Experiment no.: 09

Title: Demonstrate the use of following tools:

- Samspade
- Nslookup
- Whois
- Tracert

Course Outcome: Build systems that are more secure against attacks.

Theory:

- SamSpade: Multi-tool for network diagnostics (legacy; features include DNS queries, WHOIS lookups, traceroute).
- Nslookup: DNS query tool to resolve hostnames to IPs and query DNS records.
- Whois: Retrieves domain registration and ownership information from WHOIS databases.
- Tracert / Traceroute: Shows the route packets take to reach a destination and the round-trip time per hop.

Advantages:

- Quick visibility into DNS, domain ownership, and network path issues.
- Useful during reconnaissance for troubleshooting and incident response (ethical/legal use only).
- Helps verify DNS configurations and identify misconfigurations.

Algorithm/Methodology:

1. Nslookup:
   - Run nslookup example.com to get A record; specify record types (nslookup -type=MX example.com) to query MX, TXT, etc.
2. Whois:
   - Run whois example.com or use web WHOIS clients to view registrant, registrar, creation/expiry dates.
3. Tracert/traceroute:
   - Run tracert example.com (Windows) or traceroute example.com (Linux/Mac) to view intermediate hops and latency.
4. SamSpade:
   - Use built-in modules for DNS, WHOIS, traceroute, and other lookup tasks (note: SamSpade is older — many functions are replaced by modern CLI tools).
5. Record outputs and interpret results: DNS misconfigurations, stale records, routing bottlenecks, or suspicious registrar info.

SamSpade

SamSpade is a graphical network query tool used to gather information about domains and IP addresses. It provides several utilities such as Whois lookup, DNS lookup, traceroute, ping, and email header analysis. It is primarily used in network troubleshooting and for investigating spam or cyber incidents. SamSpade allows users to view domain registration details, identify mail servers, trace routes, and analyze the origin of network connections in a simple interface.

Purpose:

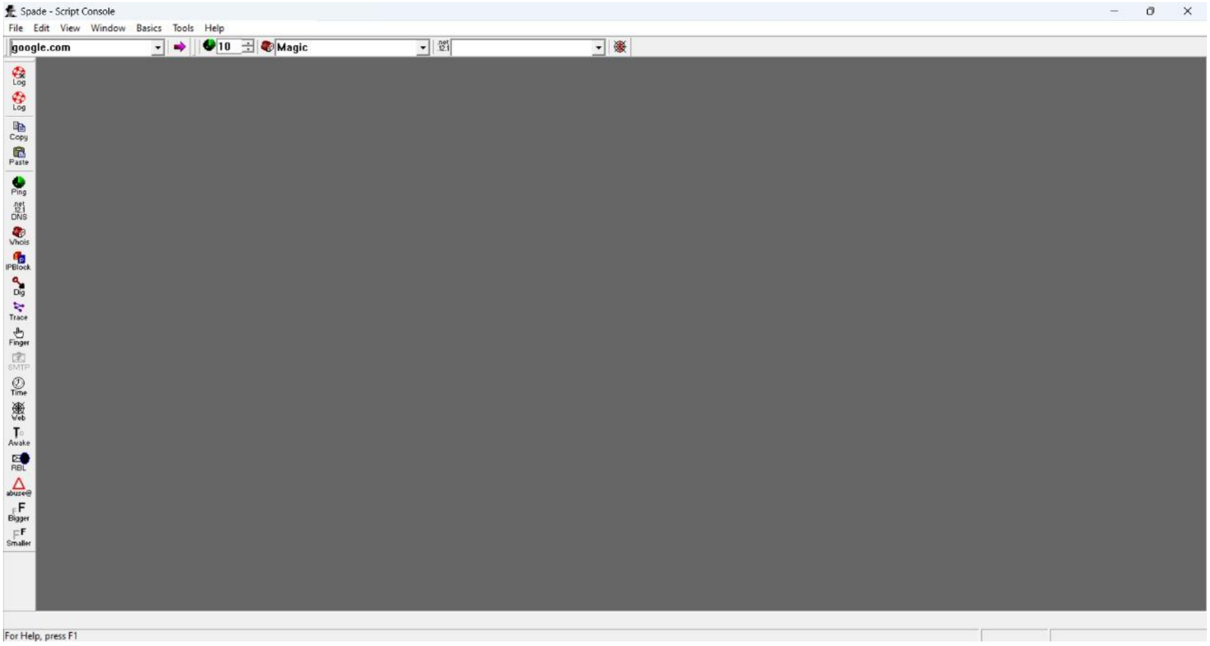
- To collect domain information and trace internet connections.
- To perform DNS queries and Whois lookups for identifying domain owners.
- To analyze spam or suspicious email origins.

Steps:

1. Open the SamSpade application.
2. Enter a domain name (for example, google.com) in the address bar.
3. Click on the desired operation such as Whois, Trace, or DNS.
4. The results will display information related to the selected operation.

Output:

The tool displays details like domain registrar, registration and expiry dates, DNS servers, and IP tracing information.

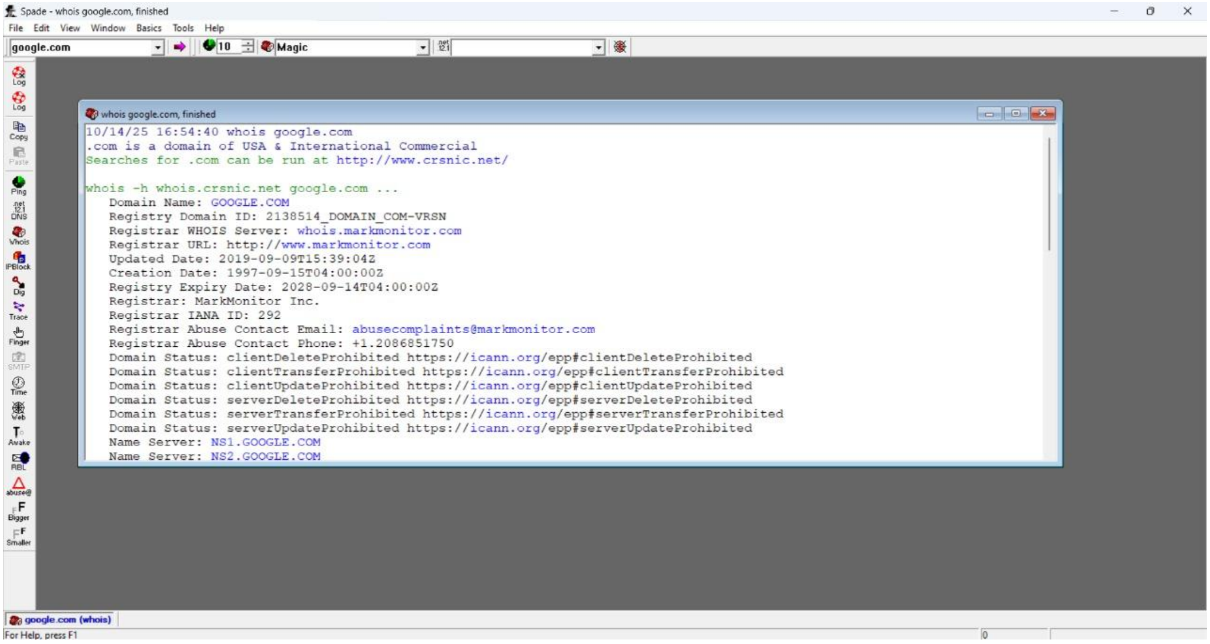


google.com

10

Magic

For Help, press F1



```
10/14/25 16:54:40 whois google.com
.com is a domain of USA & International Commercial
Searches for .com can be run at http://www.crsnic.net/

whois -h whois.crsnic.net 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
```

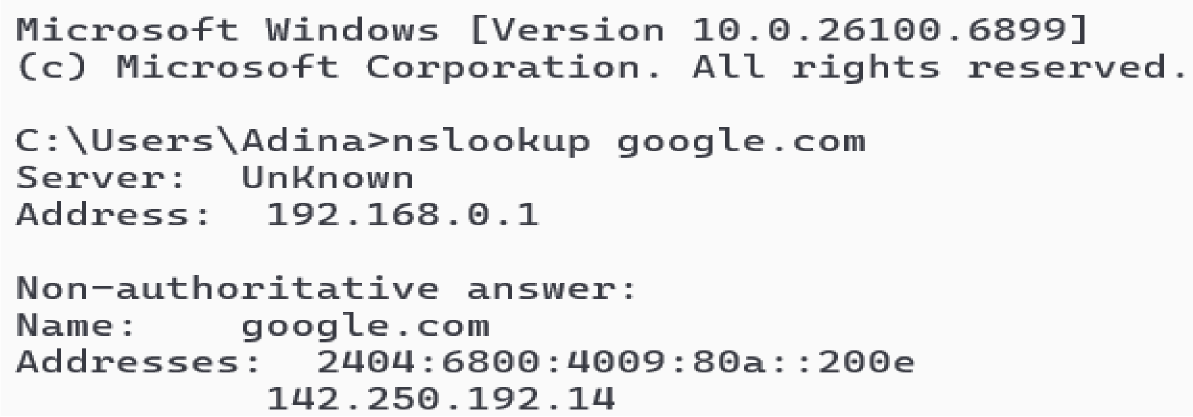
2. Nslookup

Theory:
Nslookup (Name Server Lookup) is a command-line tool used to query Domain Name System (DNS) servers to obtain domain name or IP address mappings. It helps network administrators verify DNS configurations and troubleshoot domain-related problems. The tool can be used in both interactive and non-interactive modes.

Purpose:

- To find the IP address corresponding to a domain name.
- To verify DNS records and detect DNS issues.

Command Syntax:
nslookup [domain name]



```
Microsoft Windows [Version 10.0.26100.6899]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Adina>nslookup google.com
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4009:80a::200e
          142.250.192.14
```

Result:
Displays the IP address and DNS server information of the specified domain.

3. Whois

Theory:
Whois is a network utility that retrieves domain registration details from a global database maintained by domain registrars. It provides information such as the domain owner’s name, organization, contact information, registration date, expiry date, and name servers. This tool is commonly used for domain verification and cyber investigation purposes.

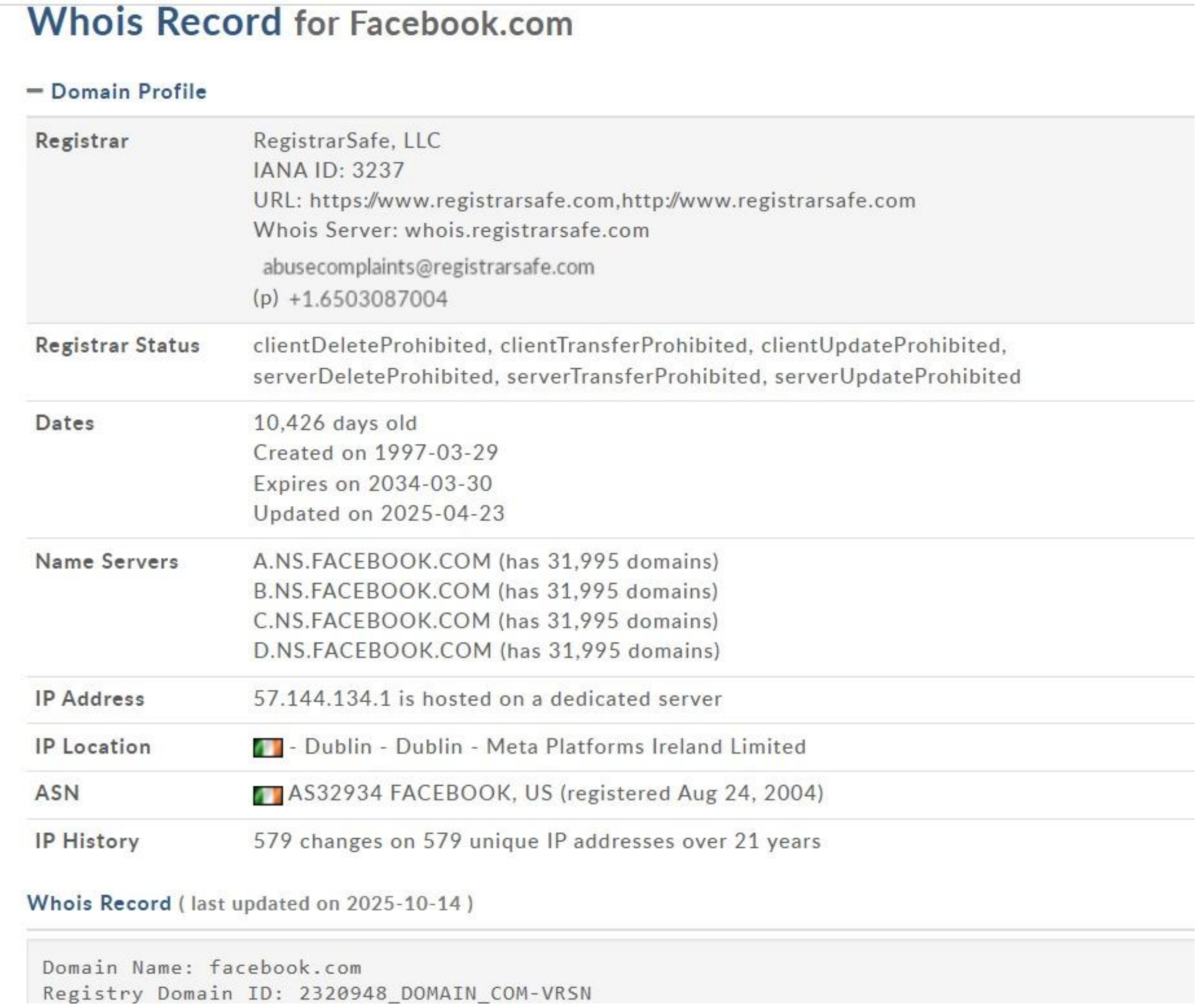
Purpose:

- To identify the registered owner and administrative details of a domain.
- To verify domain authenticity and detect potential fraudulent sites.

Command Syntax:

```
whois [domain name]
```

Result:
Displays registration details such as registrar, creation and expiry dates, and contact email of the domain owner.



Whois Record for Facebook.com

− Domain Profile

Registrar	RegistrarSafe, LLC IANA ID: 3237 URL: https://www.registrarsafe.com,http://www.registrarsafe.com Whois Server: whois.registrarsafe.com abusecomplaints@registrarsafe.com (p) +1.6503087004
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited
Dates	10,426 days old Created on 1997-03-29 Expires on 2034-03-30 Updated on 2025-04-23
Name Servers	A.NS.FACEBOOK.COM (has 31,995 domains) B.NS.FACEBOOK.COM (has 31,995 domains) C.NS.FACEBOOK.COM (has 31,995 domains) D.NS.FACEBOOK.COM (has 31,995 domains)
IP Address	57.144.134.1 is hosted on a dedicated server
IP Location	🇮🇪 - Dublin - Dublin - Meta Platforms Ireland Limited
ASN	🇮🇪 AS32934 FACEBOOK, US (registered Aug 24, 2004)
IP History	579 changes on 579 unique IP addresses over 21 years

Whois Record (last updated on 2025-10-14)

```
Domain Name: facebook.com
Registry Domain ID: 2320948_DOMAIN_COM-VRSN
```

4. Tracert

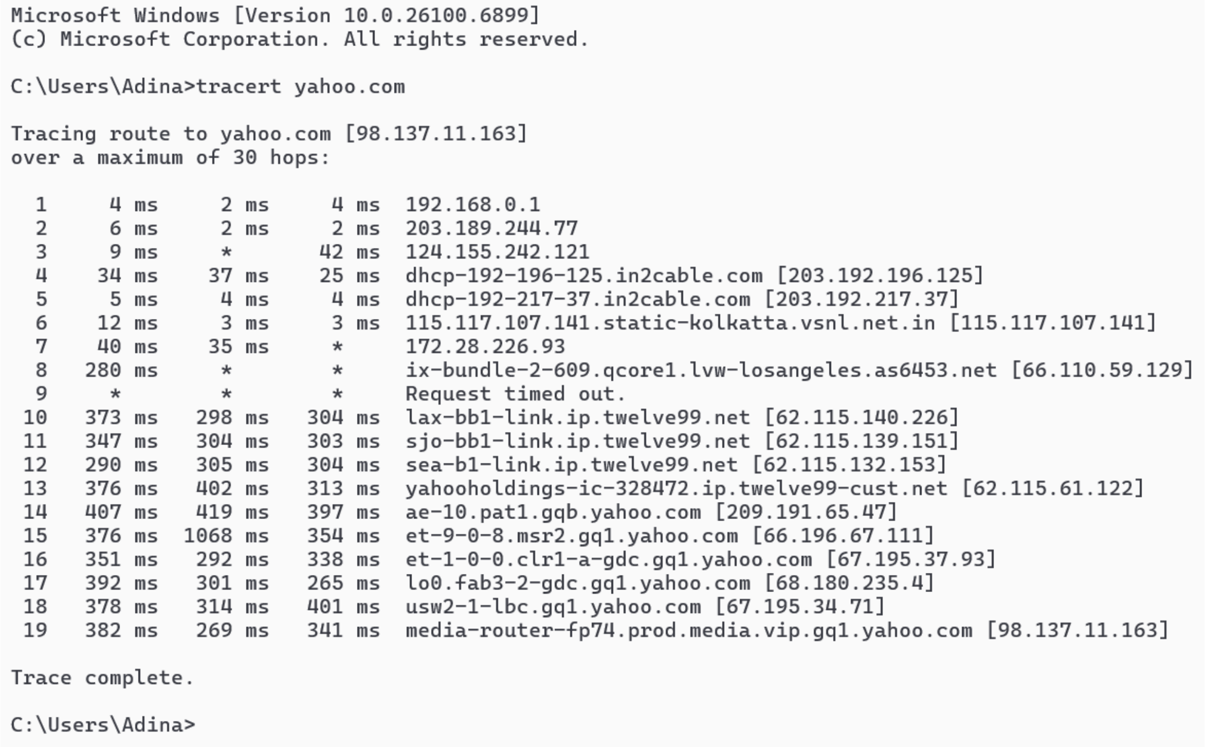
Theory:
Tracert (Trace Route) is a command-line utility used to track the route that data packets take from the local computer to a destination host. It helps identify each hop (router or gateway) along the path and measures the time it takes to reach each. This tool is useful for diagnosing network connectivity problems and locating where delays or failures occur.

Purpose:

- To trace the path packets take to reach a destination.
- To detect network delays or failures along the route.

Command Syntax:

tracert [domain name or IP address]
Result:
Displays each hop between the local system and the destination server along with the response time for each hop.



```
Microsoft Windows [Version 10.0.26100.6899]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Adina>tracert yahoo.com

Tracing route to yahoo.com [98.137.11.163]
over a maximum of 30 hops:

  1     4 ms     2 ms     4 ms  192.168.0.1
  2     6 ms     2 ms     2 ms  203.189.244.77
  3     9 ms     *       42 ms  124.155.242.121
  4    34 ms    37 ms    25 ms  dhcp-192-196-125.in2cable.com [203.192.196.125]
  5     5 ms     4 ms     4 ms  dhcp-192-217-37.in2cable.com [203.192.217.37]
  6    12 ms     3 ms     3 ms  115.117.107.141.static-kolkatta.vsnl.net.in [115.117.107.141]
  7    40 ms    35 ms     *     172.28.226.93
  8   280 ms     *        *     ix-bundle-2-609.qcore1.lvw-losangeles.as6453.net [66.110.59.129]
  9     *        *        *     Request timed out.
 10   373 ms   298 ms   304 ms  lax-bb1-link.ip.twelve99.net [62.115.140.226]
 11   347 ms   304 ms   303 ms  sjo-bb1-link.ip.twelve99.net [62.115.139.151]
 12   290 ms   305 ms   304 ms  sea-b1-link.ip.twelve99.net [62.115.132.153]
 13   376 ms   402 ms   313 ms  yahooholdings-ic-328472.ip.twelve99-cust.net [62.115.61.122]
 14   407 ms   419 ms   397 ms  ae-10.pat1.gqb.yahoo.com [209.191.65.47]
 15   376 ms  1068 ms   354 ms  et-9-0-8.msr2.gq1.yahoo.com [66.196.67.111]
 16   351 ms   292 ms   338 ms  et-1-0-0.clr1-a-gdc.gq1.yahoo.com [67.195.37.93]
 17   392 ms   301 ms   265 ms  lo0.fab3-2-gdc.gq1.yahoo.com [68.180.235.4]
 18   378 ms   314 ms   401 ms  usw2-1-lbc.gq1.yahoo.com [67.195.34.71]
 19   382 ms   269 ms   341 ms  media-router-fp74.prod.media.vip.gq1.yahoo.com [98.137.11.163]

Trace complete.

C:\Users\Adina>
```

Conclusion:
I have successfully demonstrated the use of SamSpade, Nslookup, Whois, and Tracert tools.