

Http



Https

Lab - Finding Information from SSL Certificates

SSL certificates are an essential part of online security. They are used to both encrypt data as it transmitted and establish that a website can be trusted as a source or destination for data. It is important to understand the identification and encryption information that is available in SSL certificates.

Objectives

- View Certificate Information on Hosts
- Access Detailed Certificate Information
- Use SSL Analysis Tools in Kali
- Use Kali Tools to Gather Certificate Information

Background / Scenario

SSL/TLS certificates functions.

1. They provide a way that the ownership of a website can be validated by people who are accessing it.
2. They provide a means by which communication between a client and server is encrypted so that it cannot be read or altered by unauthorized parties.
3. They provide the information required for a browser to create a secure, encrypted connection to a website over the HTTPS protocol.

Certificates are used behind the scenes as users browse the internet. In most cases, users are not aware that they are in use. The users become aware of them if a certificate is missing, out of date, or misconfigured.

Certificate information can be viewed locally for a website that is currently displayed in a browser by clicking the padlock icon next to the **URL** in the browser. Certificates are also stored locally for the certificate authorities themselves. There are various ways to view them. The format of public key certificate information is specified by the **X.509 standard**.

Ethical hackers can use public certificate information in the reconnaissance phase of penetration tests. Certificate information can reveal details about an organization including domain and subdomain names, issuance and expiration dates, and certificate public keys. In addition, certain versions of software, such as OpenSSL, have widely known vulnerabilities that can be exploited, including vulnerability to the heartbleed bug. In addition, it is possible that some certificates could use weak encryption algorithms.

Required Resources

- Kali VM customized for Ethical Hacker course
- Internet access

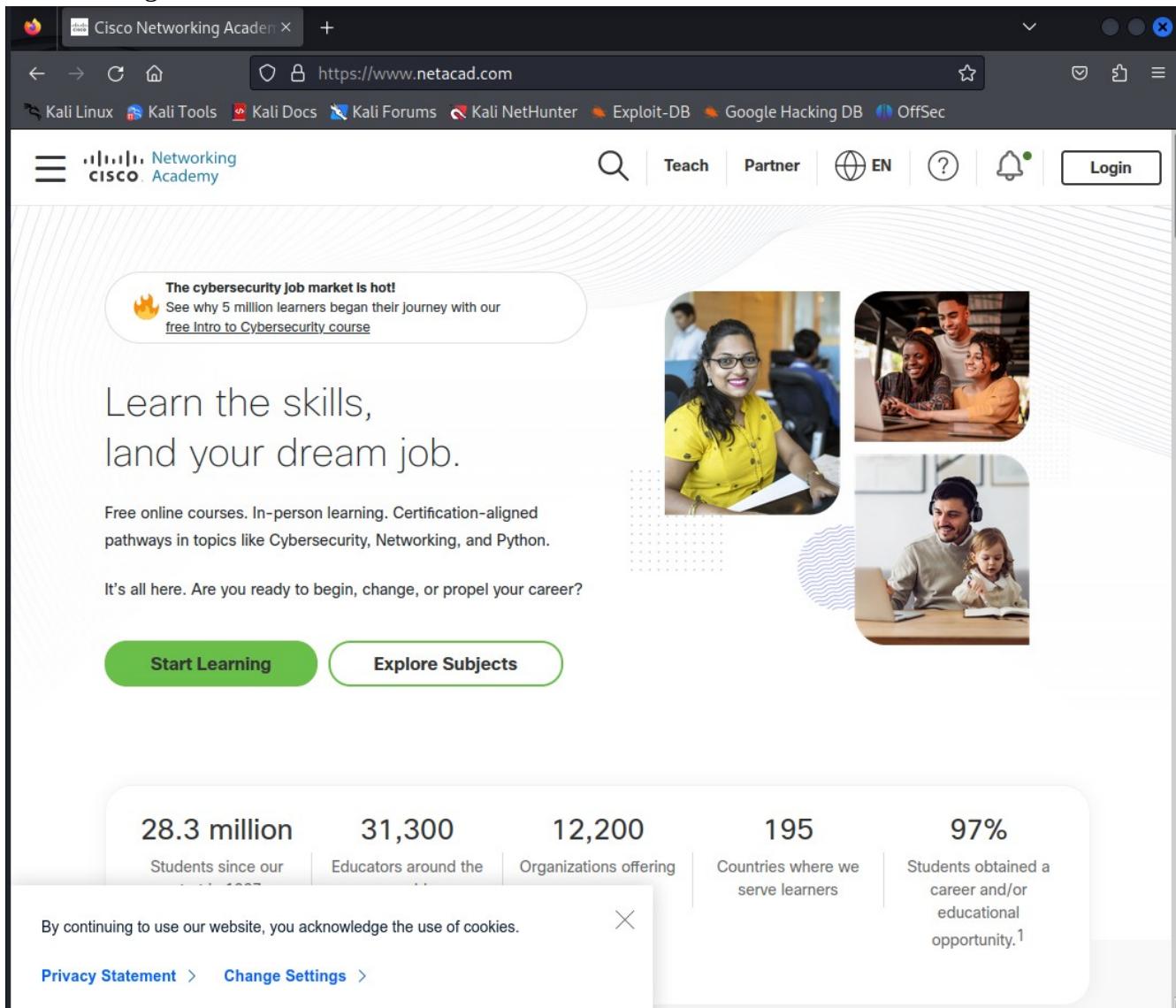
Instructions

Part 1: View Certificate Information on Hosts

Some SSL certificates are stored locally on network hosts. These certificates allow secure communication between a host and a server through a certificate chain. A host stores intermediate and root certificates as part of the SSL authentication process.

Step 1: View site certificates from a browser.

- Navigate to [netacad.com](https://www.netacad.com).



- In most browsers, a padlock icon appears next to the URL of the site that is currently displayed. Click the padlock icon and explore the settings available.

Cisco Networking Academy

Site information for www.netacad.com

Connection secure

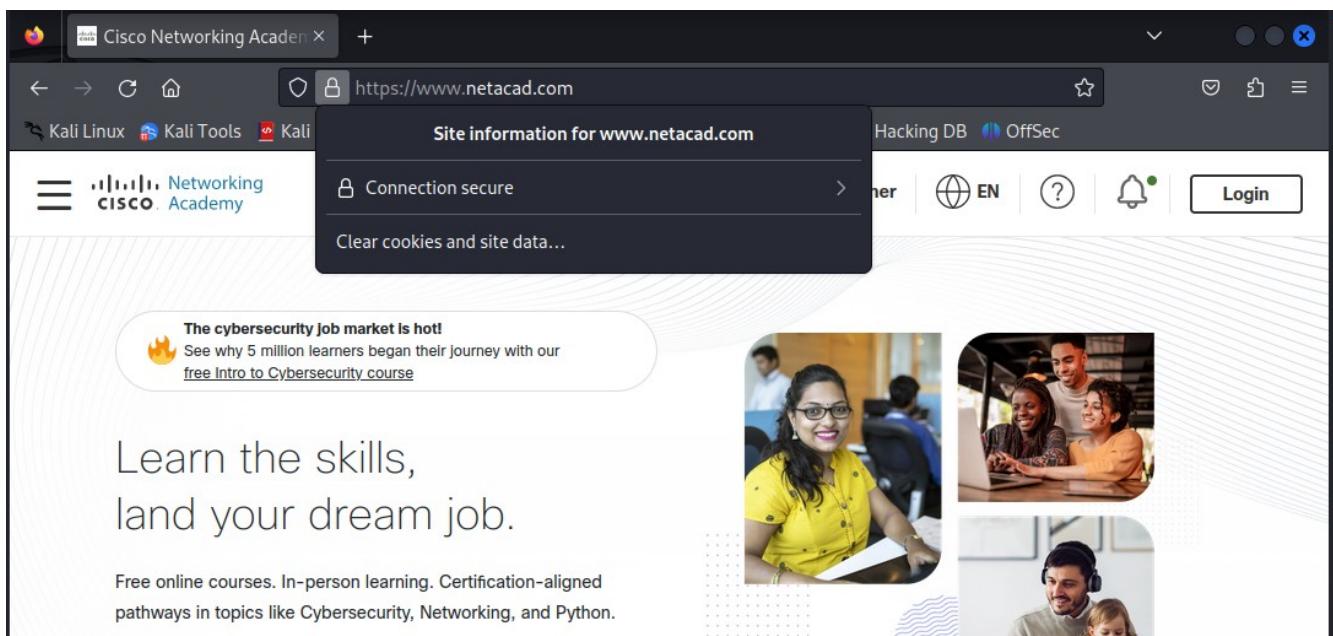
Clear cookies and site data...

The cybersecurity job market is hot!

See why 5 million learners began their journey with our [free Intro to Cybersecurity course](#)

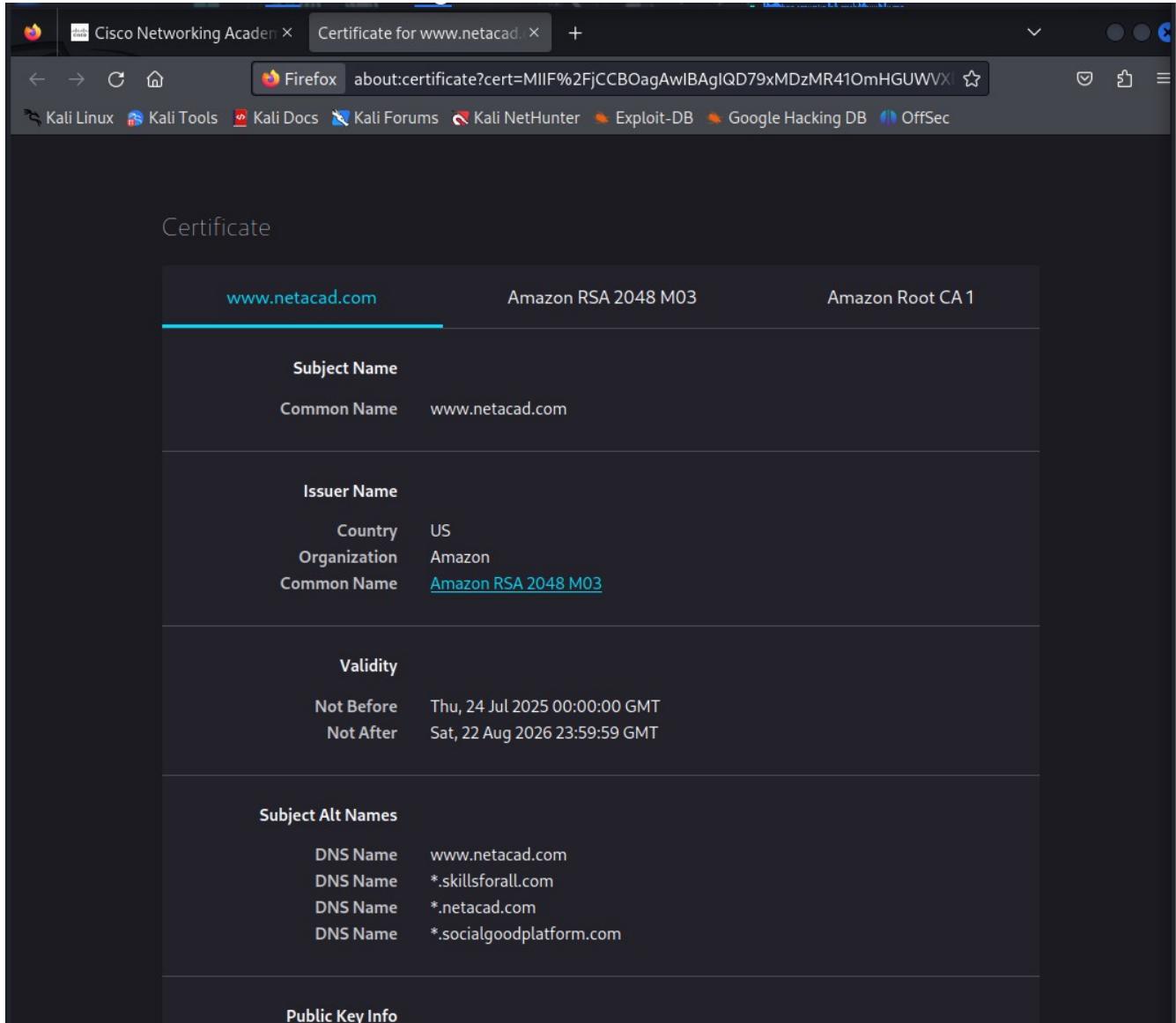
Learn the skills, land your dream job.

Free online courses. In-person learning. Certification-aligned pathways in topics like Cybersecurity, Networking, and Python.



- c. Most browsers have a certificate manager that permits viewing details of certificates for websites or root certificates for certificate authorities. View certificate information while

browsing, using the padlock, or by opening certificate information from the browser security settings.



The screenshot shows a Firefox browser window with the title "Cisco Networking Academy" and the tab "Certificate for www.netacad.com". The address bar shows the URL "about:certificate?cert=MIIF%2FjCCBOagAwIBAgIQD79xMDzMR41OmHGUWVXl". The browser interface includes a toolbar with icons for back, forward, search, and refresh, and a menu bar with "File", "Edit", "View", "Tools", "Help". Below the toolbar is a navigation bar with links to "Kali Linux", "Kali Tools", "Kali Docs", "Kali Forums", "Kali NetHunter", "Exploit-DB", "Google Hacking DB", and "OffSec".

The main content area displays the certificate details for "www.netacad.com".

Subject Name	Amazon RSA 2048 M03	Amazon Root CA 1
Common Name	www.netacad.com	
Issuer Name		
Country	US	
Organization	Amazon	
Common Name	Amazon RSA 2048 M03	
Validity		
Not Before	Thu, 24 Jul 2025 00:00:00 GMT	
Not After	Sat, 22 Aug 2026 23:59:59 GMT	
Subject Alt Names		
DNS Name	www.netacad.com	
DNS Name	*.skillsforall.com	
DNS Name	*.netacad.com	
DNS Name	*.socialgoodplatform.com	
Public Key Info		

d. Look at the details for the Cisco Skills for All certificate and answer the following questions.

What domain was the certificate issued to? What organization issued it?

Answer Area

socialgoodplatform.com by Amazon

|

Show Answer

View the certificate. When will it expire?

Answer Area

Sat, 22 Aug 2026

Show Answer

What is the certificate signature encryption algorithm?

Answer Area

SHA-256 with RSA Encryption

Show Answer

Issuer Name
Country US
Organization Amazon
Common Name Amazon RSA 2048 M03
Validity
Not Before Thu, 24 Jul 2025 00:00:00 GMT
Not After Sat, 22 Aug 2026 23:59:59 GMT
Subject Alt Names
DNS Name www.netacad.com
DNS Name *.skillsforall.com
DNS Name *.netacad.com
DNS Name *.socialgoodplatform.com
Public Key Info
Algorithm RSA
Key Size 2048
Exponent 65537
Modulus CC:2F:1B:95:29:34:AE:19:D7:39:8F:74:44:B3:92:C4:78:7B:E6:13:64:0B:A9:BD:...
Miscellaneous
Serial Number 0F:BF:71:30:3C:CC:47:8D:4E:98:71:94:59:55:E5:89
Signature Algorithm SHA-256 with RSA Encryption
Version 3

Step 2: View stored certificates in the operating system.

- Microsoft Windows has a security management application that is part of the Microsoft Management Console. Enter **certmgr.msc** in the search box and press Enter to open it.

To continue, please type the characters below:

urhiz

Submit

About this page

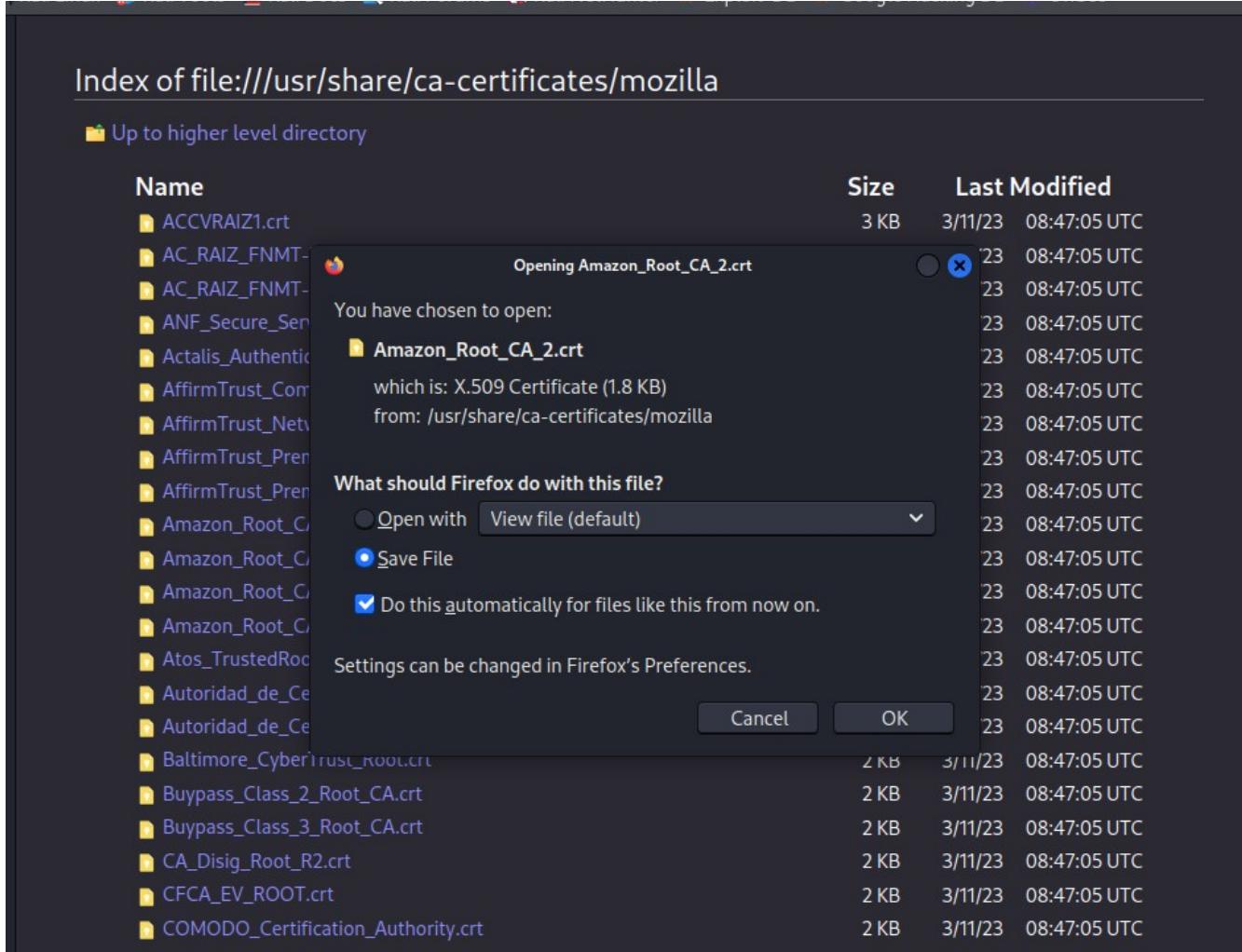
Our systems have detected unusual traffic from your computer network. This page checks to see if it's really you sending the requests, and not a robot. [Why did this happen?](#)

IP address: 154.159.237.199
Time: 2025-12-19T14:00:11Z
URL: https://www.google.com/search?client=firefox-b-e&q=certmgr.m
sc

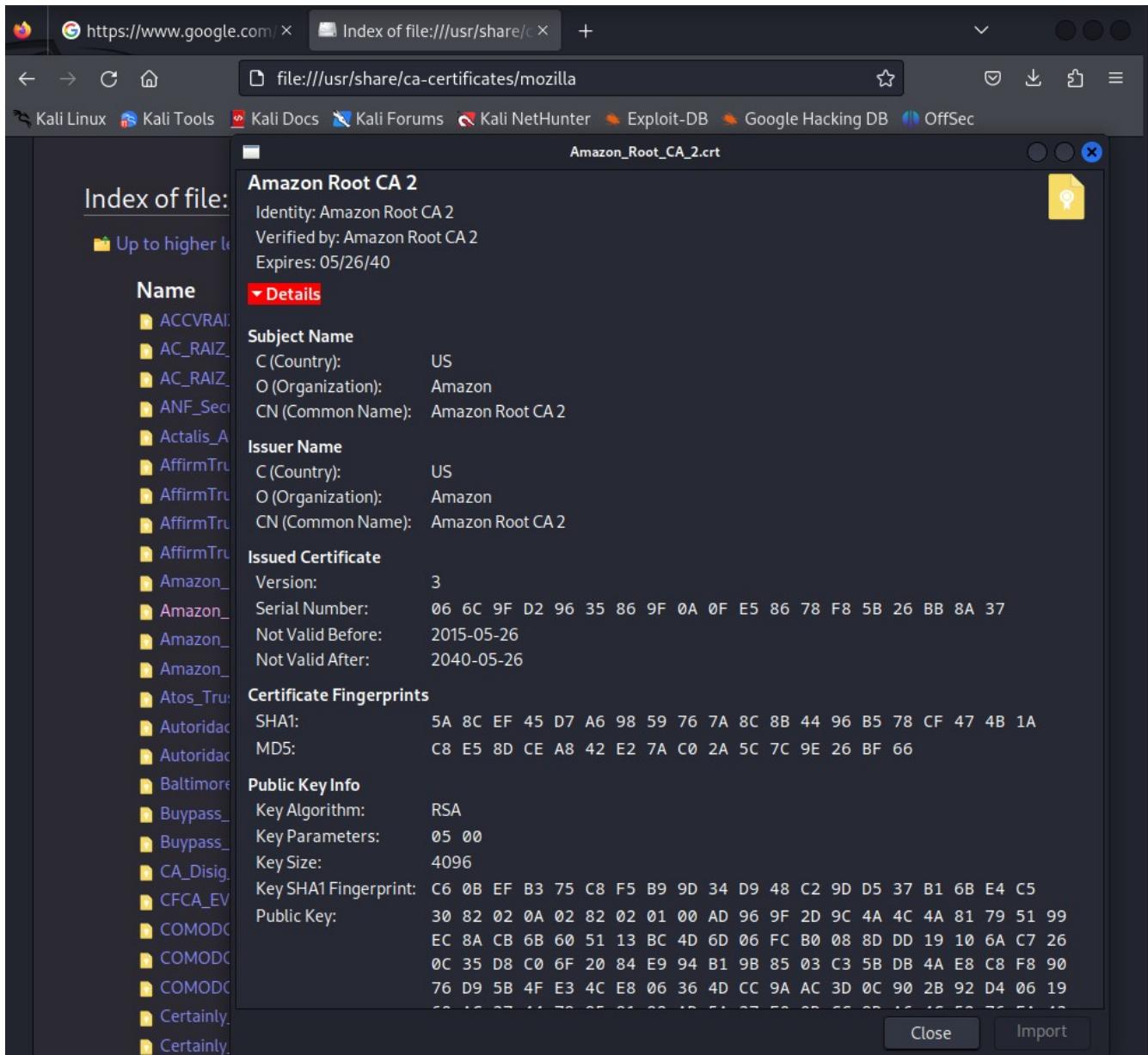
In Kali, you can find the stored certificates in the /usr/share/ca-certificates/mozilla folder.

Name	Size	Last Modified
ACCVRAIZ1.crt	3 KB	3/11/23 08:47:05 UTC
AC_RAIZ_FNMT-RCM.crt	2 KB	3/11/23 08:47:05 UTC
AC_RAIZ_FNMT-RCM_SERVIDORES_SEGUROS.crt	1 KB	3/11/23 08:47:05 UTC
ANF_Secure_Server_Root_CA.crt	3 KB	3/11/23 08:47:05 UTC
Actalis_Authentication_Root_CA.crt	3 KB	3/11/23 08:47:05 UTC
AffirmTrust_Commercial.crt	2 KB	3/11/23 08:47:05 UTC
AffirmTrust_Networking.crt	2 KB	3/11/23 08:47:05 UTC
AffirmTrust_Premium.crt	2 KB	3/11/23 08:47:05 UTC
AffirmTrust_Premium_ECC.crt	1 KB	3/11/23 08:47:05 UTC
Amazon_Root_CA_1.crt	2 KB	3/11/23 08:47:05 UTC
Amazon_Root_CA_2.crt	2 KB	3/11/23 08:47:05 UTC
Amazon_Root_CA_3.crt	1 KB	3/11/23 08:47:05 UTC
Amazon_Root_CA_4.crt	1 KB	3/11/23 08:47:05 UTC
Atos_TrustedRoot_2011.crt	2 KB	3/11/23 08:47:05 UTC
Autoridad_de_Certificacion_FirmaProfesional_CIF_A62634068.crt	3 KB	3/11/23 08:47:05 UTC
Autoridad_de_Certificacion_FirmaProfesional_CIF_A62634068_2.crt	3 KB	3/11/23 08:47:05 UTC
Baltimore_CyberTrust_Root.crt	2 KB	3/11/23 08:47:05 UTC
Buypass_Class_2_Root_CA.crt	2 KB	3/11/23 08:47:05 UTC
Buypass_Class_3_Root_CA.crt	2 KB	3/11/23 08:47:05 UTC
CA_Disig_Root_R2.crt	2 KB	3/11/23 08:47:05 UTC
CFCA_EV_ROOT.crt	2 KB	3/11/23 08:47:05 UTC
COMODO_Certification_Authority.crt	2 KB	3/11/23 08:47:05 UTC
COMODO_ECC_Certification_Authority.crt	1 KB	3/11/23 08:47:05 UTC
COMODO_RSA_Certification_Authority.crt	3 KB	3/11/23 08:47:05 UTC
Certainly_Root_E1.crt	1 KB	3/11/23 08:47:05 UTC
Certainly_Root_R1.crt	2 KB	3/11/23 08:47:05 UTC

Right-click a certificate and select **Open With “ViewFile”** to access the information for a certificate.



- b. Access information about trusted root and intermediate certificates in Windows by selecting the appropriate certificate folders in the management app.



In Kali, access the certificates folder and use `ls -l | grep root` to list root certificate files, or search for the word **root** in the file manager window.

```

File Actions Edit View Help
(kali㉿Kali)-[~] $ cd /usr/share/ca-certificates/mozilla/
(kali㉿Kali)-[/usr/share/ca-certificates/mozilla]
$ ls -l | grep root
-rw-r--r-- 1 root root 2772 Mar 11 2023 ACCVRAIZ1.crt
-rw-r--r-- 1 root root 1972 Mar 11 2023 AC_RAIZ_FNMT-RCM.crt
-rw-r--r-- 1 root root 904 Mar 11 2023 AC_RAIZ_FNMT-RCM_SERVIDORES_SEGUROS.crt
-rw-r--r-- 1 root root 2118 Mar 11 2023 ANF_Secure_Server_Root_CA.crt
-rw-r--r-- 1 root root 2049 Mar 11 2023 Actalis_Authentication_Root_CA.crt
-rw-r--r-- 1 root root 1204 Mar 11 2023 AffirmTrust_Commercial.crt
-rw-r--r-- 1 root root 1204 Mar 11 2023 AffirmTrust_Networking.crt
-rw-r--r-- 1 root root 1891 Mar 11 2023 AffirmTrust_Premium.crt
-rw-r--r-- 1 root root 753 Mar 11 2023 AffirmTrust_Premium_ECC.crt
-rw-r--r-- 1 root root 1188 Mar 11 2023 Amazon_Root_CA_1.crt
-rw-r--r-- 1 root root 1883 Mar 11 2023 Amazon_Root_CA_2.crt
-rw-r--r-- 1 root root 656 Mar 11 2023 Amazon_Root_CA_3.crt
-rw-r--r-- 1 root root 737 Mar 11 2023 Amazon_Root_CA_4.crt
-rw-r--r-- 1 root root 1261 Mar 11 2023 Atos_TrustedRoot_2011.crt
-rw-r--r-- 1 root root 2167 Mar 11 2023 Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068.crt
-rw-r--r-- 1 root root 2167 Mar 11 2023 Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068_2.crt
-rw-r--r-- 1 root root 1261 Mar 11 2023 Baltimore_CyberTrust_Root.crt
-rw-r--r-- 1 root root 1915 Mar 11 2023 Buypass_Class_2_Root_CA.crt
-rw-r--r-- 1 root root 1915 Mar 11 2023 Buypass_Class_3_Root_CA.crt
-rw-r--r-- 1 root root 1935 Mar 11 2023 CA_Disig_Root_R2.crt
-rw-r--r-- 1 root root 1984 Mar 11 2023 CFCA_EV_ROOT.crt
-rw-r--r-- 1 root root 1489 Mar 11 2023 COMODO_Certification_Authority.crt
-rw-r--r-- 1 root root 940 Mar 11 2023 COMODO_ECC_Certification_Authority.crt
-rw-r--r-- 1 root root 2086 Mar 11 2023 COMODO_RSA_Certification_Authority.crt
-rw-r--r-- 1 root root 741 Mar 11 2023 Certainly_Root_E1.crt
-rw-r--r-- 1 root root 1891 Mar 11 2023 Certainly_Root_R1.crt
-rw-r--r-- 1 root root 1330 Mar 11 2023 Certigna.crt
-rw-r--r-- 1 root root 2264 Mar 11 2023 Certigna_Root_CA.crt
-rw-r--r-- 1 root root 891 Mar 11 2023 Certum_EC-384_CA.crt
-rw-r--r-- 1 root root 1354 Mar 11 2023 Certum_Trusted_Network_CA.crt
-rw-r--r-- 1 root root 2078 Mar 11 2023 Certum_Trusted_Network_CA_2.crt
-rw-r--r-- 1 root root 2053 Mar 11 2023 Certum_Trusted_Root_CA.crt
-rw-r--r-- 1 root root 1517 Mar 11 2023 Comodo AAA Services_root.crt
-rw-r--r-- 1 root root 1050 Mar 11 2023 D-TRUST_BR_Root_CA_1_2020.crt
-rw-r--r-- 1 root root 1050 Mar 11 2023 D-TRUST_EV_Root_CA_1_2020.crt
-rw-r--r-- 1 root root 1517 Mar 11 2023 D-TRUST_Root_Class_3_CA_2_2009.crt
-rw-r--r-- 1 root root 1537 Mar 11 2023 D-TRUST_Root_Class_3_CA_2_EV_2009.crt
-rw-r--r-- 1 root root 1350 Mar 11 2023 DigiCert_Assured_ID_Root_CA.crt
-rw-r--r-- 1 root root 1306 Mar 11 2023 DigiCert_Assured_ID_Root_G2.crt
-rw-r--r-- 1 root root 851 Mar 11 2023 DigiCert_Assured_ID_Root_G3.crt
-rw-r--r-- 1 root root 1338 Mar 11 2023 DigiCert_Global_Root_CA.crt

```

The names of the root certificate files refer to the certificate authority that granted them. What are three of the most common certificate authorities on your computer? Research them on the internet. What is the cost of a single domain basic SSL certificate for one year?

Answer Area

DigiCert \$150 to \$250+
GlobalSign \$249 USD
Go_Daddy \$100-\$200

Part 2: Access Detailed Certificate Information Online

Certificate Transparency (CT) is an open framework for monitoring and auditing the issuance of SSL/TLS certificates. CT requires that all publicly trusted certificate authorities (CAs) log all issued certificates in publicly available, tamper-evident, and auditable logs. These logs can be monitored to detect any fraudulent or malicious issuance of SSL/TLS certificates, including certificates issued for domains that the attacker does not control.

In OSINT, CT logs can be used to gather information about SSL/TLS certificates used by an organization or a specific domain. By analyzing CT logs, analysts can identify certificate issuances and their associated domains, as well as any anomalies or irregularities in certificate issuance. CT logs can also be used to monitor for any unauthorized SSL/TLS certificate issuance, which could indicate a potential security breach.

CT logs can be accessed through various CT log servers and APIs. There are also several CT monitoring tools available, such as CertSpotter and Censys, which can help automate the process of monitoring CT logs for specific domains or SSL/TLS certificates.

- a. Open a browser and navigate to <https://crt.sh>

The screenshot shows a Firefox browser window with the address bar set to https://crt.sh. The main content area displays the crt.sh Certificate Search interface. At the top, there is a search bar with placeholder text: "Enter an Identity (Domain Name, Organization Name, etc), a Certificate Fingerprint (SHA-1 or SHA-256) or a crt.sh ID:". Below the search bar is a green "Search" button and a link to "Advanced...". At the bottom left, there is a copyright notice: "© Sectigo Limited 2015-2025. All rights reserved." and the Sectigo logo.

- b. Enter the Skills for All URL in the search box and click **Search**.

crt.sh Certificate Search

Enter an **Identity** (Domain Name, Organization Name, etc),
a **Certificate Fingerprint** (SHA-1 or SHA-256) or a **crt.sh ID**:

<https://www.netacad.com/>

Search [Advanced...](#)

© Sectigo Limited 2015-2025. All rights reserved.



- c. The resulting table lists comprehensive information for certificates issued to netacad.com and related subdomains. The list goes back to 2016. crt.sh

Sectigo Limited 2015-2025. All rights reserved.

[OffSec](#) [Kali Linux](#) [Kali Tools](#) [Kali Docs](#) [Kali Forums](#) [Kali NetHunter](#) [Exploit-DB](#) [Google Hacking DB](#) [\(513\) YouTube](#) [Temp Mail - Disposable...](#)

crt.sh Identity Search [RSS](#) [CSV](#) [JSON](#) [Group by Issuer](#)

Criteria Type: Identity Match: ILIKE Search: 'www.netacad.com'

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching identities	Issuer Name
	19680859197	2025-07-24	2025-07-24	2026-08-22	www.netacad.com	C=US, O=Amazon, CN=Amazon RSA 2048 M03	
	17983832592	2025-04-21	2026-04-20	2026-04-21	www.netacad.com	C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1	
	14706706471	2024-09-27	2024-08-23	2025-09-21	www.netacad.com	C=US, O=Amazon, CN=Amazon RSA 2048 M03	
	14257386433	2024-08-23	2024-08-23	2025-09-21	www.netacad.com	C=US, O=Amazon, CN=Amazon RSA 2048 M03	
	13550832877	2024-06-28	2024-05-13	2025-05-12	www.netacad.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1	
	13039266155	2024-05-14	2023-06-23	2024-06-22	www.netacad.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1	
	13035370115	2024-05-13	2024-05-13	2025-05-12	www.netacad.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1	
	9727651147	2023-06-23	2023-06-23	2024-04-20	www.netacad.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1	
	7164052090	2023-06-09	2023-06-09	2024-07-20	www.netacad.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1	
	3993592686	2021-08-18	2021-08-18	2022-08-04	www.netacad.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA	
	4993755924	2021-08-04	2021-08-04	2022-08-04	www.netacad.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA	
	2845577186	2020-05-23	2020-05-20	2021-08-19	www.netacad.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA	
	2836075445	2020-05-20	2020-05-20	2021-08-19	www.netacad.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA	
	1285246519	2019-03-16	2019-02-25	2020-05-26	www.netacad.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA	
	1230555599	2019-02-25	2019-02-25	2020-05-26	www.netacad.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA	
	380976162	2018-04-07	2018-03-27	2019-04-26	www.netacad.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA	
	368026413	2018-03-27	2018-03-27	2019-04-26	www.netacad.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA	
	217096199	2017-09-24	2017-09-22	2018-12-22	www.netacad.com	C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server CA - G4	
	215635739	2017-09-22	2017-09-22	2018-12-22	www.netacad.com	C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server CA - G4	
	69506709	2016-12-21	2016-10-31	2017-10-31	www.netacad.com	C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server CA - G4	
	49056580	2016-10-31	2016-10-31	2017-10-31	www.netacad.com	C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server CA - G4	
	42510572	2016-06-24	2016-06-24	2016-06-24	www.netacad.com	C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server CA - G4	
	23039085	2016-06-24	2016-06-24	2017-06-24	www.netacad.com	C=US, O=Symantec Corporation, OU=Symantec Class 3 Secure Server CA - G4	

Sectigo Limited 2015-2025. All rights reserved.

- d. provides IDs for the certificates but these IDs are relevant to crt.sh only. Clicking an ID takes you to the available certificate details

The screenshot shows the crt.sh Certificate Search interface for certificate ID 19868059197. Key sections include:

- Summary:** Includes a link to report problems with the certificate.
- Certificate Transparency:** Log entries for the certificate, showing entries from Google, Digicert, and Mozilla.
- Revocation:** A table showing revocation status across various mechanisms.
- Certificate Fingerprints:** SHA-256 and SHA-1 fingerprints, and a detailed certificate data section.

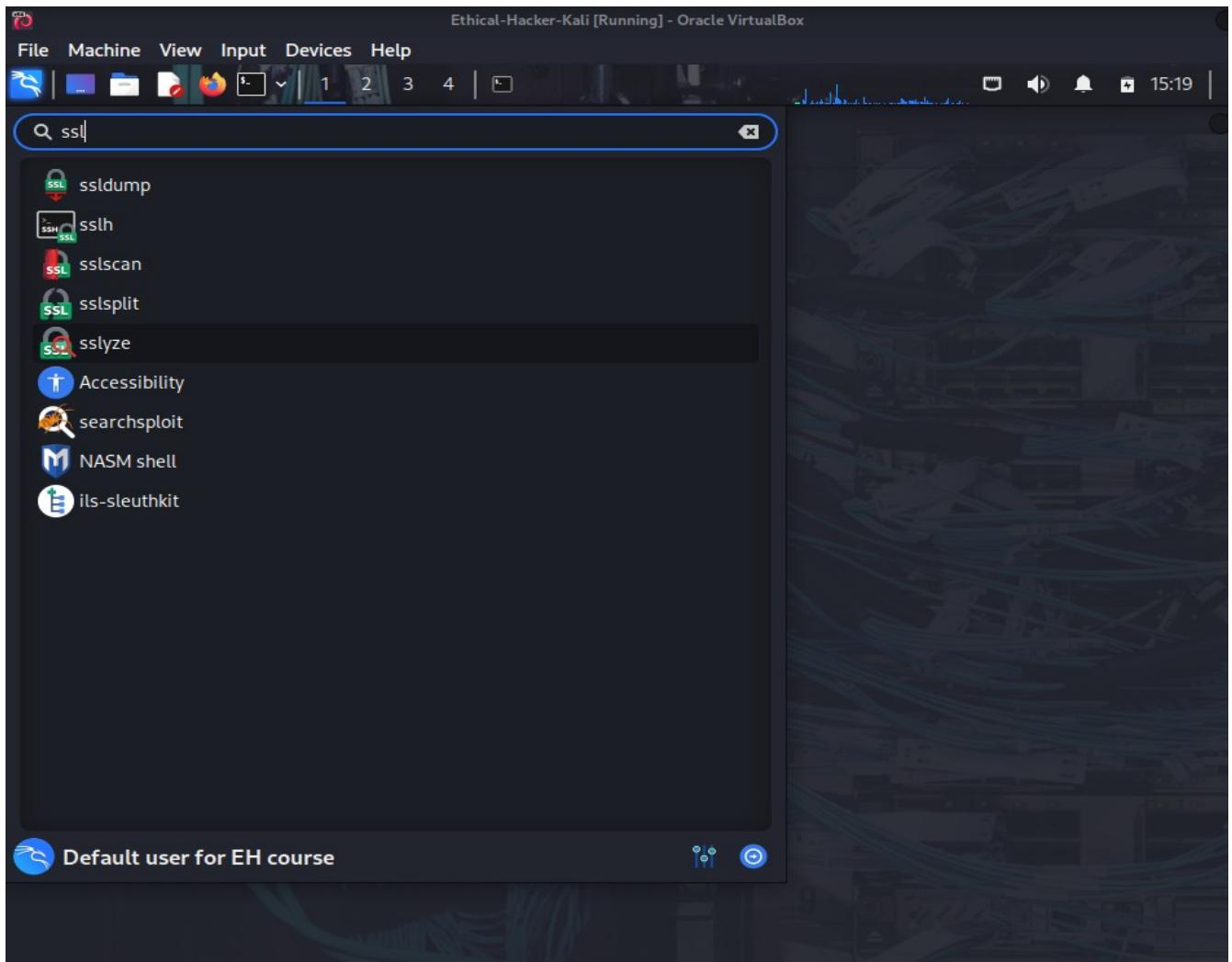
The detailed certificate data section includes:

- Subject:** www.netacad.com
- Issuer:** (CA ID: 2427105)
- Validity:** Not Before: Jul 22 08:00:00 2025 GMT, Not After: Aug 22 23:59:59 2026 GMT
- Subject Public Key Info:** RSA Public-Key: (2048 bit), Modulus: 00:cc:2f:1b:95:29:34:ae:19:d7:39:8f:74:44:b3:92:c0:78:1e:6d:59:64:3c:39:39:39:b9:35:87:29:41:f9:53:54:73:68:35:1a:51:f8:39:14:27:a1:3d:5a:55:67:49:f9:d4:30:06:78:19:6e:49:44:ac:34:21:d1:a1:8d:ee:c9:bc:c8:6a:a6:76:6d:3a:78:01:e6:e4:af:59:d5:24:a2:b9:3c:55:b6:ea:82:f9:ae:8b:00:46:5f:a8:b2:22:10:2a:29:8b:b9:14:b5:a7:2d:78:77:0f:ec:3c:a6:bc:10:2e:13:c9:07:93:6e:88:ce:d6:14:cd:61:2b:f1:8b:bb:6b.

Part 3: Use SSL Analysis Tools in Kali

Step 1: Investigate Kali Tools

- Start the Kali virtual machine and log in.
- Start a terminal session.
- Kali comes with several SSL-related tools. Click the Kali programs icon and search on the term **ssl**.
- Use the Kali tools reference to complete the table below for the five SSL tools included with your Kali distribution.



Tool	Description	Recon, Exploitation, or Utility
sslscan	Queries SSL services to determine what ciphers are supported	Reconnaissance
ssldump	Analyze and decode SSL traffic	Exploitation
sslh	Running multiple services on port 443	Utility
sslsplit	Enable MitM attacks on SSL encrypted network connections	Exploitation
sslyze	Analyze the SSL configuration of a server by connecting to it	Reconnaissance

Part 4: Use Kali Tools to Gather Certificate Information

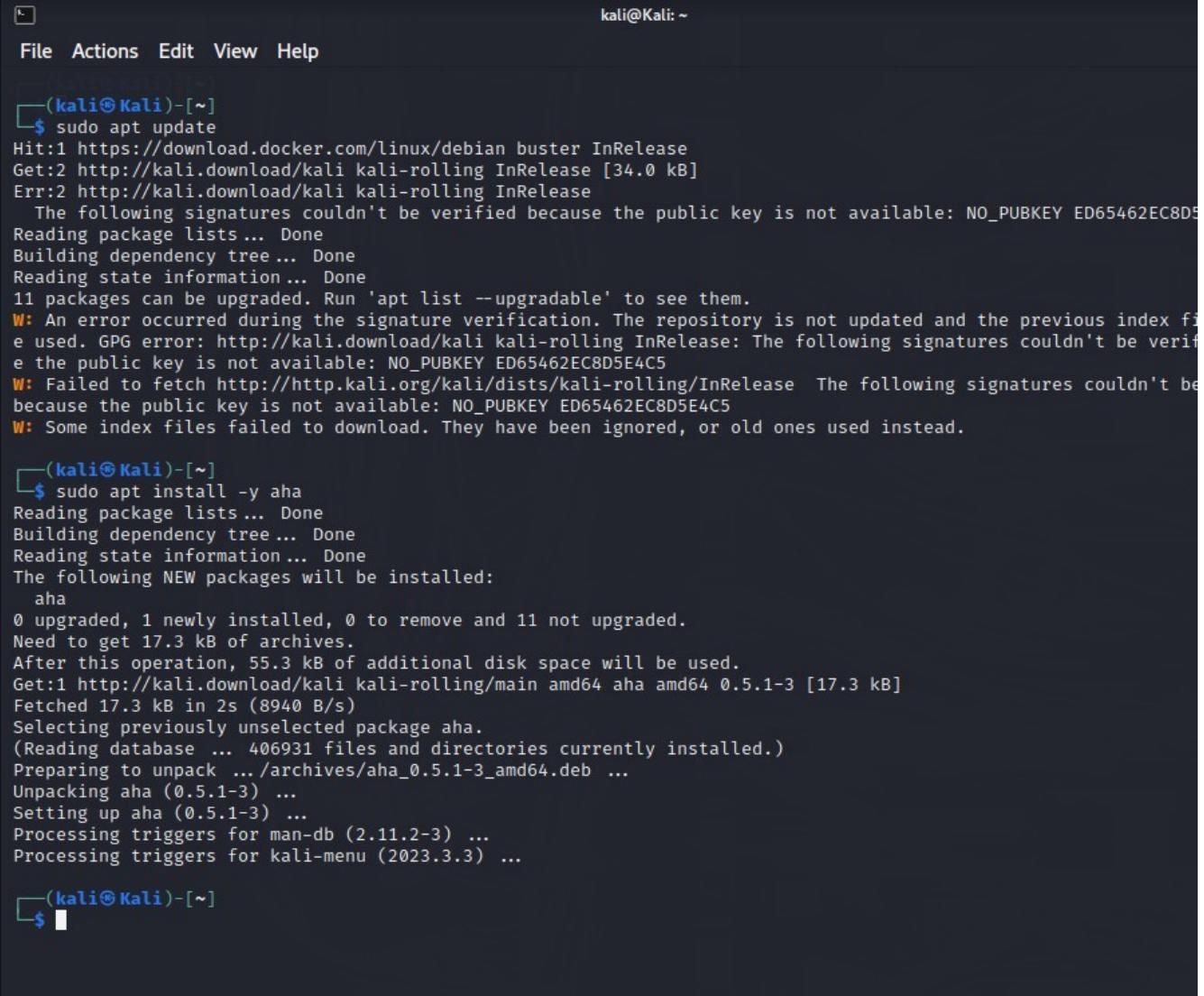
As you know, **sslscan** is a Kali tool reconnaissance that will gather information about SSL certificates that are associated with domains. It is a command line utility. We will use **sslscan** to gather information about certificates and use another utility, called **aha**, to output the results to an HTML file.

Step 1: Install aha.

The application **aha** creates a standard HTML file that captures the output of terminal commands to standard HTML files. Aha captures any color coding and basic formatting of the command output. It also has command line options that allow you to specify your own formatting, such as background color, stylesheets to apply, and word wrap, among other settings.

Update your apt package information with the **apt update** command. This requires root privileges.

Install aha with the **sudo apt install -y aha** command. The option **-y** assumes **yes** is the answers to all prompts and can run non-interactively. In this case, you are giving permission to install aha.



```
kali@Kali: ~
File Actions Edit View Help

└─(kali㉿Kali)-[~]
$ sudo apt update
Hit:1 https://download.docker.com/linux/debian buster InRelease
Get:2 http://kali.download/kali kali-rolling InRelease [34.0 kB]
Err:2 http://kali.download/kali kali-rolling InRelease
  The following signatures couldn't be verified because the public key is not available: NO_PUBKEY ED65462EC8D5E4C5
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
11 packages can be upgraded. Run 'apt list --upgradable' to see them.
W: An error occurred during the signature verification. The repository is not updated and the previous index file used. GPG error: http://kali.download/kali kali-rolling InRelease: The following signatures couldn't be verified because the public key is not available: NO_PUBKEY ED65462EC8D5E4C5
W: Failed to fetch http://http.kali.org/kali/dists/kali-rolling/InRelease  The following signatures couldn't be because the public key is not available: NO_PUBKEY ED65462EC8D5E4C5
W: Some index files failed to download. They have been ignored, or old ones used instead.

└─(kali㉿Kali)-[~]
$ sudo apt install -y aha
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  aha
0 upgraded, 1 newly installed, 0 to remove and 11 not upgraded.
Need to get 17.3 kB of archives.
After this operation, 55.3 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 aha amd64 0.5.1-3 [17.3 kB]
Fetched 17.3 kB in 2s (8940 B/s)
Selecting previously unselected package aha.
(Reading database ... 406931 files and directories currently installed.)
Preparing to unpack .../archives/aha_0.5.1-3_amd64.deb ...
Unpacking aha (0.5.1-3) ...
Setting up aha (0.5.1-3) ...
Processing triggers for man-db (2.11.2-3) ...
Processing triggers for kali-menu (2023.3.3) ...

└─(kali㉿Kali)-[~]
$
```

Step 2: Run sslscan and save the output to an HTML file.

- From a terminal command line, execute the command to run **sslscan** with the netacad.com target.

```
File Machine View Input Devices Help
File Actions Edit View Help
kali@Kali:[~]
$ ./sslscan netacad.com
Version: 0.8.1-teststatic
OpenSSL 1.1.1u-dev xx XXX xxxx
Connected to 44.206.106.175

Testing SSL server netacad.com on port 443 using SNI name netacad.com

SSL/TLS Protocols:
SSLv3 disabled
SSLv2 disabled
TLSv1.0 disabled
TLSv1.1 disabled
TLSv1.2 enabled
TLSv1.3 enabled

TLS Fallback SCSV:
Server supports TLS Fallback SCSV

TLS renegotiation:
Session renegotiation not supported

TLS Compression:
Compression disabled

Heartbleed:
TLSv1.3 not vulnerable to heartbleed
TLSv1.2 not vulnerable to heartbleed

Supported Server Cipher(s):
Preferred TLSv1.3 128 bits TLS_AES_128_GCM_SHA256      Curve 25519 DHE 253
Accepted  TLSv1.3 256 bits TLS_AES_256_GCM_SHA384      Curve 25519 DHE 253
Accepted  TLSv1.3 256 bits TLS_CHACHA20_POLY1305_SHA256 Curve 25519 DHE 253
Preferred TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve 25519 DHE 253
Accepted  TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve 25519 DHE 253

Server Key Exchange Group(s):
TLSv1.3 384 bits secp384r1 (NIST P-384)
TLSv1.3 384 bits secp384r1 (NIST P-384)
TLSv1.3 256 bits secp256r1 (NIST P-256)
TLSv1.3 128 bits x25519
TLSv1.2 128 bits secp256r1 (NIST P-256)
TLSv1.2 256 bits secp384r1 (NIST P-384)
TLSv1.2 384 bits secp511r1 (NIST P-511)
TLSv1.2 128 bits x25519

SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength: 2048
Subject: netacad.com
AltNames: DNS:netacad.com, DNS:*.netacad.com

Issuer: Amazon RSA 2048 M04

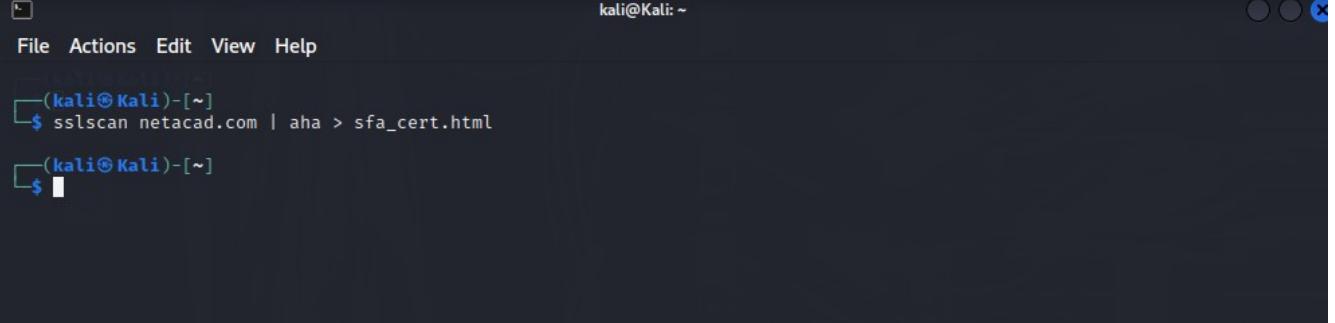
Not valid before: Dec 5 00:00:00 2025 GMT
Not valid after: Jan 3 23:59:59 2027 GMT

(kali㉿Kali)-[~]
$
```

After a brief delay you should see the results of scan begin to appear in the terminal window. The output is color coded to make it easier to interpret the severity of any issues detected. The meaning of the color coding is as follows:

- Red background text – NULL cipher. No encryption was used.
- Red – broken cipher (less than or equal to 40-bit), vulnerable or broken protocol such as SSLv2 or SSLv3 or broken certificate signing algorithm such as MD5.
- Yellow – weak cipher (less than or equal to 56-bit) or weak signing algorithm such as SHA-1.
- Purple – anonymous cipher such as ADH or AECDH.

While sslscan provides options for outputting results in text or XML file formats, the readability of HTML and the preservation of color coding is provided by aha. To use aha, pipe the output of the sslscan command to aha and then redirect the output of aha to a HTML file.



```
(kali㉿Kali)-[~]
$ sslscan netacad.com | aha > sfa_cert.html
(kali㉿Kali)-[~]
$
```

A screenshot of a terminal window titled "kali@Kali: ~". The window has a dark background and light-colored text. At the top, there's a menu bar with "File", "Actions", "Edit", "View", and "Help". Below the menu, the terminal prompt "(kali㉿Kali)-[~]" appears twice, followed by a dollar sign (\$) which is partially cut off. Between the two prompts, the command "sslscan netacad.com | aha > sfa_cert.html" is typed. The window has standard window controls (minimize, maximize, close) at the top right corner.

sslscan will save the file in the Kali Home directory as indicated by the prompt. You can add a path to the filename or run the terminal from a destination directory to save it elsewhere.

Locate the HTML file and open it with Firefox. The output should be like that of the terminal except that the background is white. The original color coding should be intact.

The screenshot shows a Firefox browser window with the title bar "stdin". The address bar displays "file:///home/kali/sfa_cert.html". Below the address bar, the Kali Linux desktop environment is visible with various icons like Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec.

A message bar at the top of the Firefox window says: "Open previous tabs? You can restore your previous session from the Firefox application menu ⚙, under History." with a "Show me how" button.

The main content area of the browser shows the output of a SSL/TLS test. The output is as follows:

```
version: 2.0.16-static
OpenSSL 1.1.1u-dev  xx XXX xxxx

connected to 44.206.106.175

Testing SSL server netacad.com on port 443 using SNI name netacad.com

SSL/TLS Protocols:
SSLv2      disabled
SSLv3      disabled
TLSv1.0    disabled
TLSv1.1    disabled
TLSv1.2    enabled
TLSv1.3    enabled

TLS Fallback SCSV:
Server supports TLS Fallback SCSV

TLS renegotiation:
Session renegotiation not supported

TLS Compression:
Compression disabled

Heartbleed:
TLSv1.3 not vulnerable to heartbleed
TLSv1.2 not vulnerable to heartbleed

Supported Server Cipher(s):
REFERRED TLSv1.3 128 bits TLS_AES_128_GCM_SHA256      Curve 25519 DHE 253
ACCEPTED TLSv1.3 256 bits TLS_AES_256_GCM_SHA384      Curve 25519 DHE 253
ACCEPTED TLSv1.3 256 bits TLS_CHACHA20_POLY1305_SHA256 Curve 25519 DHE 253
REFERRED TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve 25519 DHE 253
ACCEPTED TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve 25519 DHE 253

Server Key Exchange Group(s):
TLSv1.3 128 bits secp256r1 (NIST P-256)
TLSv1.3 192 bits secp384r1 (NIST P-384)
TLSv1.3 260 bits secp521r1 (NIST P-521)
TLSv1.3 128 bits x25519
TLSv1.2 128 bits secp256r1 (NIST P-256)
TLSv1.2 192 bits secp384r1 (NIST P-384)
TLSv1.2 260 bits secp521r1 (NIST P-521)
TLSv1.2 128 bits x25519
```