Project 2: Network Reconnaissance
Domain Analysis: google.com

Ray Li

November 11, 2025

1 Domain: google.com (Commercial)

1.1 Domain Registration

Command: `whois google.com`

(a) **Official registrant:** Google LLC. The domain is registered openly (not privately or by proxy).

(b) **Contact information:**

- Phone number: +1.2086851750 (Registrar abuse contact via MarkMonitor Inc.)
- Physical address: Not provided in whois output
- Email: Contact forms available through `https://domains.markmonitor.com/whois/google.com`
- Registrar: MarkMonitor Inc. (Registrar IANA ID: 292)

(c) **Domain dates:**

- Creation Date: September 15, 1997
- Expiry Date: September 14, 2028
- Domain age: Approximately 28 years old

1.2 DNS Analysis

Commands: `dig www.google.com A`, `dig google.com MX`, `dig google.com NS`

(a) **IP Address:** 142.250.65.228 (IPv4) and 2607:f8b0:4006:817::2004 (IPv6)

(b) **Geolocation:** [REQUIRES ACCESS: Browser access to `http://iplocation.net`]

- Geolocation lookup not completed - requires web browser access

(c) **DNS Records returned:**

- A record: 142.250.65.228
- AAAA record: 2607:f8b0:4006:817::2004
- NS records: ns1.google.com, ns2.google.com, ns3.google.com, ns4.google.com

- SOA record: Primary nameserver ns1.google.com, admin email dns-admin.google.com

(d) **Mail server:** Yes, google.com has MX record pointing to smtp.google.com (priority 10)

(e) **DNSSEC support:** unsigned (from whois output)

1.3 IP Routing

Command: `traceroute www.google.com`

(a) **Number of hops:** Approximately 12 hops from my location

(b) **Route consistency:** No, packets took different routes. At hop 10, three different IP addresses were observed (142.251.65.108, 216.239.43.62, 142.250.46.190), indicating load balancing or multiple paths.

(c) **Identifiable routers:** 9 out of 12 hops were identifiable. Hops 6, 7, and 9 showed asterisks (*), indicating routers that did not respond to ICMP probes.

(d) **Last identifiable router geolocation:**

- IP: 209.85.255.52 or 142.250.81.228 (last hop)
- Hostname: lga25s74-in-f4.1e100.net
- [REQUIRES ACCESS: Browser access to `http://iplocation.net`] Geolocation lookup not completed

1.4 TCP Port Scanning

Command: `nmap www.google.com`

[REQUIRES ACCESS: nmap command-line tool not installed]

(a) Port scan results not available - nmap tool required for installation

1.5 PKI Certificate Analysis

Command: `openssl s_client -connect www.google.com:443 -servername www.google.com`

(a) **Cipher suite:** TLS_AES_256_GCM_SHA384 (TLS 1.3)

(b) **Public key:**

- Type: Elliptic Curve (EC)
- Curve: P-256 (prime256v1)
- Size: 256 bits

(c) **Certificate validity:**

- Valid from: October 13, 2025 08:39:42 GMT
- Valid until: January 5, 2026 08:39:41 GMT
- Validity period: Approximately 84 days (about 3 months)

(d) **Root Certificate Authority:**

- Root CA: GlobalSign Root CA (C=BE, O=GlobalSign nv-sa, OU=Root CA, CN=GlobalSign Root CA)
- Intermediate CAs in chain:
  - GTS Root R1 (C=US, O=Google Trust Services LLC, CN=GTS Root R1)
  - WR2 (C=US, O=Google Trust Services, CN=WR2)
- Root CA key type and expiration date: Requires extracting and examining root certificate details

(e) **Other domains:** Only www.google.com is listed in the Subject Alternative Names (SAN) field.

(f) **Intermediate certificates:** 2 intermediate certificates in the chain:

- Certificate 1: WR2 (Google Trust Services)
- Certificate 2: GTS Root R1 (Google Trust Services LLC)

(g) **Extended Validation (EV):** No, this is a standard Domain Validated (DV) certificate (indicated by policy 2.23.140.1.2.1)

(h) **Certificate revocation:**

- OCSP responder: Yes, `http://o.pki.goog/wr2`
- CRL distribution point: Yes, `http://c.pki.goog/wr2/oQ6nyr8F0m0.crl`

(i) **Certificate Transparency:**

- SCTs embedded: 2 Signed Certificate Timestamps found in certificate
- First logged: October 13, 2025 09:39:43 GMT (Log ID: 96:97:64:BF:...)
- Second logged: October 13, 2025 09:39:43 GMT (Log ID: 16:83:2D:AB:...)
- [REQUIRES ACCESS: Browser access to `https://crt.sh`] Total CT log count not retrieved

1.6 TLS Configuration

Reference: Qualys SSL Labs (`https://www.ssllabs.com/ssltest/`)

[REQUIRES ACCESS: Browser access to SSL Labs required for complete analysis]

Partial analysis from openssl testing:

(a) **TLS/SSL versions supported:**

- TLS 1.3: Confirmed supported (Protocol: TLSv1.3)
- Complete version support list: Requires SSL Labs full report

(b) **Most-preferred cipher suite:**

- Negotiated cipher: TLS_AES_256_GCM_SHA384
- Forward secrecy: Yes (TLS 1.3 provides forward secrecy)

- Server's most-preferred cipher (vs. what was negotiated): Requires SSL Labs report

(c) **Client compatibility:** Requires SSL Labs client simulation results

(d) **HSTS support:** Requires HTTP header inspection or SSL Labs report

(e) **SSL Labs grade:** Requires accessing SSL Labs report

1.7 Tor and VPN Analysis

[REQUIRES ACCESS: NYU VPN client, Tor Browser, and browser access to `https://2ip.io/`]

(a) **Normal connection (no VPN/Tor):**

- IP address: Requires browser access to 2ip.io
- Geolocation: Requires browser access to 2ip.io
- Reverse DNS: Requires DNS lookup tool

(b) **Via NYU VPN and Tor:**

- NYU VPN IP: Requires NYU VPN client installation and connection
- Tor IP: Requires Tor Browser installation

(c) **Tor exit node details:**

- [REQUIRES ACCESS: Tor Browser and access to `https://metrics.torproject.org/rs.html`]
- Nickname: Requires Tor connection and relay search
- Uptime: Requires Tor connection and relay search
- Bandwidth: Requires Tor connection and relay search
- Flags: Requires Tor connection and relay search

(d) **Access via VPN/Tor:**

- Access testing: Requires NYU VPN and Tor Browser
- Rendering differences: Requires testing with both connections

2 Summary

2.1 Key Findings for google.com

Verified findings:

- **Domain maturity:** Domain created September 15, 1997 (28 years old), registered to Google LLC, expires September 14, 2028
- **DNS Infrastructure:**
  - Four nameservers: ns1.google.com, ns2.google.com, ns3.google.com, ns4.google.com
  - Mail server: smtp.google.com (priority 10)

- IPv4 and IPv6 support confirmed (A and AAAA records present)
- DNSSEC: unsigned

- **Network routing:** 12 hops observed, with load balancing evident (multiple IPs at hop 10)
- **Certificate details:**
  - Public key: EC P-256 (256-bit)
  - Validity: 84 days (Oct 13, 2025 to Jan 5, 2026)
  - Issuer chain: WR2 (Google Trust Services) → GTS Root R1 → GlobalSign Root CA
  - Certificate Transparency: 2 SCTs embedded
  - Revocation: OCSP and CRL distribution point present
  - Not an Extended Validation certificate
- **TLS support:** TLS 1.3 confirmed with TLS_AES_256_GCM_SHA384 cipher

Analysis limitations:

- Complete TLS version support and preferred ciphers require SSL Labs
- Port scanning requires nmap installation
- Geolocation requires browser access to iplocation.net
- VPN and Tor analysis require client software installation