

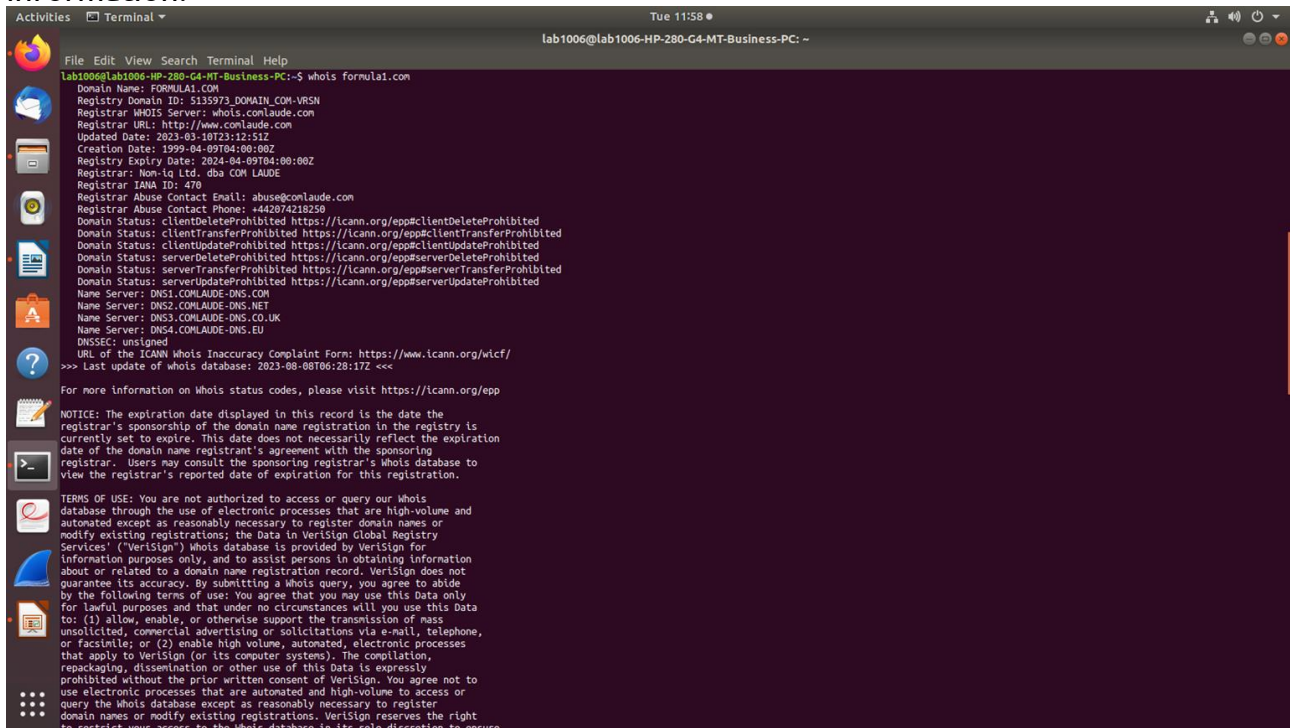
Assignment 6

Aim: To study the uses of network reconnaissance tools like whois, dig, traceroute, nslookup, nikto, dimtry to gather information about networks and domain registers.

Lo-mapped: LO-3

Theory:

1. whois: The whois command displays information about a website's record. You may get all the information about a website regarding its registration and owner's information.



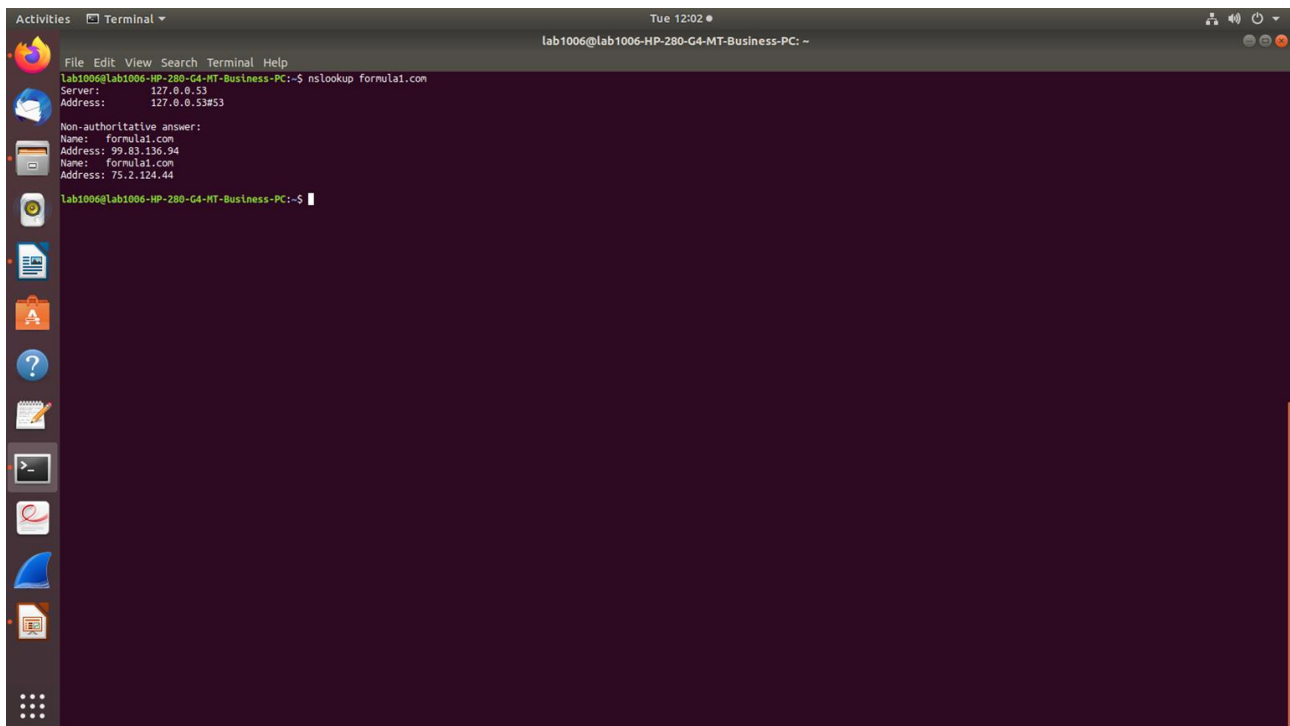
```
Lab1006@Lab1006-HP-280-G4-MT-Business-PC:~$ whois formulai.com
Domain Name: FORMULAI.COM
Registry Domain ID: 5135973_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.conlaude.com
Registrar URL: http://www.conlaude.com
Updated Date: 2023-03-10T23:12:51Z
Creation Date: 1999-04-09T04:00:00Z
Registry Expiry Date: 2024-04-09T04:00:00Z
Registrar: Non-ig Ltd. dba COM LAUDE
Registrar IANA ID: 476
Registrar Abuse Contact Email: abuse@conlaude.com
Registrar Abuse Contact Phone: +442074218250
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: DNS1.COMLAUDE-DNS.COM
Name Server: DNS3.COMLAUDE-DNS.CO.UK
Name Server: DNS4.COMLAUDE-DNS.EU
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-08-08T06:28:17Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
```

2. nslookup: (stands for “Name Server Lookup”) is a useful command for getting information from the DNS server. It is a network administration tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or any other specific DNS record. It is also used to troubleshoot DNS-related problems.

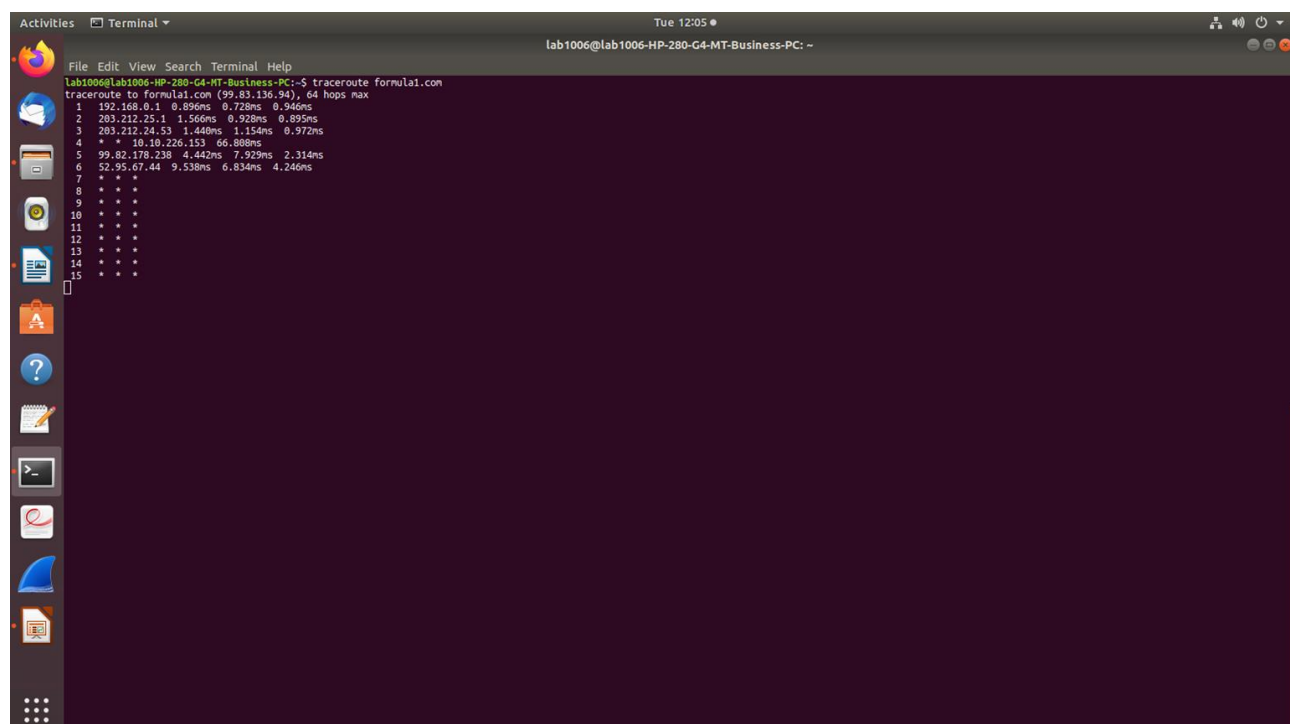


```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nslookup formula1.com
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   formula1.com
Address: 99.83.136.94
Name:   formula1.com
Address: 75.2.124.44

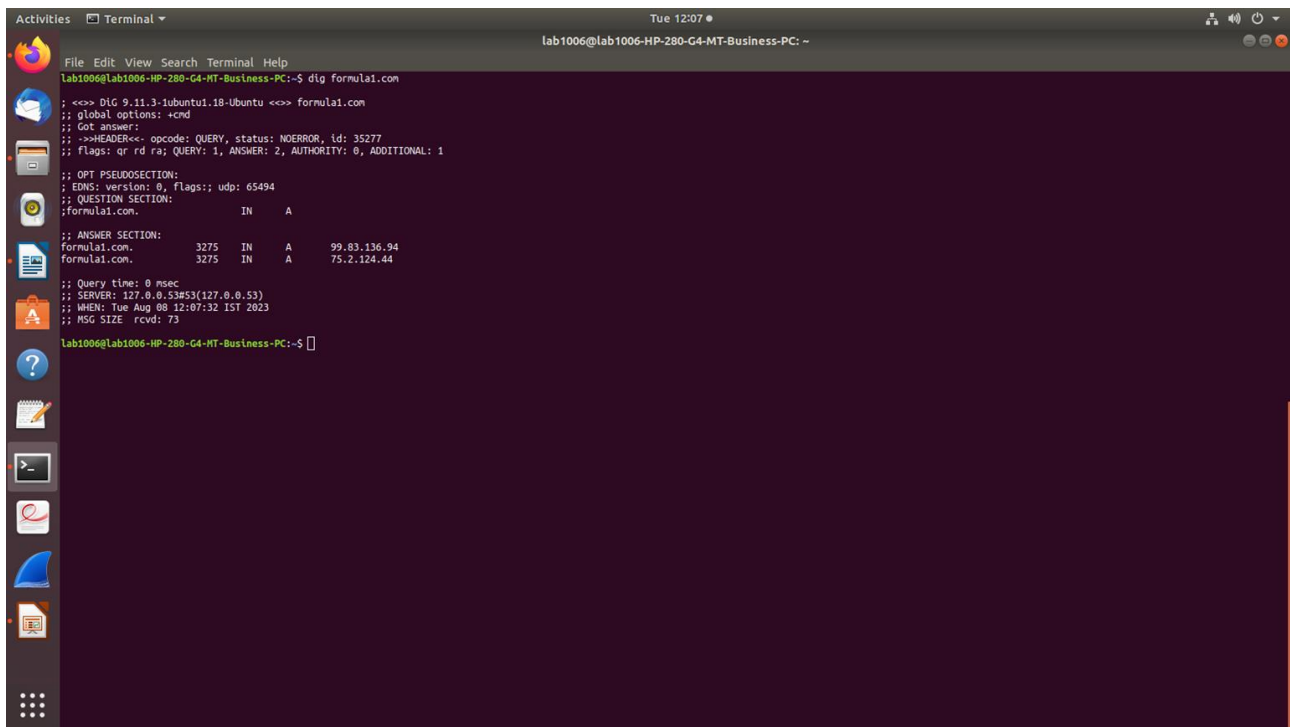
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

3. traceroute: traceroute command is a network troubleshooting utility that helps us determine the number of hops and packets traveling path required to reach a destination. It is used to display how the data transmitted from a local machine to a remote machine. Loading a web page is one of the common examples of the traceroute. A web page loading transfers data through a network and routers. The traceroute can display the routes, IP addresses, and hostnames of routers over a network. It can be useful for diagnosing network issues.



```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ traceroute formula1.com
traceroute to formula1.com (99.83.136.94), 64 hops max
 1  192.168.0.1  0.896ms  0.728ms  0.946ms
 2  283.212.25.1  1.566ms  0.928ms  0.895ms
 3  283.212.24.53  1.448ms  1.154ms  0.972ms
 4  * * 10.10.226.153  66.888ms
 5  99.82.178.238  4.442ms  7.929ms  2.314ms
 6  52.95.67.44  9.538ms  6.834ms  4.246ms
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
```

4. dig: Linux dig command stands for **Domain Information Groper**. This command is used for tasks related to DNS lookup to query DNS name servers. It mainly deals with troubleshooting DNS related problems. It is a flexible utility for examining the DNS (Domain Name Servers). It is used to perform the DNS lookups and returns the queried answers from the name server. Usually, it is used by most DNS administrators to troubleshoot the DNS problems. It is a straightforward tool and provides a clear output. It is more functional than other lookups tools.



```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ dig formula1.com

;<<<> DIG 9.11.3-1ubuntu1.18-Ubuntu <<<> formula1.com
;; global options: +cmd
;; Got answer:
;;->HEADER<- opcode: QUERY, status: NOERROR, id: 35277
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 65494
;; QUESTION SECTION:
;formula1.com.                IN      A

;; ANSWER SECTION:
formula1.com.                3275    IN      A      99.83.136.94
formula1.com.                3275    IN      A      75.2.124.44

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Tue Aug 08 12:07:32 IST 2023
;; MSG SIZE rcvd: 73

lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

5. Nikto is an Open Source software written in Perl language that is used to scan a web-server for the vulnerability that can be exploited and can compromise the server. It can also check for outdated version details of 1200 server and can detect problems with specific version details of over 200 servers. It can also fingerprint server using favicon.ico files present in the server. It is not designed to be a particularly a stealth tool rather than it is designed to be fast and time-efficient to achieve the task in very little time. Because of this, a web admin can easily detect that its server is being scanned by looking into the log files.

It can also show some items that do not have security problem but are info only which shows how to take full use of it to secure the web-server more properly.

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ dig formulal.com
; <<> DLG 9.11.3-1ubuntu1.18-Ubuntu <<> formulal.com
;; global options: +cmd
;; Got answer:
;;->HEADER<<- opcode: QUERY, status: NOERROR, id: 35277
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 65494
;; QUESTION SECTION:
;; formulal.com.                IN      A
;; ANSWER SECTION:
formulal.com.      3275    IN      A      99.83.136.94
formulal.com.      3275    IN      A      75.2.124.44
;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Tue Aug 08 12:07:32 IST 2023
;; MSG SIZE rcvd: 73

lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nikto -h tsec.edu
- Nikto v2.1.5
+-----+
+ Target IP:      162.241.70.62
+ Target Hostname: tsec.edu
+ Target Port:    80
+ Start Time:     2023-08-08 12:08:28 (GMT+5.5)
+-----+
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ Root page / redirects to: https://tsec.edu/
+-----+
```

6. dmitry: Dmitry stands for **DeepMagic Information Gathering Tool**. Dmitry is a **free** and **open-source** tool that is available on **GitHub**. We used this tool for information gathering. Dmitry is a **command-line** tool. With the help of the Dmitry tool, we can gather information about the target, which we can then use for **social engineering attacks**. It can be used to collect a variety of useful information.

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ dmitry formulal.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:99.83.136.94
HostName:formulal.com

Gathered Inet-whois information for 99.83.136.94
-----
inetnum:          98.158.238.0 - 101.55.255.255
netname:          NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:            IPv4 address block not managed by the RIPE NCC
remarks:          -----
remarks:          For registration information,
remarks:          you can consult the following sources:
remarks:          IANA
remarks:          http://www.iana.org/assignments/ipv4-address-space
remarks:          http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:          http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:          AFRINIC (Africa)
remarks:          http://www.afrinic.net/ whois.afrinic.net
remarks:          APNIC (Asia Pacific)
remarks:          http://www.apnic.net/ whois.apnic.net
remarks:          ARIN (Northern America)
remarks:          http://www.arin.net/ whois.arin.net
remarks:          LACNIC (Latin America and the Caribbean)
remarks:          http://www.lacnic.net/ whois.lacnic.net
remarks:          -----
remarks:          EU # Country is really world wide
country:          IANA1-RIPE
admin-c:          IANA1-RIPE
tech-c:           IANA1-RIPE
status:           ALLOCATED UNSPECIFIED
mnt-by:           RIPE-NCC-HM-MNT
created:          2021-03-29T13:41:55Z
last-modified:    2021-03-29T13:41:55Z
source:           RIPE

role:             Internet Assigned Numbers Authority
address:          see http://www.iana.org.
admin-c:          IANA1-RIPE
tech-c:           IANA1-RIPE
nic-hdl:          IANA1-RIPE
remarks:          For more information on IANA services
remarks:          go to IANA web site at http://www.iana.org.
mnt-by:           RIPE-NCC-MNT
created:          1978-01-01T00:00:00Z
last-modified:    2001-06-27T00:31:27Z
```

```
Activities Terminal Tue 12:10 lab1006@lab1006-HP-280-G4-MT-Business-PC: -
File Edit View Search Terminal Help

Gathered Inic-whois information for formulai.com
-----
Domain Name: FORMULAI.COM
Registry Domain ID: S135973 DOMAIN.COM-VRSN
Registrar WHOIS Server: whois.conlaude.com
Registrar URL: http://www.conlaude.com
Updated Date: 2023-03-10T03:12:51Z
Creation Date: 1999-04-09T04:00:00Z
Registry Expiry Date: 2024-04-09T04:00:00Z
Registrar: Non-ig Ltd. dba COM LAUDE
Registrar IANA ID: 470
Registrar Abuse Contact Email: abuse@conlaude.com
Registrar Abuse Contact Phone: +442074218250
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: DNS1.COMLAUDE-DNS.COM
Name Server: DNS2.COMLAUDE-DNS.NET
Name Server: DNS3.COMLAUDE-DNS.CO.UK
Name Server: DNS4.COMLAUDE-DNS.EU
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-08-08T06:39:54Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data to:
(1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability. VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.

Gathered Netcraft information for formulai.com
-----
Retrieving Netcraft.com information for formulai.com
Netcraft.com Information gathered

Gathered Subdomain information for formulai.com
-----
Searching Google.com:80...
HostName:www.formulai.com
HostIP:108.159.61.125
HostName:account.formulai.com
HostIP:108.158.61.61
HostName:fitv.formulai.com
HostIP:108.158.46.80
HostName:tickets.formulai.com
HostIP:104.18.11.147
HostName:corp.formulai.com
HostIP:18.66.41.45
HostName:fistore.formulai.com
HostIP:23.46.9.9
HostName:fantasy.formulai.com
HostIP:18.66.41.6
HostName:fistore4.formulai.com
HostIP:23.46.9.48
Searching Altavista.com:80...
Found 8 possible subdomain(s) for host formulai.com, Searched 0 pages containing 0 results

Gathered E-Mail information for formulai.com
-----
Searching Google.com:80...
Searching Altavista.com:80...
Found 0 E-Mail(s) for host formulai.com, Searched 0 pages containing 0 results

Gathered TCP Port information for 99.83.136.94
-----
Port State
```

```
Activities Terminal Tue 12:10 lab1006@lab1006-HP-280-G4-MT-Business-PC: -
File Edit View Search Terminal Help

that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability. VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.

Gathered Netcraft information for formulai.com
-----
Retrieving Netcraft.com information for formulai.com
Netcraft.com Information gathered

Gathered Subdomain information for formulai.com
-----
Searching Google.com:80...
HostName:www.formulai.com
HostIP:108.159.61.125
HostName:account.formulai.com
HostIP:108.158.61.61
HostName:fitv.formulai.com
HostIP:108.158.46.80
HostName:tickets.formulai.com
HostIP:104.18.11.147
HostName:corp.formulai.com
HostIP:18.66.41.45
HostName:fistore.formulai.com
HostIP:23.46.9.9
HostName:fantasy.formulai.com
HostIP:18.66.41.6
HostName:fistore4.formulai.com
HostIP:23.46.9.48
Searching Altavista.com:80...
Found 8 possible subdomain(s) for host formulai.com, Searched 0 pages containing 0 results

Gathered E-Mail information for formulai.com
-----
Searching Google.com:80...
Searching Altavista.com:80...
Found 0 E-Mail(s) for host formulai.com, Searched 0 pages containing 0 results

Gathered TCP Port information for 99.83.136.94
-----
Port State
```

Conclusion: In this assignment we performed various network tools and implemented the same commands.