

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.

```
=====
IPsec VPN server is now ready for use!

Connect to your new VPN with these details:

Server IP: 137.184.135.150
IPsec PSK: nx3g2bSP2ZSJFteRvUge
Username: vpnuser
Password: mFS9vxJZChGquYqy

Write these down. You'll need them to connect!

Important notes:  https://git.io/vpnnotes
Setup VPN clients: https://git.io/vpnclients
IKEv2 guide:      https://git.io/ikev2
=====
```

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

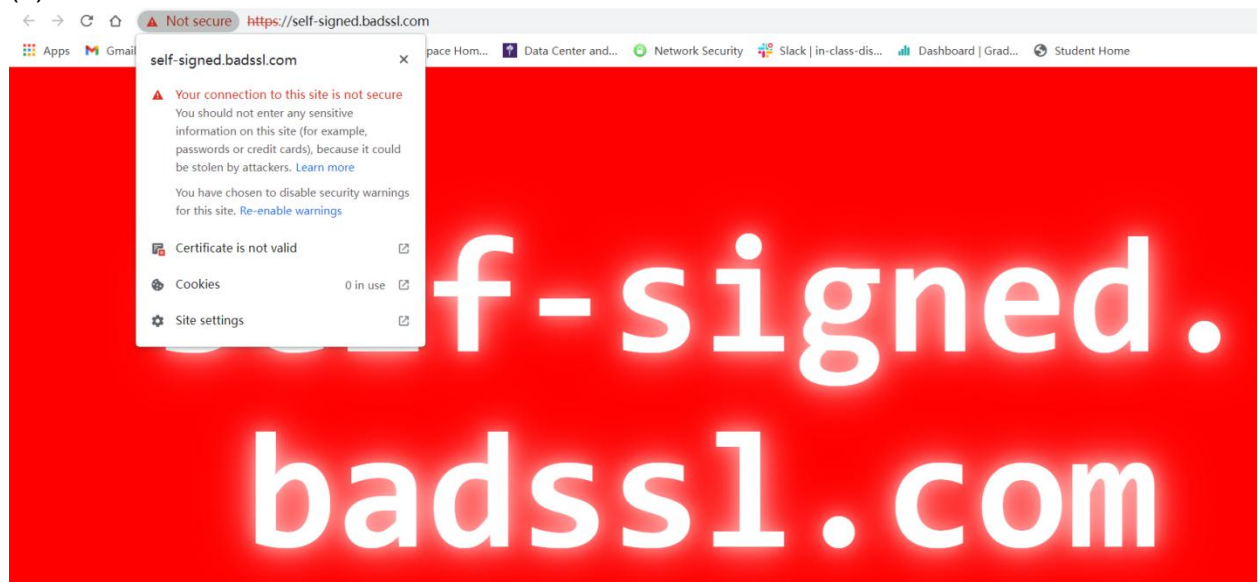
1. Visit <https://self-signed.badssl.com/>
2. Visit <https://expired.badssl.com/>
3. Visit <https://revoked.badssl.com/>

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

Questions

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

(1) .



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)



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](#)

Hide advanced

Reload

revoked.badssl.com normally uses encryption to protect your information. When Chrome tried to connect to revoked.badssl.com this time, the website sent back unusual and incorrect credentials. This may happen when an attacker is trying to pretend to be revoked.badssl.com, or a Wi-Fi sign-in screen has interrupted the connection. Your information is still secure because Chrome stopped the connection before any data was exchanged.

You cannot visit revoked.badssl.com right now because its certificate has been revoked. Network errors and attacks are usually temporary, so this page will probably work later.

(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



(2) the certificate has expired



(3) The certificate is revoked.



Task 3. Set up MITMproxy.

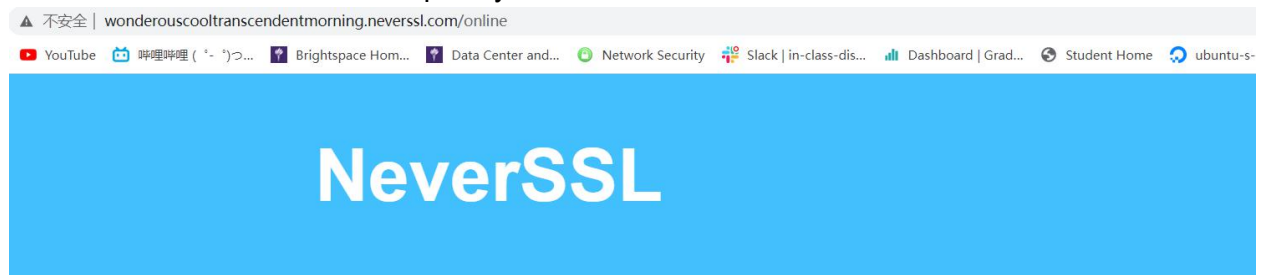
Steps

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.



What?

This website is for when you try to open Facebook, Google, Amazon, etc on a wifi network, and nothing happens. Type "http://neverssl.com" into your browser's url bar, and you'll be able to log on.

How?

neverssl.com will never use SSL (also known as TLS). No encryption, no strong authentication, no [HSTS](#), no HTTP/2.0, just plain old unencrypted HTTP and forever stuck in the dark ages of internet security.

Why?

16:00:24	HTTP	GET	neverssl.com /	304	[no content]	11ms
16:00:24	HTTP	GET	g.neverssl.com /online	200	text/html 1.16k	11ms
16:00:24	HTTP	GET	g.neverssl.com /favicon.ico	200	image/png 124b	11ms

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.



您的连接不是私密连接

攻击者可能会试图从 **www.nytimes.com** 窃取您的信息（例如：密码、通讯内容或信用卡信息）。[了解详情](#)

NET::ERR_CERT_AUTHORITY_INVALID



如果您想获得 Chrome 最高级别的安全保护，请[开启增强型保护](#)

隐藏详情

返回安全连接

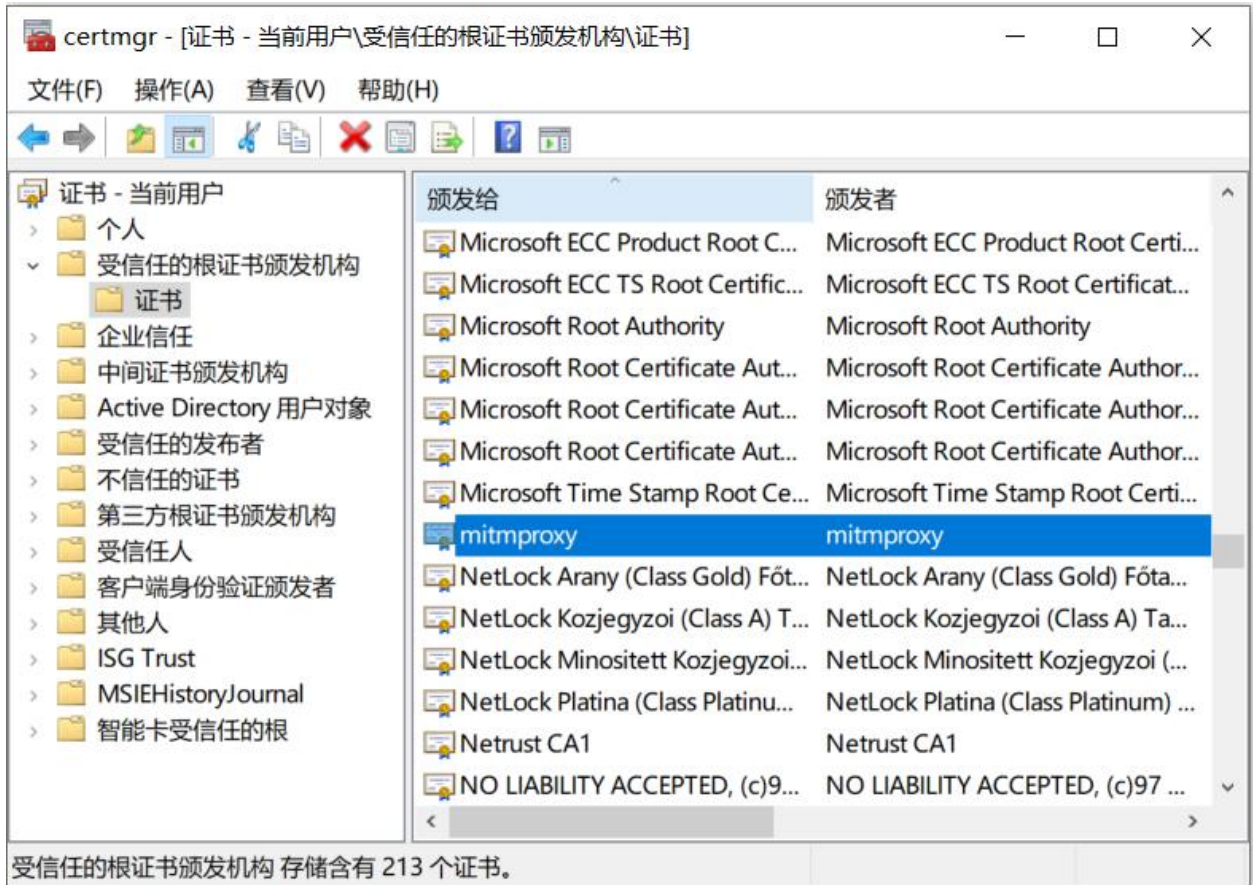
此服务器无法证明它是**www.nytimes.com**；您计算机的操作系统不信任其安全证书。出现此问题的原因可能是配置有误或您的连接被拦截了。

[继续前往www.nytimes.com \(不安全\)](#)

```
o 16:05:21 HTTPS GET www.nytimes.com / 200 text/html ...79k 34ms
o 16:05:21 HTTPS GET www.nytimes.com /vi-assets/static-assets/global-2c70a72e6a867f256c6... 200 text/css 1.93k 15ms
o 16:05:22 HTTPS GET www.nytimes.com /vi-assets/static-assets/adslot-feb7290c590e882a0c5...
o 16:05:22 HTTPS GET www.nytimes.com /vi-assets/static-assets/vendor-5252235bad21decf391...
o 16:05:22 HTTPS GET www.nytimes.com /vi-assets/static-assets/home-601f5ba0a1d509a65f5f...
o 16:05:22 HTTPS GET www.nytimes.com /vi-assets/static-assets/main-b3ef82dc60fee0afcf72...
```

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

What?

This website is for when you try to open Facebook, Google, Amazon, etc on a wifi network, and nothing happens. Type "http://neverssl.com" into your browser's url bar, and you'll be able to log on.

How?

neverssl.com will never use SSL (also known as TLS). No encryption, no strong authentication, no [HSTS](#), no HTTP/2.0, just plain old unencrypted HTTP and forever stuck in the dark ages of internet security.

Why?

Normally, that's a bad idea. You should always use SSL and secure encryption when possible. In fact, it's such a bad idea that most websites are now using https by default.

```
o 16:22:20 HTTP GET ...m.neverssl.com /online 200 text/html 1.16k 73ms
o 16:22:21 HTTP GET ...m.neverssl.com /favicon.ico 200 image/png 124b 15ms
```

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.

nytimes.com

The New York Times

Today's Paper

World U.S. Politics N.Y. Business Opinion Tech Science Health Sports Arts Books Style Food Travel Magazine T Magazine Real Estate Video

LIVE
Migrant Crisis Turns Dire, as West Accuses Belarus of Engineering It

With thousands of migrants stranded at the Poland-Belarus border, a standoff between the countries escalated, as each blamed the other for the crisis.

Poland stood by its hard-line border policy while Belarus's leader said he could disrupt the natural gas flow through his country to Europe. Here's the latest.

The Associated Press and Reuters

What We Know So Far About Waning Vaccine Effectiveness

Vaccines offer strong protection against severe Covid, but many studies show their protection decreases over time. How much that matters is up for debate.

LIVE 21m ago
Coronavirus Updates

Europe had over half of the world's Covid...

Vaccine Effectiveness Against Any Infection Over Time

Moderna Canadian study
Pfizer Canadian study
Pfizer U.S. study

Shaded region shows the range

Casa Magazines Has Seen It All

New York's West Village has changed a lot since the 1990s, but this palace of printed matter has remained a pillar of the neighborhood.

Tim Barber for The New York Times

The elaborate "TikTok hair" that's become popular among young men has surprisingly ancient roots.

Over a decade after its publication, one book on dating has people firmly in its grip.

Opinion
CHARLES M. BLOW

```

16:23:18 HTTPS GET www.nytimes.com / 200 text/html ...82k 96ms
16:23:18 HTTPS GET g1.nytimes.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.nytimes.com /newsgraphics/2021/coronavirus-tracking/_app/assets... 200 text/css 149b 108ms
16:23:19 HTTPS GET ...atic01.nytimes.com /newsgraphics/2021/coronavirus-tracking/_app/assets... 200 text/css 1.85k 108ms
16:23:19 HTTPS GET ...atic01.nytimes.com /newsgraphics/2021/coronavirus-tracking/_app/assets... 200 text/css 1.17k 107ms
16:23:19 HTTPS GET ...atic01.nytimes.com /newsgraphics/2021/coronavirus-tracking/_app/assets... 200 text/css 601b 107ms
16:23:19 HTTPS GET www.nytimes.com /vi-assets/static-assets/vendor-5252235bad21decf391... 200 text/css 3.42k 107ms
16:23:19 HTTPS GET www.nytimes.com /vi-assets/static-assets/home-601f5ba0a1d509a65f5f... 200
16:23:19 HTTPS GET www.nytimes.com /vi-assets/static-assets/main-b3ef82dc60fee0afc72... 200
16:23:19 HTTPS GET ...atic01.nytimes.com /newsgraphics/2021/coronavirus-tracking/images/svg/... 200 image/svg+xml 539b 261ms
16:23:19 HTTPS GET ...;49matic01.nytimes.com /newsgraphics/2021/coronavirus-tracking/images/svg/... 200 image/svg+xml 536b 260ms
16:23:19 HTTPS GET ...atic01.nytimes.com /images/2018/04/02/opinion/charles-m-blow/charles-m... 200 image/png ...14k 260ms
16:23:19 HTTPS GET ...atic01.nytimes.com /images/2018/08/02/opinion/02swisher/02swisher-thum... 200 image/png ...26k 291ms
16:23:19 HTTPS GET ...atic01.nytimes.com /images/2021/07/01/opinion/opcollins-headshot-2021/... 200 image/png ...79k 259ms
16:23:19 HTTPS GET ...atic01.nytimes.com /images/2021/11/10/us/vaccine-waning-immunity-promo... 200 image/webp ...51k 241ms
16:23:19 HTTPS GET ...atic01.nytimes.com /ads/tpc-check.html 200 text/html 550b 240ms
16:23:19 HTTPS GET ...atic01.nytimes.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.



502 Bad Gateway

Certificate verify failed: self signed certificate

The MITMproxy does not trust the self-signed certificate.

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

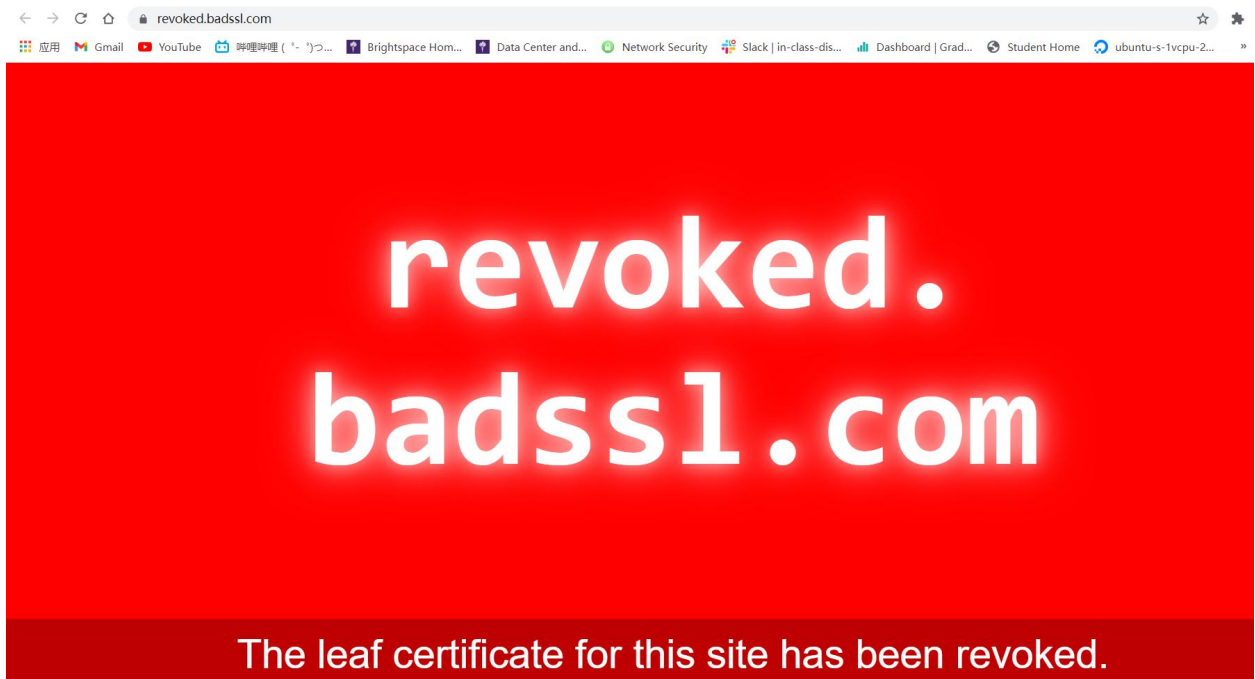


502 Bad Gateway

Certificate verify failed: certificate has expired

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.

18:14:27	HTTPS GET	nytimes.com	/event.png?impid=aia30a98f5a740d29c5d15b72420805a&gdp=8&gdp_consent=8msrcanlm=906&msrcannum=3&eid=108...	301	[no content]	15ms
18:14:27	HTTPS GET	tpsc-nyc.doubleverify.com	/event.png?impid=aia30a98f5a740d29c5d15b72420805a&gdp=8&gdp_consent=8msrcanlm=906&msrcannum=3&eid=108...	204	[no content]	22ms
18:14:27	HTTPS GET	www.nytimes.com	/bsevent.gif?impid=c0d72eb4cfa48ddaf1365d5ebfca48&mscid=kvv9t5jys5lpsroillies7beed9tawozb&dv_masver=...	200	text/html	29K 1.54s
18:14:27	HTTPS POST	tps629.doubleverify.com	/bsevent.gif?impid=c0d72eb4cfa48ddaf1365d5ebfca48&mscid=kvv9t5jys5lpsroillies7beed9tawozb&dv_masver=...	200	image/gif	860B 120ms
18:14:28	HTTPS GET	www.nytimes.com	/vi-assets/static-assets/global-2c70a726a867f256c6ccdf508c13728.css	200	text/css	1.93K 436ms
18:14:28	HTTPS GET	www.nytimes.com	/vi-assets/static-assets/adslot-feb7290c590e882a0c58.js	200	text/javascript	6.71K 528ms
18:14:29	HTTPS GET	static01.nytimes.com	/images/2021/11/10/us/vaccine-waning-immunity-promo-1636565127879/vaccine-waning-immunity-promo-1636565...	200	image/png	553K 567ms
18:14:29	HTTPS GET	static01.nytimes.com	/newsgraphics/2021/coronavirus-tracking/_app/assets/start-61d1577b.css	200	text/css	149B 567ms
18:14:29	HTTPS GET	static01.nytimes.com	/newsgraphics/2021/coronavirus-tracking/_app/assets/pages/_layout.svelte-724ae041.css	200	text/css	1.85K 583ms
18:14:29	HTTPS GET	static01.nytimes.com	/newsgraphics/2021/coronavirus-tracking/_app/assets/index-b19a7d8e.css	200	text/css	1.17K 583ms
18:14:29	HTTPS GET	static01.nytimes.com	/newsgraphics/2021/coronavirus-tracking/_app/assets/index-78905180.css	200	text/css	601B 583ms
18:14:29	HTTPS GET	static01.nytimes.com	/newsgraphics/2021/coronavirus-tracking/_app/assets/pages/embeds/[type]-dashboard/index.html.svelte-b41...	200	text/css	3.42K 576ms
18:14:29	HTTPS GET	static01.nytimes.com	/newsgraphics/2021/coronavirus-tracking/images/svg/timeseries/USA/USA-cases-two-weeks.svg	200	image/svg+xml	539B 575ms
18:14:29	HTTPS GET	static01.nytimes.com	/newsgraphics/2021/coronavirus-tracking/images/svg/timeseries/USA/USA-deaths-two-weeks.svg	200	image/svg+xml	536B 590ms
18:14:29	HTTPS GET	static01.nytimes.com	/newsgraphics/2021/coronavirus-tracking/images/maps/NYT-World/hotspots-state.png	200	image/png	73K 6.25s
18:14:29	HTTPS GET	static01.nytimes.com	/newsgraphics/2021/coronavirus-tracking/images/maps/NYT-World/hotspots.png	200	image/png	44K 6.40s
18:14:29	HTTPS GET	static01.nytimes.com	/images/2021/11/11/climate/11cli-Reparations1b-threeByTwoSmallAt2X.jpg?format=pjpg&...	200	image/jpeg	27K 6.12s
18:14:29	HTTPS GET	static01.nytimes.com	/images/2021/11/14/arts/14beatles114beatles1-threeByTwoSmallAt2X.jpg?format=pjpg&quality=75&auto=webp&...	200	image/jpeg	99K 6.12s
18:14:29	HTTPS GET	static01.nytimes.com	/images/2021/11/10/us/10rittenhouse-110rittenhouse-1-threeByTwoSmallAt2X-v2.jpg?format=pjpg&quality=75...	200	image/jpeg	57K 5.43s
18:14:29	HTTPS GET	static01.nytimes.com	/images/2021/11/11/world/11china-briefing-politics/11china-briefing-politics-threeByTwoSmallAt2X-v2.jpg...	200	image/jpeg	69K 5.43s
18:14:29	HTTPS GET	static01.nytimes.com	/images/2021/11/10/us/politics/10dc-gop-backlash-110dc-gop-backlash-1-threeByTwoSmallAt2X-v3.jpg?forma...	200	image/jpeg	92K 4.59s
18:14:29	HTTPS GET	static01.nytimes.com	/images/2021/11/10/multimedia/00xp-tombburst-1/00xp-tombburst-8-threeByTwoSmallAt2X.jpg?format=pjpg&qua...	200	image/jpeg	45K 5.43s
18:14:29	HTTPS GET	static01.nytimes.com	/images/2021/11/14/arts/14SHRIK1/14SHRIK1-threeByTwoSmallAt2X.jpg?format=pjpg&quality=75&auto=webp&di...	200	image/jpeg	68K 6.12s
18:14:29	HTTPS GET	static01.nytimes.com	/images/2018/04/02/opinion/02swisher/02swisher-thumbLarge.png	200	image/png	14K 6.65s
18:14:29	HTTPS GET	static01.nytimes.com	/images/2021/11/08/opinion/08Potter-art/08Potter-art-threeByTwoSmallAt2X.jpg?format=pjpg&quality=75&aut...	200	image/jpeg	72K 2.21s
18:14:29	HTTPS GET	static01.nytimes.com	/images/2018/04/03/opinion/03frank-bruni/03frank-bruni-thumbLarge.png	200	image/png	48K 5.50s
18:14:29	HTTPS GET	static01.nytimes.com	/images/2021/07/01/opinion/01collins-headshot-2021/opcollins-headshot-2021-thumbLarge.png	200	image/png	79K 5.50s
18:14:29	HTTPS GET	static01.nytimes.com	/images/2021/11/11/opinion/sunday/11nelson/11nelson-threeByTwoSmallAt2X.jpg?format=pjpg&quality=75&auto...	200	image/jpeg	88K 4.71s
18:14:29	HTTPS GET	static01.nytimes.com	/images/2018/08/02/opinion/02swisher/02swisher-thumbLarge.png	200	image/png	26K 6.12s
18:14:29	HTTPS GET	static01.nytimes.com	/images/2021/10/13/well/11ambriefing-promo/11ambriefing-promo-square320-v3.jpg?format=pjpg&quality=75&a...	200	image/jpeg	9.5K 2.38s
18:14:29	HTTPS GET	static01.nytimes.com	/images/2021/11/11/podcasts/11THEODAILY-mckeeney/11THEODAILY-mckeeney-square320.jpg?format=pjpg&quality=7...	200	image/jpeg	91K 4.76s
18:14:29	HTTPS GET	static01.nytimes.com	/images/2020/05/17/multimedia/at-home-icon/at-home-icon-square320.png?format=pjpg&quality=75&auto=webp&...	200	image/png	9.57K 2.39s
18:14:29	HTTPS GET	static01.nytimes.com	/images/2020/05/17/multimedia/at-home-icon/at-home-icon-square320.png?format=pjpg&quality=75&auto=webp&...	200	image/png	9.57K 2.39s



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

21:28:07	HTTPS GET	smetrics.bankofamerica.com /b/ss/baamprod/5/boaCustom041918a/s1636752487703/AQB-18bh-635&bw-375&cdp-2&ce-10TF-8&g-https%3A%2F%2Fsec...	200	image/gif	43b	53ms
21:29:06	HTTPS POST	www.amtrak.com /j_Bm3d/-cN/0uW/1vTCOnSR/5E1V2zDT57Ec/SuNsVyob/H5g/SVWw2c148	201	application/json	18b	230ms
21:29:06	HTTPS GET	www.facebook.com /tr/?id=31823398255744&ev-PagoV1u&d1-https%3A%2F%2Fwww.amtrak.com%2Fusara1ipass&e1-S1f=false&t6-16367...	200	image/gif	44b	147ms
21:29:06	HTTPS GET	px.ads.linkedin.com /collect?v=2&fmt=js&pid=1392169&time=1636752540&0&url=https%3A%2F%2Fwww.amtrak.com%2Fusara1ipass&cook1...	200	[no content]		155ms
21:29:07	HTTPS GET	analytics.twitter.com /i/adsc?type=page&iprversion=1.0.4&p_id=twitter&p_user_id=0&txn_id=nydp&events=330&5022pagariv&2...	200	tion/javascript	57b	178ms

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.

- 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

- 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.

23:01:42	HTTPS GET	pbs.twimg.com /media/t_2jv-BVcAQ1kV/format-jpg&name=50b200	200	image/jpeg	53b	200ms
23:01:42	HTTPS GET	pbs.twimg.com /media/t_2jv-BVcAQ1kV/format-jpg&name=50b200	200	image/jpeg	55k	76ms
23:01:46	HTTPS GET	pbs.twimg.com /profile_images/143655453177568774/ISkafI_x96.jpg	404	[no content]		93ms
23:01:46	HTTPS GET	pbs.twimg.com /profile_images/143655453177568774/ISkafI_reasonably_small.jpg	404	[no content]		90ms
23:01:46	HTTPS GET	pbs.twimg.com /profile_images/1401952348629467140/16p4HdI_reasonably_small.jpg	404	[no content]		98ms
23:01:51	HTTPS GET	pbs.twimg.com /profile_images/143655453177568774/ISkafI_reasonably_small.jpg	404	[no content]		19ms
23:01:51	HTTPS GET	pbs.twimg.com /profile_images/143655453177568774/ISkafI_reasonably_small.jpg	404	[no content]		70ms
23:01:51	HTTPS GET	pbs.twimg.com /profile_images/143655453177568774/ISkafI_reasonably_small.jpg	404	[no content]		18ms
23:01:51	HTTPS GET	pbs.twimg.com /profile_images/143655453177568774/ISkafI_reasonably_small.jpg	404	[no content]		16ms
23:01:58	HTTPS GET	pbs.twimg.com /profile_images/143655453177568774/ISkafI_x96.jpg	404	[no content]		122ms
23:01:58	HTTPS GET	pbs.twimg.com /profile_images/1401952348629467140/16p4HdI_reasonably_small.jpg	404	[no content]		127ms
23:01:58	HTTPS GET	pbs.twimg.com /profile_images/143655453177568774/ISkafI_reasonably_small.jpg	404	[no content]		127ms

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.