Jincheng Tian
Security Lab 4, HTTP Breaking

Task1:
Questions

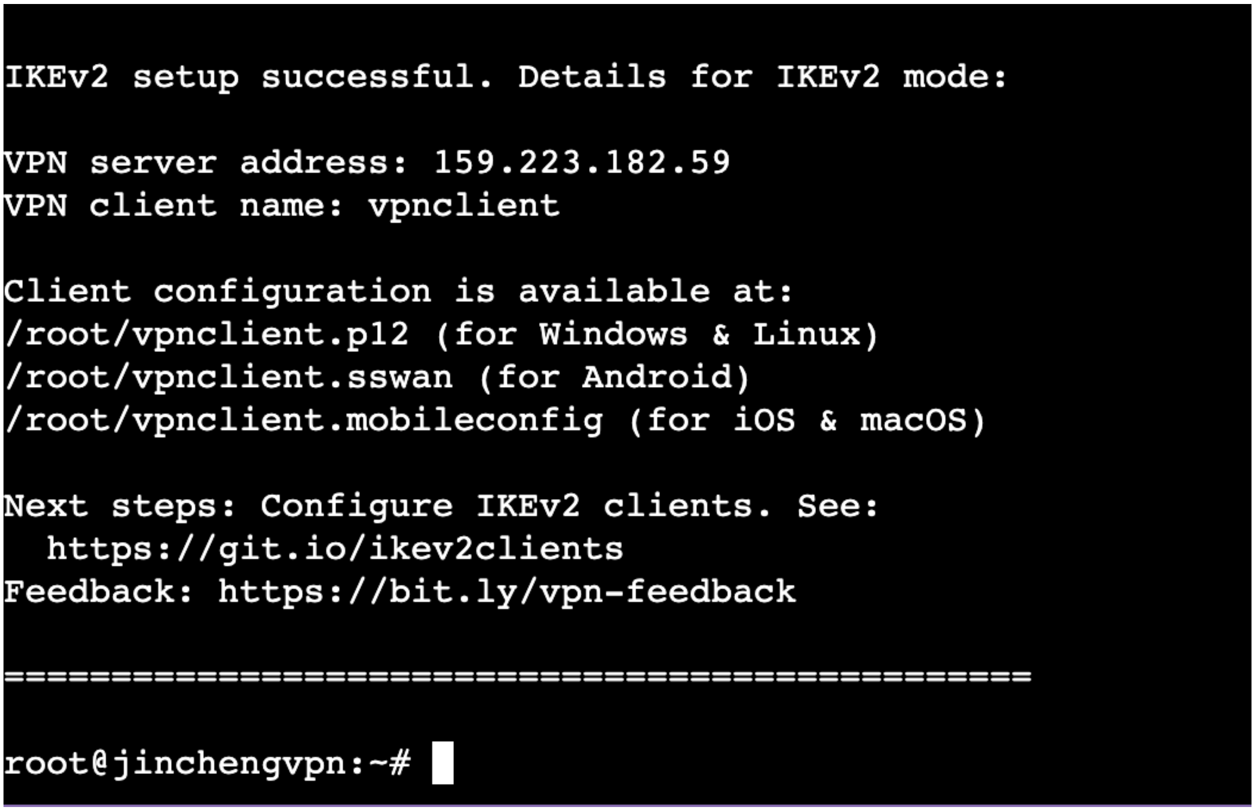
1. **What is the IP address shown in Step 1 above?**

   98.109.152.85

2. **What is the IP address of your Digital Ocean instance (from Step 2 above)?**

   159.223.182.59

3. **Include a screenshot that shows you've set up the L2TP VPN server correctly in Step 3.**



```
IKEv2 setup successful. Details for IKEv2 mode:

VPN server address: 159.223.182.59
VPN client name: vpnclient

Client configuration is available at:
/root/vpnclient.p12 (for Windows & Linux)
/root/vpnclient.sswan (for Android)
/root/vpnclient.mobileconfig (for iOS & macOS)

Next steps: Configure IKEv2 clients. See:
  https://git.io/ikev2clients
Feedback: https://bit.ly/vpn-feedback

================================================

root@jinchengvpn:~# 
```

4. **What is the IP address shown in Step 5?**

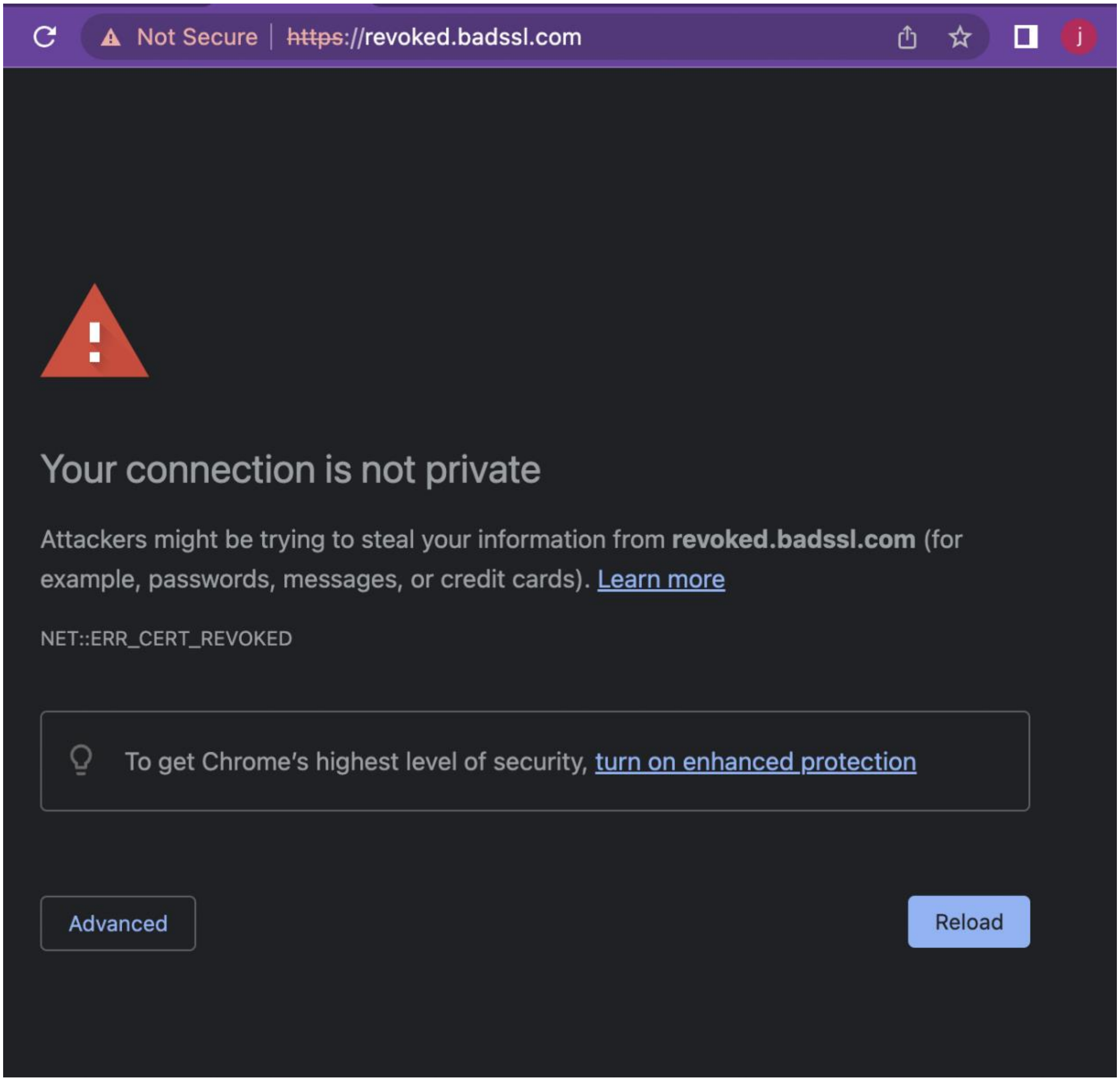
   159.223.182.59
   It is the same as the server machine ip address.

5. **Please explain why the IP address in Step 5 is different from the IP address in Step 1.**

Since we have already connected with the vpn, so our ip address with be the same as vpn.
The first one is reading our local ip address.

Task 2. Experiment with certificates
Questions

1. **What is your observation in visiting the site? Include a screenshot of your browser.**



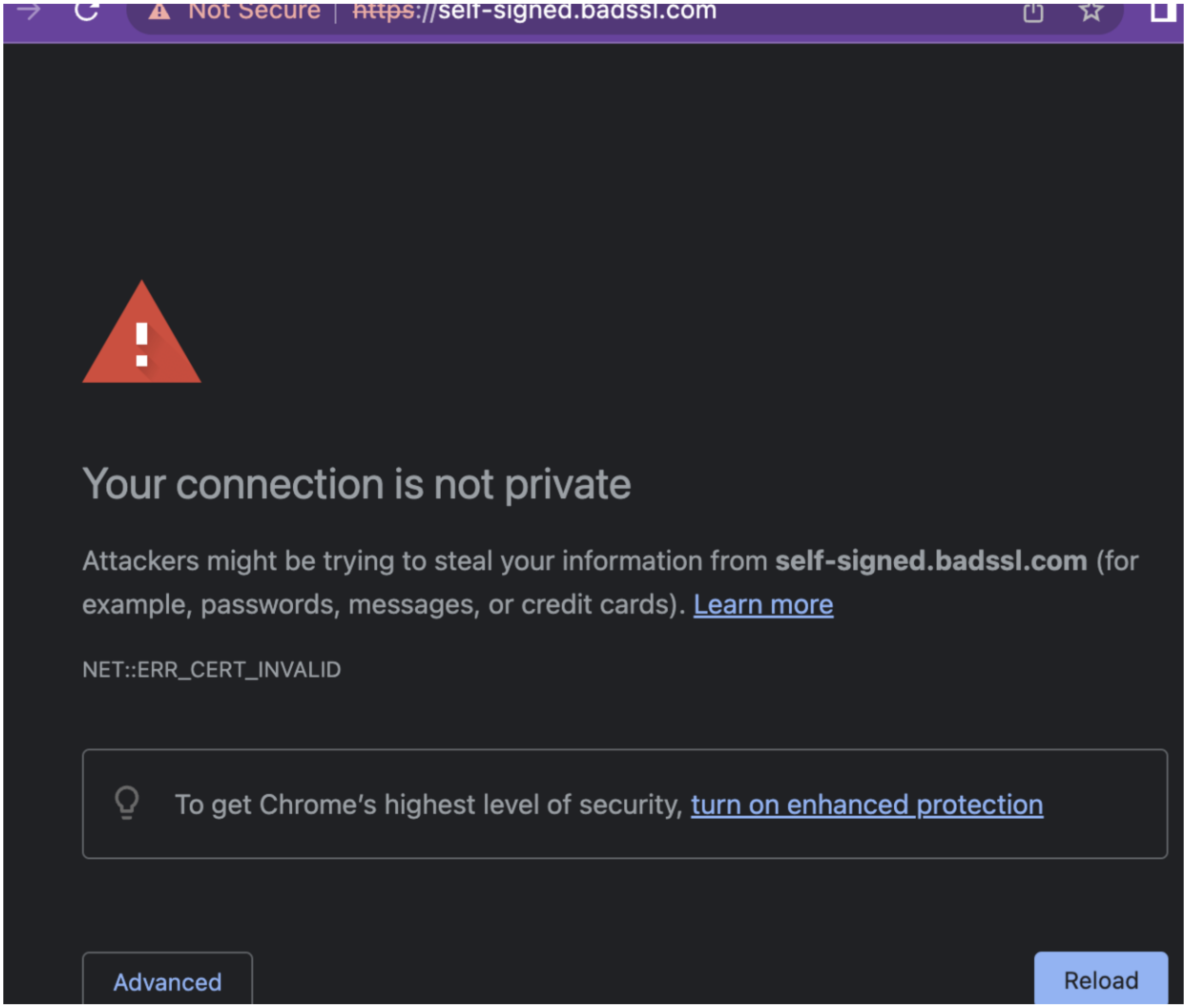
Not Secure | ~~https~~://revoked.badssl.com

Your connection is not private

Attackers might be trying to steal your information from **revoked.badssl.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_REVOKED

To get Chrome's highest level of security, turn on enhanced protection

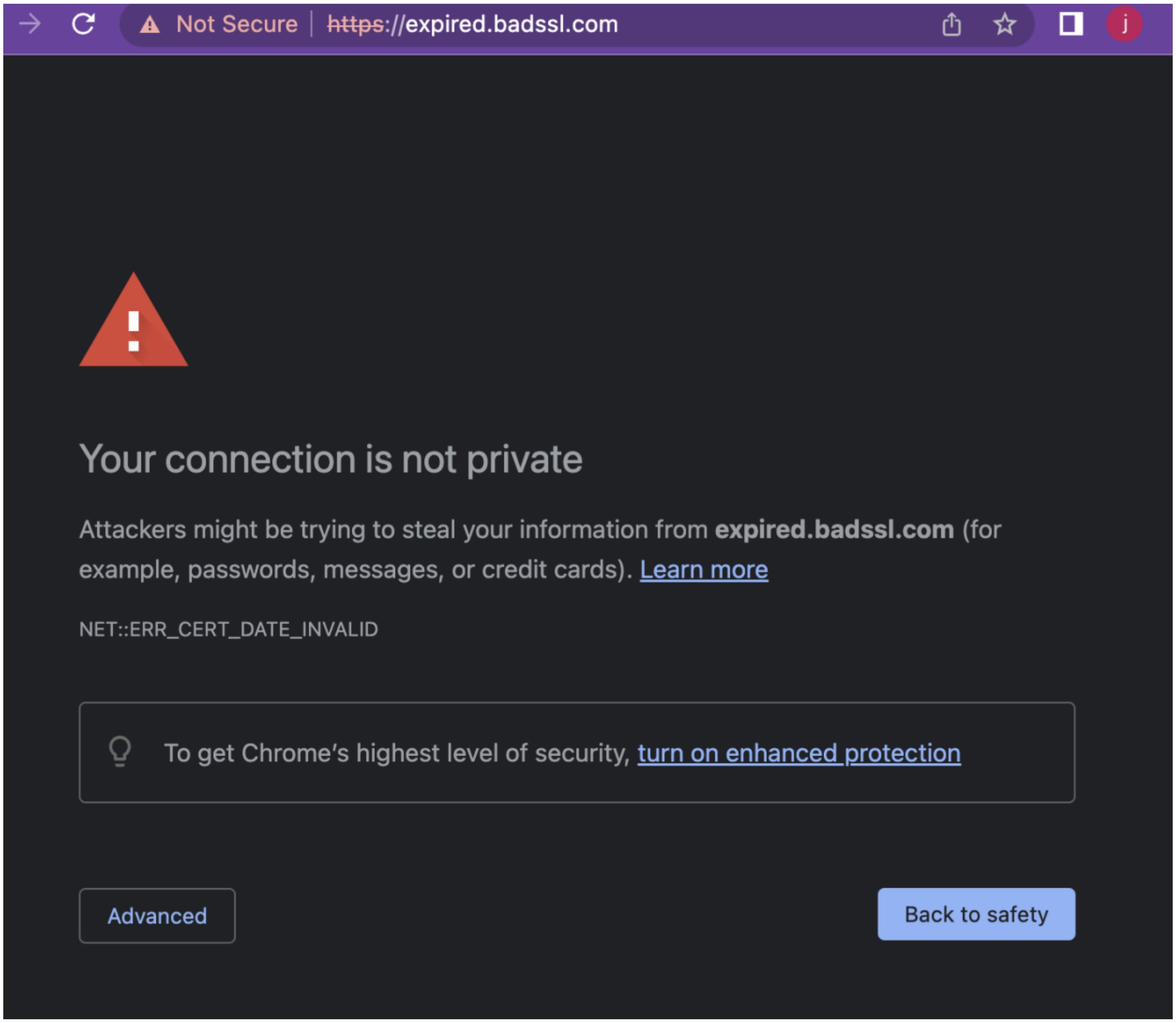


Your connection is not private

Attackers might be trying to steal your information from **self-signed.badssl.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_INVALID

To get Chrome's highest level of security, turn on enhanced protection



Your connection is not private

Attackers might be trying to steal your information from **expired.badssl.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_DATE_INVALID

To get Chrome's highest level of security, turn on enhanced protection

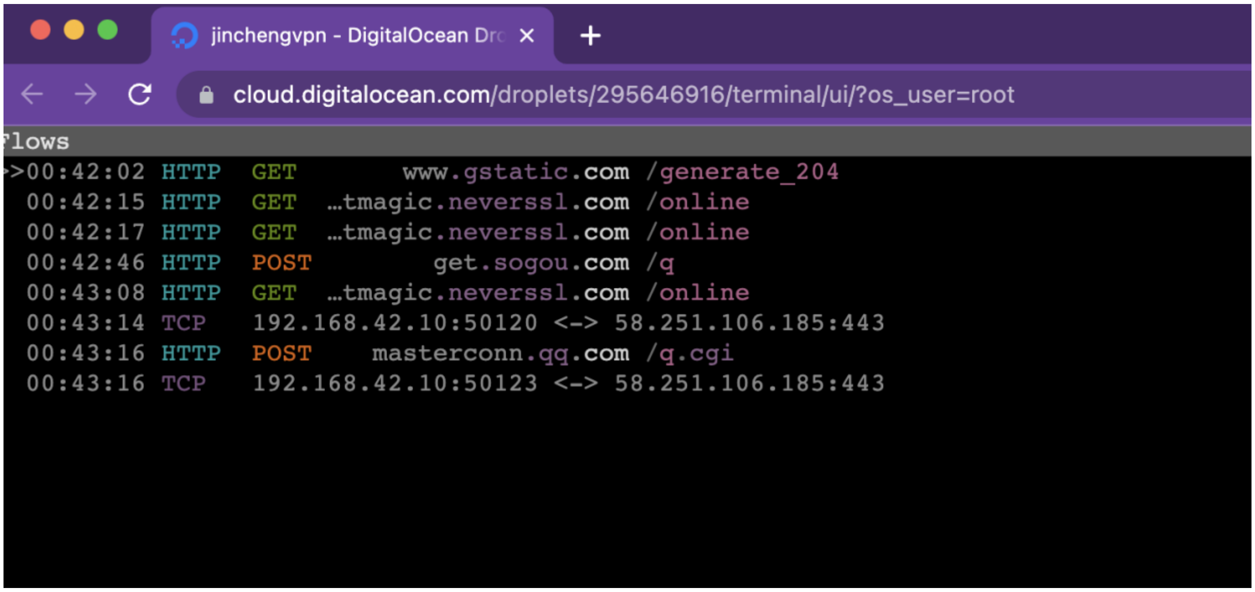
2. Explain the observation. Provide relevant information from the certificate as a part of your explanation.

I cannot access these three websites since chrome is protecting me from accessing these.

Task 3. Set up MITMproxy

Questions

1. For Step 6 in this task, what do you see in the browser and on MITMproxy? Please include the relevant screenshots and explain your observations.

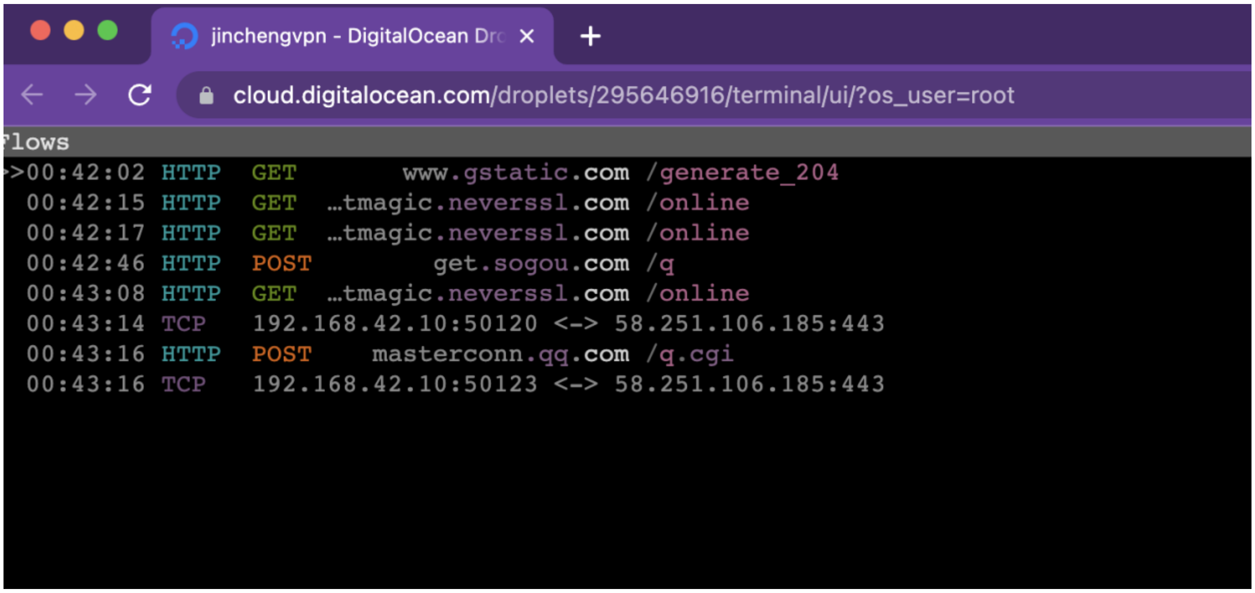


jinchengvpn - DigitalOcean Drc
cloud.digitalocean.com/droplets/295646916/terminal/ui/?os_user=root

```
Flows
>00:42:02 HTTP  GET        www.gstatic.com /generate_204
 00:42:15 HTTP  GET   …tmagic.neverssl.com /online
 00:42:17 HTTP  GET   …tmagic.neverssl.com /online
 00:42:46 HTTP  POST         get.sogou.com /q
 00:43:08 HTTP  GET   …tmagic.neverssl.com /online
 00:43:14 TCP   192.168.42.10:50120 <-> 58.251.106.185:443
 00:43:16 HTTP  POST     masterconn.qq.com /q.cgi
 00:43:16 TCP   192.168.42.10:50123 <-> 58.251.106.185:443
```

As we can see, there is a http get with the url of neverssl. Also, it shows me that there is no content,

2. For Step 7 in this task, what do you see in the browser and on MITMproxy? Please include the relevant screenshots and explain your observations

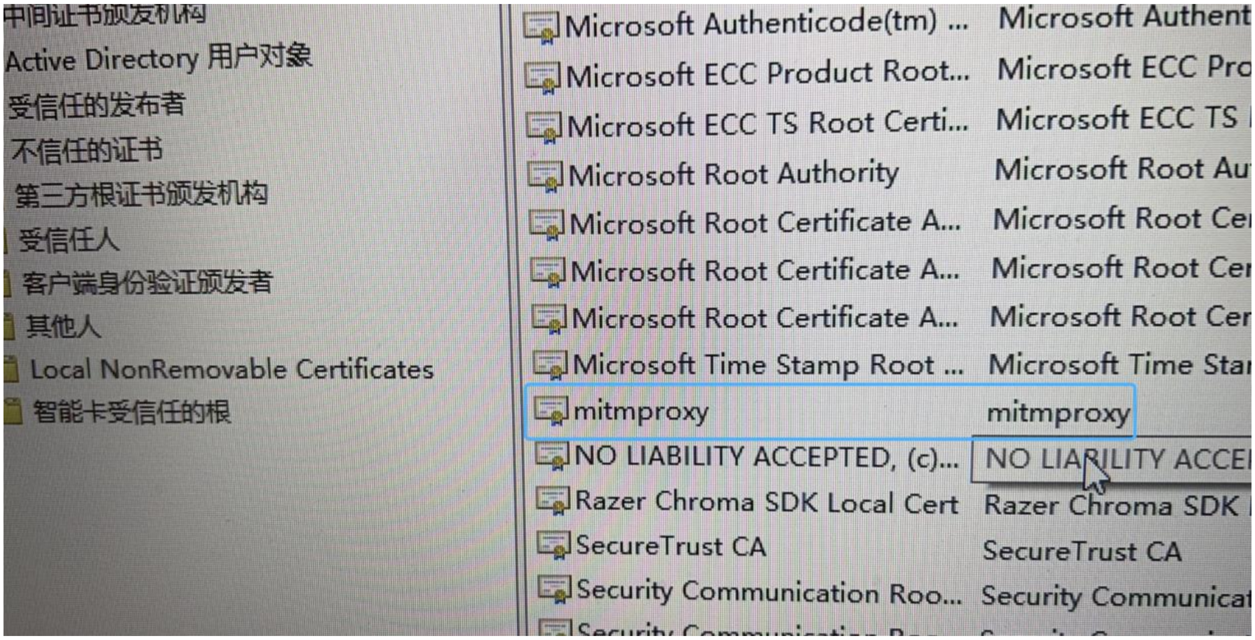


jinchengvpn - DigitalOcean Dro
cloud.digitalocean.com/droplets/295646916/terminal/ui/?os_user=root

```
Flows
>00:42:02 HTTP  GET        www.gstatic.com /generate_204
 00:42:15 HTTP  GET    …tmagic.neverssl.com /online
 00:42:17 HTTP  GET    …tmagic.neverssl.com /online
 00:42:46 HTTP  POST         get.sogou.com /q
 00:43:08 HTTP  GET    …tmagic.neverssl.com /online
 00:43:14 TCP   192.168.42.10:50120 <-> 58.251.106.185:443
 00:43:16 HTTP  POST     masterconn.qq.com /q.cgi
 00:43:16 TCP   192.168.42.10:50123 <-> 58.251.106.185:443
```

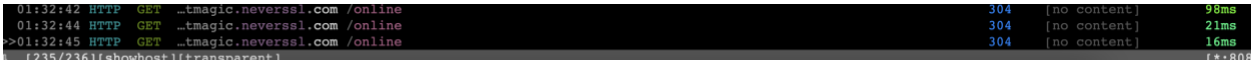
There is a http get of gstatic.com.
It shows no content. Since its not secure.

3. Once you complete Step 8, show a screenshot of the MITMproxy certificate in the root store.



Microsoft Authenticode(tm) ...	Microsoft Authent
Microsoft ECC Product Root...	Microsoft ECC Pro
Microsoft ECC TS Root Certi...	Microsoft ECC TS
Microsoft Root Authority	Microsoft Root Au
Microsoft Root Certificate A...	Microsoft Root Cer
Microsoft Root Certificate A...	Microsoft Root Cer
Microsoft Root Certificate A...	Microsoft Root Cer
Microsoft Time Stamp Root ...	Microsoft Time Star
mitmproxy	mitmproxy
NO LIABILITY ACCEPTED, (c)...	NO LIABILITY ACCE
Razer Chroma SDK Local Cert	Razer Chroma SDK
SecureTrust CA	SecureTrust CA
Security Communication Roo...	Security Communicat

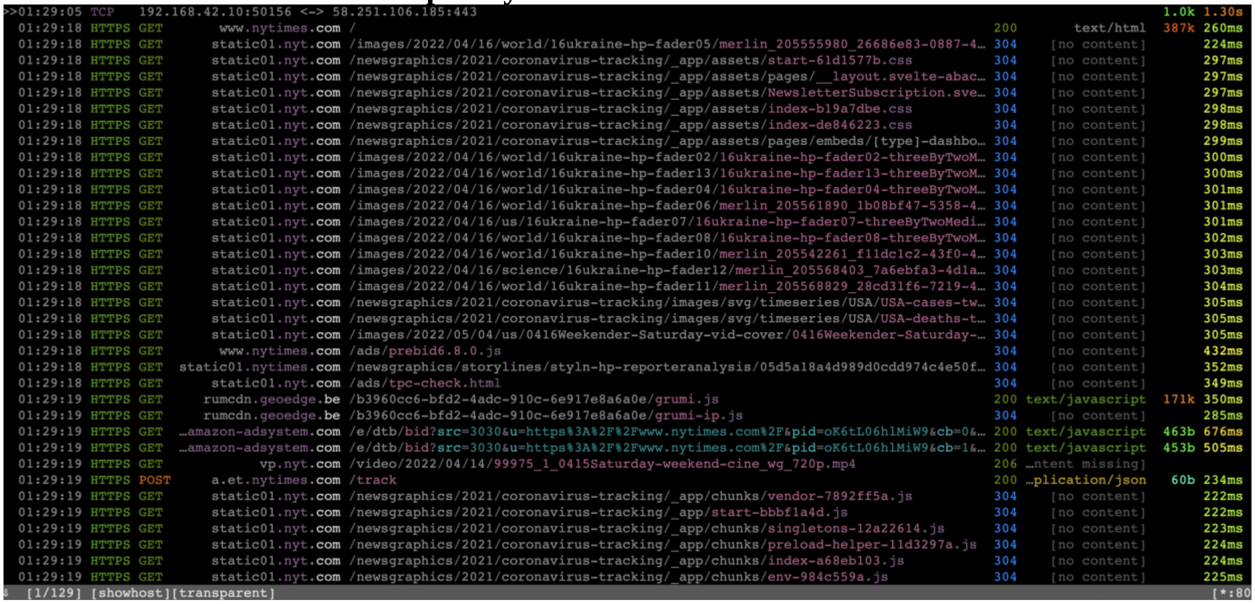
4. For Step 9, what do you see in the browser and on MITMproxy? Please include the relevant screenshots and explain your observations.



```
 01:32:42 HTTP  GET  …tmagic.neverssl.com /online                                        304   [no content]       98ms
 01:32:44 HTTP  GET  …tmagic.neverssl.com /online                                        304   [no content]       21ms
>>01:32:45 HTTP  GET  …tmagic.neverssl.com /online                                        304   [no content]       16ms
  [235/236][showhost][transparent]                                                                              [*:808
```

The mitmproxy showing me the same thing.

6. **For Step 10, what do you see in the browser and on MITMproxy? Please include the relevant screenshots and explain your observations.**



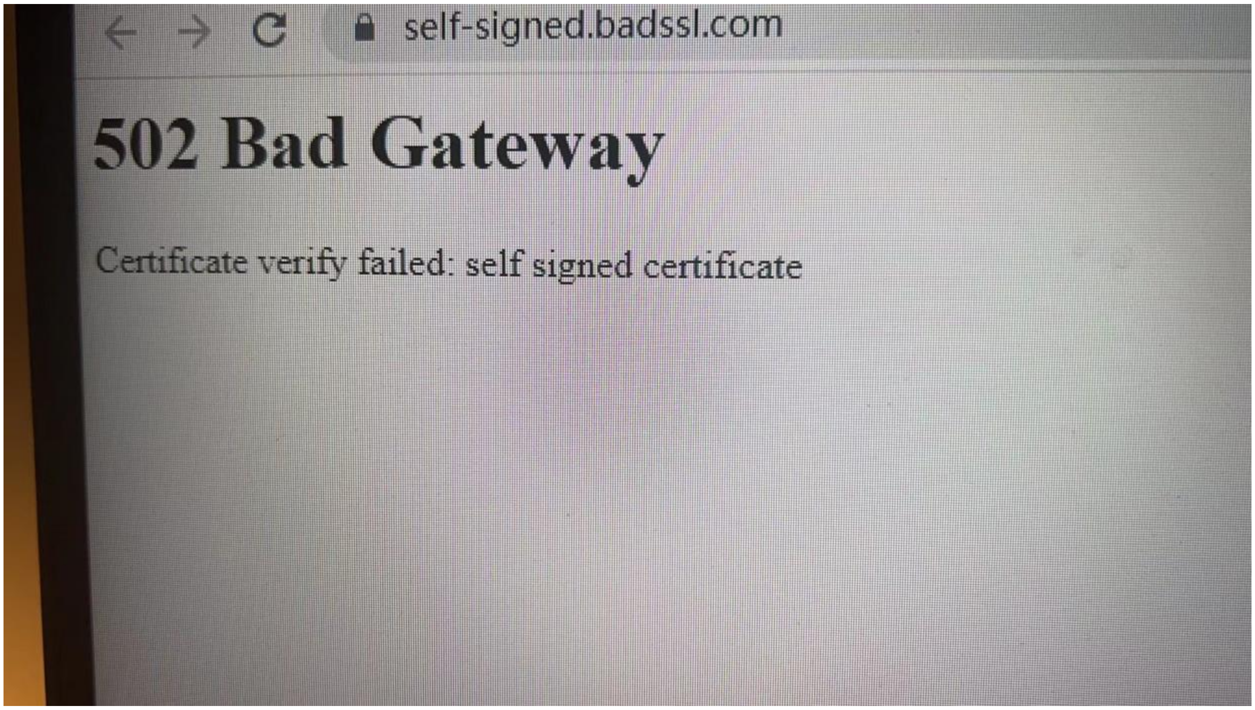
```
>>01:29:05 TCP   192.168.42.10:50156 <-> 58.251.106.185:443                                                                1.0k 1.30s
  01:29:18 HTTPS GET       www.nytimes.com /                                                                       200       text/html 387k 260ms
  01:29:18 HTTPS GET      static01.nyt.com /images/2022/04/16/world/16ukraine-hp-fader05/merlin_205555980_26686e83-0887-4… 304   [no content]  224ms
  01:29:18 HTTPS GET      static01.nyt.com /newsgraphics/2021/coronavirus-tracking/_app/assets/start-61d1577b.css         304   [no content]  297ms
  01:29:18 HTTPS GET      static01.nyt.com /newsgraphics/2021/coronavirus-tracking/_app/assets/pages/__layout.svelte-abac… 304   [no content]  297ms
  01:29:18 HTTPS GET      static01.nyt.com /newsgraphics/2021/coronavirus-tracking/_app/assets/NewsletterSubscription.sve… 304   [no content]  297ms
  01:29:18 HTTPS GET      static01.nyt.com /newsgraphics/2021/coronavirus-tracking/_app/assets/index-b19a7dbe.css         304   [no content]  298ms
  01:29:18 HTTPS GET      static01.nyt.com /newsgraphics/2021/coronavirus-tracking/_app/assets/index-de846223.css         304   [no content]  298ms
  01:29:18 HTTPS GET      static01.nyt.com /newsgraphics/2021/coronavirus-tracking/_app/assets/pages/embeds/[type]-dashbo… 304   [no content]  299ms
  01:29:18 HTTPS GET      static01.nyt.com /images/2022/04/16/world/16ukraine-hp-fader02/16ukraine-hp-fader02-threeByTwoM… 304   [no content]  300ms
  01:29:18 HTTPS GET      static01.nyt.com /images/2022/04/16/world/16ukraine-hp-fader13/16ukraine-hp-fader13-threeByTwoM… 304   [no content]  300ms
  01:29:18 HTTPS GET      static01.nyt.com /images/2022/04/16/world/16ukraine-hp-fader04/16ukraine-hp-fader04-threeByTwoM… 304   [no content]  301ms
  01:29:18 HTTPS GET      static01.nyt.com /images/2022/04/16/world/16ukraine-hp-fader06/merlin_205561890_1b08bf47-5358-4… 304   [no content]  301ms
  01:29:18 HTTPS GET      static01.nyt.com /images/2022/04/16/us/16ukraine-hp-fader07/16ukraine-hp-fader07-threeByTwoMedi… 304   [no content]  301ms
  01:29:18 HTTPS GET      static01.nyt.com /images/2022/04/16/world/16ukraine-hp-fader08/16ukraine-hp-fader08-threeByTwoM… 304   [no content]  302ms
  01:29:18 HTTPS GET      static01.nyt.com /images/2022/04/16/world/16ukraine-hp-fader10/merlin_205542261_f11dc1c2-43f0-4… 304   [no content]  303ms
  01:29:18 HTTPS GET      static01.nyt.com /images/2022/04/16/science/16ukraine-hp-fader12/merlin_205568403_7a6ebfa3-4d1a… 304   [no content]  303ms
  01:29:18 HTTPS GET      static01.nyt.com /images/2022/04/16/world/16ukraine-hp-fader11/merlin_205568829_28cd31f6-7219-4… 304   [no content]  304ms
  01:29:18 HTTPS GET      static01.nyt.com /newsgraphics/2021/coronavirus-tracking/images/svg/timeseries/USA/USA-cases-tw… 304   [no content]  305ms
  01:29:18 HTTPS GET      static01.nyt.com /newsgraphics/2021/coronavirus-tracking/images/svg/timeseries/USA/USA-deaths-t… 304   [no content]  305ms
  01:29:18 HTTPS GET      static01.nyt.com /images/2022/05/04/us/0416Weekender-Saturday-vid-cover/0416Weekender-Saturday-… 304   [no content]  305ms
  01:29:18 HTTPS GET       www.nytimes.com /ads/prebid6.8.0.js                                                     304   [no content]  432ms
  01:29:18 HTTPS GET  static01.nytimes.com /newsgraphics/storylines/styln-hp-reporteranalysis/05d5a18a4d989d0cdd974c4e50f… 304   [no content]  352ms
  01:29:18 HTTPS GET      static01.nyt.com /ads/tpc-check.html                                                     304   [no content]  349ms
  01:29:19 HTTPS GET     rumcdn.geoedge.be /b3960cc6-bfd2-4adc-910c-6e917e8a6a0e/grumi.js                          200 text/javascript 171k 350ms
  01:29:19 HTTPS GET     rumcdn.geoedge.be /b3960cc6-bfd2-4adc-910c-6e917e8a6a0e/grumi-ip.js                       304   [no content]  285ms
  01:29:19 HTTPS GET  …amazon-adsystem.com /e/dtb/bid?src=3030&u=https%3A%2F%2Fwww.nytimes.com%2F&pid=oK6tL06hlMiW9&cb=0&… 200 text/javascript 463b 676ms
  01:29:19 HTTPS GET  …amazon-adsystem.com /e/dtb/bid?src=3030&u=https%3A%2F%2Fwww.nytimes.com%2F&pid=oK6tL06hlMiW9&cb=1&… 200 text/javascript 453b 505ms
  01:29:19 HTTPS GET            vp.nyt.com /video/2022/04/14/99975_1_0415Saturday-weekend-cine_wg_720p.mp4        206 …ntent missing]
  01:29:19 HTTPS POST      a.et.nytimes.com /track                                                                  200 …plication/json  60b 234ms
  01:29:19 HTTPS GET      static01.nyt.com /newsgraphics/2021/coronavirus-tracking/_app/chunks/vendor-7892ff5a.js          304   [no content]  222ms
  01:29:19 HTTPS GET      static01.nyt.com /newsgraphics/2021/coronavirus-tracking/_app/start-bbbf1a4d.js                  304   [no content]  222ms
  01:29:19 HTTPS GET      static01.nyt.com /newsgraphics/2021/coronavirus-tracking/_app/chunks/singletons-12a22614.js      304   [no content]  223ms
  01:29:19 HTTPS GET      static01.nyt.com /newsgraphics/2021/coronavirus-tracking/_app/chunks/preload-helper-11d3297a.js  304   [no content]  224ms
  01:29:19 HTTPS GET      static01.nyt.com /newsgraphics/2021/coronavirus-tracking/_app/chunks/index-a68eb103.js           304   [no content]  224ms
  01:29:19 HTTPS GET      static01.nyt.com /newsgraphics/2021/coronavirus-tracking/_app/chunks/env-984c559a.js             304   [no content]  225ms
⇩  [1/129] [showhost][transparent]                                                                                       [*:80
```

Instead of showing me the error, it is actuall showing me the actual content and nytimes url.

6. Briefly explain how MITMproxy allows you to intercept TLS traffic in Steps 9 and 10.

MITM proxy and Charles proxy are HTTP monitors that allow developers to see all HTTP and SSL/HTTPS communication between the client and the server. The main idea behind MITM, which stands for Man-In-The-Middle, is to appear to be the server to the client and the client to the server, while in the middle we can monitor traffic flowing from both sides using the MITM proxy monitor.

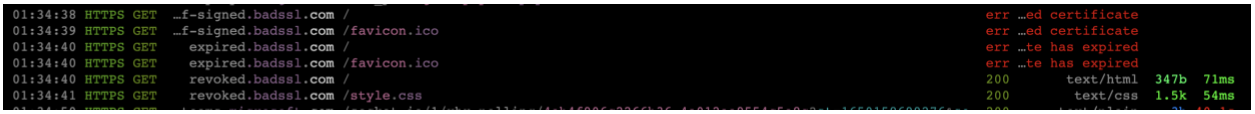
7. **For Step 11, what do you observe and why? Please include any relevant screenshots.**



self-signed.badssl.com

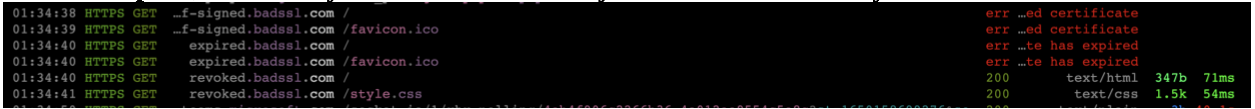
502 Bad Gateway

Certificate verify failed: self signed certificate

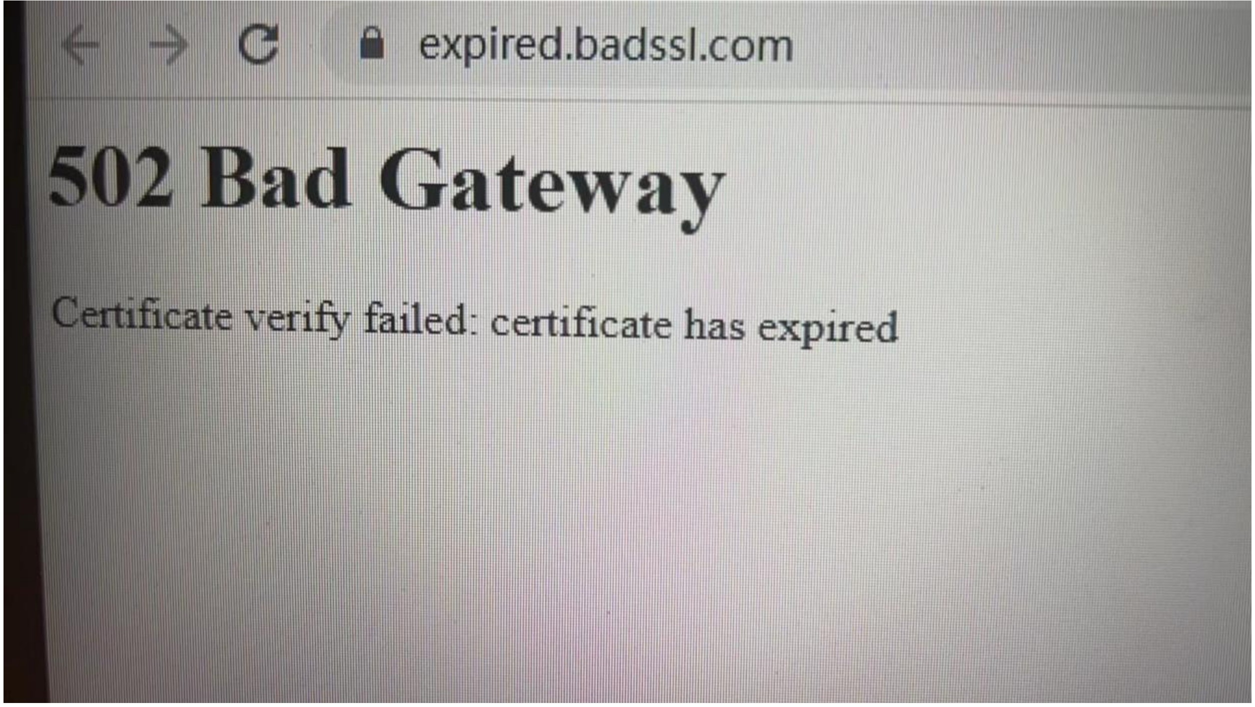


```
01:34:38 HTTPS GET  …f-signed.badssl.com /                                                           err …ed certificate
01:34:39 HTTPS GET  …f-signed.badssl.com /favicon.ico                                                err …ed certificate
01:34:40 HTTPS GET    expired.badssl.com /                                                           err …te has expired
01:34:40 HTTPS GET    expired.badssl.com /favicon.ico                                                err …te has expired
01:34:40 HTTPS GET    revoked.badssl.com /                                                           200       text/html  347b  71ms
01:34:41 HTTPS GET    revoked.badssl.com /style.css                                                  200        text/css  1.5k  54ms
```

8. For Step 12, what do you observe and why? Please include any relevant screenshots.



```
01:34:38 HTTPS GET  …f-signed.badssl.com /                                                    err …ed certificate
01:34:39 HTTPS GET  …f-signed.badssl.com /favicon.ico                                         err …ed certificate
01:34:40 HTTPS GET    expired.badssl.com /                                                    err …te has expired
01:34:40 HTTPS GET    expired.badssl.com /favicon.ico                                         err …te has expired
01:34:40 HTTPS GET    revoked.badssl.com /                                                    200        text/html  347b   71ms
01:34:41 HTTPS GET    revoked.badssl.com /style.css                                           200         text/css  1.5k   54ms
```

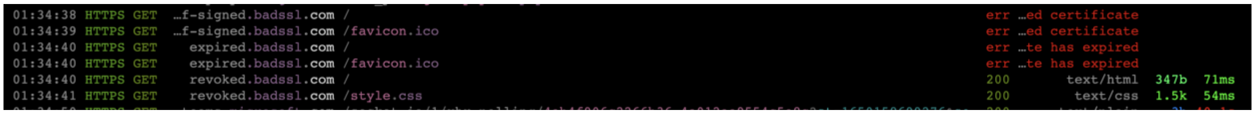


expired.badssl.com

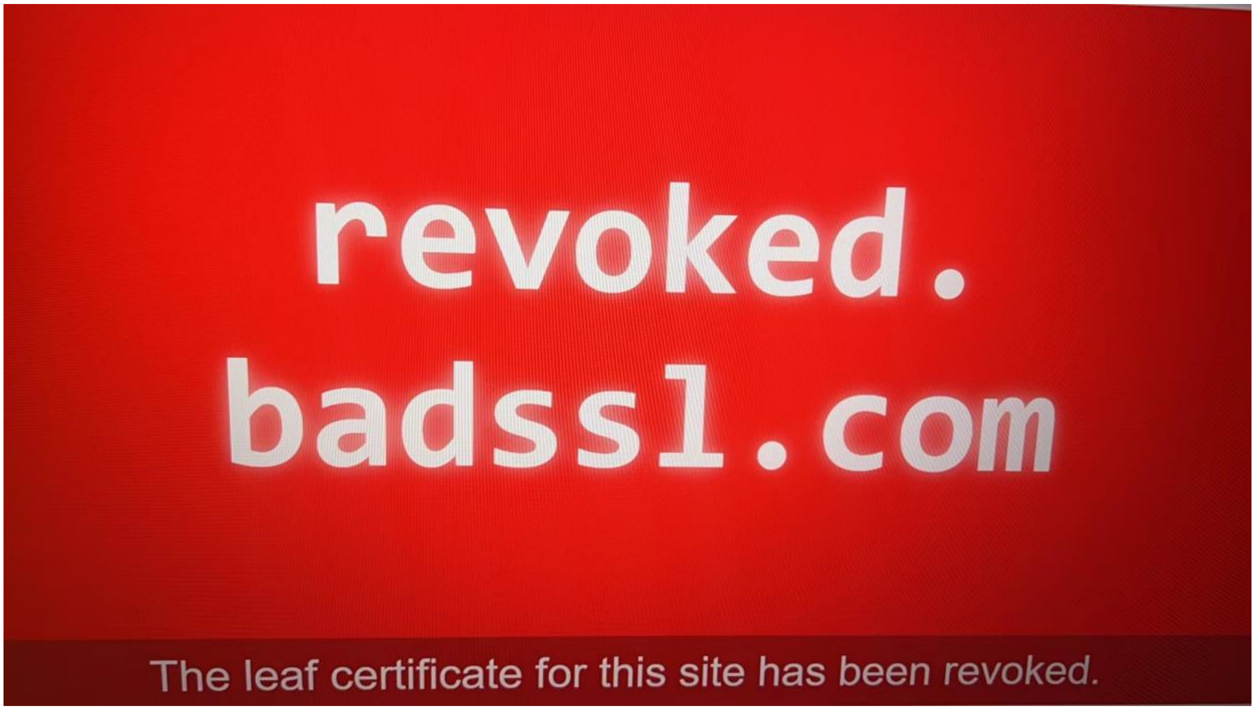
502 Bad Gateway

Certificate verify failed: certificate has expired

9. For Step 13, what do you observe and why? Please include any relevant screenshots.



```
01:34:38 HTTPS GET  …f-signed.badssl.com /                                                    err …ed certificate
01:34:39 HTTPS GET  …f-signed.badssl.com /favicon.ico                                         err …ed certificate
01:34:40 HTTPS GET    expired.badssl.com /                                                    err …te has expired
01:34:40 HTTPS GET    expired.badssl.com /favicon.ico                                         err …te has expired
01:34:40 HTTPS GET    revoked.badssl.com /                                                    200        text/html  347b   71ms
01:34:41 HTTPS GET    revoked.badssl.com /style.css                                           200         text/css  1.5k   54ms
```



revoked.
badssl.com

The leaf certificate for this site has been revoked.