

Data Gathering and Footprinting on a Targeted Web Site

Section 1: Hands-On Demonstration

Part 1: Technical Research

1. Whois Query (Sam Spade)
5. Make a screen capture showing the Whois results with the date and time of the search and paste it into your Lab Report file.



```
whois.apple.com,finished
02/16/25 18:22:59 whois apple.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 apple.com ...
Domain Name: APPLE.COM
Registry Domain ID: 1225976_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.comlaude.com
Registrar URL: http://www.comlaude.com
Updated Date: 2025-01-21T23:06:01Z
Creation Date: 1987-02-19T05:00:00Z
Registry Expiry Date: 2026-02-20T05:00:00Z
Registrar: Nom-iq Ltd. dba COM LAUDE
Registrar IANA ID: 470
Registrar Abuse Contact Email: abuse@comlaude.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: A.NS.APPLE.COM
Name Server: B.NS.APPLE.COM
Name Server: C.NS.APPLE.COM
Name Server: D.NS.APPLE.COM
DNSSEC: unsigned
```

9. Make a screen capture showing the ping results and paste it into your Lab Report file.

```
ping apple.com, finished
02/16/25 18:26:16 ping apple.com
Ping apple.com (17.253.144.10) ...
 1 Addr:17.253.144.10, RTT: 1ms, TTL: 54
 2 Addr:17.253.144.10, RTT: 1ms, TTL: 54
 3 Addr:17.253.144.10, RTT: 1ms, TTL: 54
 4 Addr:17.253.144.10, RTT: 1ms, TTL: 54
 5 Addr:17.253.144.10, RTT: 1ms, TTL: 54
 6 Addr:17.253.144.10, RTT: 2ms, TTL: 54
 7 Addr:17.253.144.10, RTT: 1ms, TTL: 54
 8 Addr:17.253.144.10, RTT: 2ms, TTL: 54
 9 Addr:17.253.144.10, RTT: 1ms, TTL: 54
10 Addr:17.253.144.10, RTT: 1ms, TTL: 54
```

13. Repeat steps 3-12 for the following domains:

Microsoft.com

```
whois microsoft.com, finished
02/16/25 18:27:55 whois microsoft.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 microsoft.com ...
Domain Name: MICROSOFT.COM
Registry Domain ID: 2724960_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2023-08-18T16:15:54Z
Creation Date: 1991-05-02T04:00:00Z
Registry Expiry Date: 2025-05-03T04:00:00Z
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: NS1-39.AZURE-DNS.COM
Name Server: NS2-39.AZURE-DNS.NET
Name Server: NS3-39.AZURE-DNS.ORG
Name Server: NS4-39.AZURE-DNS.INFO
DNSSEC: unsigned
```

ping microsoft.com, finished

```
02/16/25 18:27:59 ping microsoft.com
Ping microsoft.com (20.112.250.133) ...
1 Addr:20.112.250.133, RTT: 34ms, TTL: 106
2 Addr:20.112.250.133, RTT: 34ms, TTL: 106
3 Addr:20.112.250.133, RTT: 34ms, TTL: 106
4 Addr:20.112.250.133, RTT: 34ms, TTL: 106
5 Addr:20.112.250.133, RTT: 35ms, TTL: 106
6 Addr:20.112.250.133, RTT: 35ms, TTL: 106
7 Addr:20.112.250.133, RTT: 35ms, TTL: 106
8 Addr:20.112.250.133, RTT: 34ms, TTL: 106
9 Addr:20.112.250.133, RTT: 34ms, TTL: 106
10 Addr:20.112.250.133, RTT: 35ms, TTL: 106
```

Facebook.com

whois facebook.com, finished

```
02/16/25 18:28:46 whois facebook.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 facebook.com ...
Domain Name: FACEBOOK.COM
Registry Domain ID: 2320948_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrarsafe.com
Registrar URL: http://www.registrarsafe.com
Updated Date: 2024-04-24T19:06:12Z
Creation Date: 1997-03-29T05:00:00Z
Registry Expiry Date: 2033-03-30T04:00:00Z
Registrar: RegistrarSafe, LLC
Registrar IANA ID: 3237
Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
Registrar Abuse Contact Phone: +1-650-308-7004
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: A.NS.FACEBOOK.COM
Name Server: B.NS.FACEBOOK.COM
Name Server: C.NS.FACEBOOK.COM
Name Server: D.NS.FACEBOOK.COM
DNSSEC: unsigned
```

```
ping facebook.com, finished
02/16/25 18:28:50 ping facebook.com
Ping facebook.com (57.144.174.1) ...
1 Addr:57.144.174.1, RTT: 13ms, TTL: 51
2 Addr:57.144.174.1, RTT: 14ms, TTL: 51
3 Addr:57.144.174.1, RTT: 13ms, TTL: 51
4 Addr:57.144.174.1, RTT: 20ms, TTL: 51
5 Addr:57.144.174.1, RTT: 13ms, TTL: 51
6 Addr:57.144.174.1, RTT: 13ms, TTL: 51
7 Addr:57.144.174.1, RTT: 13ms, TTL: 51
8 Addr:57.144.174.1, RTT: 13ms, TTL: 51
9 Addr:57.144.174.1, RTT: 15ms, TTL: 51
10 Addr:57.144.174.1, RTT: 13ms, TTL: 51
```

2. Nslookup (Command Prompt)

18. Make a screen capture showing the nslookup results and paste it into your Lab Report file.

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nslookup apple.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: apple.com
Addresses: 2620:149:af0::10
           17.253.144.10
```

19. Repeat steps 17-18 for the following domains:

Microsoft.com

```
C:\Users\Administrator>nslookup microsoft.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: microsoft.com
Addresses: 2603:1030:b::152
           2603:1030:20e::23c
           2603:1010:3::5b
           2603:1030:c02:8::14
           2603:1020:201:10::10f
           20.76.201.171
           20.70.246.20
           20.236.44.162
           20.231.239.246
           20.112.250.133
```

Facebook.com

```
C:\Users\Administrator>nslookup facebook.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: facebook.com
Addresses: 2a03:2880:f357:1:face:b00c:0:25de
           57.144.174.1
```

3. Tracert (Command Prompt)

21. Make a screen capture showing the tracert results and paste it into your Lab Report file.

```
C:\Users\Administrator>tracert apple.com

Tracing route to apple.com [17.253.144.10]
over a maximum of 30 hops:

 1    <1 ms      <1 ms      <1 ms  192.168.80.254
 2      1 ms      <1 ms      <1 ms  172.18.249.250
 3      *        <1 ms      *        172.18.0.1
 4      1 ms      1 ms      1 ms  76.75.74.129
 5      *        *        *        Request timed out.
 6      1 ms      1 ms      1 ms  be2723.ccr31.yyz02.atlas.cogentco.com [154.54.165.177]
 7     21 ms     21 ms      2 ms  ae4.bar4.tor1.sp.lumen.tech [4.68.38.245]
 8      2 ms      1 ms      1 ms  apple-compu.bar4.toronto1.level3.net [4.1.113.206]
 9     13 ms     10 ms     18 ms  apple.com.ai [17.253.144.10]

Trace complete.
```

22. Repeat steps 20-21 for the following domains:

Microsoft.com

```

Tracing route to microsoft.com [20.236.44.162]
over a maximum of 30 hops:

 1  <1 ms    <1 ms    <1 ms  192.168.80.254
 2  1 ms    <1 ms    <1 ms  172.18.249.250
 3  *        *        <1 ms  172.18.0.1
 4  1 ms    1 ms    <1 ms  76.75.74.129
 5  *        *        *      Request timed out.
 6  2 ms    1 ms    1 ms  be4149.ccr32.yyz02.atlas.cogentco.com [154.54.165.181]
 7  2 ms    1 ms    1 ms  38.32.158.162
 8  9 ms    2 ms    1 ms  ae22-0.icr01.yto20.ntwk.msn.net [104.44.237.151]
 9  61 ms   61 ms   61 ms  be-120-0.ibr02.yto20.ntwk.msn.net [104.44.20.165]
10  61 ms   61 ms   61 ms  be-7-0.ibr02.cle02.ntwk.msn.net [104.44.29.105]
11  62 ms   137 ms  76 ms  be-3-0.ibr02.ch2.ntwk.msn.net [104.44.29.253]
12  61 ms   65 ms   61 ms  be-6-0.ibr02.dsm05.ntwk.msn.net [104.44.18.217]
13  68 ms   60 ms   61 ms  be-12-0.ibr02.jnb21.ntwk.msn.net [104.44.19.101]
14  61 ms   61 ms   62 ms  be-7-0.ibr02.mwh01.ntwk.msn.net [104.44.18.225]
15  60 ms   62 ms   66 ms  ae168-0.icr05.mwh01.ntwk.msn.net [104.44.32.233]
16  *        *        *      Request timed out.
17  *        *        *      Request timed out.
18  *        *        *      Request timed out.
19  *        *        *      Request timed out.
20  *        *        *      Request timed out.
21  60 ms   60 ms   60 ms  20.236.44.162

```

Trace complete.

Facebook.com

```

C:\Users\Administrator>tracert facebook.com

Tracing route to facebook.com [157.240.249.35]
over a maximum of 30 hops:

 1  <1 ms    <1 ms    <1 ms  192.168.80.254
 2  1 ms    <1 ms    <1 ms  172.18.249.251
 3  *        *        *      Request timed out.
 4  1 ms    1 ms    1 ms  76.75.74.129
 5  *        *        *      Request timed out.
 6  1 ms    2 ms    1 ms  be4149.ccr32.yyz02.atlas.cogentco.com [154.54.165.181]
 7  7 ms    6 ms    7 ms  be2994.ccr22.cle04.atlas.cogentco.com [154.54.31.233]
 8  13 ms   13 ms   13 ms  be2718.ccr42.ord01.atlas.cogentco.com [154.54.7.129]
 9  13 ms   13 ms   14 ms  be2766.ccr41.ord03.atlas.cogentco.com [154.54.46.178]
10  51 ms   14 ms   14 ms  38.32.97.34
11  13 ms   14 ms   13 ms  po208.asw03.ord5.tfbnw.net [129.134.53.186]
12  14 ms   13 ms   14 ms  psw03.ord5.tfbnw.net [129.134.82.164]
13  15 ms   17 ms   15 ms  mswiap.01.ord5.tfbnw.net [129.134.117.31]
14  13 ms   13 ms   13 ms  edge-star-mini-shv-01-ord5.facebook.com [157.240.249.35]

Trace complete.

```

Part 2: Public Domain Research

Using Google as your search engine, locate the following information about your target organization and record it in your Lab Report file. Use screen captures in your Lab Report file where necessary to illustrate your findings.

Name of the target organization - Walmart Inc.

Domain name and extension (domain.ext) for the target organization (for example, amazon.com) - walmart.com

URLs for the e-commerce website and any social networking sites -

E-commerce Website: <https://www.walmart.com>
Facebook: <https://www.facebook.com/walmart>
Twitter: <https://twitter.com/Walmart>
Instagram: <https://www.instagram.com/walmart>
LinkedIn: <https://www.linkedin.com/company/walmar>

Physical address of the main headquarters location used by the target company; use Google Maps to locate the building. - 702 SW 8th St, Bentonville, Arkansas, 72716-6209, USA



Names of officers (for example, CEO, president, and CIO) at the organization -

Chairman: Greg Penner

President and CEO: Doug McMillon

Number of employees at each major physical location - Approximately 2.1 million associates worldwide

Business partners or clients of the organization - Many suppliers and vendors from across the globe

Section 2: Applied Learning

Part 1: Technical Research

5. Resize and move the command prompt window and the Sam Spade window as necessary, then compare the data generated by both tools.

```
C:\Users\Administrator>whois walmart.com
WHOIS Server: whois.corporatedomains.com

Domain Name: walmart.com
Registry Domain ID: 269816_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2024-08-26T10:56:37Z
Creation Date: 1995-02-23T00:00:00Z
Registrar Registration Expiration Date: 2025-09-23T19:29:40Z
Registrar: CSC CORPORATE DOMAINS, INC.
Sponsoring Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: serverDeleteProhibited http://www.icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited http://www.icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited http://www.icann.org/epp#serverUpdateProhibited
Registry Registrant ID:
Registrant Name: Not Disclosed
Registrant Organization: Not Disclosed
Registrant Street: Not Disclosed
Registrant City: Bentonville
Registrant State/Province: AR
Registrant Postal Code: 72716-0520
Registrant Country: US
Registrant Phone: +Not Disclosed
Registrant Phone Ext:
Registrant Fax: +Not Disclosed
Registrant Fax Ext:
Registrant Email: Not Disclosed
Registry Admin ID:
Admin Name: Not Disclosed
Admin Organization: Not Disclosed
Admin Street: Not Disclosed
Admin City: Bentonville
Admin State/Province: AR
Admin Postal Code: 72716-0520
Admin Country: US
Admin Phone: +Not Disclosed
Admin Phone Ext:
Admin Email: Not Disclosed
Admin Fax: Not Disclosed
```

```
whois_walmart
02/16/25 19:07:46 whois walmart.com@crsnic

whois -h whois.crsnic.net walmart.com ...
Domain Name: WALMART.COM
Registry Domain ID: 269816_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: http://cscdbs.com
Updated Date: 2024-08-26T14:56:37Z
Creation Date: 1995-02-23T05:00:00Z
Registry Expiry Date: 2025-09-23T19:29:40Z
Registrar: CSC Corporate Domains, Inc.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: 8887802723
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
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: A1-185.AKAM.NET
Name Server: A10-66.AKAM.NET
Name Server: A22-67.AKAM.NET
Name Server: A3-64.AKAM.NET
Name Server: A5-65.AKAM.NET
Name Server: A8-66.AKAM.NET
Name Server: PDNSWM1.ULTRADNS.NET
Name Server: PDNSWM2.ULTRADNS.NET
Name Server: PDNSWM3.ULTRADNS.ORG
```

A main difference that I found in the command prompt version is that it does not include many nameserver details. The samsrade version shows multiple CDN and DNS nameserver details, showing their reliance on a CDN.

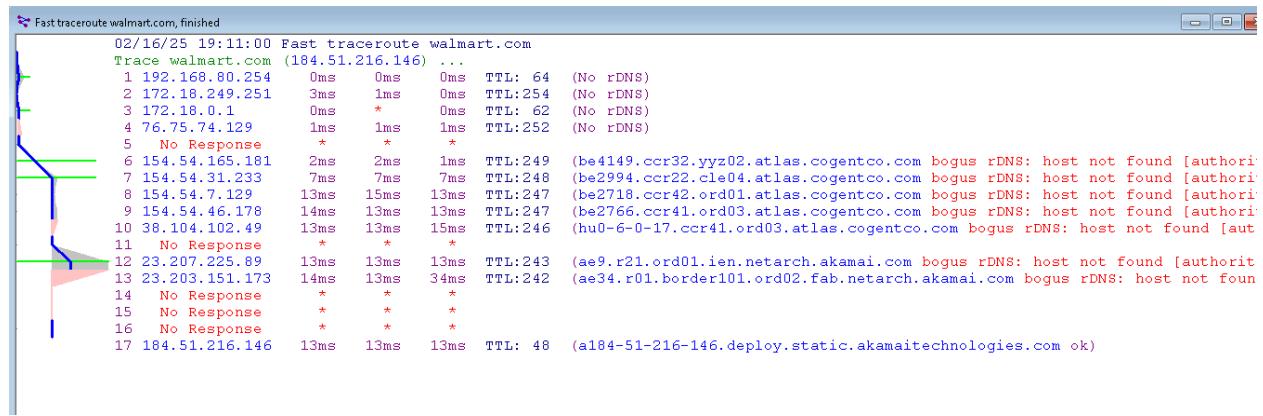
8. Resize and move the command prompt window and the Sam Spade window as necessary, then compare the data generated by both tools.

```
C:\Users\Administrator>tracert walmart.com

Tracing route to walmart.com [184.51.216.146]
over a maximum of 30 hops:

 1  <1 ms    <1 ms    <1 ms  192.168.80.254
 2  1 ms    <1 ms    <1 ms  172.18.249.251
 3  <1 ms    <1 ms    <1 ms  172.18.0.1
 4  2 ms     2 ms     2 ms  76.75.74.129
 5  *         *         * Request timed out.
 6  1 ms     1 ms     1 ms  be4149.ccr32.yyz02.atlas.cogentco.com [154.54.165.181]
 7  7 ms     7 ms     7 ms  be2994.ccr22.cle04.atlas.cogentco.com [154.54.31.233]
 8  37 ms    15 ms    13 ms  be2718.ccr42.ord01.atlas.cogentco.com [154.54.7.129]
 9  14 ms    13 ms    13 ms  be2766.ccr41.ord03.atlas.cogentco.com [154.54.46.178]
10  16 ms    16 ms    17 ms  hu0-6-0-17.ccr41.ord03.atlas.cogentco.com [38.104.102.49]
11  *         *         * Request timed out.
12  13 ms    13 ms    13 ms  ae9.r21.ord01.ien.netarch.akamai.com [23.207.225.89]
13  23 ms    14 ms    14 ms  ae34.r01.border101.ord02.fab.netarch.akamai.com [23.203.151.173]
14  *         *         * Request timed out.
15  *         *         * Request timed out.
16  *         *         * Request timed out.
17  13 ms    13 ms    13 ms  a184-51-216-146.deploy.static.akamaitechnologies.com [184.51.216.146]

Trace complete.
```



Samsrade tracert is much faster than the windows tracert but does not get as many details. We can tell that they are using some sort of firewall filtering since both tracerts had no response and request timed outs in their reports.

14. Resize and move the command prompt window and the Sam Spade window as necessary to compare the data generated by both tools.

```
>
C:\Users\Administrator>nslookup
Default Server: dns.google
Address: 8.8.8.8

> set type=any
> walmart.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
walmart.com      HINFO CPU = RFC8482> 184.51.216.146
Server: dns.google
Address: 8.8.8.8

Name: a184-51-216-146.deploy.static.akamaitechnologies.com
Address: 184.51.216.146

>
>
```

```
dig_walmart
02/16/25 19:29:46 dig walmart.com @ 9.9.9.9
Dig walmart.com@Pdnswm2.ultradns.net (156.154.65.4) ...
Authoritative Answer
Query for walmart.com type=255 class=1
walmart.com HINFO (Host Info) Cpu:RFC8482 Os:
walmart.com NS (Nameserver) Pdnswm5.ultradns.info
walmart.com NS (Nameserver) Pdnswm1.ultradns.net
walmart.com NS (Nameserver) Pdnswm6.ultradns.co.uk
walmart.com NS (Nameserver) Pdnswm2.ultradns.net
walmart.com NS (Nameserver) Pdnswm4.ultradns.org
walmart.com NS (Nameserver) a22-67.akam.net
walmart.com NS (Nameserver) a3-64.akam.net
walmart.com NS (Nameserver) a10-66.akam.net
walmart.com NS (Nameserver) a1-185.akam.net
walmart.com NS (Nameserver) a8-66.akam.net
walmart.com NS (Nameserver) a5-65.akam.net
walmart.com NS (Nameserver) Pdnswm3.ultradns.org
Dig walmart.com@a3-64.akam.net (96.7.49.64) ...
Authoritative Answer
Query for walmart.com type=255 class=1
walmart.com SOA (Zone of Authority)
Primary NS: pdns1.ultradns.net
Responsible person: hostmaster@walmart.com
serial:2024071121
refresh:3600s (60 minutes)
retry:3600s (60 minutes)
expire:604800s (7 days)
minimum-ttl:300s (5 minutes)
walmart.com NS (Nameserver) pdnswm1.ultradns.net
walmart.com NS (Nameserver) pdnswm3.ultradns.org
walmart.com NS (Nameserver) pdnswm5.ultradns.info
walmart.com NS (Nameserver) a22-67.akam.net
walmart.com NS (Nameserver) pdnswm2.ultradns.net
walmart.com NS (Nameserver) a3-64.akam.net
walmart.com NS (Nameserver) a5-65.akam.net
```

I relied on the traceroute IP instead of the nslookup one since it gave me 8.8.8.8 for walmart. Nsfocuses on IP resolution while the samspade dig tool went deeper into walmarths DNS infrastructure view.

17. In your Lab Report, record any useful technical information you gathered for your target domain in this part.

The start of authority data that I got seems important to see about walmarths DNS configuration.

```
> set type=soa
> walmart.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
walmart.com
    primary name server = pdns1.ultradns.net
    responsible mail addr = hostmaster.walmart.com
    serial   = 2024071121
    refresh  = 3600 (1 hour)
    retry    = 3600 (1 hour)
    expire   = 604800 (7 days)
    default TTL = 300 (5 mins)
>
```

Section 3: Lab Challenge and Analysis

Part 1: Analysis and Discussion

Research Sam Spade to discover more information about the tools it includes. Briefly describe the purpose and expected results for each tool found on the Basics and Tools menus of Sam Spade.

Basics Menu:

Ping – Checks network connectivity and response time for a target host.

Nslookup – Queries DNS records to obtain IP addresses and other domain information.

Whois – Finds domain registration details for ownership and expiration.

IP Block – Identifies the owner of a given IP range or subnet.

Dig – Performs a detailed DNS lookup, retrieving various domain records.

Traceroute – Maps the path that packets take to reach a target server, showing intermediate hops.

Finger – Attempts to retrieve user information from a remote system (if available).

SMTP Verify – Checks if an email address exists on a target mail server.

Time – Queries a time server to retrieve current network time information.

Blacklist – Checks whether a given IP address or domain is listed on known spam/security blacklists.

Abuse Lookup – Looks up abuse contact information for a given domain or IP, useful for reporting abuse or security concerns.

Tools Menu:

Zone Transfer – Attempts to retrieve an entire DNS zone file from a misconfigured DNS server.

SMTP Relay Check – Tests whether an email server allows open relaying.

Scan Addresses – Scans a range of IP addresses to identify active hosts.

Crawl Website – Analyzes a website's structure by following and mapping links.

Browse Web – A basic web browsing tool for interacting with a target website.

Check Cancels – Searches for canceled newsgroup messages.
Fast Traceroute – A quicker version of Traceroute, showing network hops.
Slow Traceroute – A more detailed, step by step traceroute analysis.
S-Lang Command – Allows execution of scripted commands for automation.
Decode URL – Decodes encoded URLs to reveal their original form.
Parse Email Headers – Analyzes email headers to trace the source of an email.

Part 2: Tools and Commands

How can you identify the physical location of an IP address? Identify the physical location of the servers for the three domains you explored in Section 1 of this lab: Apple.com, Microsoft.com, and Facebook.com.

I can use nslookup or dig to find the IP address of a domain then use online tools, something like <https://ipinfo.io/> to get the general address location of their server.

Apple.com - 204.26.57.1: Riverside, California, USA

Microsoft.com - 150.171.16.39: Redmond, Washington, USA

Facebook.com - 129.89.218.12: Milwaukee, Wisconsin, USA