Lab 3

Do not write your name or Net ID anywhere in this lab report. Also make sure that your name or Net ID should not appear anywhere in the screenshots.

In this lab, you will be asked to intercept HTTPS traffic using an L2TP IPSEC tunnel along with MITMproxy. Most of the steps are similar to what Danny discussed in class. If you're not sure, please refer to the class recordings.

Task 1. Set up a VPN server.

Steps

1. On your computer's browser, go to "https://api.ipify.org".
2. Get a Ubuntu 20 virtual machine on Digital Ocean (or other similar cloud providers). From now onwards, we shall call this virtual machine the Cloud VM.
3. Set up an L2TP with IPSEC VPN server on the Cloud VM by following these instructions.
4. Connect your computer (or your Kali Linux virtual machine) to the VPN server. If you're running Kali, you may not be able to see the L2TP option under VPN; in this case, run "*sudo apt update; sudo apt install network-manager-l2tp-gnome*" in the terminal to install L2TP support.
5. On your computer's browser, go to "https://api.ipify.org".

Questions

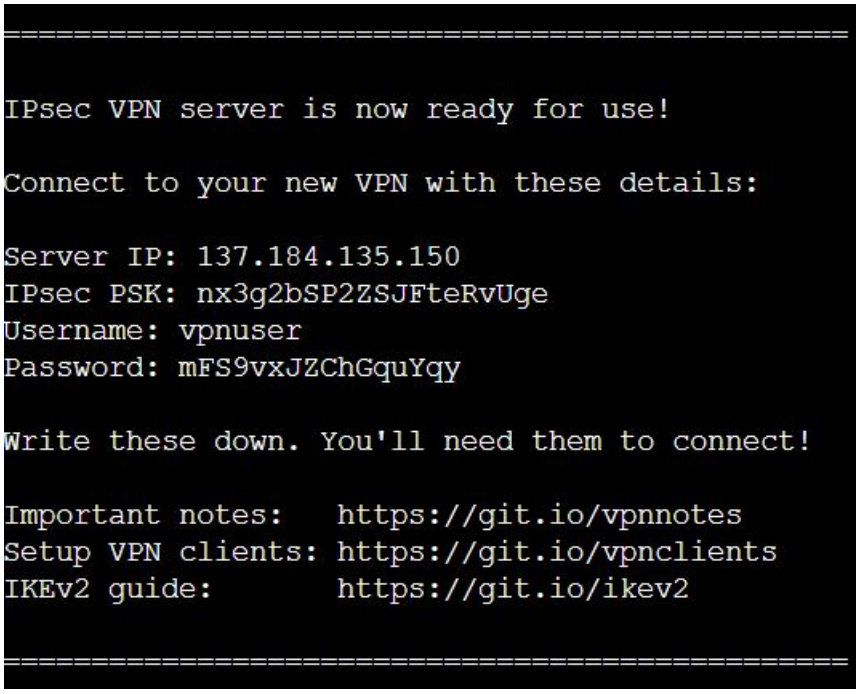
1. What is the IP address shown in Step 1?

184.152.32.58

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

137.184.135.150

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



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

137.184.135.150

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

Because I am using VPN.

Task 2. Experiment with certificates.

Do the following steps on your computer (or on a Kali Linux VM). Feel free to use a browser of your choice.

Steps

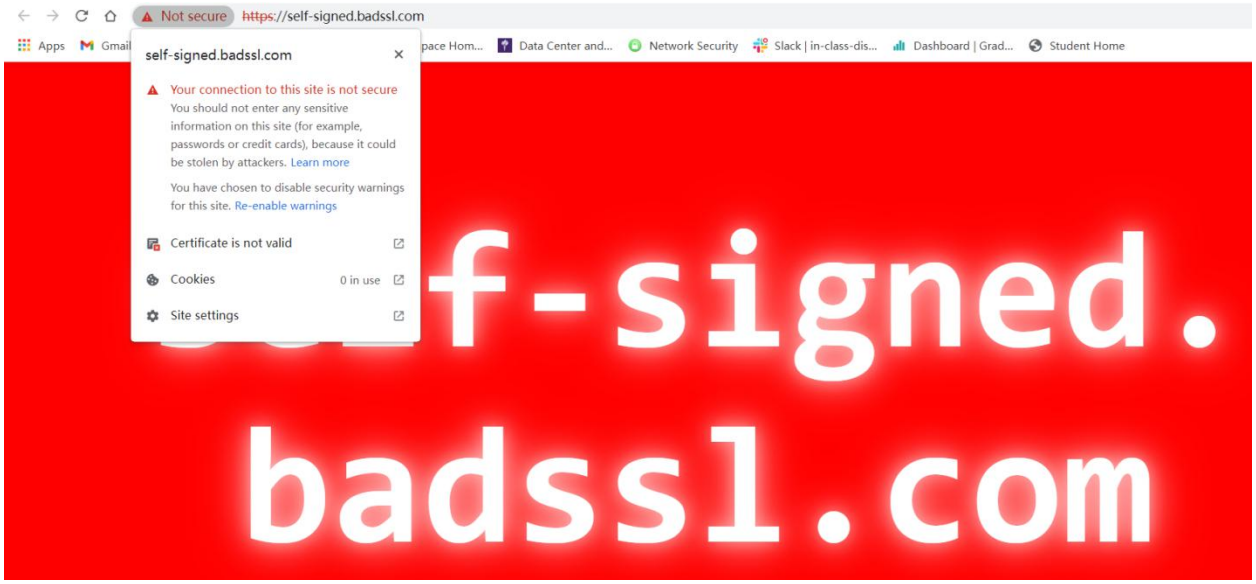
1. Visit https://self-signed.badssl.com/
2. Visit https://expired.badssl.com/
3. Visit https://revoked.badssl.com/

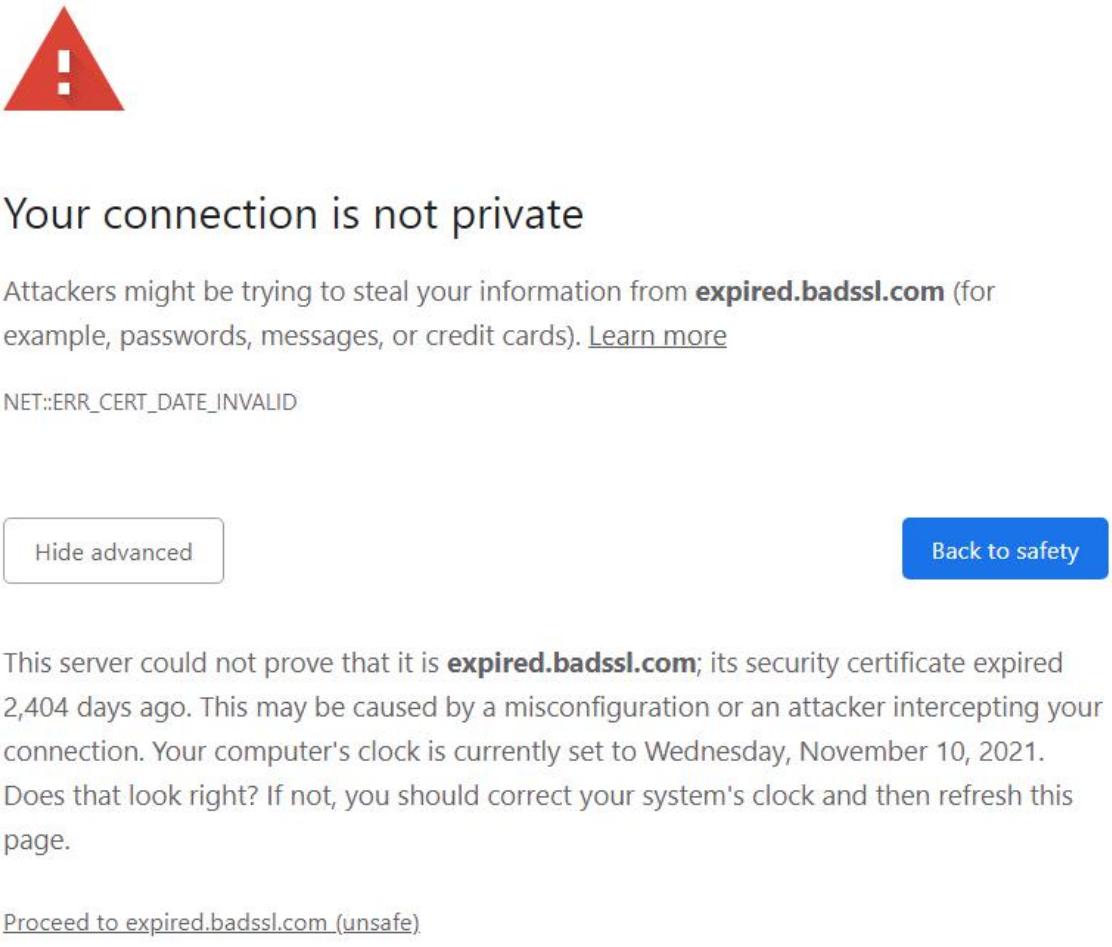
For each of the steps above, answer the following questions:

Questions

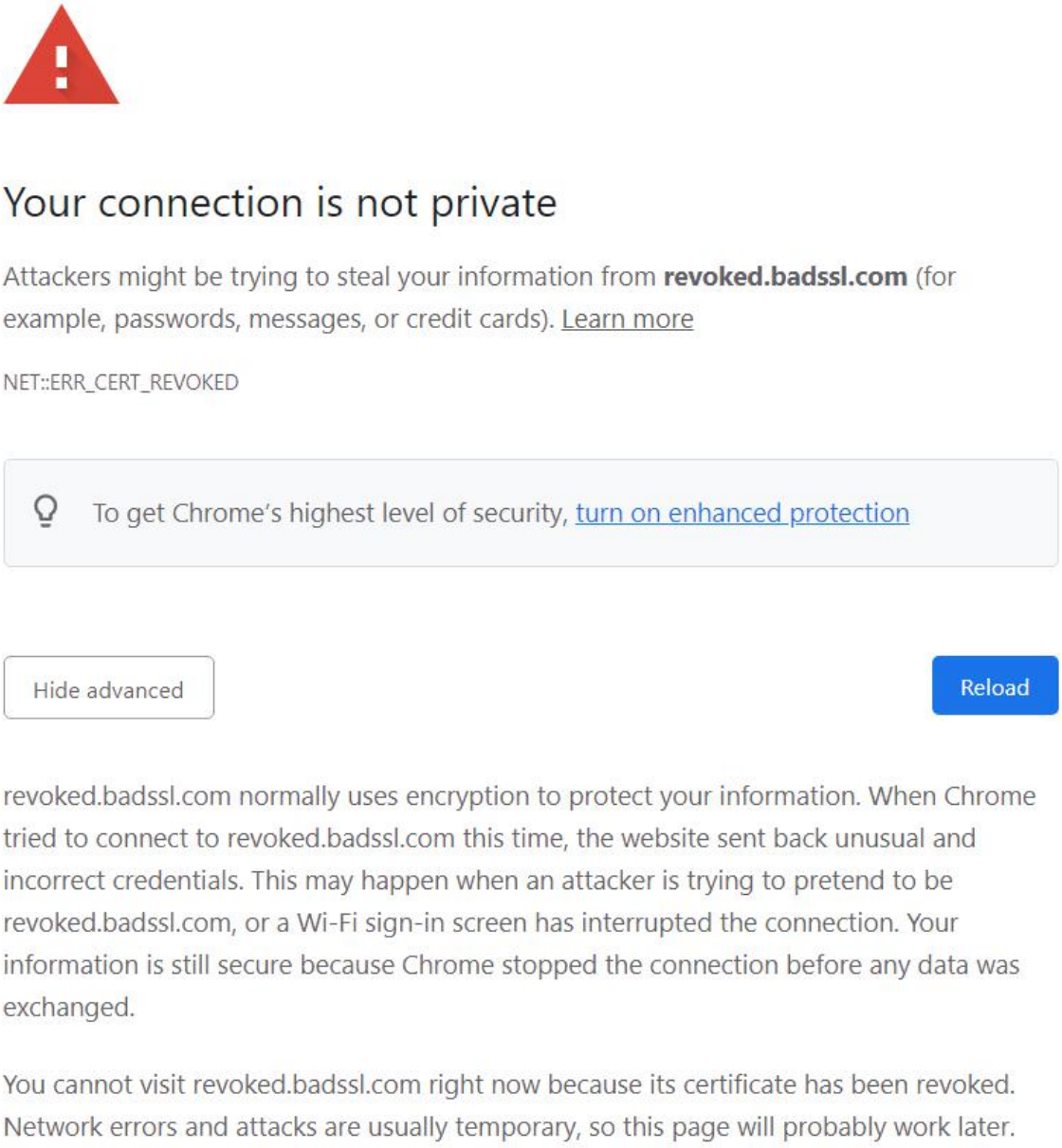
1. What is your observation? Include a screenshot of your browser.

(1) .


Not secure
https://self-signed.badssl.com
Apps
Gmail
Data Center and...
Network Security
Slack | in-class-dis...
Dashboard | Grad...
Student Home
self-signed.badssl.com
Your connection to this site is not secure
You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more
You have chosen to disable security warnings for this site. Re-enable warnings
Certificate is not valid
Cookies
0 in use
Site settings
f-signed.
badssl.com


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
Hide advanced
Back to safety
This server could not prove that it is **expired.badssl.com**; its security certificate expired 2,404 days ago. This may be caused by a misconfiguration or an attacker intercepting your connection. Your computer's clock is currently set to Wednesday, November 10, 2021. Does that look right? If not, you should correct your system's clock and then refresh this page.
Proceed to expired.badssl.com (unsafe)

(2)



(3)

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

(1) CA signing this certificate is not trusted by the root store

(2) the certificate has expired

(3) The certificate is revoked.

Task 3. Set up MITMproxy.

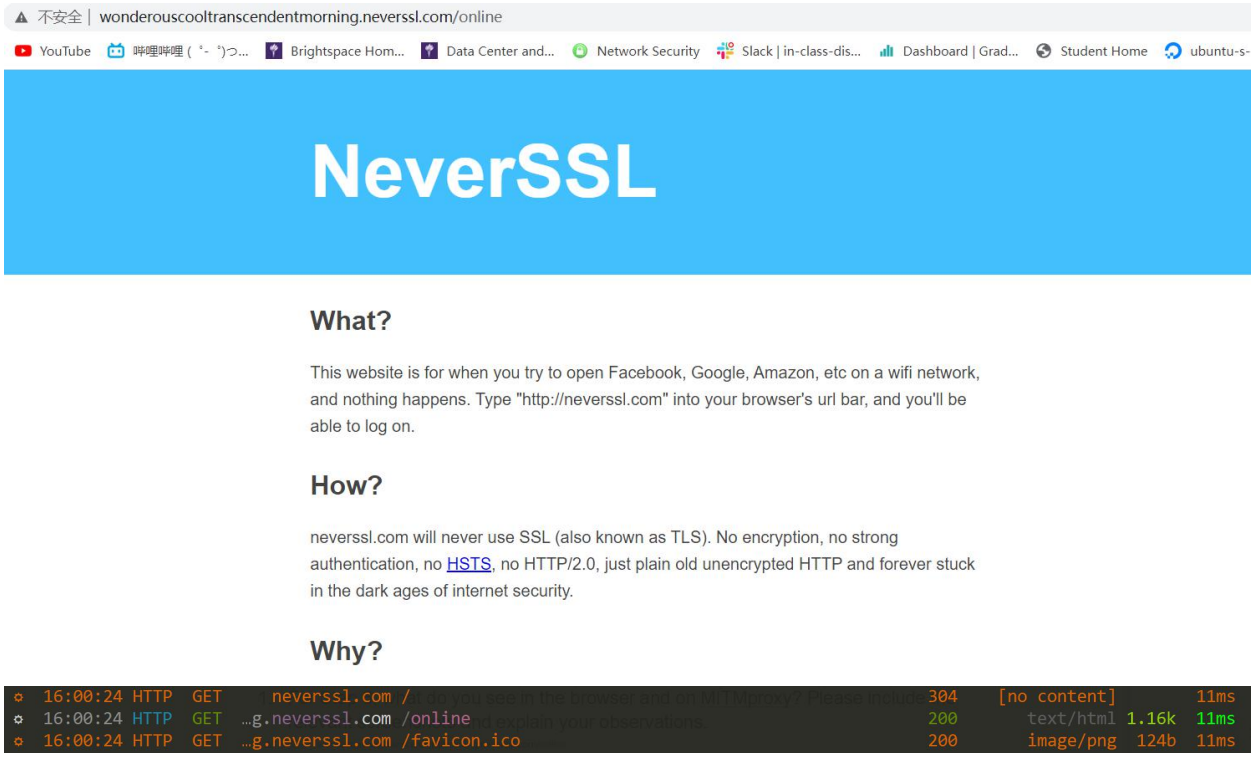
Steps

1. On the Cloud VM, set up MITMproxy per these instructions.
2. Configure the appropriate iptable rules so that network traffic from the VPN server is forwarded to the MITMproxy. Remember to turn on IP forwarding and also replace “eth0” with the appropriate L2TP interface (such as “ppp0”) when you configure the IP table rules.
3. Do not install the MITMproxy certificate authority yet.
4. Make sure to keep the L2TP tunnel running (which you established in Task 1).
5. On the Cloud VM, run MITMproxy on the command line: “*./mitmproxy --mode transparent --showhost*”. Press “F” to follow new flows.
6. On your computer (or Kali Linux VM), open http://neverssl.com/ in the browser.

7. On your computer (or Kali Linux VM), open https://www.nytimes.com/ in the browser.
8. Install the MITMproxy certificate authority on your computer (or Kali Linux) by following the “Quick Setup” section.
9. On your computer (or Kali Linux VM), open http://neverssl.com/ in the browser.
10. On your computer (or Kali Linux VM), open https://www.nytimes.com/ in the browser.
11. Visit https://self-signed.badssl.com/
12. Visit https://expired.badssl.com/
13. Visit https://revoked.badssl.com/

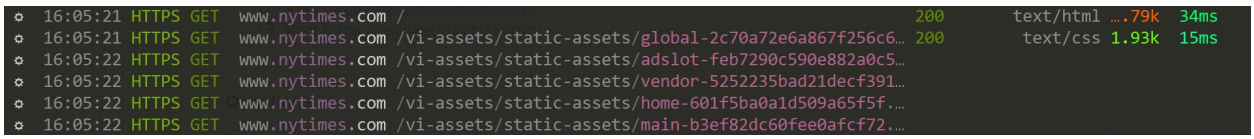
Questions

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



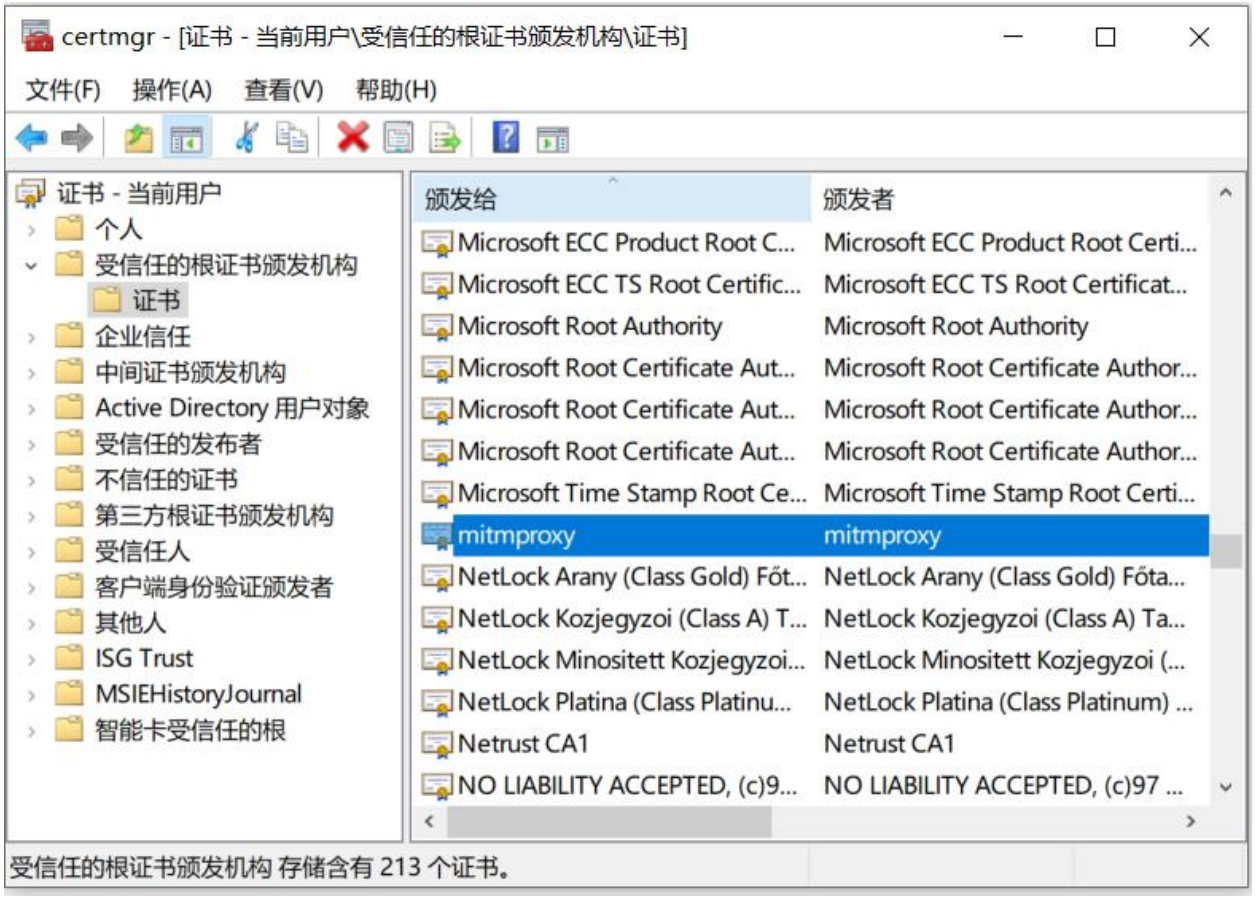
The neverssl website shows up normally, because it does not use https to encrypt message.

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

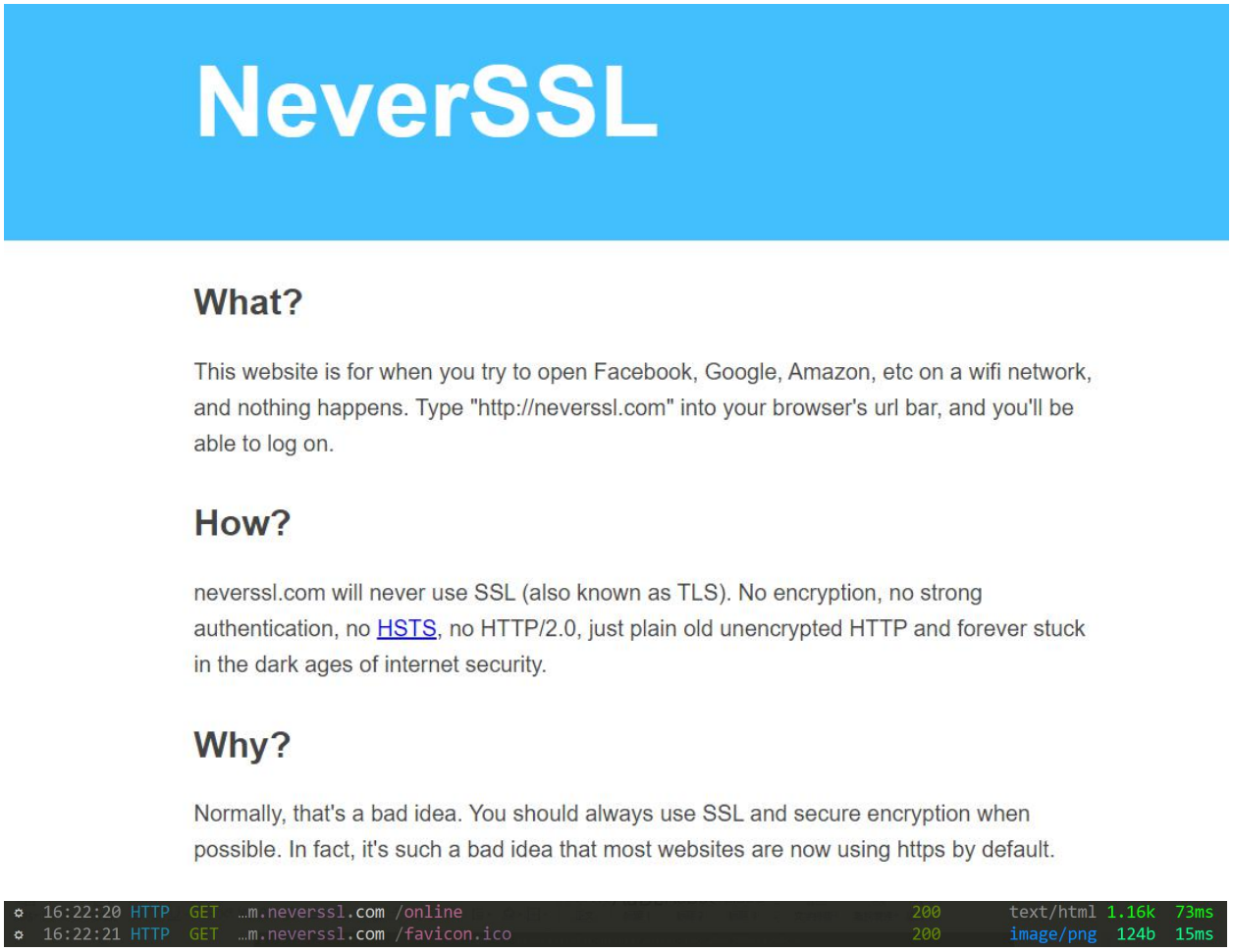


The nytimes website does not show up, because the CA signing the certificate is mitmproxy, which is not trusted.

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

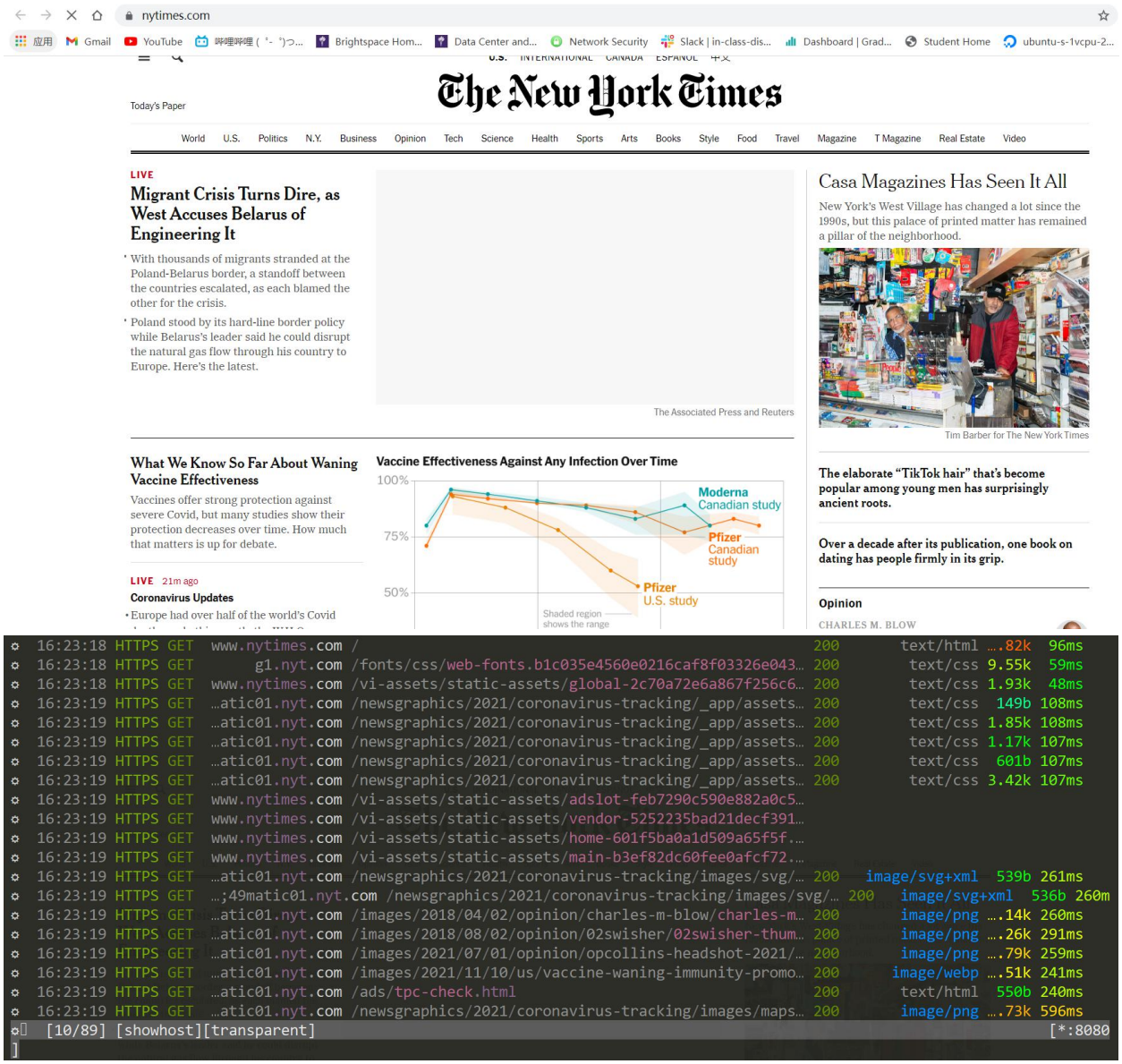


4. For Step 9, what do you see in the browser and on MITMproxy? Please include the relevant screenshots and explain your observations.



Neverssl works all fine, it does not use https.

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




```
16:23:18 HTTPS GET  www.nytimes.com /                                                    200  text/html ….82k  96ms
16:23:18 HTTPS GET  g1.nyt.com /fonts/css/web-fonts.b1c035e4560e0216caf8f03326e043…      200  text/css 9.55k  59ms
16:23:18 HTTPS GET  www.nytimes.com /vi-assets/static-assets/global-2c70a72e6a867f256c6…  200  text/css 1.93k  48ms
16:23:19 HTTPS GET  …atic01.nyt.com /newsgraphics/2021/coronavirus-tracking/_app/assets…  200  text/css  149b 108ms
16:23:19 HTTPS GET  …atic01.nyt.com /newsgraphics/2021/coronavirus-tracking/_app/assets…  200  text/css 1.85k 108ms
16:23:19 HTTPS GET  …atic01.nyt.com /newsgraphics/2021/coronavirus-tracking/_app/assets…  200  text/css 1.17k 107ms
16:23:19 HTTPS GET  …atic01.nyt.com /newsgraphics/2021/coronavirus-tracking/_app/assets…  200  text/css  601b 107ms
16:23:19 HTTPS GET  …atic01.nyt.com /newsgraphics/2021/coronavirus-tracking/_app/assets…  200  text/css 3.42k 107ms
16:23:19 HTTPS GET  www.nytimes.com /vi-assets/static-assets/adslot-feb7290c590e882a0c5…
16:23:19 HTTPS GET  www.nytimes.com /vi-assets/static-assets/vendor-5252235bad21decf391…
16:23:19 HTTPS GET  www.nytimes.com /vi-assets/static-assets/home-601f5ba0a1d509a65f5f.…
16:23:19 HTTPS GET  www.nytimes.com /vi-assets/static-assets/main-b3ef82dc60fee0afcf72.…
16:23:19 HTTPS GET  …atic01.nyt.com /newsgraphics/2021/coronavirus-tracking/images/svg/… 200  image/svg+xml  539b 261ms
16:23:19 HTTPS GET  …;49matic01.nyt.com /newsgraphics/2021/coronavirus-tracking/images/svg/… 200  image/svg+xml  536b 260m
16:23:19 HTTPS GET  …atic01.nyt.com /images/2018/04/02/opinion/charles-m-blow/charles-m… 200  image/png ….14k 260ms
16:23:19 HTTPS GET  …atic01.nyt.com /images/2018/08/02/opinion/02swisher/02swisher-thum… 200  image/png ….26k 291ms
16:23:19 HTTPS GET  …atic01.nyt.com /images/2021/07/01/opinion/opcollins-headshot-2021/… 200  image/png ….79k 259ms
16:23:19 HTTPS GET  …atic01.nyt.com /images/2021/11/10/us/vaccine-waning-immunity-promo… 200  image/webp ….51k 241ms
16:23:19 HTTPS GET  …atic01.nyt.com /ads/tpc-check.html                                  200  text/html  550b 240ms
16:23:19 HTTPS GET  …atic01.nyt.com /newsgraphics/2021/coronavirus-tracking/images/maps… 200  image/png ….73k 596ms
[10/89] [showhost][transparent]                                                                              [*:8080
]
```

Not that the nytimes website shows up, because we now trust mitmproxy in root, some image still does not shows up maybe because of certificate pinning.

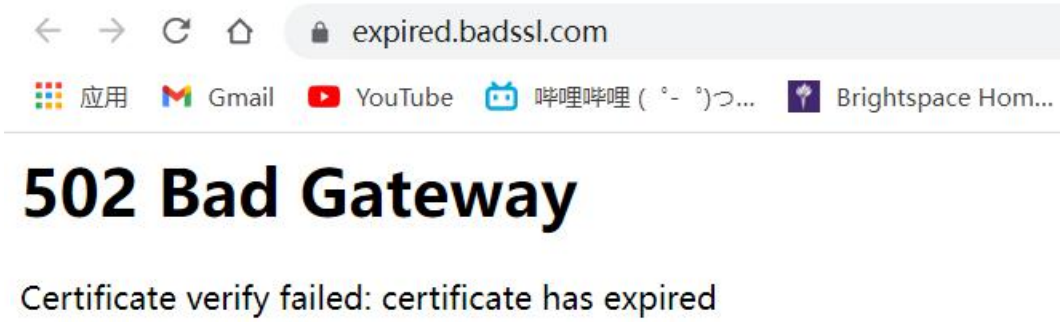
6. Briefly explain how MITMproxy allows you to intercept TLS traffic in Steps 9 and 10.

MITMproxy pretend to be the server to the client host, but it does not has the server's private key to encrypt the message thus it cannot use the certificate signed by the trusted CA. So to initiate a TLS session, the client should first install the mitmproxy in the root store manually, then it can trust the certificate signed by the mitmproxy it self and use it to decrypt the https message.

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

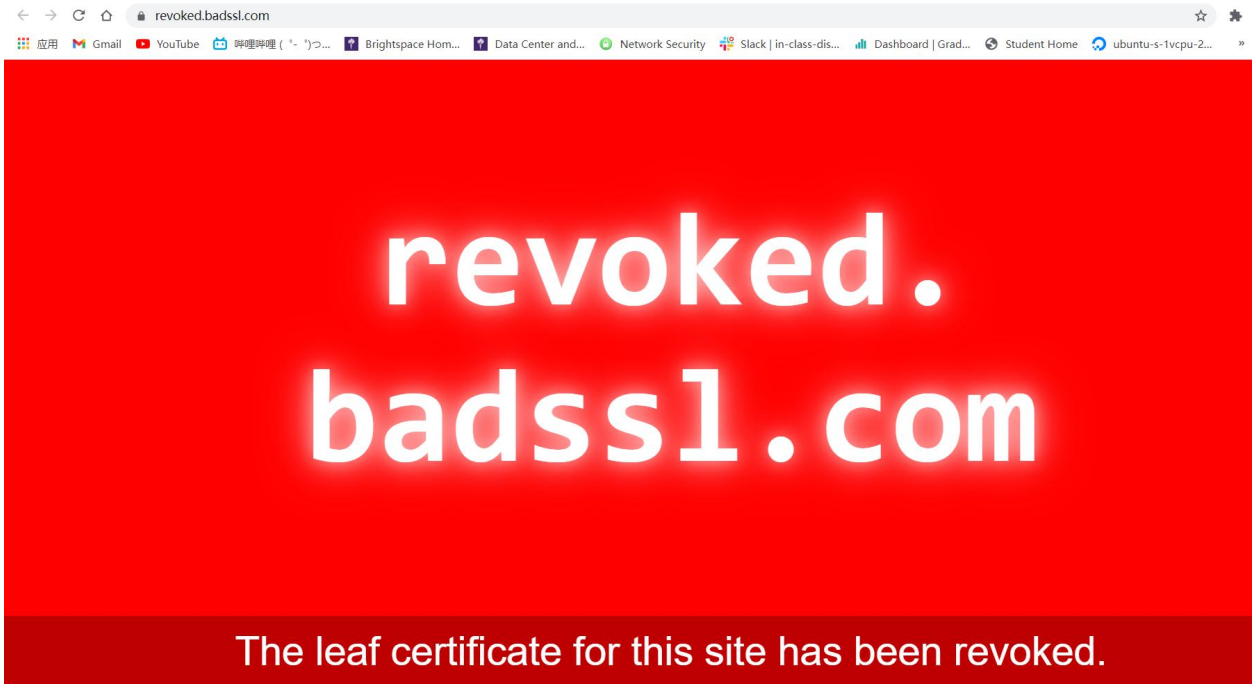
The MITMproxy does not trust the self-signed certificate.

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



The MITMproxy does not trust the expired certificate.

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



The certificate of this website is revoked, but mitmproxy did nothing about it, meaning that the revocation is not inside of mitmproxy's certificate revocation list

Task 4. Intercepting app traffic. [10 Bonus Points]

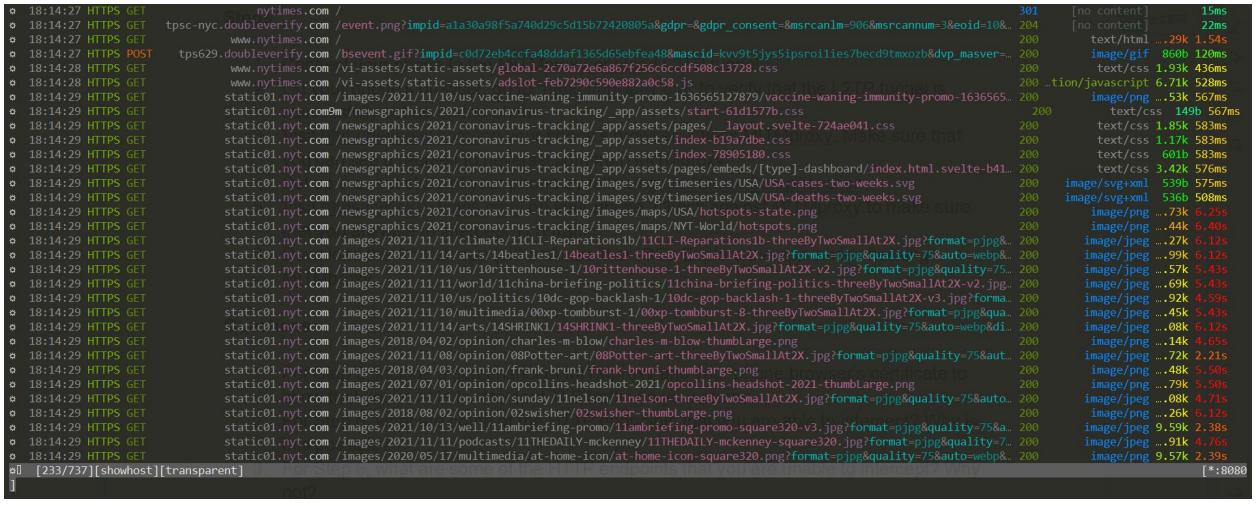
This task is optional. If you decide to complete this task, you will get at most 10 bonus points toward your final grade.

Steps

1. Connect your phone to the MITMproxy-enabled L2TP tunnel.
2. On your phone's browser, go to "https://api.ipify.org" to verify that the L2TP tunnel is successfully set up on the phone.
3. Visit http://neverssl.com/ on your phone's browser. Check MITMproxy. Make sure that you can see a request to neverssl.com from MITMproxy.
4. Set up the root store of your phone by following the "Quick Setup" section.
5. Visit https://www.nytimes.com/ on your phone. Check against MITMproxy to make sure that you are able to intercept TLS traffic.
6. Download the Amtrak app (either Android or iOS). Explore the app while checking MITMproxy.

Questions

1. For Step 5, include a screenshot of MITMproxy and your phone browser's certificate to show that you're able to intercept TLS traffic on your phone.



2. For Step 6, what are some of the HTTP endpoints that you are able to intercept? Why is this possible?

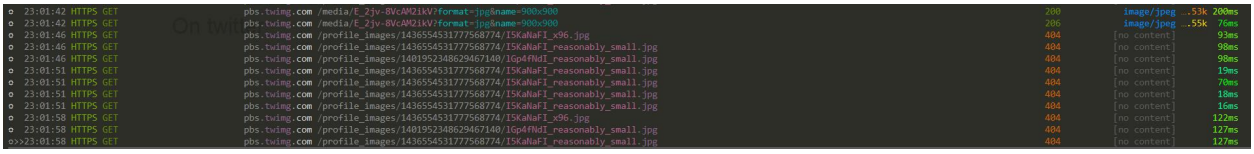
This is possible because mitmproxy is the one actually initiating TLS session with the target server, and then it encrypts the message with its own private key and has the client trust the self-signed certificate by letting the client install mitmproxy in its root store.

3. For Step 6, what are some of the HTTP endpoints that you are unable to intercept? Why not?

Actually, I cannot see any endpoint that I am unable to intercept

4. Repeat Step 6 with another app of your choice (other than Amtrak), such that you are able to intercept *some* of its TLS traffic. Describe what you see and explain your observations.

On twitter mobile app, I am unable to intercept most of the endpoints.



This is because twitter is using certificate pinning, causing the client to pin a certificate to a particular CA. Thus, the certificate signed by the mitmproxy is not trusted.