Name: Shreya Jakhar Choudhary (sc8941)

Domains: netflix.com, eff.org, and india.gov.in.

SECTION 1 Domain Registration

1. **First, lookup the official ownership information for this domain: whois example.com**

    a. Who is the official registrant? Is it registered openly, privately, or by proxy?
    - netflix.com
        - Official Registrant: Netflix, Inc.
        - The registrant information is openly available and not registered privately or by proxy.
    - eff.org
        - Official Registrant: Electronic Frontier Foundation
        - The registrant information is partially redacted for privacy, indicating the use of privacy protection services.
    - india.gov.in
        - Official Registrant: National Informatics Centre
        - The registrant information is partially redacted, which is common for government domains to protect privacy.

    b. Do they provide a phone number? A physical address? Are these plausible?
    - netflix.com
        - Phone Number: Not publicly listed.
        - Physical Address: Not publicly listed.
        - Plausibility: The address corresponds to Netflix's headquarters, confirming its authenticity.
    - eff.org
        - Phone Number: Not publicly listed.
        - Physical Address: Not publicly listed.
        - Plausibility: While specific contact details are redacted for privacy, the registrant organization is accurately identified.
    - india.gov.in
        - Phone Number: Not publicly listed.
        - Physical Address: Not publicly listed.
        - Plausibility: The registrant is a recognized government body, confirming the legitimacy of the registration.

    All of them have the Registrar Abuse email and phone number.

    c. When was the domain created, and when is it registered until?
    - netflix.com
        - Creation Date: November 11, 1997.
        - Expiration Date: November 10, 2025.
    - eff.org
        - Creation Date: October 10, 1990.
        - Expiration Date: October 9, 2025.

- india.gov.in
    - Creation Date: September 26, 2005.
    - Expiration Date: September 26, 2025.

SECTION 2 DNS

2. Resolve this domain's IP address using DNS: dig +trace www.example.com ANY.

a. What is the domain's IP address?
- netflix.com
    - 18.189.65.196
    - 3.12.3.40
    - 3.137.95.47
- eff.org
    - 199.232.88.201
- india.gov.in
    - 23.200.3.235
    - 23.200.3.233

b. Querying this domain's IP address using iplocation.net, what city, latitude and longitude do you get?
- netflix.com
    - All the IP addresses had following location:
        - City: Columbus
        - Latitude: 39.9614
        - Longitude: -82.9977
- eff.org
    - All the IP addresses had following location:
        - City: Newark
        - Latitude: 40.7323
        - Longitude: -74.1736
- india.gov.in
    - All the IP addresses had following location:
        - City: Edison
        - Latitude: 40.5187
        - Longitude: -74.4121

c. Which records are returned, besides A records?
- netflix.com
    - NS, CNAME
- eff.org
    - NS, CNAME
- india.gov.in
    - NS, CNAME

d. Does the domain have a mail server?
- netflix.com
    - Yes, Netflix has mail servers, and they rely on Google's email infrastructure.
- eff.org

    - Yes, eff.org has mail servers, eff-org.mail.protection.outlook.com (Microsoft Outlook infrastructure) and mail2.eff.org.
- india.gov.in
    - Yes, there is an MX record pointing to mailgw.nic.in.

e. Does it support DNSSEC?
- netflix.com
    - No
- eff.org
    - No
- india.gov.in
    - No

SECTION 3 IP Routing

3. Check your IP path to this domain: traceroute www.example.com

a. How many hops does the connection have?
- netflix.com
    - Count: 64
- eff.org
    - Count: 64
- india.gov.in
    - Count: 9

b. How many could not be identified (likely internal data center hops)?
- netflix.com
    - Count: 57
- eff.org
    - Count: 60
- india.gov.in
    - Count: 5

c. For the last identifiable router on the path-what geolocation is provided by iplocation.net?
- netflix.com
    - 108.166.248.8
    - City: Columbus
    - Latitude: 39.9614
    - Longitude: -82.9977
- eff.org
    - 140.222.19.111
    - City: Maimi
    - Latitude:25.7743
    - Longitude: -80.1936
- india.gov.in
    - 23.57.90.103
    - City: Secaucus
    - Latitude: 40.7967
    - Longitude: -74.0556

SECTION 4 TCP

4. Next, query for open ports at this domain: nmap www.example.com.

a. Which ports are open and which services do they represent?
- netflix.com
  - PORT STATE SERVICE
    53/tcp open domain
    80/tcp open http
    443/tcp open https
- eff.org
  - PORT STATE SERVICE
    53/tcp open domain
    80/tcp open http
    443/tcp open https
- india.gov.in
  - PORT STATE SERVICE
    53/tcp open domain
    80/tcp open http
    443/tcp open https

SECTION 5 PKI

5. Connect to the domain's web site using your browser to inspect its certificate for HTTPS.

a. Which ciphersuite did the site negotiate with your browser?
- netflix.com
  - TLS_AES_256_GCM_SHA384
- eff.org
  - ECDHE-RSA-CHACHA20-POLY1305
- india.gov.in
  - TLS_AES_256_GCM_SHA384

b. What size and type of public key does the certificate include?
- netflix.com
  - Public Key and Size: Elliptic Curve Public Key and 256 bit
- eff.org
  - Public Key and Size: PKCS #1 RSA Encryption and 2048 bit
- india.gov.in
  - Public Key and Size: PKCS #1 RSA Encryption and 2048 bit

c. When does the certificate expire and what is its total validity period?
- netflix.com
  - Expires On: Wednesday, September 24, 2025
  - Total Validity Period: ~366 days.
- eff.org
  - Expires On: Tuesday, January 28, 2025

        - Total Validity Period: ~89 days from today
    - india.gov.in
        - Expires On: Monday, December 16, 2024
        - Total Validity Period: ~89 days from today

d. Which root Certificate Authority issued the site's certificate? What size and type of public key does the root CA use and when does it expire?
    - netflix.com
        - CN = DigiCert Secure Site ECC CA-1 and O = DigiCert Inc
        - Public Key and Size: PKCS #1 RSA Encryption and 2048 bit
        - Expires On: 11/9/31, 7:00:00 PM EST
    - eff.org
        - CN = R11 and O = Let's Encrypt
        - Public Key and Size: PKCS #1 RSA Encryption and 4096 bits
        - Expires On: 6/4/35, 7:04:38 AM EDT
    - india.gov.in
        - CN = R11 and O = Let's Encrypt
        - Public Key and Size: PKCS #1 RSA Encryption and 4096 bits
        - Expires On: 6/4/35, 7:04:38 AM EDT

e. Which other domains share this certificate?
    - netflix.com
        - DNS Name: account.netflix.com
        - DNS Name: ca.netflix.com
        - DNS Name: netflix.ca
        - DNS Name: netflix.com
        - DNS Name: signup.netflix.com
        - DNS Name: www.netflix.ca
        - DNS Name: www1.netflix.com
        - DNS Name: www2.netflix.com
        - DNS Name: www3.netflix.com
        - DNS Name: develop-stage.netflix.com
        - DNS Name: release-stage.netflix.com
        - DNS Name: www.netflix.com
        - DNS Name: tv.netflix.com
        - DNS Name: embed.develop-stage.netflix.com
        - DNS Name: embed.release-stage.netflix.com
    - eff.org
        - DNS Name: *.eff.org
        - DNS Name: *.staging.eff.org
    - india.gov.in
        - DNS Name: www.india.gov.in
        - DNS Name: www.xn--i1bj3fqcyde.xn--11b7cb3a6a.xn--h2brj9c

f. How many intermediate certificates are in the certificate chain (possibly zero)?
    - netflix.com
        - Count: 1
    - eff.org
        - Count: 1
    - india.gov.in
        - Count: 1

g. Is the site using an extended validation certificate?
   - netflix.com
     - No
   - eff.org
     - No
   - india.gov.in
     - No

h. Does the certificate include an OCSP responder? Does it include a CRL distribution point?
   - netflix.com
     - OCSP Responder: URI: http://ocsp.digicert.com
     - CRL Distribution Points:
       - URI: http://crl3.digicert.com/DigiCertSecureSiteECCCA-1.crl
       - URI: http://crl4.digicert.com/DigiCertSecureSiteECCCA-1.crl
   - eff.org
     - OCSP Responder: URI: http://r11.o.lencr.org
   - india.gov.in
     - OCSP Responder: URI: http://r11.o.lencr.org

i. Look up the certificate (e.g. by its hash) in the Certificate Transparency search engine https://crt.sh. How many CT logs include this certificate? When was it first logged?
   - netflix.com
     - Count: 10
     - 3rd October 2024
   - eff.org
     - Count: 2
     - 30th October 2024
   - india.gov.in
     - Count: 7
     - 17th September 2024

SECTION 6 TLS

6. Finally, check the domain's Qualys SSL report card: (https://www.ssllabs.com/ssltest/)

a. Which versions of TLS/SSL are supported?
   - netflix.com
     - TLS 1.0
     - TLS 1.1
     - TLS 1.2
     - TLS 1.3
   - eff.org
     - TLS 1.2
   - india.gov.in

- TLS 1.2
- TLS 1.3

b. What is the server's most-preferred cipher suite? Does this provide forward secrecy?
   - netflix.com
     - For TLS 1.3: TLS_AES_128_GCM_SHA256
     - For TLS 1.2: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
     - Forward Secrecy with modern browsers.
   - eff.org
     - For TLS 1.2: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
     - Forward Secrecy with most browsers, ROBUST.
   - india.gov.in
     - For TLS 1.3: TLS_AES_256_GCM_SHA384
     - For TLS 1.2: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
     - Forward Secrecy with most browsers, ROBUST.

c. Did the server fail to complete a handshake with any of the clients simulated by Qualys?
   - netflix.com
     - Yes
   - eff.org
     - No, worked for all.
   - india.gov.in
     - No, worked for all.

d. Does the server support Strict Transport Security (HSTS)? With what max-age?
   - netflix.com
     - Yes and max-age=31536000
   - eff.org
     - Yes and max-age=63072000
   - india.gov.in
     - Invalid: Server provided more than one HSTS header

e. Finally-if the server received lower than an A grade, what caused it to lose points?
   - netflix.com
     - Grade: B
     - Reasoning: TLS 1.1 and TLS 1.0 are enabled, which reduces the overall score and protocol support.
   - eff.org
     - Grade: A+
   - india.gov.in
     - Grade: A

SECTION 7 Wrap-Up/Comparison

7. Finally, write a few sentences describing what you learned from investigating and analyzing your three chosen domains. What was surprising to you? How would

you compare the overall security of these domains? What do you think explains the differences?

Analyzing the three domains, netflix.com, eff.org, and india.gov.in, was a great experience to learn and highlight how different organizations approach security based on their goals. One of the things that stood out was the variation in certificate choices. Netflix uses a high-assurance certificate from DigiCert with modern cryptography. In contrast, both EFF and India's government rely on Let's Encrypt, which offers free certificates.

Another surprising discovery was that none of the domains use DNSSEC, a technology that could help prevent DNS spoofing. Given that india.gov.in is a government site and eff.org is a digital security advocate, I expected at least one of them to implement it.

The differences in public key sizes also caught my attention. Netflix uses ECC-based cryptography, which is faster, while Let's Encrypt employs 2048-bit RSA for its intermediate certificates and 4096-bit RSA for its root. This shows a balance between modern efficiency and strong cryptographic foundations across all three domains.

Overall, the level of security reflects the priorities and resources of each organization. Netflix focuses on scalable solutions to protect its global audience. EFF uses accessible and open tools that align with its mission, whereas India's government site adopts standard HTTPS protections but could improve trust and security by implementing DNSSEC and considering EV certificates.