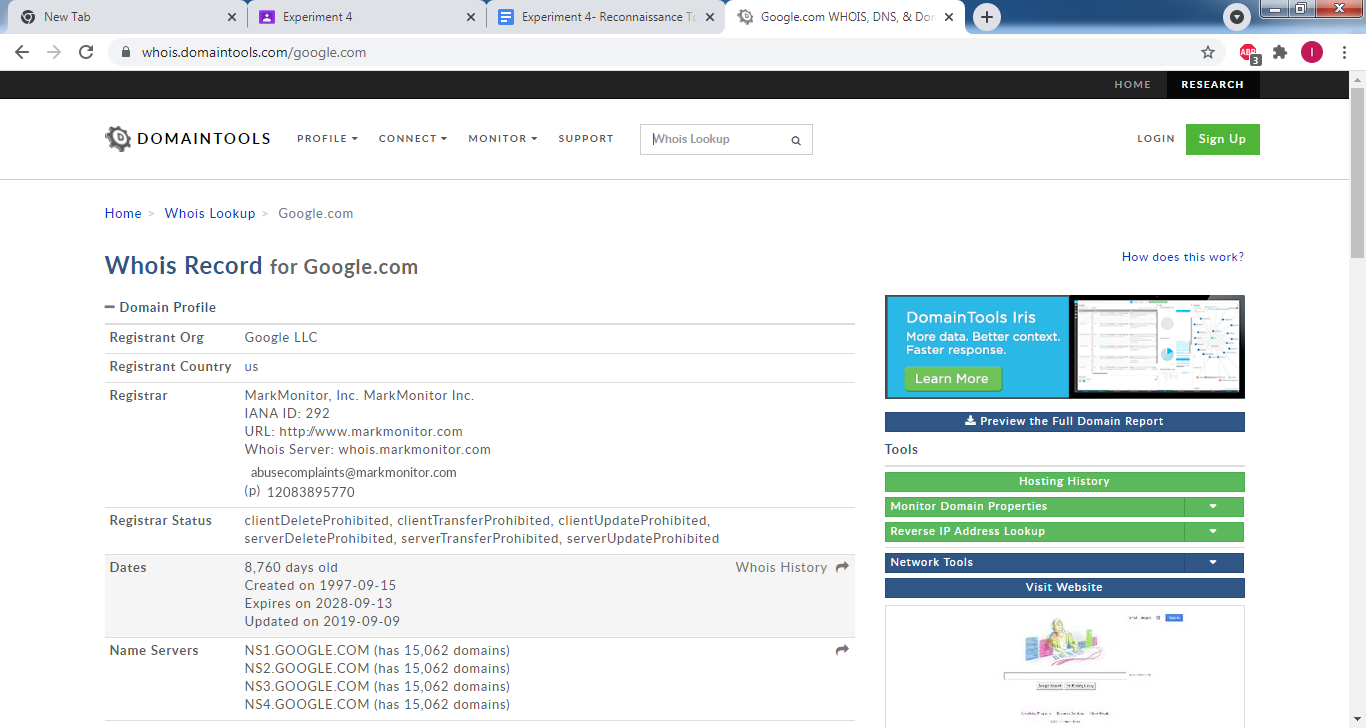
**1. whois:**

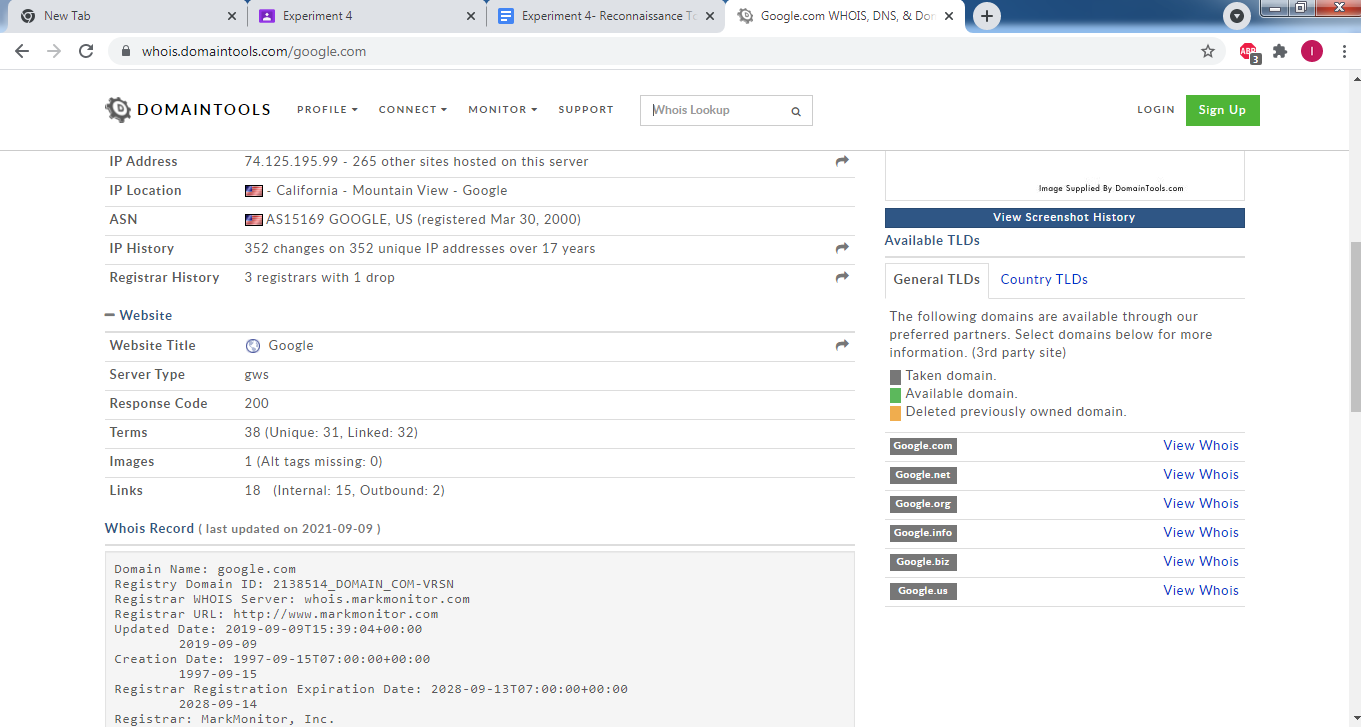
**whois** is the Linux utility for searching an object in a **whois** database. The **whois** database of a domain is the publicly displayed information about a domain's ownership, billing, technical, administrative and nameserver information. Running a **whois** on your domain will look the domain up at the registrar for the domain information. All domains have **whois** information. **whois** database can be queried to obtain the following information

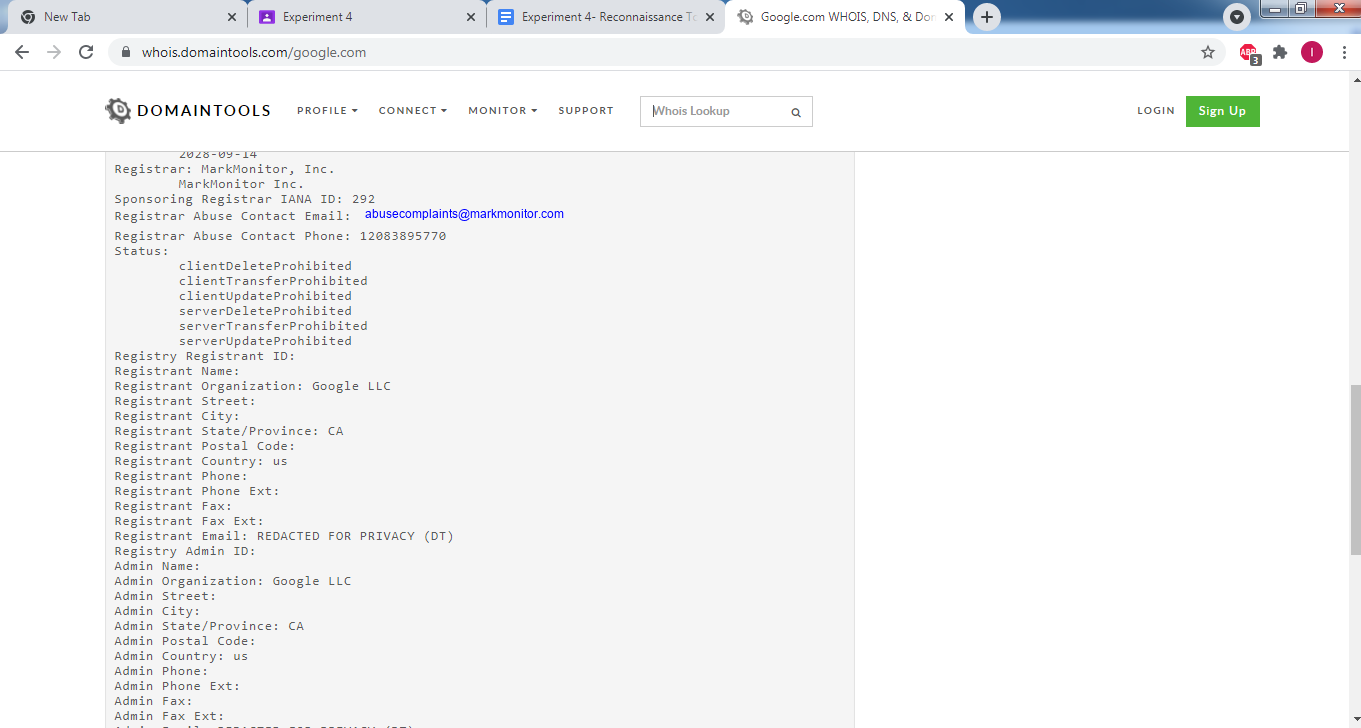
* Administrative contact details, including names, email addresses and telephone numbers
* Mailing addresses for office locations relating to the target organization
* Details of authoritative name servers for each given domain

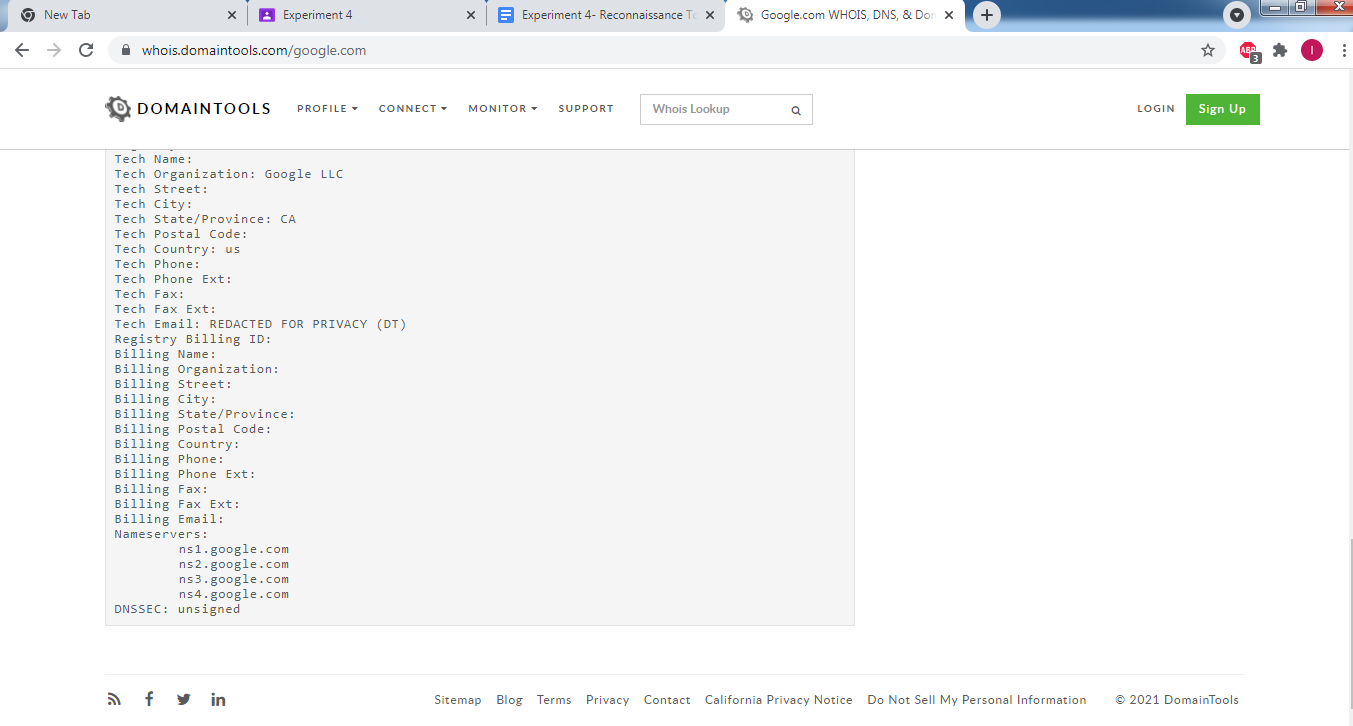
whois google.com

**Output:**









**2. dig:**

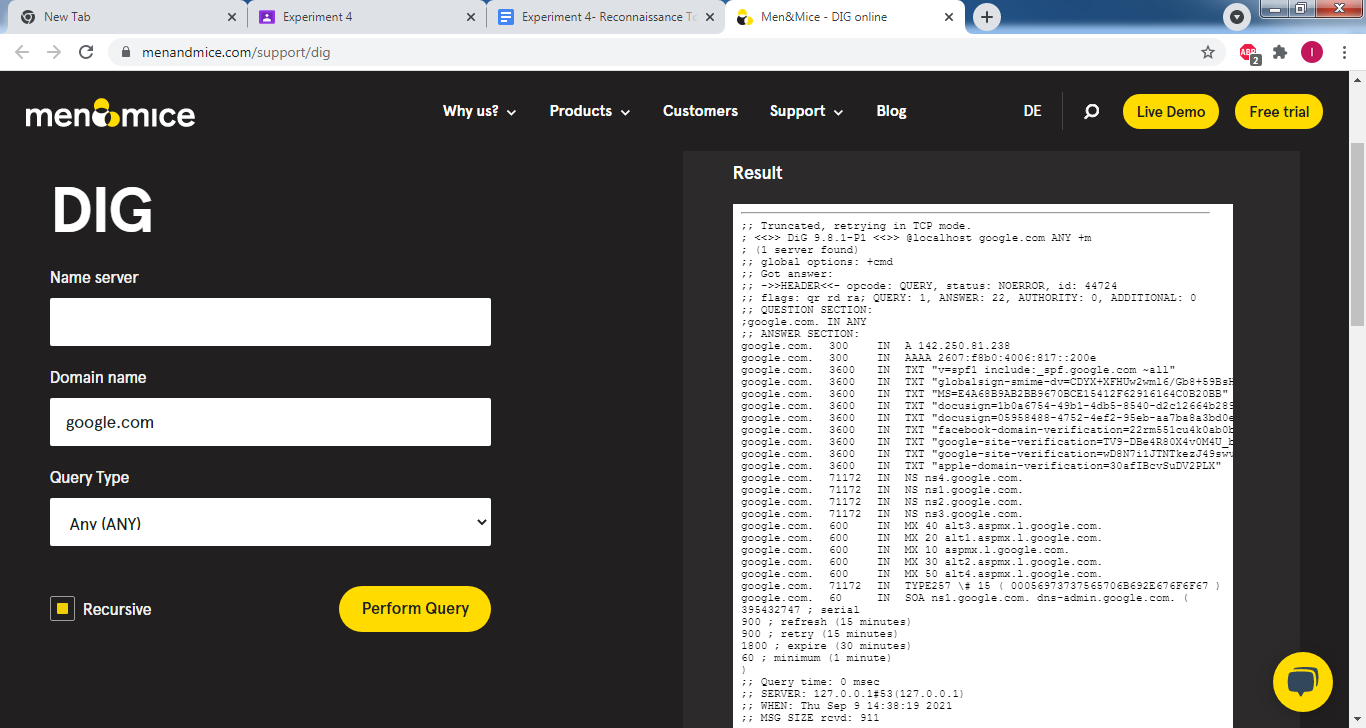
dig is a networking tool that can query DNS servers for information. It can be very helpful for diagnosing problems with domain pointing and is a good way to verify that the configuration is working. The most basic way to use dig is to specify the domain we wish to query:

The dig command output has the following sections:

* Header: This displays the dig command version number, the global options used by the dig command and few additional header information.
* QUESTION SECTION: This displays the question it asked the DNS. i.e This is your input.
* ANSWER SECTION: This displays the answer it receives from the DNS. i.e This is your output.
* AUTHORITY SECTION: This displays the DNS name server that has the authority to respond to this query. Basically this displays available name servers
* ADDITIONAL SECTION: This displays the ip address of the name servers listed in the AUTHORITY SECTION.
* Stats section at the bottom displays few dig command statistics including how much it took to execute this query

dig redhat.com

**Output:**

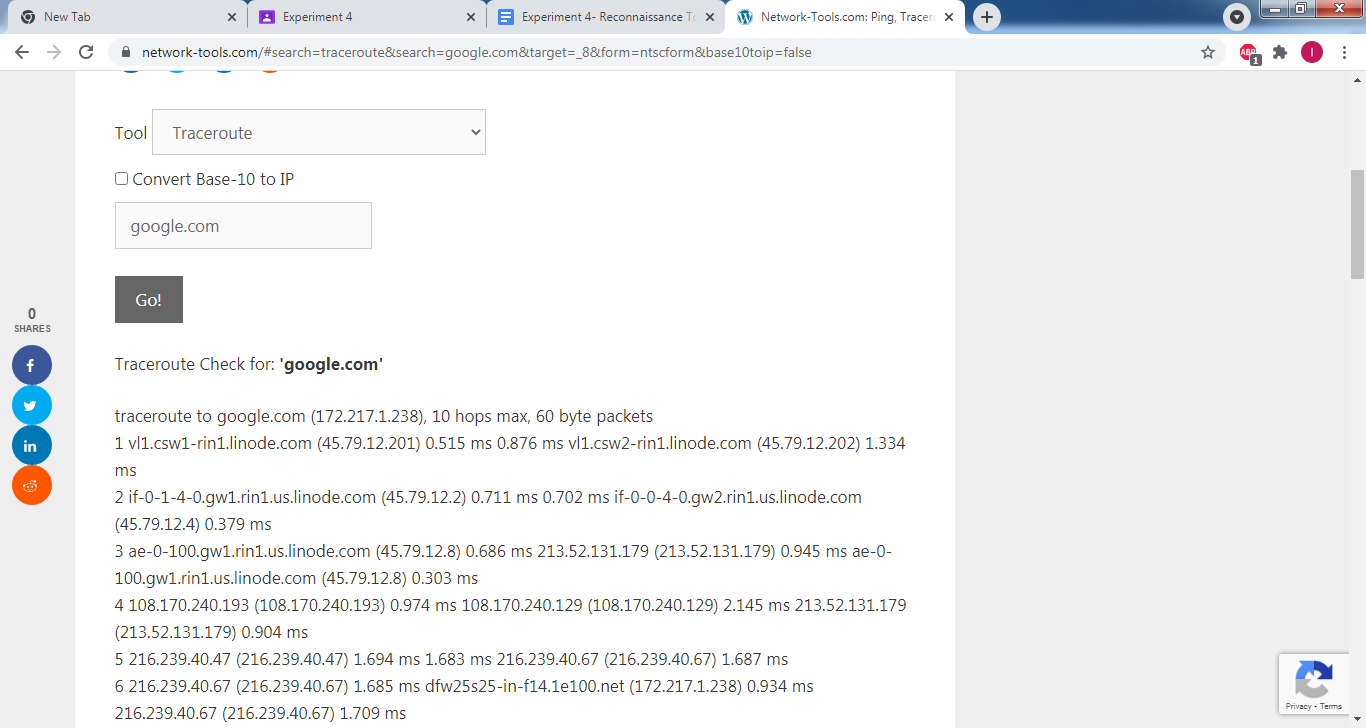


**3. traceroute:**

traceroute prints the route that packets take to reach a destination. traceroute utility uses the TTL field in the IP header to achieve its operation. TTL field describes how much hops a particular packet will take while traveling on the network. So, this effectively outlines the lifetime of the packet on the network. This field is usually set to 32. 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, the router sends an ICMP error message of ―Time exceeded, back to the source from where the packet was generated. The ICMP packet that is sent back contains the IP address of the router. So traceroute incrementally fetches the IP of all the routers between the source and the destination.

Ex: traceroute google.com

**Output:**



**4. nslookup:**

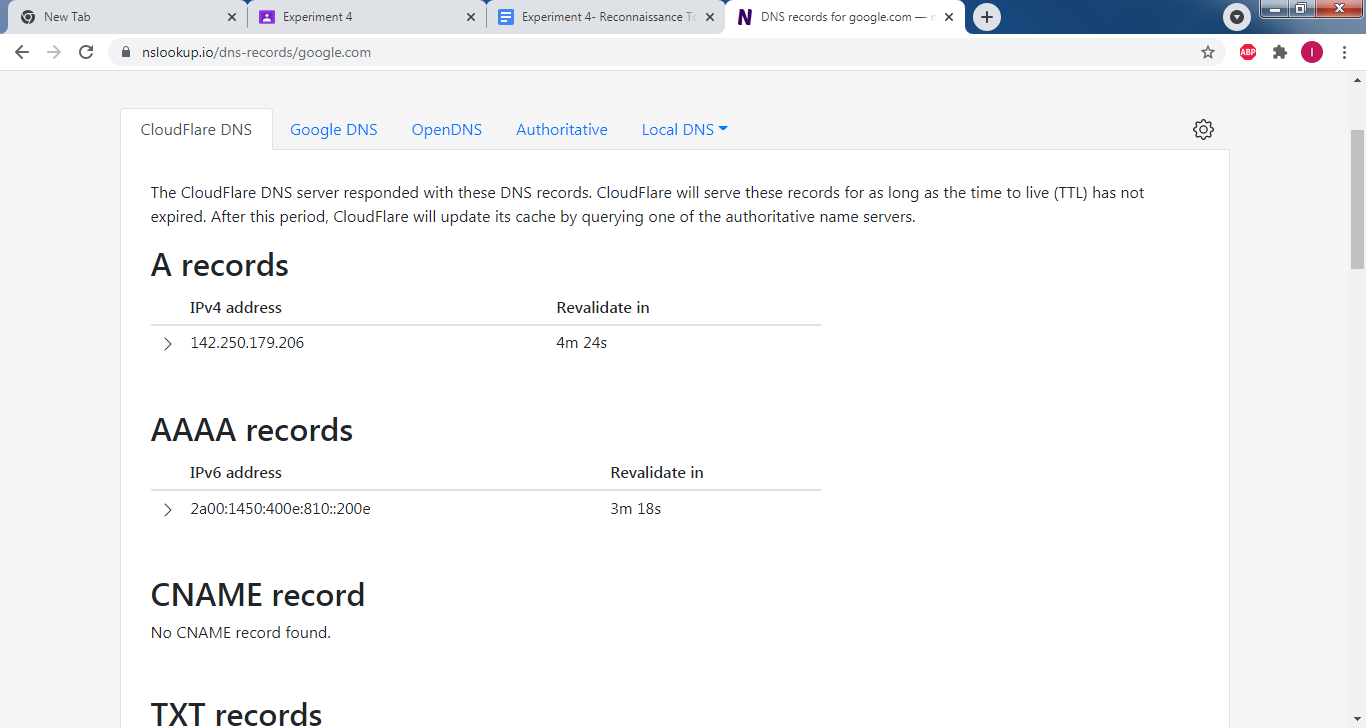
The nslookup command is used to query internet name servers interactively for information. nslookup, which stands for "name server lookup" is a useful tool for finding out information about a named domain. By default, nslookup will translate a domain name to an IP address and vice versa.

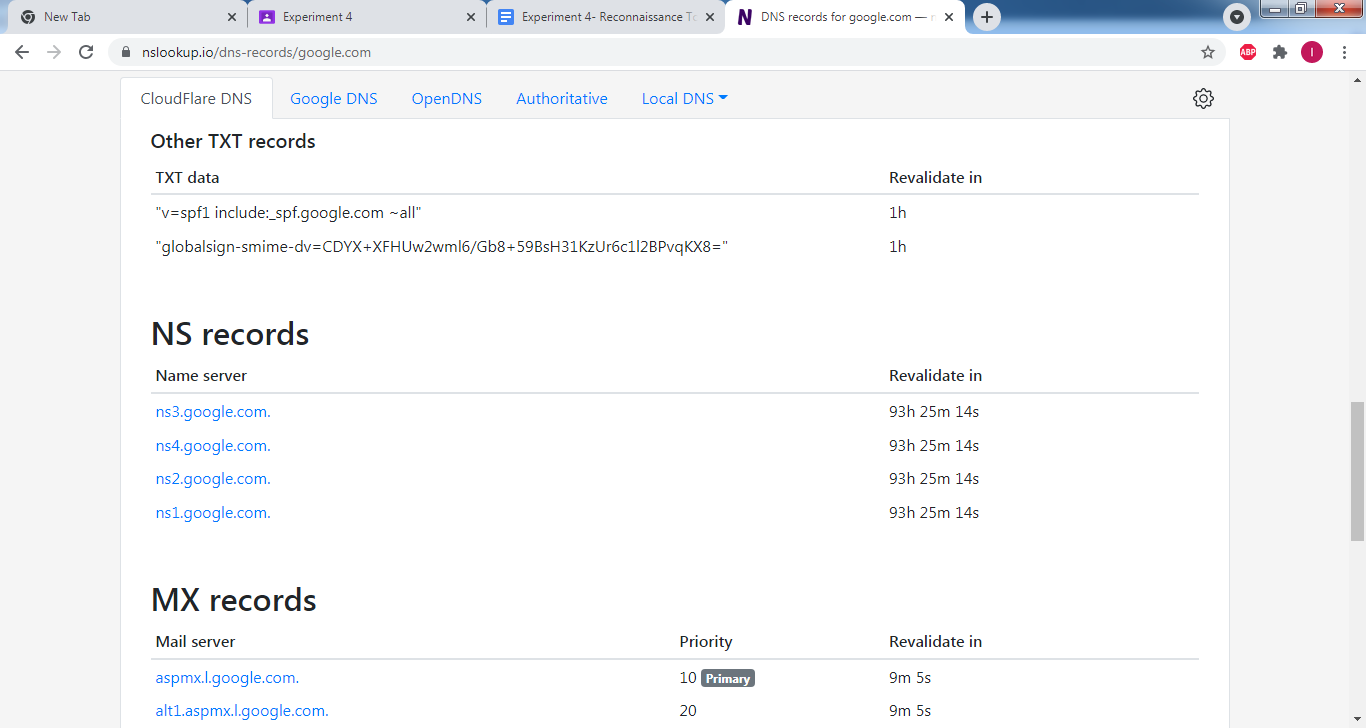
Using nslookup we can query for following information

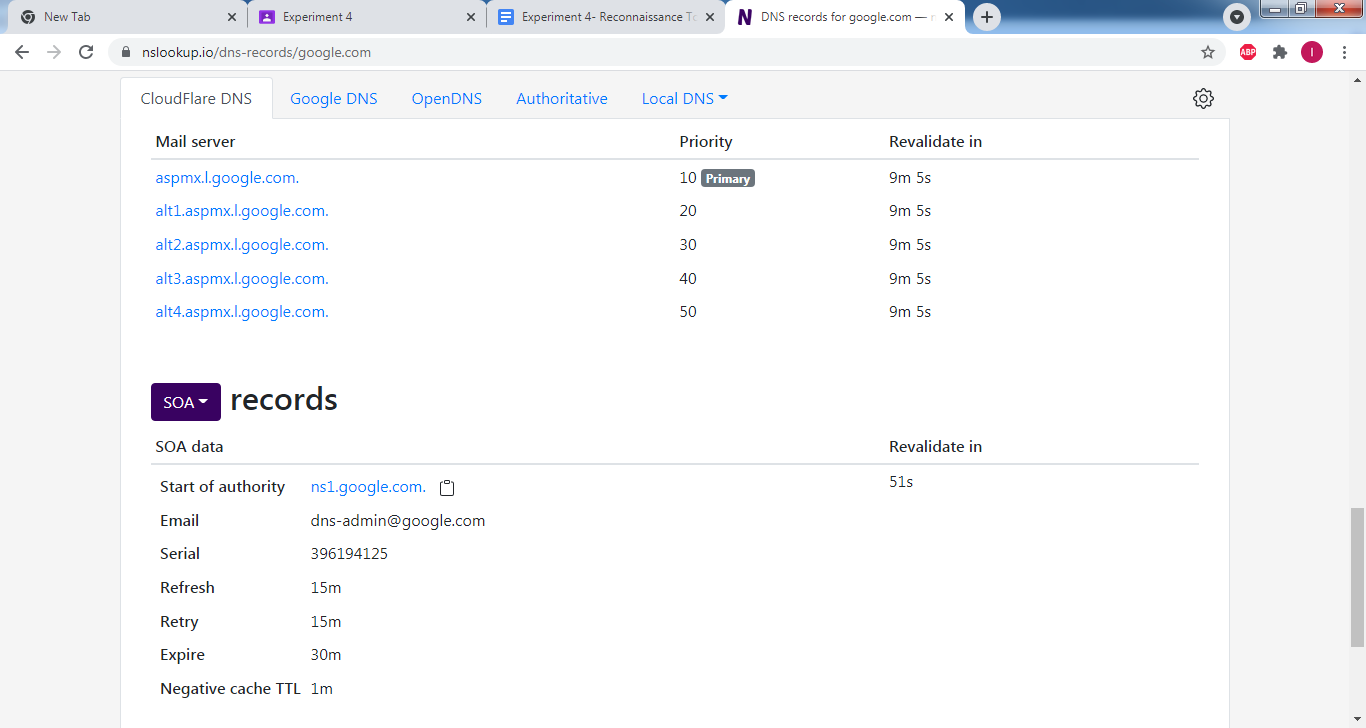
|  |  |
| --- | --- |
| **nslookup parameter values** | **Type of query** |
| A | IPv4 address |
| AAAA | IPv6 address |
| MX | Domain name mailserver (mail exchanger) |
| NS | Domain name name server |
| PTR | “Pointer” entry (pinpoints the host name that corresponds to an IP address) |
| SOA | “Start-of-Authority” entry (details about the administration of the DNS zone) |

nslookup google.com

**Output:**

****

****

****

**Conclusion:** Thus we have successfully studied network reconnaissance tools.