Mini-Project #3
SSL Certificate Experiments

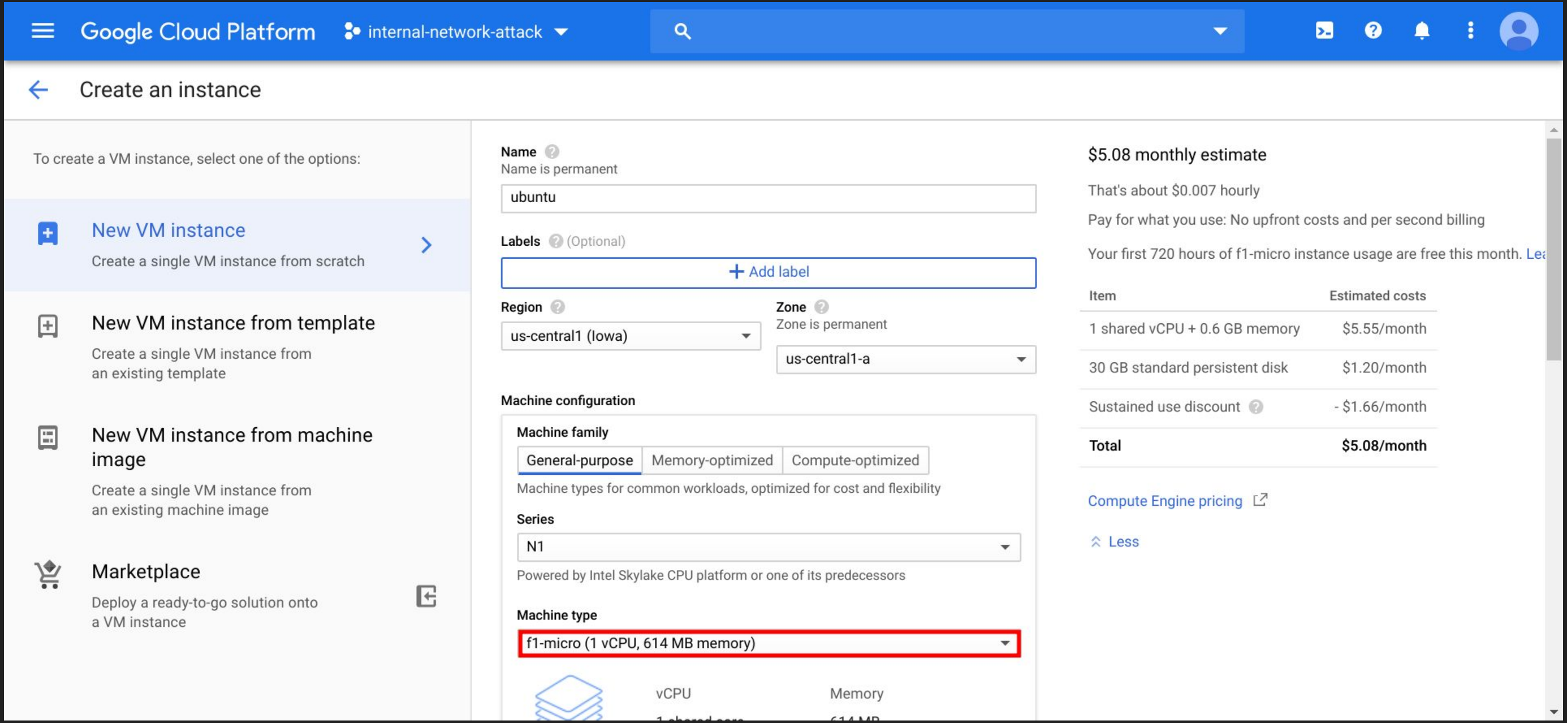
0866007 胡孝德

Set up a web server supporting HTTPS with perfect forward secrecy.

1.1 Create VM on Google Cloud Platform

Item	Settings
Machine	f1-micro (1 shared vCPU, 614 MB memory)
Disk	30 GB HDD
Image	Ubuntu 18.04 TLS Minimal
Firewall	Allow HTTP, HTTPS traffic
IP (static)	35.239.2.77

1.1 Create VM on Google Cloud Platform



Create an instance

To create a VM instance, select one of the options:

New VM instance
Create a single VM instance from scratch

New VM instance from template
Create a single VM instance from an existing template

New VM instance from machine image
Create a single VM instance from an existing machine image

Marketplace
Deploy a ready-to-go solution onto a VM instance

Name
Name is permanent
ubuntu

Labels (Optional)
+ Add label

Region
us-central1 (Iowa)

Zone
Zone is permanent
us-central1-a

Machine configuration

Machine family
General-purpose | Memory-optimized | Compute-optimized
Machine types for common workloads, optimized for cost and flexibility

Series
N1
Powered by Intel Skylake CPU platform or one of its predecessors

Machine type
f1-micro (1 vCPU, 614 MB memory)

vCPU | Memory

$5.08 monthly estimate

That's about $0.007 hourly

Pay for what you use: No upfront costs and per second billing

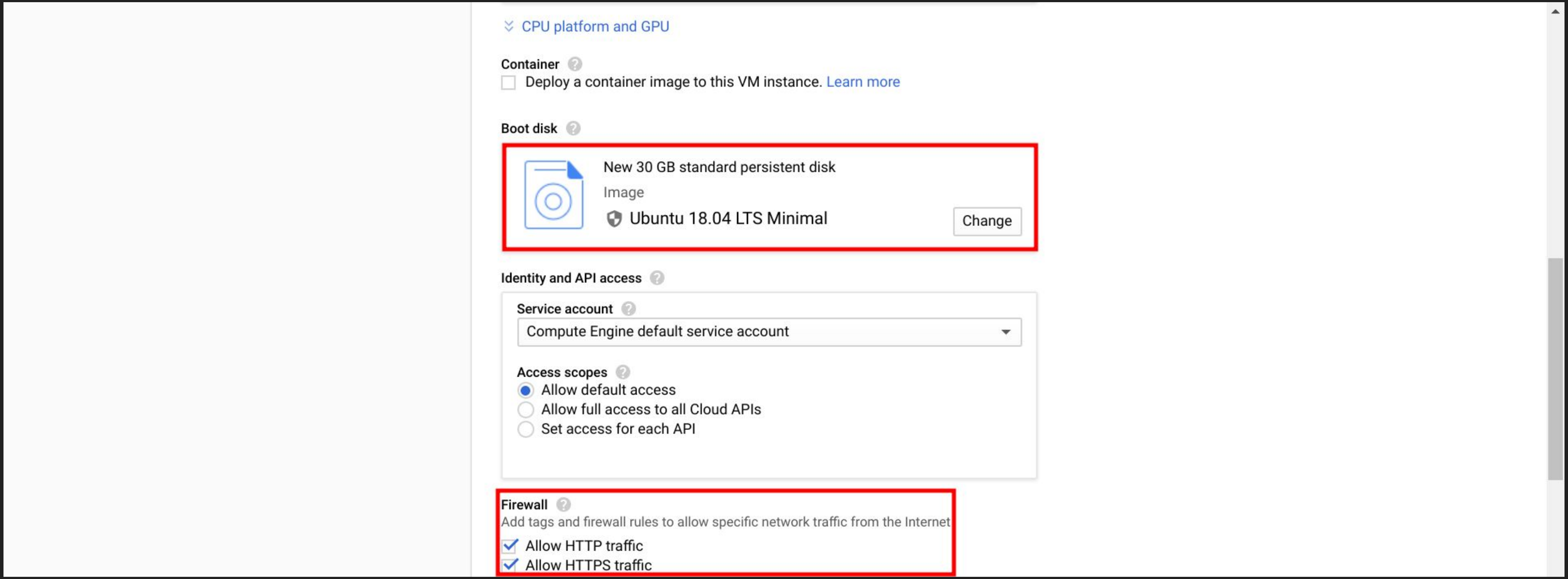
Your first 720 hours of f1-micro instance usage are free this month. Lea

Item	Estimated costs
1 shared vCPU + 0.6 GB memory	$5.55/month
30 GB standard persistent disk	$1.20/month
Sustained use discount	- $1.66/month
Total	**$5.08/month**

Compute Engine pricing

Less

1.1 Create VM on Google Cloud Platform



Container

□ Deploy a container image to this VM instance. Learn more

Boot disk

New 30 GB standard persistent disk

Image

Ubuntu 18.04 LTS Minimal

Identity and API access

Service account

Compute Engine default service account

Access scopes

● Allow default access

○ Allow full access to all Cloud APIs

○ Set access for each API

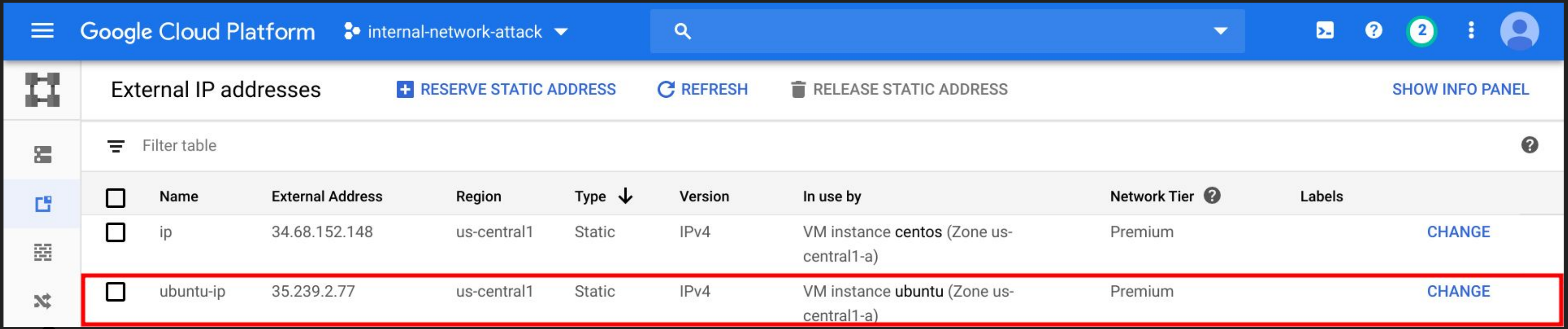
Firewall

Add tags and firewall rules to allow specific network traffic from the Internet

☑ Allow HTTP traffic

☑ Allow HTTPS traffic

1.1 Create VM on Google Cloud Platform

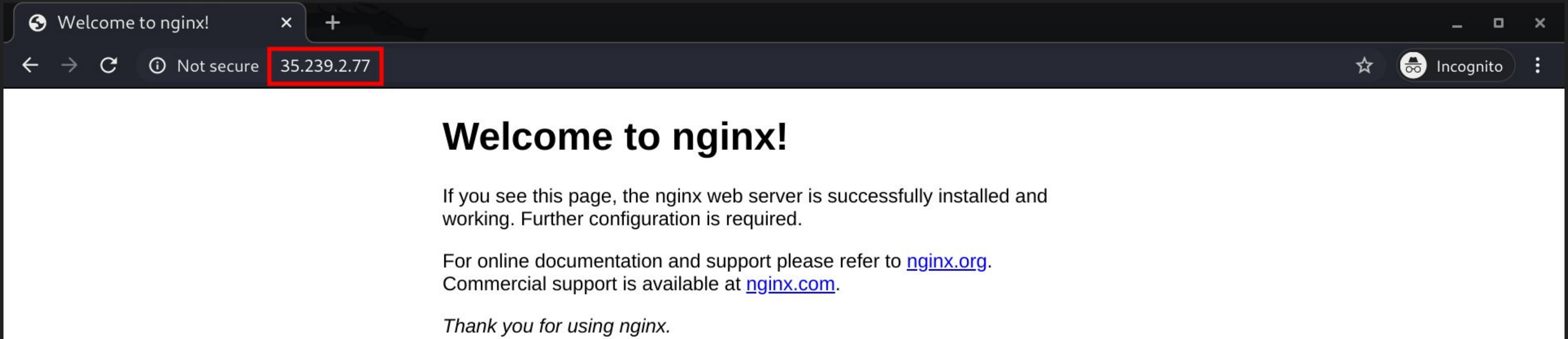


□	Name	External Address	Region	Type ↓	Version	In use by	Network Tier	Labels	
□	ip	34.68.152.148	us-central1	Static	IPv4	VM instance centos (Zone us-central1-a)	Premium		CHANGE
□	ubuntu-ip	35.239.2.77	us-central1	Static	IPv4	VM instance ubuntu (Zone us-central1-a)	Premium		CHANGE

- Install necessary packages
  - sudo apt update
  - sudo apt install vim less bash-completion policykit-1
  - sudo timedatectl set-timezone Asia/Taipei

1.2 Install Nginx Web Server

- sudo apt install nginx



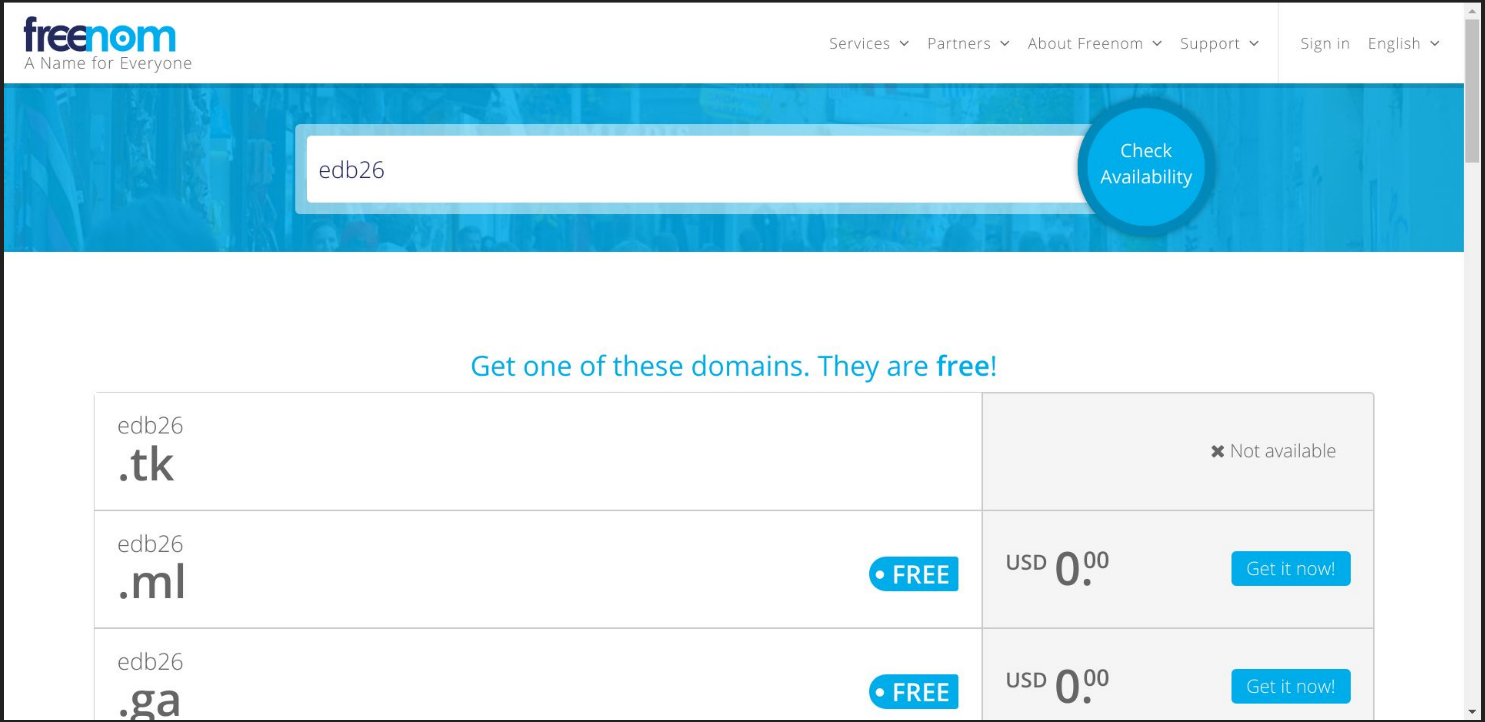
Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

1.3 Register a New Domain at freenom.com



edb26

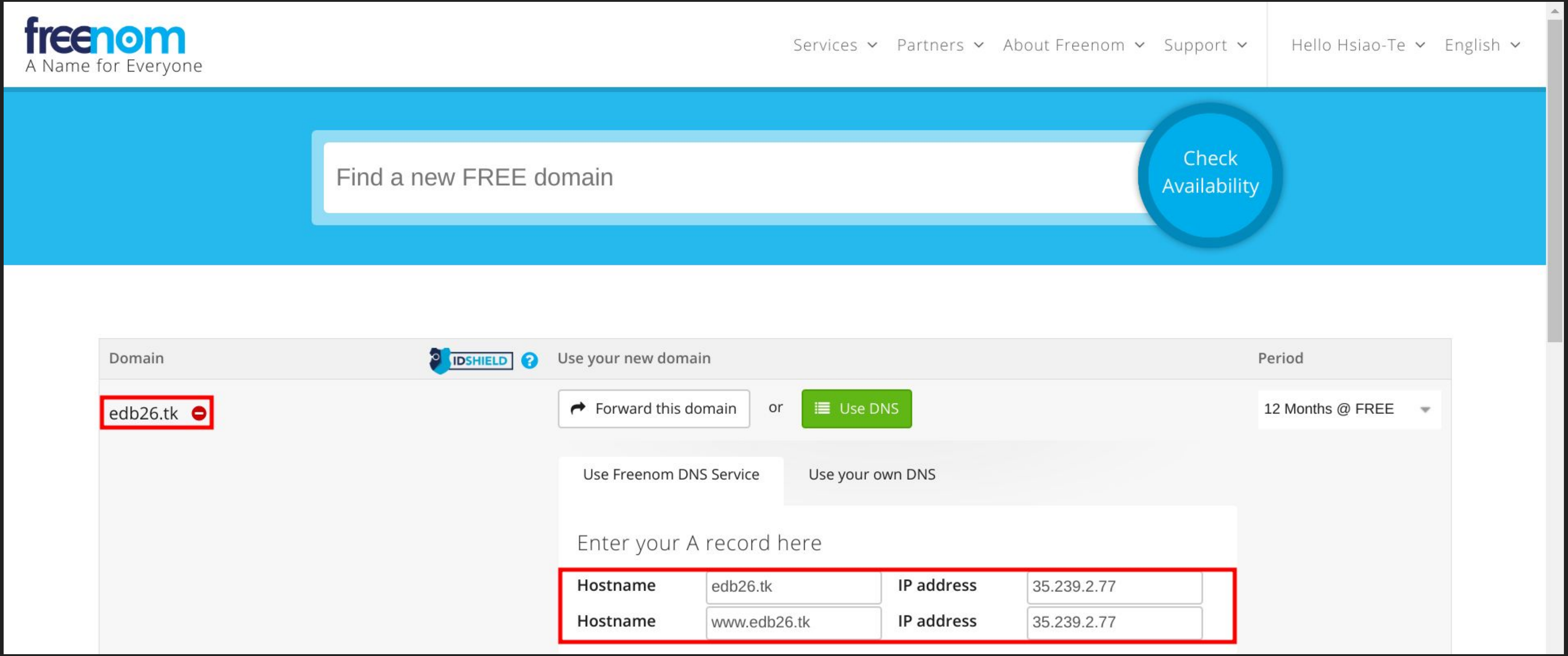
Get one of these domains. They are **free**!

edb26 **.tk** ✖ Not available

edb26 **.ml** FREE USD $0.^{00}$ Get it now!

edb26 **.ga** FREE USD $0.^{00}$ Get it now!

1.3 Register a New Domain at freenom.com

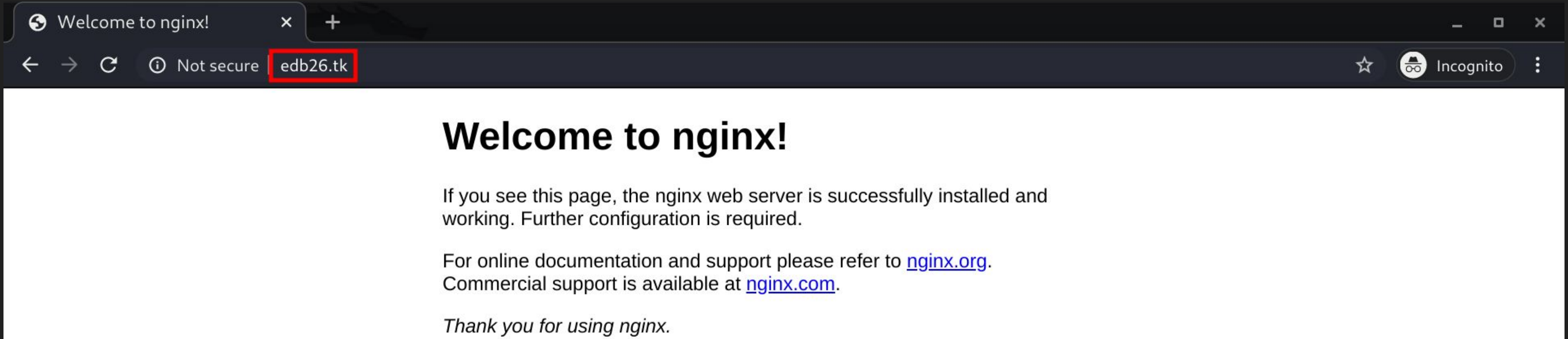


Domain	Use your new domain	Period
edb26.tk		12 Months @ FREE

Enter your A record here

Hostname	edb26.tk	IP address	35.239.2.77
Hostname	www.edb26.tk	IP address	35.239.2.77

1.3 Register a New Domain at freenom.com



Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

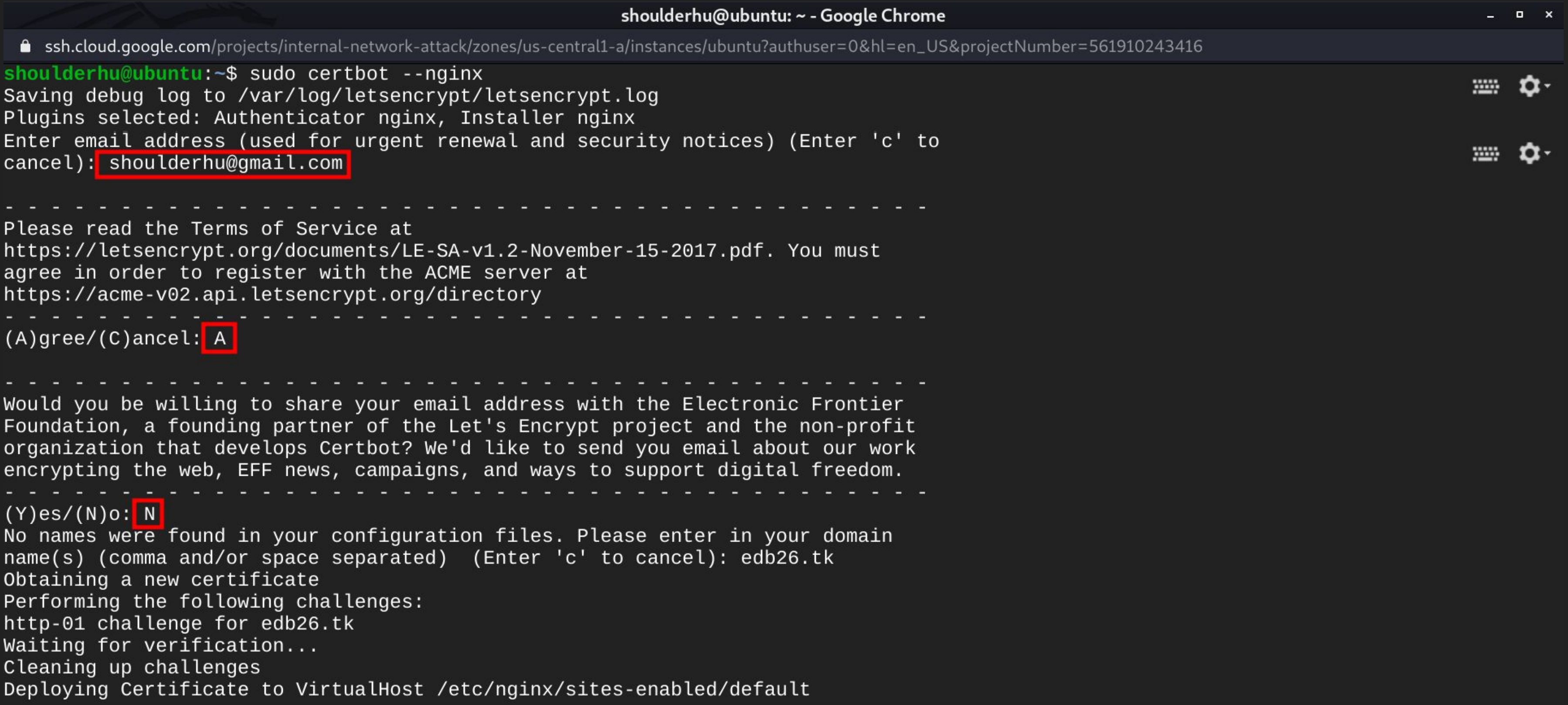
For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

1.4 Configure Nginx with Let's Encrypt Certificate

- Add Certbot PPA
  - sudo apt update
  - sudo apt install software-properties-common
  - sudo add-apt-repository universe
  - sudo add-apt-repository ppa:certbot/certbot
- Install Certbot
  - sudo apt install certbot python-certbot-nginx
- Get and install your certificates
  - sudo certbot --nginx

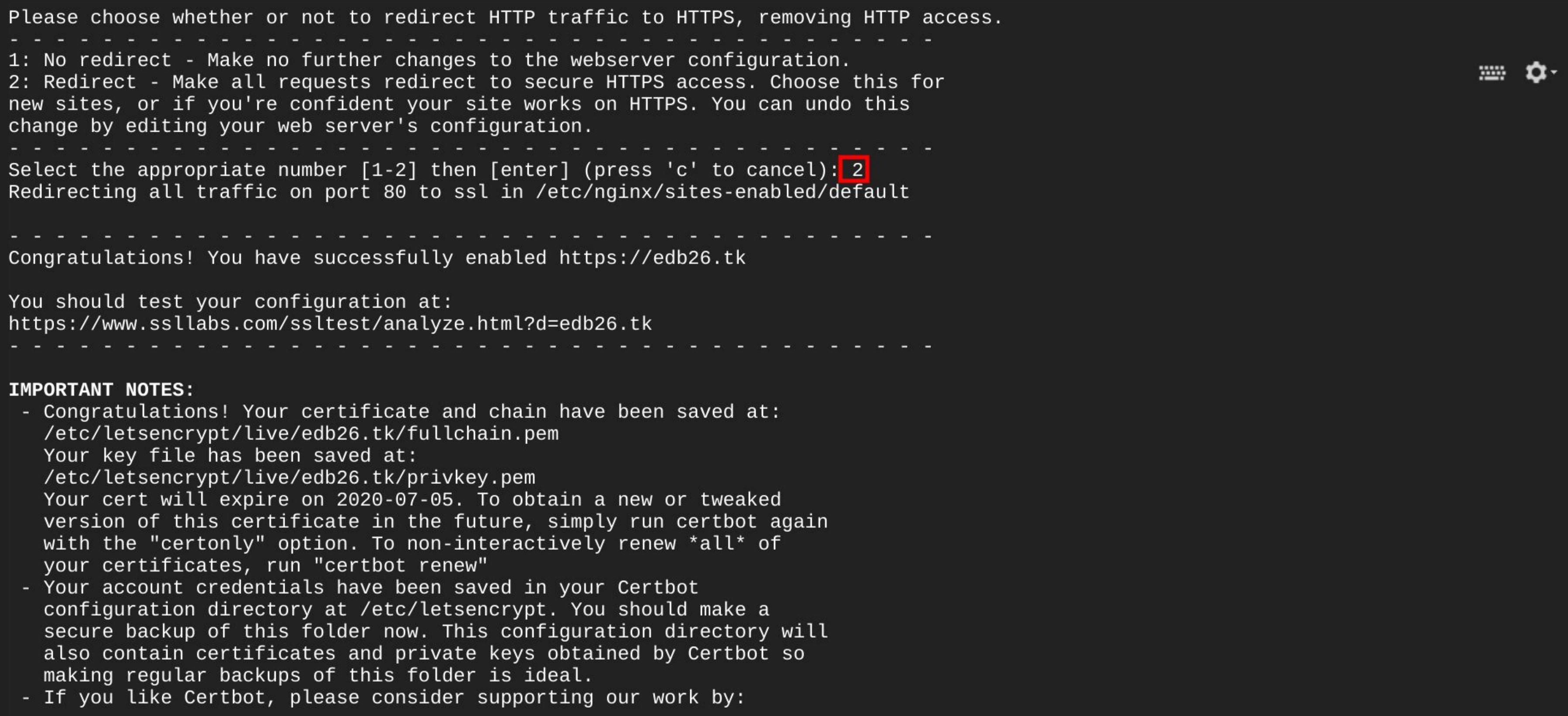
1.4 Configure Nginx with Let's Encrypt Certificate



shoulderhu@ubuntu: ~ - Google Chrome
ssh.cloud.google.com/projects/internal-network-attack/zones/us-central1-a/instances/ubuntu?authuser=0&hl=en_US&projectNumber=561910243416

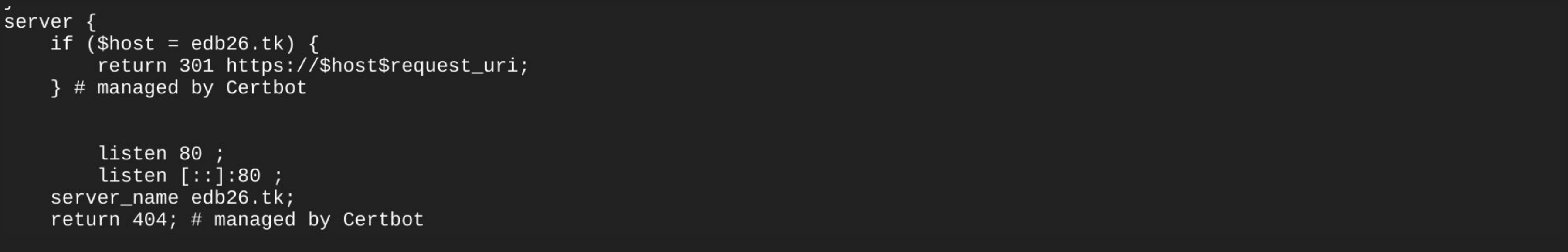
```
shoulderhu@ubuntu:~$ sudo certbot --nginx
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator nginx, Installer nginx
Enter email address (used for urgent renewal and security notices) (Enter 'c' to
cancel): shoulderhu@gmail.com

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. You must
agree in order to register with the ACME server at
https://acme-v02.api.letsencrypt.org/directory
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(A)gree/(C)ancel: A

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Would you be willing to share your email address with the Electronic Frontier
Foundation, a founding partner of the Let's Encrypt project and the non-profit
organization that develops Certbot? We'd like to send you email about our work
encrypting the web, EFF news, campaigns, and ways to support digital freedom.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: N
No names were found in your configuration files. Please enter in your domain
name(s) (comma and/or space separated)  (Enter 'c' to cancel): edb26.tk
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for edb26.tk
Waiting for verification...
Cleaning up challenges
Deploying Certificate to VirtualHost /etc/nginx/sites-enabled/default
```

1.4 Configure Nginx with Let's Encrypt Certificate

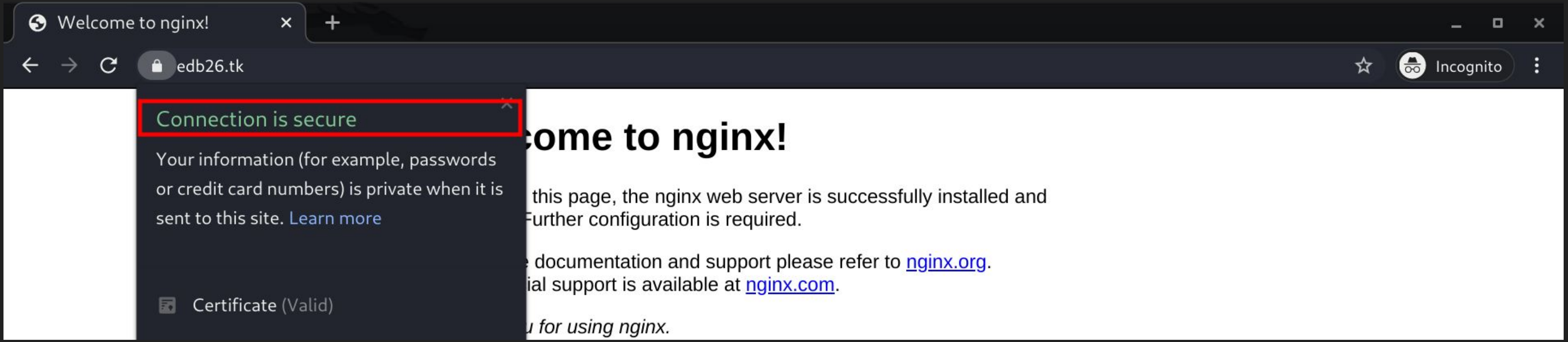


```
Please choose whether or not to redirect HTTP traffic to HTTPS, removing HTTP access.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: No redirect - Make no further changes to the webserver configuration.
2: Redirect - Make all requests redirect to secure HTTPS access. Choose this for
new sites, or if you're confident your site works on HTTPS. You can undo this
change by editing your web server's configuration.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate number [1-2] then [enter] (press 'c' to cancel): 2
Redirecting all traffic on port 80 to ssl in /etc/nginx/sites-enabled/default

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Congratulations! You have successfully enabled https://edb26.tk

You should test your configuration at:
https://www.ssllabs.com/ssltest/analyze.html?d=edb26.tk
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/edb26.tk/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/edb26.tk/privkey.pem
   Your cert will expire on 2020-07-05. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot again
   with the "certonly" option. To non-interactively renew *all* of
   your certificates, run "certbot renew"
 - Your account credentials have been saved in your Certbot
   configuration directory at /etc/letsencrypt. You should make a
   secure backup of this folder now. This configuration directory will
   also contain certificates and private keys obtained by Certbot so
   making regular backups of this folder is ideal.
 - If you like Certbot, please consider supporting our work by:
```

1.4 Configure Nginx with Let's Encrypt Certificate



```
server {
    if ($host = edb26.tk) {
        return 301 https://$host$request_uri;
    } # managed by Certbot


        listen 80 ;
        listen [::]:80 ;
    server_name edb26.tk;
    return 404; # managed by Certbot
```



Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Certificate (Valid)

ome to nginx!

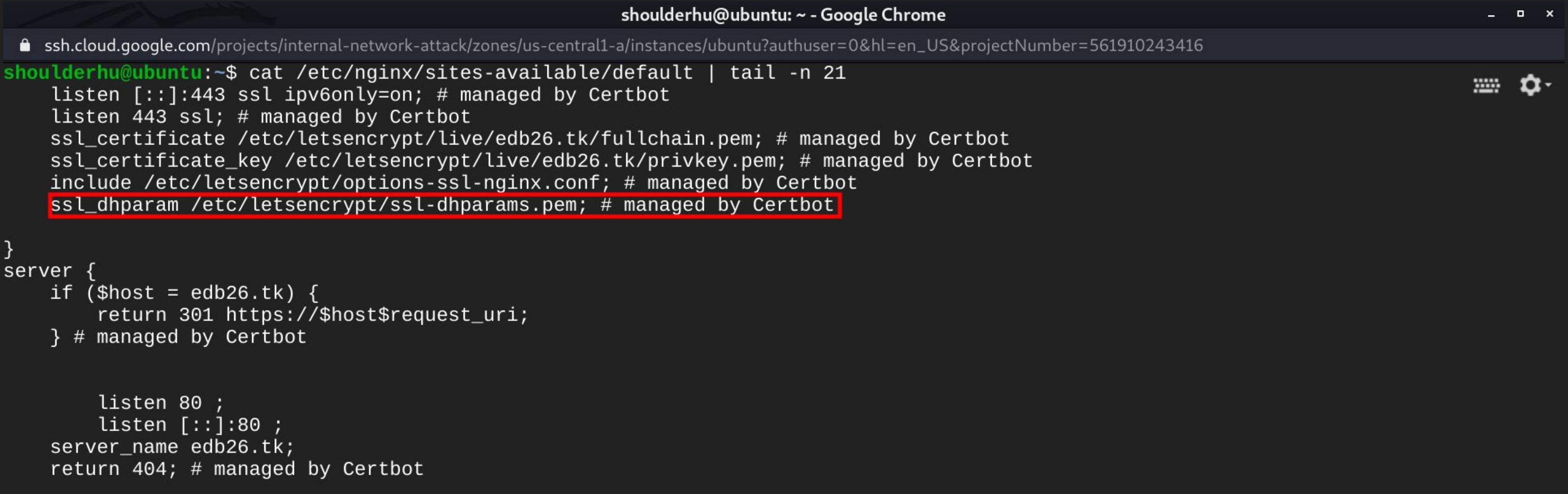
this page, the nginx web server is successfully installed and
Further configuration is required.

documentation and support please refer to nginx.org.
ial support is available at nginx.com.

u for using nginx.

1.5 Check SSL Perfect Forward Secrecy

- /etc/nginx/sites-available/default



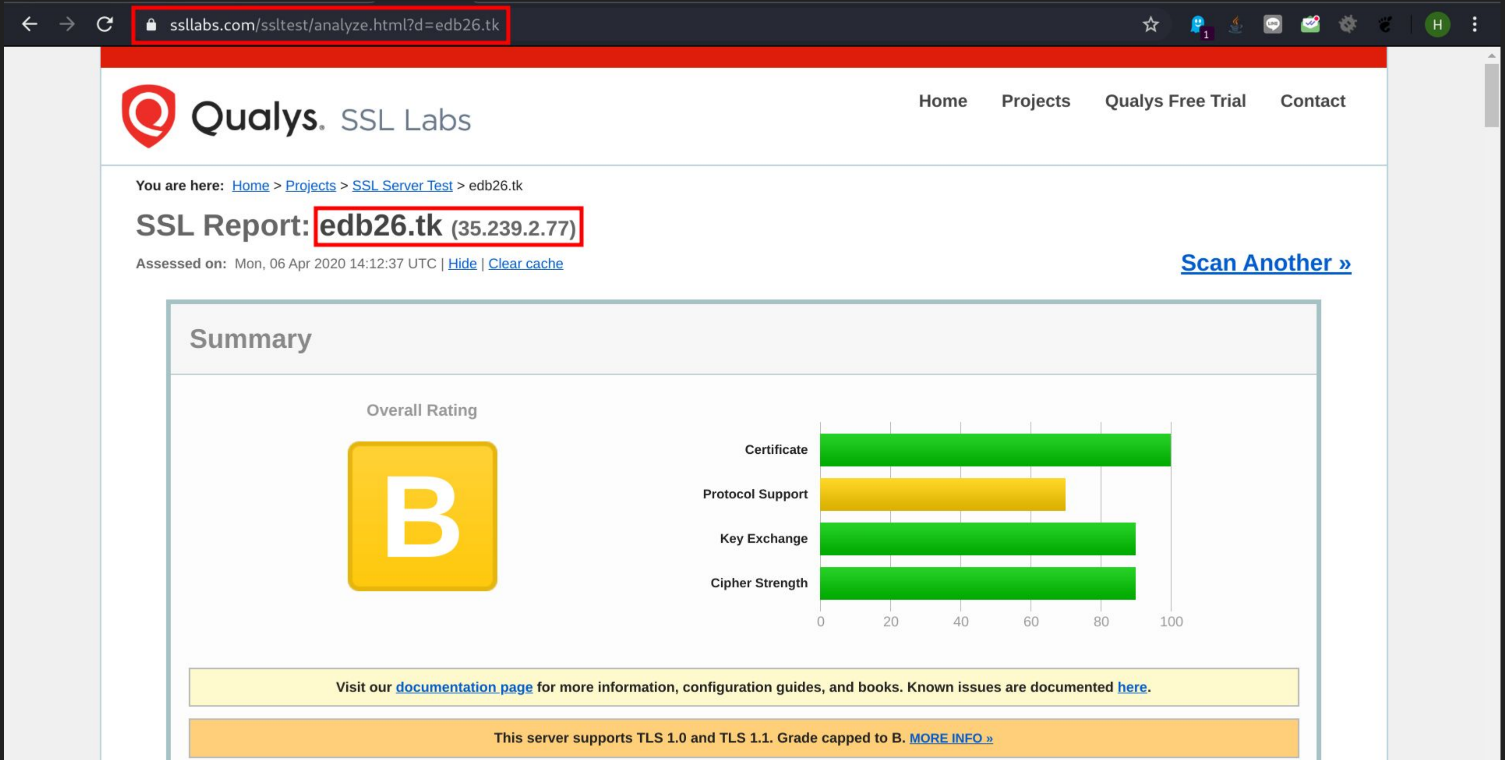
shoulderhu@ubuntu: ~ - Google Chrome

ssh.cloud.google.com/projects/internal-network-attack/zones/us-central1-a/instances/ubuntu?authuser=0&hl=en_US&projectNumber=561910243416

```
shoulderhu@ubuntu:~$ cat /etc/nginx/sites-available/default | tail -n 21
    listen [::]:443 ssl ipv6only=on; # managed by Certbot
    listen 443 ssl; # managed by Certbot
    ssl_certificate /etc/letsencrypt/live/edb26.tk/fullchain.pem; # managed by Certbot
    ssl_certificate_key /etc/letsencrypt/live/edb26.tk/privkey.pem; # managed by Certbot
    include /etc/letsencrypt/options-ssl-nginx.conf; # managed by Certbot
    ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem; # managed by Certbot

}
server {
    if ($host = edb26.tk) {
        return 301 https://$host$request_uri;
    } # managed by Certbot


        listen 80 ;
        listen [::]:80 ;
    server_name edb26.tk;
    return 404; # managed by Certbot
```

1.5 Check SSL Perfect Forward Secrecy

- SSL Labs



You are here: Home > Projects > SSL Server Test > edb26.tk

SSL Report: edb26.tk (35.239.2.77)

Assessed on: Mon, 06 Apr 2020 14:12:37 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

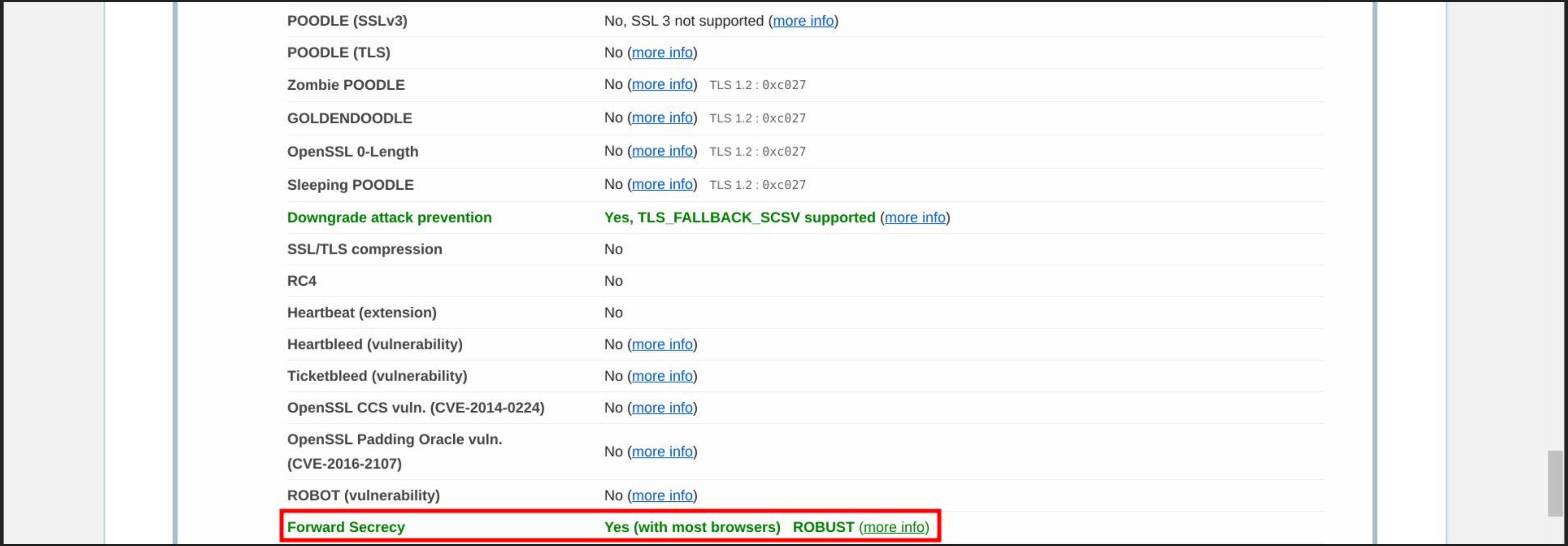
B

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »

1.5 Check SSL Perfect Forward Secrecy

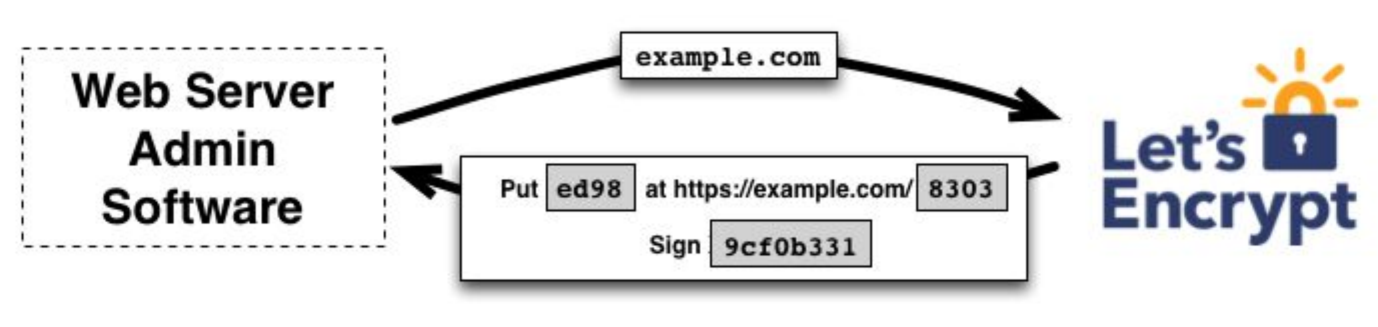
- SSL Labs



POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info) TLS 1.2 : 0xc027
GOLDENDOODLE	No (more info) TLS 1.2 : 0xc027
OpenSSL 0-Length	No (more info) TLS 1.2 : 0xc027
Sleeping POODLE	No (more info) TLS 1.2 : 0xc027
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
ROBOT (vulnerability)	No (more info)
Forward Secrecy	Yes (with most browsers) ROBUST (more info)

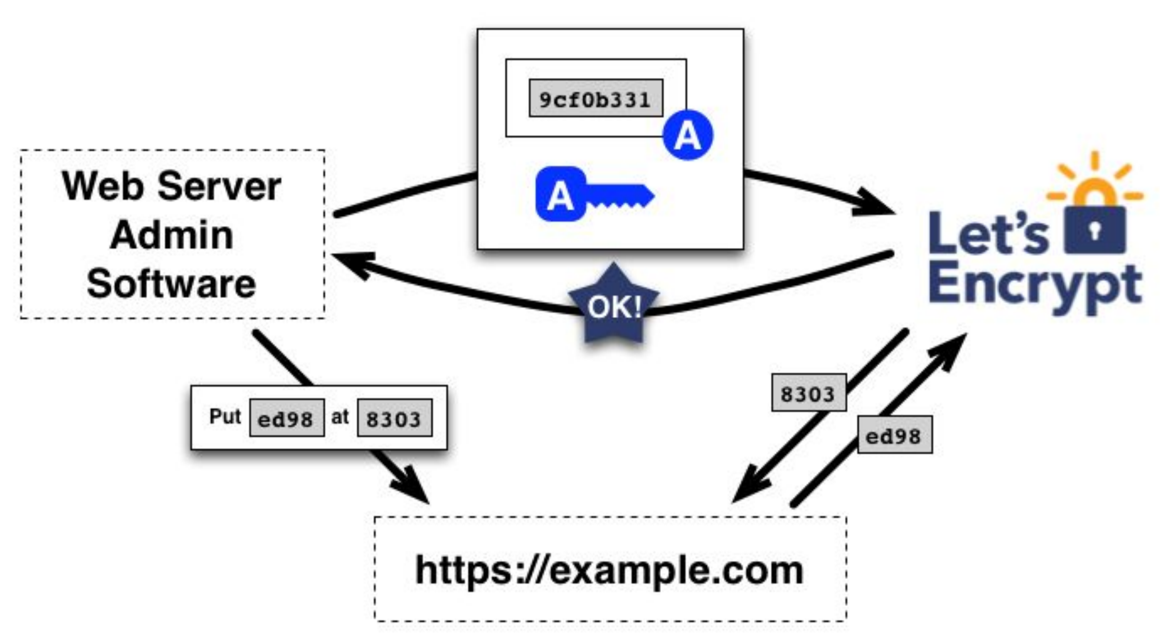
1.6 ACME protocol

- Domain Validation
  - Provisioning a **DNS record** under example.com, or
  - Provisioning an HTTP resource under a well-known URI on http://example.com/


Web Server Admin Software
example.com
Let's Encrypt
Put ed98 at https://example.com/ 8303
Sign 9cf0b331

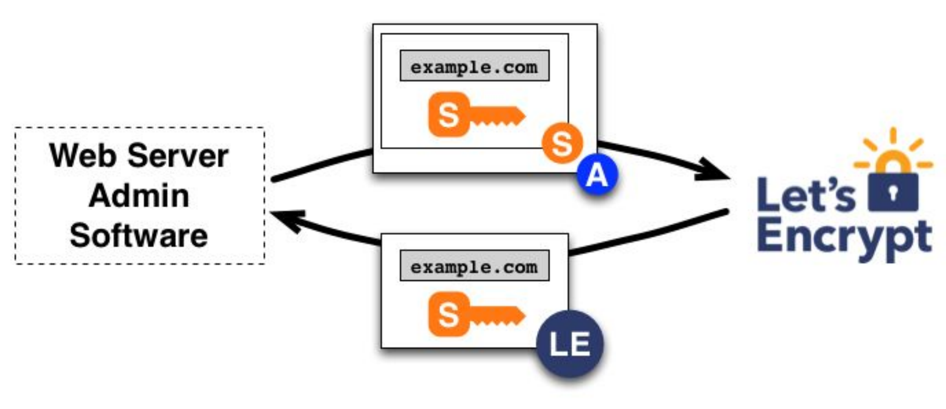
1.6 ACME protocol

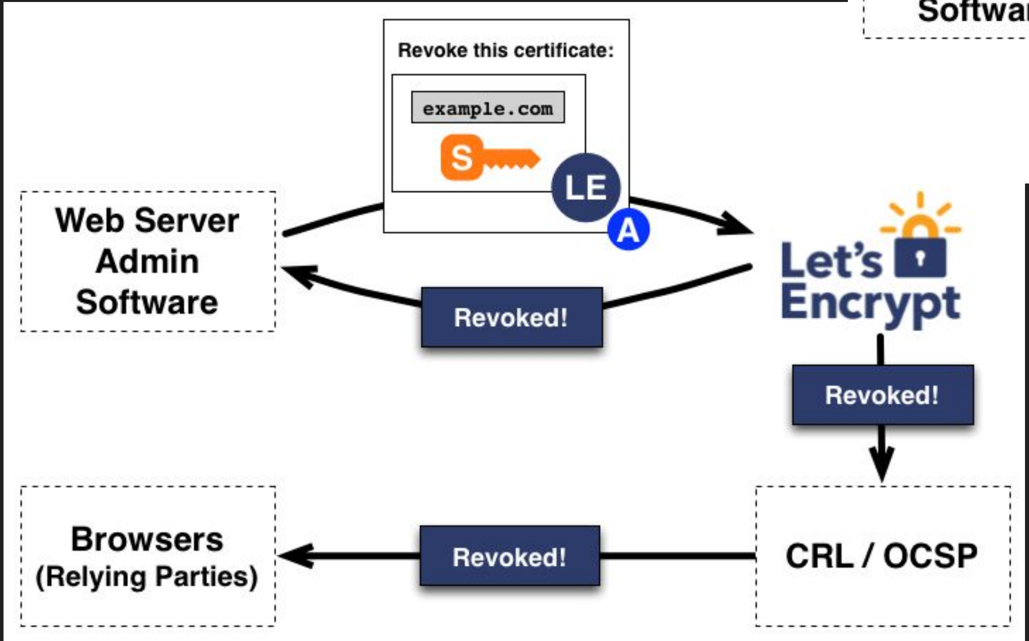
- Domain Validation



1.6 ACME protocol

- Certificate Issuance & Revocation

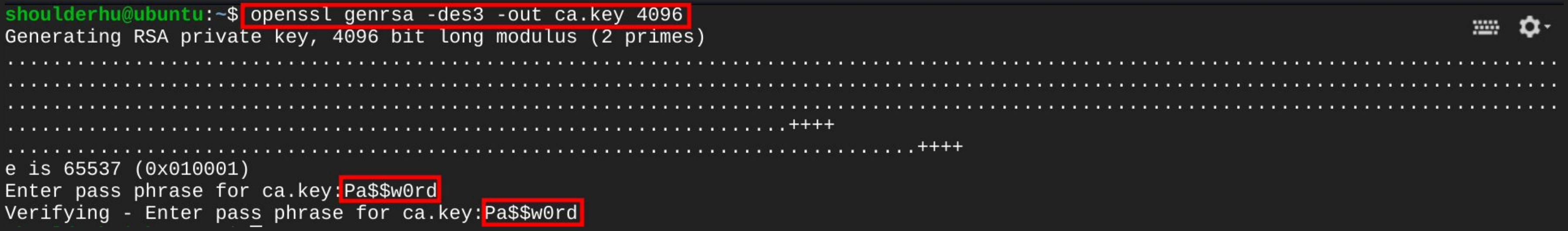




Self-signed certificate

2.1 Create Root CA

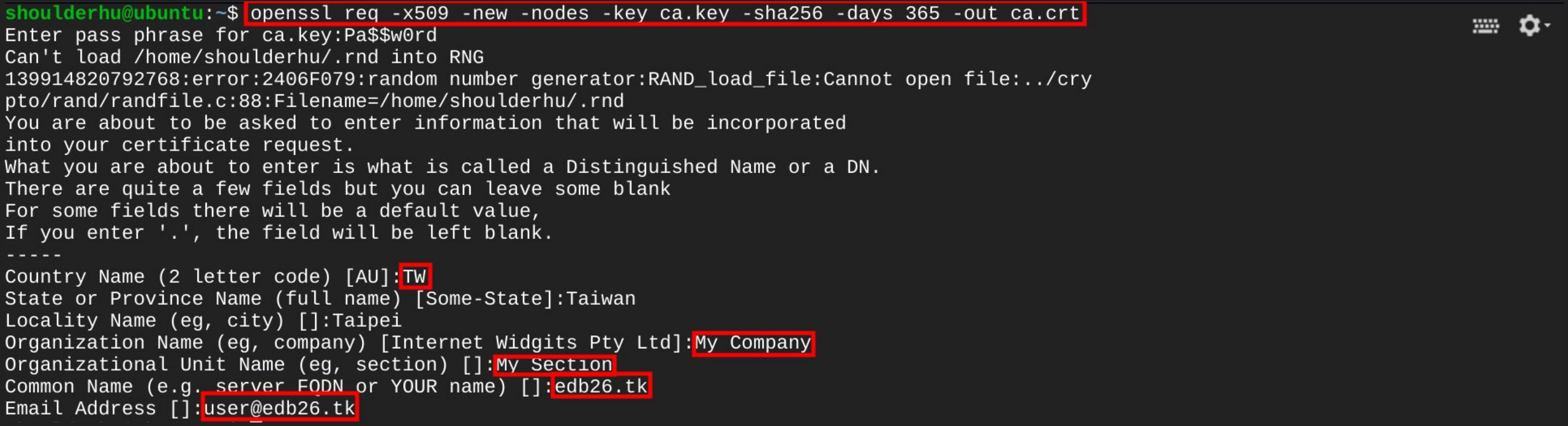
- Create Root CA Key
  - openssl genrsa -des3 -out ca.key 4096
- Create self-signed Root CA Certificate
  - openssl req -x509 -new -nodes -key ca.key -sha256 -days 365 -out ca.crt



```
shoulderhu@ubuntu:~$ openssl genrsa -des3 -out ca.key 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................................................................................
.....................................................................................................................................
.....................................................................................................................................
...................................................................++++
..............................................................................++++
e is 65537 (0x010001)
Enter pass phrase for ca.key:Pa$$w0rd
Verifying - Enter pass phrase for ca.key:Pa$$w0rd
```

2.1 Create Root CA

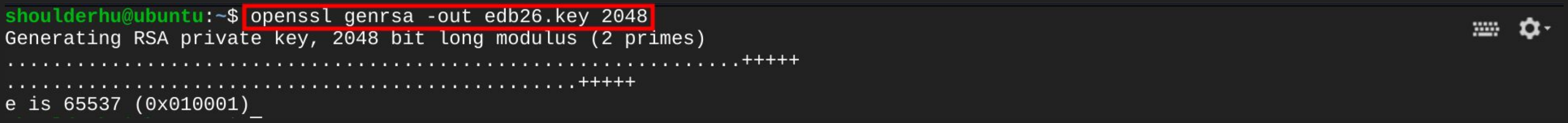
- Create Root CA Key
  - openssl genrsa -des3 -out ca.key 4096
- Create self-signed Root CA Certificate
  - openssl req -x509 -new -nodes -key ca.key -sha256 -days 365 -out ca.crt



```
shoulderhu@ubuntu:~$ openssl req -x509 -new -nodes -key ca.key -sha256 -days 365 -out ca.crt
Enter pass phrase for ca.key:Pa$$w0rd
Can't load /home/shoulderhu/.rnd into RNG
139914820792768:error:2406F079:random number generator:RAND_load_file:Cannot open file:../cry
pto/rand/randfile.c:88:Filename=/home/shoulderhu/.rnd
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:TW
State or Province Name (full name) [Some-State]:Taiwan
Locality Name (eg, city) []:Taipei
Organization Name (eg, company) [Internet Widgits Pty Ltd]:My Company
Organizational Unit Name (eg, section) []:My Section
Common Name (e.g. server FQDN or YOUR name) []:edb26.tk
Email Address []:user@edb26.tk
```

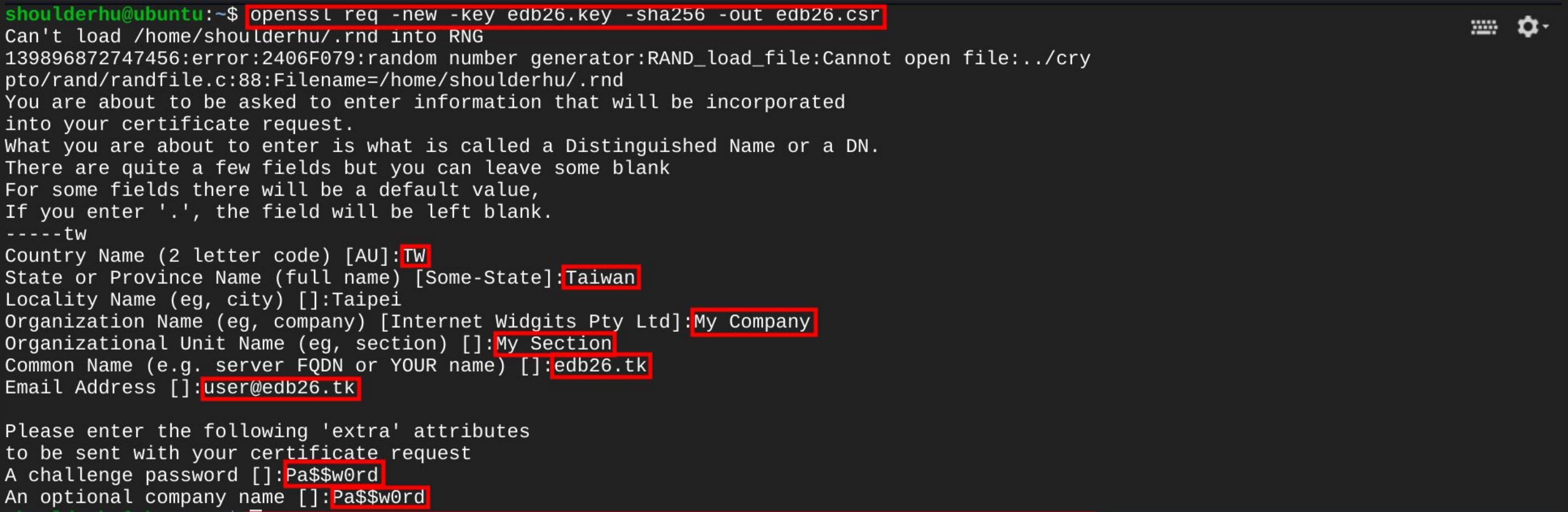
2.2 Create Server Certificate

- Create Server Key
  - openssl genrsa -out edb26.key 2048
- Create Server Certificate Signing Request (CSR)
  - openssl req -new -key edb26.key -sha256 -out edb26.csr
- Create Server Certificate using Root CA Key
  - openssl x509 -req -in edb26.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out edb26.crt -days 90 -sha256

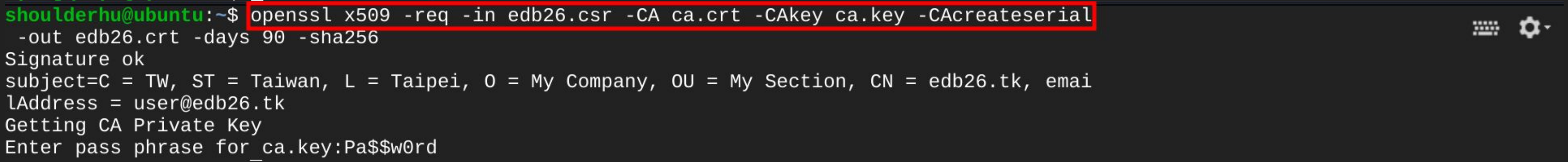


```
shoulderhu@ubuntu:~$ openssl genrsa -out edb26.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
..............................................................+++++
................................................+++++
e is 65537 (0x010001)_
```

2.2 Create Server Certificate



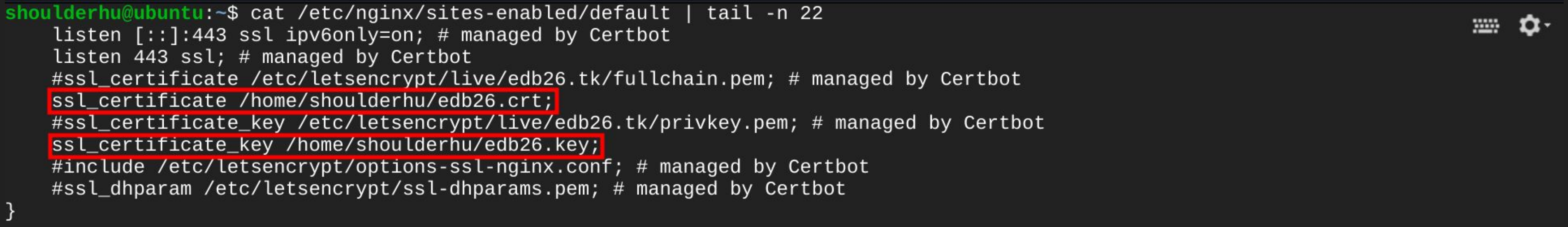
```
shoulderhu@ubuntu:~$ openssl req -new -key edb26.key -sha256 -out edb26.csr
Can't load /home/shoulderhu/.rnd into RNG
139896872747456:error:2406F079:random number generator:RAND_load_file:Cannot open file:../cry
pto/rand/randfile.c:88:Filename=/home/shoulderhu/.rnd
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----tw
Country Name (2 letter code) [AU]:TW
State or Province Name (full name) [Some-State]:Taiwan
Locality Name (eg, city) []:Taipei
Organization Name (eg, company) [Internet Widgits Pty Ltd]:My Company
Organizational Unit Name (eg, section) []:My Section
Common Name (e.g. server FQDN or YOUR name) []:edb26.tk
Email Address []:user@edb26.tk

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:Pa$$w0rd
An optional company name []:Pa$$w0rd
```



```
shoulderhu@ubuntu:~$ openssl x509 -req -in edb26.csr -CA ca.crt -CAkey ca.key -CAcreateserial
 -out edb26.crt -days 90 -sha256
Signature ok
subject=C = TW, ST = Taiwan, L = Taipei, O = My Company, OU = My Section, CN = edb26.tk, emai
lAddress = user@edb26.tk
Getting CA Private Key
Enter pass phrase for ca.key:Pa$$w0rd
```

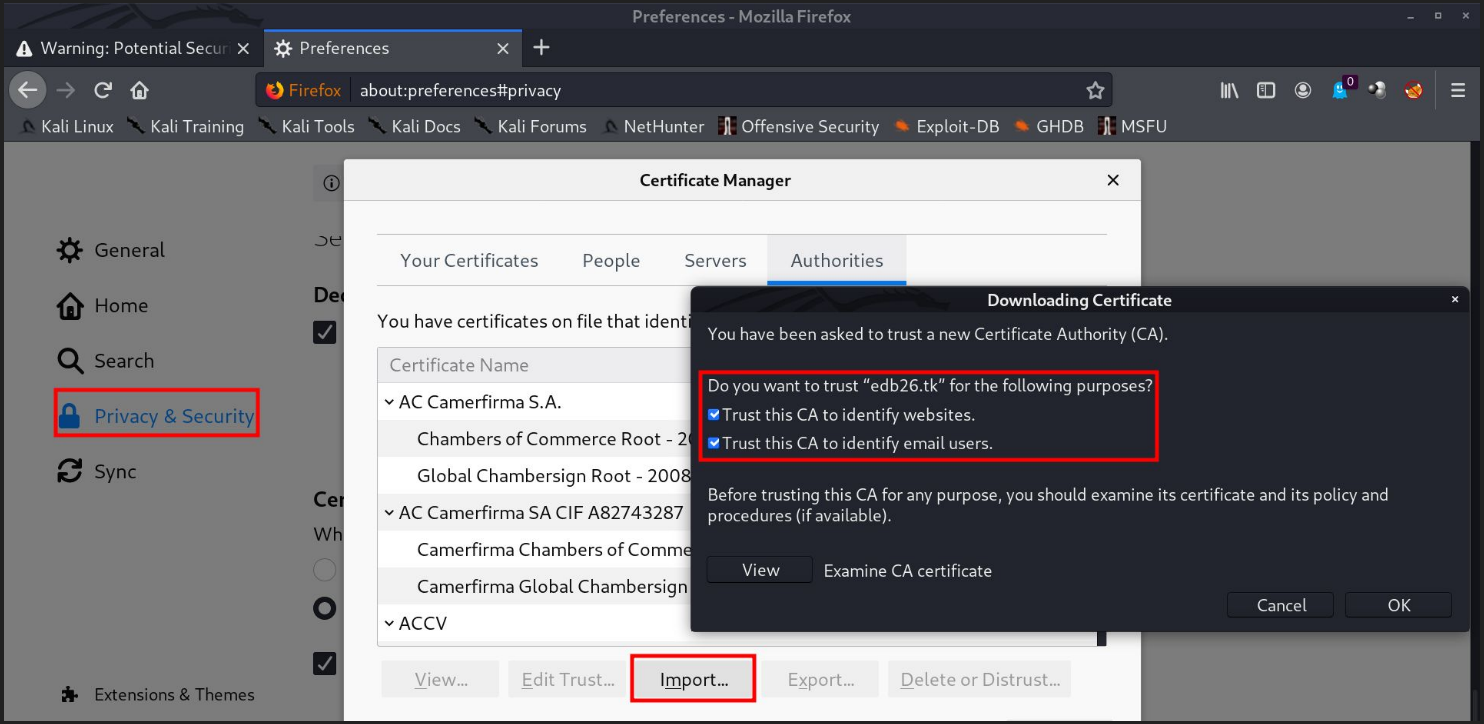
2.3 Modify Nginx Configuration file

- /etc/nginx/sites-enabled/default
  - ssl_certificate /home/shoulderhu/edb26.crt;
  - ssl_certificate_key /home/shoulderhu/edb26.key;



```
shoulderhu@ubuntu:~$ cat /etc/nginx/sites-enabled/default | tail -n 22
    listen [::]:443 ssl ipv6only=on; # managed by Certbot
    listen 443 ssl; # managed by Certbot
    #ssl_certificate /etc/letsencrypt/live/edb26.tk/fullchain.pem; # managed by Certbot
    ssl_certificate /home/shoulderhu/edb26.crt;
    #ssl_certificate_key /etc/letsencrypt/live/edb26.tk/privkey.pem; # managed by Certbot
    ssl_certificate_key /home/shoulderhu/edb26.key;
    #include /etc/letsencrypt/options-ssl-nginx.conf; # managed by Certbot
    #ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem; # managed by Certbot
}
```

2.4 Add Root CA Certificate to Firefox



Certificate Manager

Your Certificates | People | Servers | Authorities

You have certificates on file that identi

Certificate Name
AC Camerfirma S.A.
Chambers of Commerce Root - 2(
Global Chambersign Root - 2008
AC Camerfirma SA CIF A82743287
Camerfirma Chambers of Comme
Camerfirma Global Chambersign
ACCV

View... Edit Trust... Import... Export... Delete or Distrust...

Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "edb26.tk" for the following purposes?

☑ Trust this CA to identify websites.

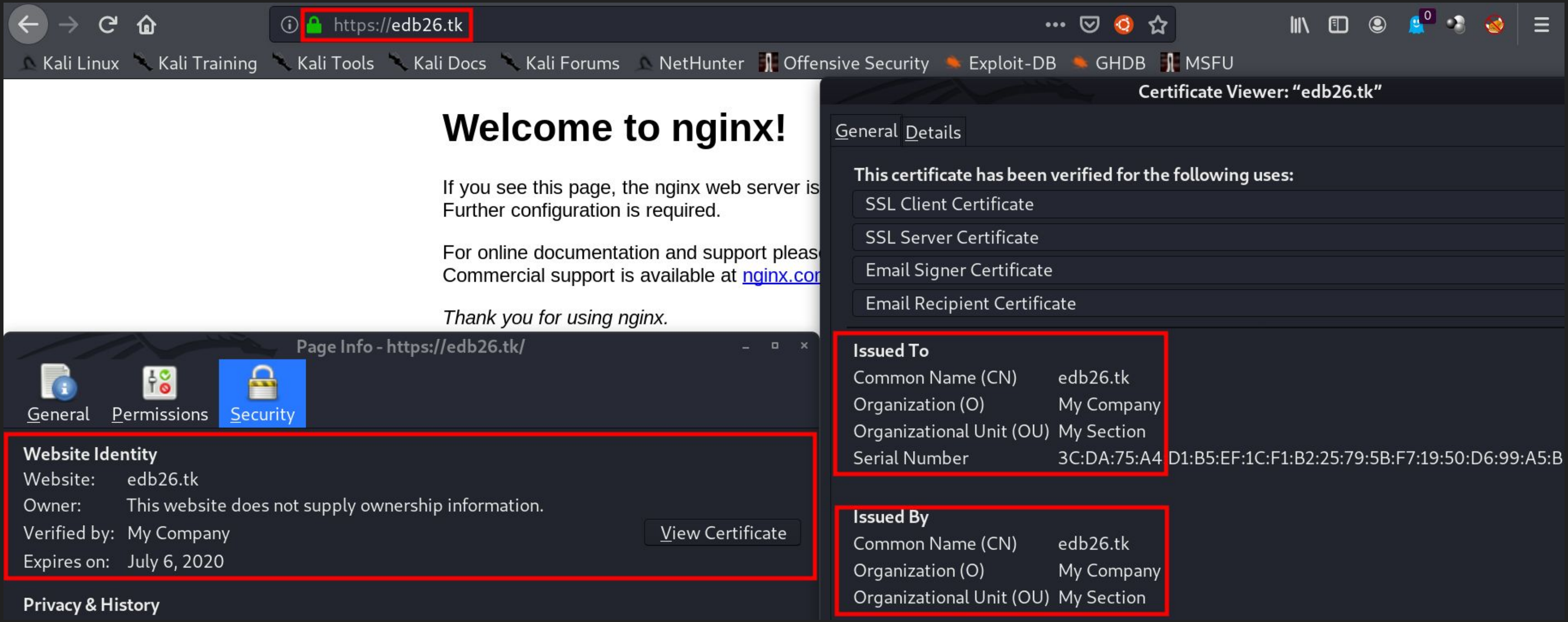
☑ Trust this CA to identify email users.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

View Examine CA certificate

Cancel OK

2.4 Add Root CA Certificate to Firefox



Welcome to nginx!

If you see this page, the nginx web server is
Further configuration is required.

For online documentation and support pleas
Commercial support is available at nginx.cor

Thank you for using nginx.

Page Info - https://edb26.tk/

Website Identity

Website:	edb26.tk
Owner:	This website does not supply ownership information.
Verified by:	My Company
Expires on:	July 6, 2020

Privacy & History

Certificate Viewer: “edb26.tk”

This certificate has been verified for the following uses:

SSL Client Certificate

SSL Server Certificate

Email Signer Certificate

Email Recipient Certificate

Issued To

Common Name (CN)	edb26.tk
Organization (O)	My Company
Organizational Unit (OU)	My Section
Serial Number	3C:DA:75:A4:D1:B5:EF:1C:F1:B2:25:79:5B:F7:19:50:D6:99:A5:B

Issued By

Common Name (CN)	edb26.tk
Organization (O)	My Company
Organizational Unit (OU)	My Section

Use man-in-the-middle to decrypt HTTPS encryption

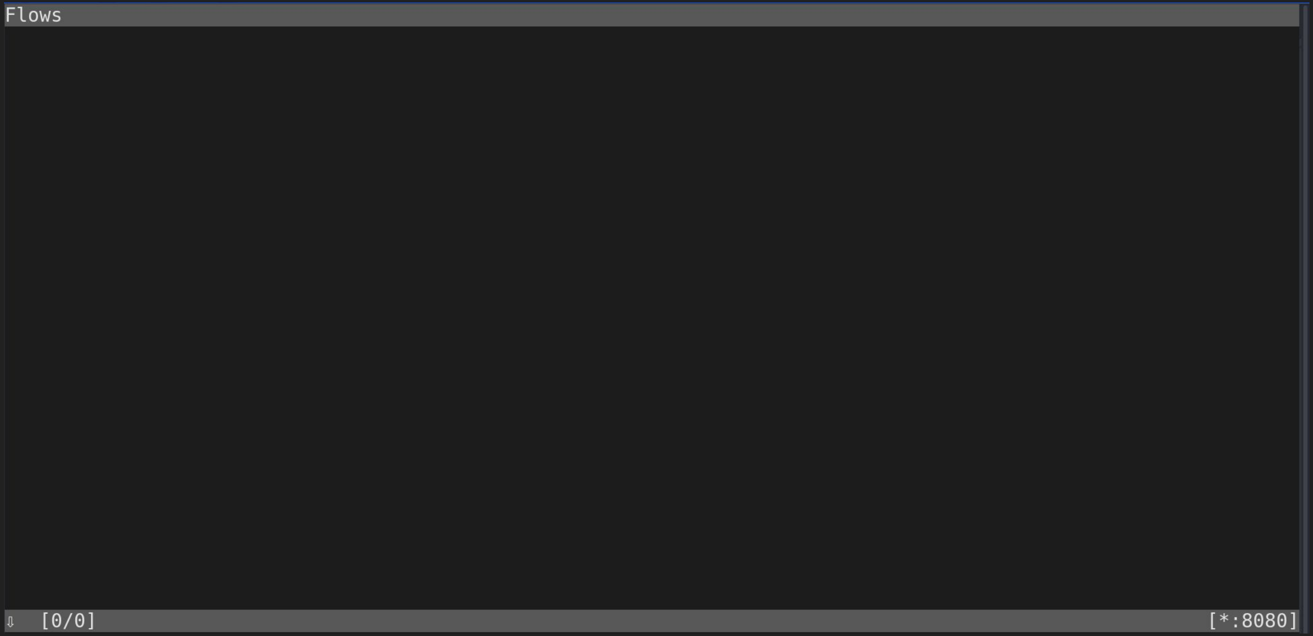
3.1 Get mitmproxy

- wget https://snapshots.mitmproxy.org/5.0.1/mitmproxy-5.0.1-linux.tar.gz
- tar xzvf mitmproxy-5.0.1-linux.tar.gz

  ```
  # mitmproxy
  # mitmdump
  # mitmweb
  ```

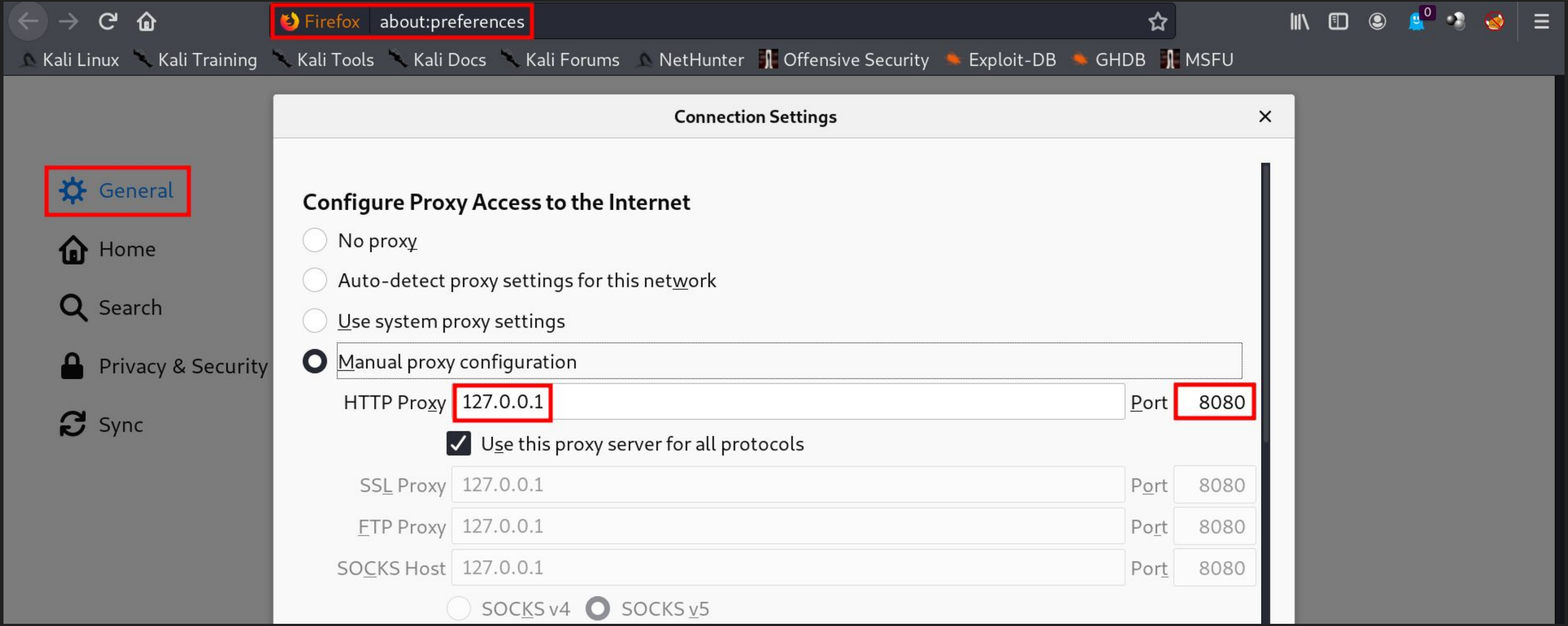
3.2 Start mitmproxy

- ./mitmproxy -p <port>



```
Flows





⇩  [0/0]                                                                   [*:8080]
```

3.3 Setup Firefox & Install mitmproxy Root CA



Connection Settings

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☑ Use this proxy server for all protocols

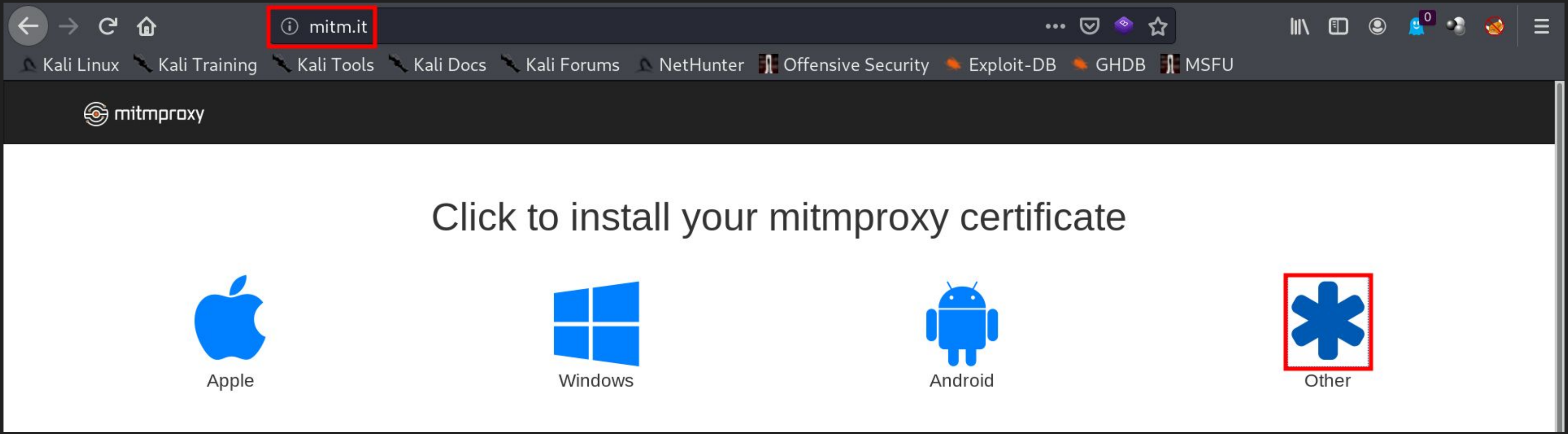
SSL Proxy 127.0.0.1 Port 8080

FTP Proxy 127.0.0.1 Port 8080

SOCKS Host 127.0.0.1 Port 8080

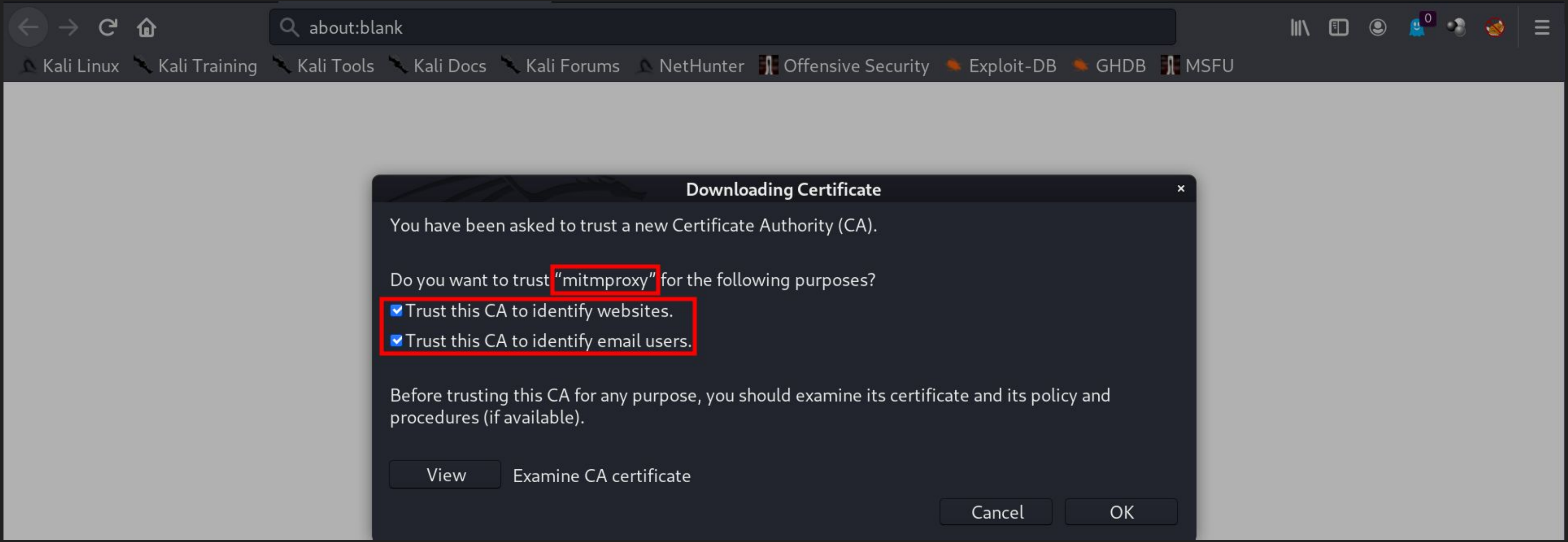
○ SOCKS v4 ● SOCKS v5

3.3 Setup Firefox & Install mitmproxy Root CA



Click to install your mitmproxy certificate

3.3 Setup Firefox & Install mitmproxy Root CA



Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "mitmproxy" for the following purposes?

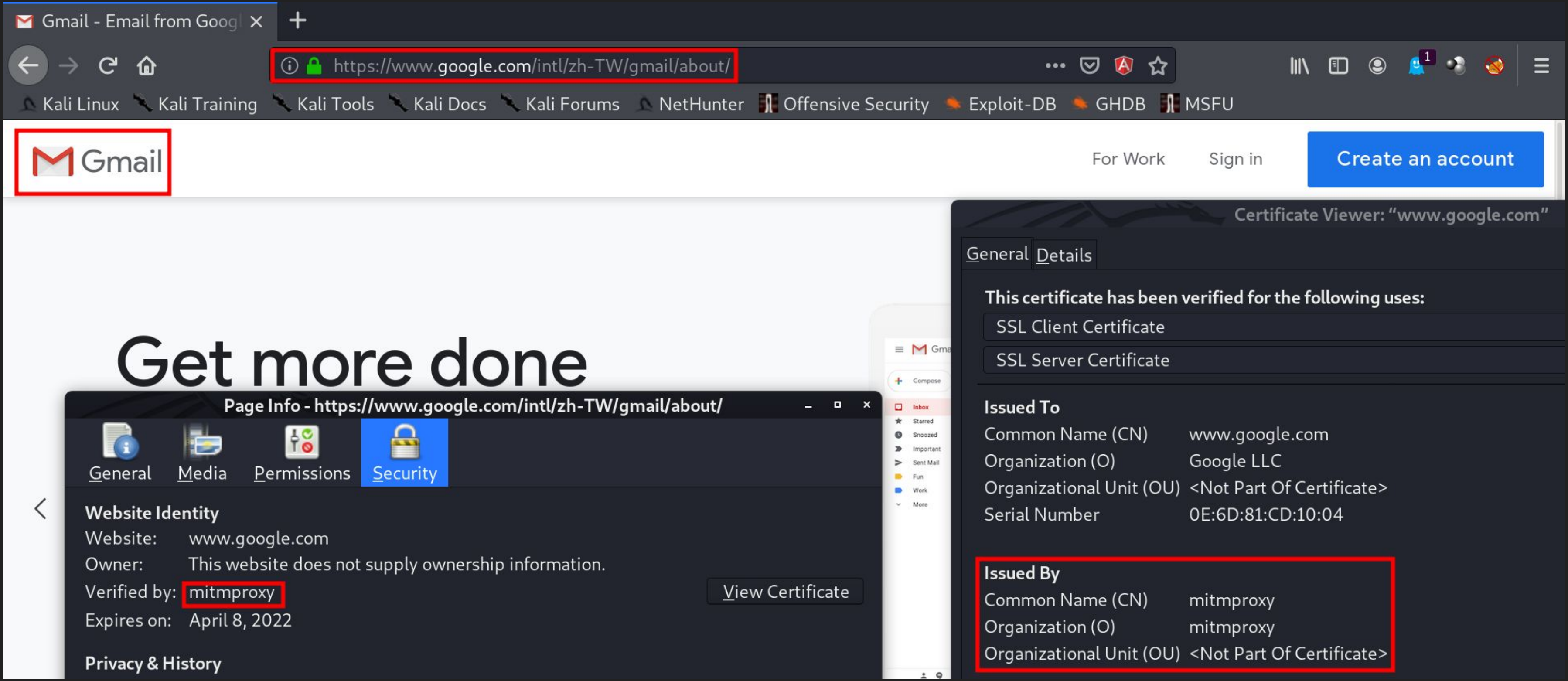
☑ Trust this CA to identify websites.

☑ Trust this CA to identify email users.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

View Examine CA certificate

3.4 Intercept & Decrypt HTTPS connection



Page Info - https://www.google.com/intl/zh-TW/gmail/about/

Website Identity

Website: www.google.com

Owner: This website does not supply ownership information.

Verified by: mitmproxy

Expires on: April 8, 2022

Privacy & History

Certificate Viewer: "www.google.com"

This certificate has been verified for the following uses:

SSL Client Certificate

SSL Server Certificate

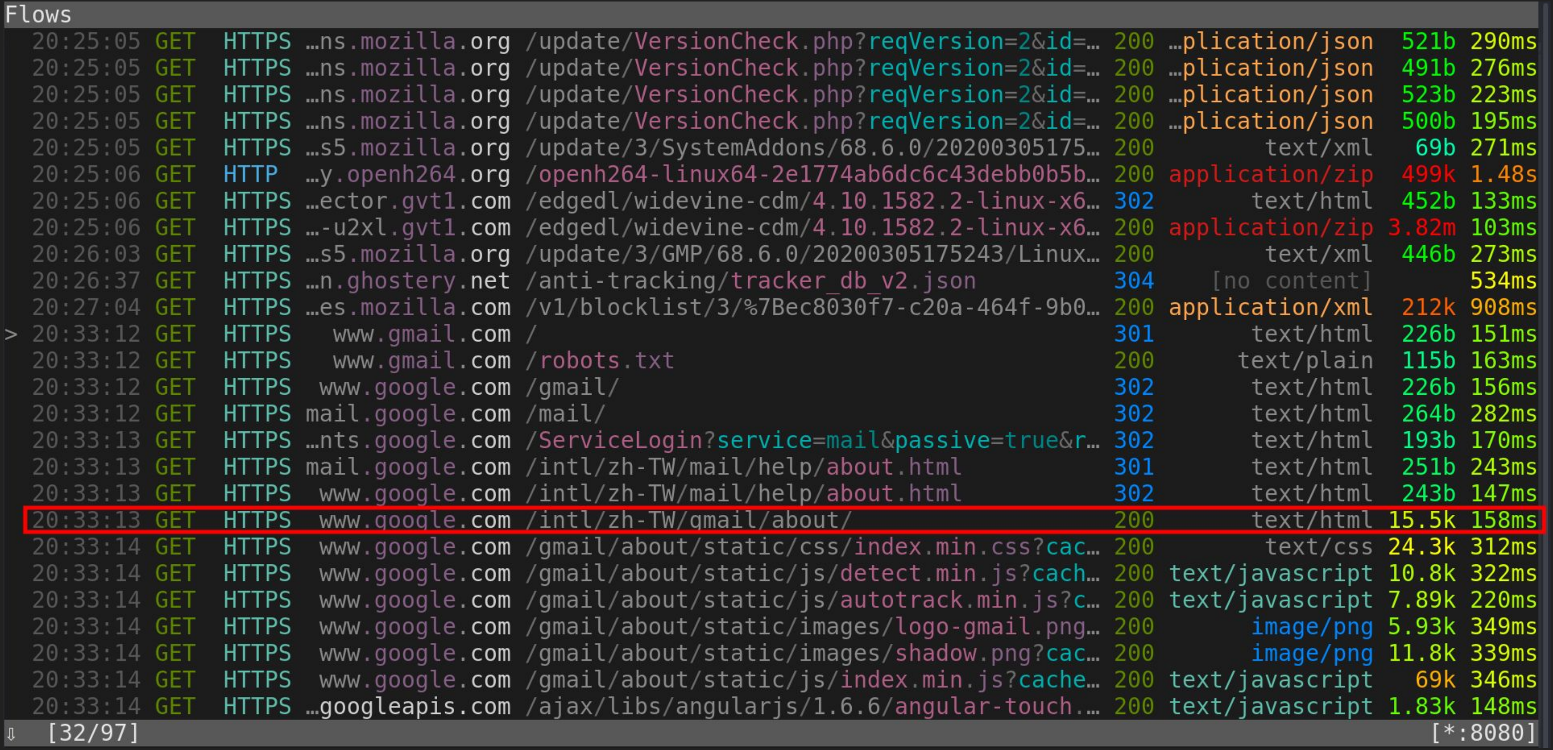
Issued To

Common Name (CN)	www.google.com
Organization (O)	Google LLC
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	0E:6D:81:CD:10:04

Issued By

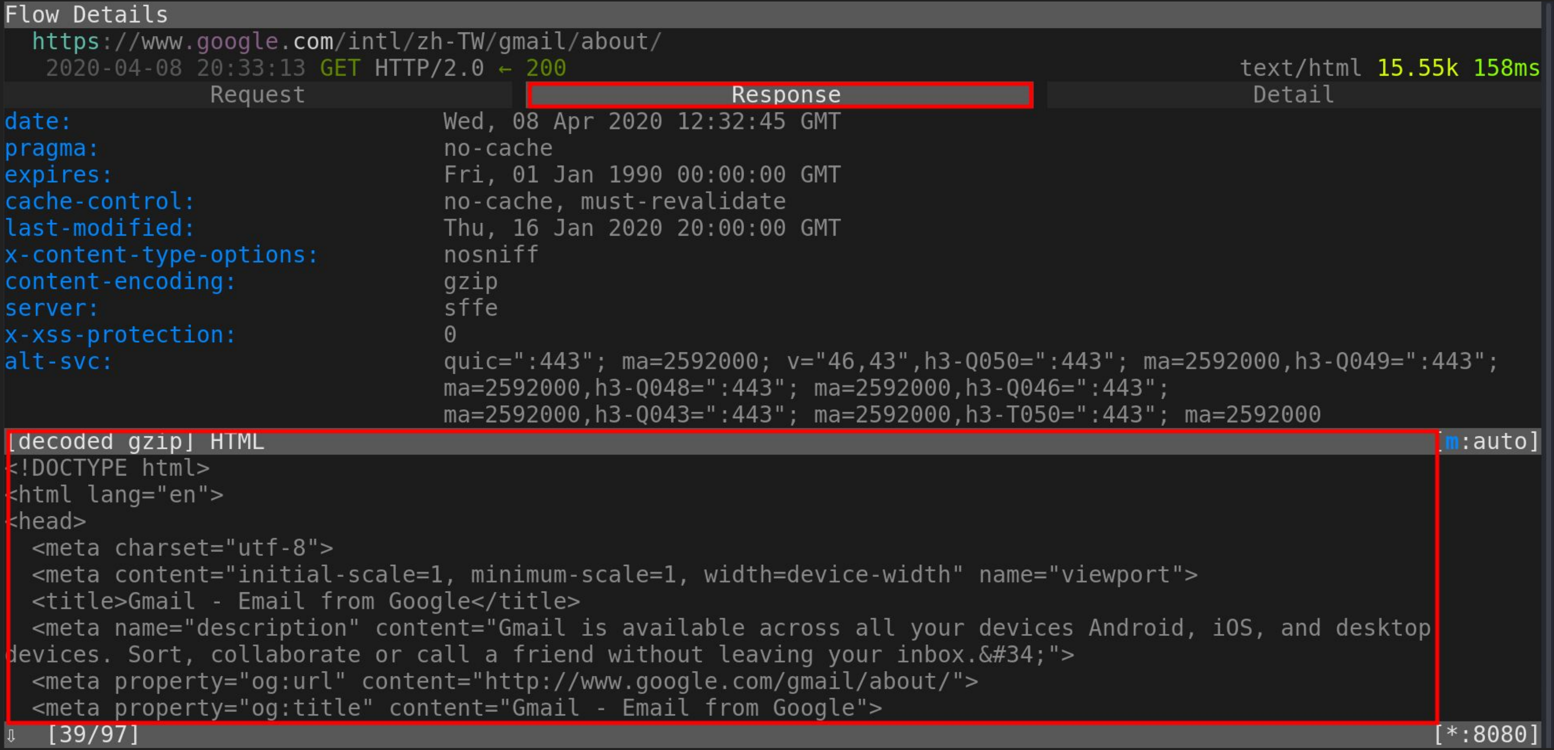
Common Name (CN)	mitmproxy
Organization (O)	mitmproxy
Organizational Unit (OU)	<Not Part Of Certificate>

3.4 Intercept & Decrypt HTTPS connection



```
Flows
  20:25:05 GET   HTTPS …ns.mozilla.org /update/VersionCheck.php?reqVersion=2&id=… 200 …plication/json  521b 290ms
  20:25:05 GET   HTTPS …ns.mozilla.org /update/VersionCheck.php?reqVersion=2&id=… 200 …plication/json  491b 276ms
  20:25:05 GET   HTTPS …ns.mozilla.org /update/VersionCheck.php?reqVersion=2&id=… 200 …plication/json  523b 223ms
  20:25:05 GET   HTTPS …ns.mozilla.org /update/VersionCheck.php?reqVersion=2&id=… 200 …plication/json  500b 195ms
  20:25:05 GET   HTTPS …s5.mozilla.org /update/3/SystemAddons/68.6.0/20200305175… 200        text/xml   69b 271ms
  20:25:06 GET   HTTP  …y.openh264.org /openh264-linux64-2e1774ab6dc6c43debb0b5b… 200 application/zip 499k 1.48s
  20:25:06 GET   HTTPS …ector.gvt1.com /edgedl/widevine-cdm/4.10.1582.2-linux-x6… 302       text/html  452b 133ms
  20:25:06 GET   HTTPS …-u2xl.gvt1.com /edgedl/widevine-cdm/4.10.1582.2-linux-x6… 200 application/zip 3.82m 103ms
  20:26:03 GET   HTTPS …s5.mozilla.org /update/3/GMP/68.6.0/20200305175243/Linux… 200        text/xml  446b 273ms
  20:26:37 GET   HTTPS …n.ghostery.net /anti-tracking/tracker_db_v2.json          304    [no content]       534ms
  20:27:04 GET   HTTPS …es.mozilla.com /v1/blocklist/3/%7Bec8030f7-c20a-464f-9b0… 200 application/xml  212k 908ms
> 20:33:12 GET   HTTPS   www.gmail.com /                                          301       text/html  226b 151ms
  20:33:12 GET   HTTPS   www.gmail.com /robots.txt                                200      text/plain  115b 163ms
  20:33:12 GET   HTTPS  www.google.com /gmail/                                    302       text/html  226b 156ms
  20:33:12 GET   HTTPS mail.google.com /mail/                                     302       text/html  264b 282ms
  20:33:13 GET   HTTPS …nts.google.com /ServiceLogin?service=mail&passive=true&r… 302       text/html  193b 170ms
  20:33:13 GET   HTTPS mail.google.com /intl/zh-TW/mail/help/about.html           301       text/html  251b 243ms
  20:33:13 GET   HTTPS  www.google.com /intl/zh-TW/mail/help/about.html           302       text/html  243b 147ms
  20:33:13 GET   HTTPS  www.google.com /intl/zh-TW/gmail/about/                   200       text/html 15.5k 158ms
  20:33:14 GET   HTTPS  www.google.com /gmail/about/static/css/index.min.css?cac… 200        text/css 24.3k 312ms
  20:33:14 GET   HTTPS  www.google.com /gmail/about/static/js/detect.min.js?cach… 200 text/javascript 10.8k 322ms
  20:33:14 GET   HTTPS  www.google.com /gmail/about/static/js/autotrack.min.js?c… 200 text/javascript 7.89k 220ms
  20:33:14 GET   HTTPS  www.google.com /gmail/about/static/images/logo-gmail.png… 200       image/png 5.93k 349ms
  20:33:14 GET   HTTPS  www.google.com /gmail/about/static/images/shadow.png?cac… 200       image/png 11.8k 339ms
  20:33:14 GET   HTTPS  www.google.com /gmail/about/static/js/index.min.js?cache… 200 text/javascript   69k 346ms
  20:33:14 GET   HTTPS …googleapis.com /ajax/libs/angularjs/1.6.6/angular-touch.… 200 text/javascript 1.83k 148ms
⇩  [32/97]                                                                                               [*:8080]
```

3.4 Intercept & Decrypt HTTPS connection



```
Flow Details
  https://www.google.com/intl/zh-TW/gmail/about/
   2020-04-08 20:33:13 GET HTTP/2.0 ← 200                                          text/html 15.55k 158ms
               Request                             Response                             Detail
date:                           Wed, 08 Apr 2020 12:32:45 GMT
pragma:                         no-cache
expires:                        Fri, 01 Jan 1990 00:00:00 GMT
cache-control:                  no-cache, must-revalidate
last-modified:                  Thu, 16 Jan 2020 20:00:00 GMT
x-content-type-options:         nosniff
content-encoding:               gzip
server:                         sffe
x-xss-protection:               0
alt-svc:                        quic=":443"; ma=2592000; v="46,43",h3-Q050=":443"; ma=2592000,h3-Q049=":443";
                                ma=2592000,h3-Q048=":443"; ma=2592000,h3-Q046=":443";
                                ma=2592000,h3-Q043=":443"; ma=2592000,h3-T050=":443"; ma=2592000
[decoded gzip] HTML                                                                                      [m:auto]
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <meta content="initial-scale=1, minimum-scale=1, width=device-width" name="viewport">
  <title>Gmail - Email from Google</title>
  <meta name="description" content="Gmail is available across all your devices Android, iOS, and desktop
devices. Sort, collaborate or call a friend without leaving your inbox.&#34;">
  <meta property="og:url" content="http://www.google.com/gmail/about/">
  <meta property="og:title" content="Gmail - Email from Google">
⇩  [39/97]                                                                                               [*:8080]
```

The End