medium.com

Mitmproxy: Your D.I.Y. Private Eye - Max’s Blog - Medium

Max Greenwald

23-29 minutes

Part 1/2: How To Install A Free Tool To Catch Companies Collecting Data About You Without Your Consent

What if I told you that every time you go to a website or open up an app, there is a company that you have never heard of that is collecting information about you? What if I told you that this website or app that you are trusting, is likely *knowingly* sharing your personal information? What if I told that the majority of websites and apps have no idea how to implement basic security practices that leave them hackable to anyone?

My name is Max and I’m a Computer Science & Public Policy major. I spent the summer of 2015 learning about privacy and security. After diving into the weeds and seeing the state of the field, I was shocked at how little the average consumer knows about what companies can and are doing to their customer’s data. Think about those questions I asked above again. What if that company has your Social Security Number? What if it has your personal health data?

An illustration from Lifehacker.com

I personally believe that consumers should have a right to own their own data and should have a right to know who is using their personal information and for what. It is for that reason that I would like share a free and open source tool called Mitmproxy that can be downloaded by anyone to investigate the privacy and security practices of companies. The tool takes 10 minutes to install and a few extra to learn what you are doing. After you will be fully equipped to catch companies collecting data about you without your permission. If you have already downloaded Mitmproxy and want to learn how to analyze the data that you are looking at, please visit Part 2: How To Analyze Mitmproxy.

But what is Mitmproxy? Mitmproxy is a network analysis tool for learning about the behind the scenes of who sends what where on your phone or computer. The name Mitmproxy comes from a type of hacker attack called a Man-in-the-Middle attack (MITM) where the attacker gets "on the wire" and looks at the information being sent back and forth — because they're in the middle of the communication.

This guide assumes that you have a Mac computer purchased in 2012 or later (or that you have OS X Mountain Lion or newer) or a Linux Computer and, if you want to analyze the behind the scenes of mobile applications, that you have an iPhone or Android phone connected to Wi-Fi. Not necessary, but you can also connect as well if you have an Ethernet instead of Wi-Fi. If you have a Windows computer you can use a similar tool called Fiddler. The setup time for Mitmproxy, if you have none of the necessary components already installed could take up to 15 minutes. But after first time installation, it will only take 30 seconds to get going for consecutive sessions. I would strongly recommend doing a bit of reading about the use of the Terminal (Mac) or Konsole (Linux) application because we will be executing lines of code from these applications. They are already installed on your computer. Try here. If ever you receive an error message and one of the setup steps could not be completed, by copy/pasting the error message into a Google search, there will be many resources to troubleshoot the problem.

The following is a step-by-step guide for learning how to install Mitmproxy.

The way Mitmproxy works is by sitting in the middle of the connection between your phone or computer, and the internet at large. Checkout this nice diagram made by Phillip Heckel on his blog post on Mitmproxy.

The communication route for how Mitmproxy intercepts traffic

While this diagram may be confusing at first, it will make sense as time goes along. Essentially we are going to, in the case of looking at the traffic between your mobile application and the internet at large, tell your phone to send all information to Mitmproxy and then tell Mitmproxy to send all information to the internet at large, which will then send back information and on and on. Remember that your phone and computer send information to a router, who then directs it to the company's servers of the website or mobile application you are trying to interact with. Something that makes Mitmproxy special is its ability to decrypt SSL encrypted or HTTPS traffic for you to see. As most companies move towards sending information over HTTPS, the information is sent all jumbled up so attackers cannot see it. But this traffic, sent in little bursts called packets, could be the juiciest information for us, the consumers, to analyze. So Mitmproxy unencrypts it for us by installing a certificate (let's call it a bribe) on your phone or computer such that is sends Mitmproxy the information in easy-to-read English. Companies have even begun to be trickier (this is a good security practice!) and told their mobile applications not to trust Mitmproxy or anyone's certificates except their own — called certificate pinning. This guide also gives you a way to break certificate pinning so you can still see the traffic flow.

Here is a quick glance of what Mitmproxy looks like in action — don't get scared, it will make sense in just a few mintues!

A typical Mitmproxy capture session

Mitmproxy Set Up Process — Installation and

Computer/Phone Environments

Continue if you have a Mac Computer or skip to the Linux Computer section

Mac Computer Installation:

The best way to get set up for your Mac computer is through using your Terminal application. We will need to install a few tools to get set up. If you have not ever coded before, you will likely need to download all of them. You will need Xcode, Command Line Tools, Homebrew, Python and Pip. If you have all of these skip below. If you're feeling a bit lazy, and know how to use Terminal a little bit, skip down to "Other set up option." Otherwise you can install Xcode and Command Line Tools by using this link.

Then you can install Homebrew by using this link or:

Open your Terminal application and type

```
ruby -e "$(curl -fsSkL raw.github.com/mxcl/homebrew/go)"
```

And then hit enter. This goes onto the internet and downloads Homebrew for you using a language called Ruby.

Then you can install Python using this link. By downloading the latest version of Python (get either the one that starts with 3.something or 2.something) this should also get you pip. If you already have Python installed make sure to update it. Skip downloading Pip, but come back and do the below step if the installation of Mitmproxy does not work.

To download pip use this link or in Terminal type:

```
python get-pip.py
```

And then hit enter.

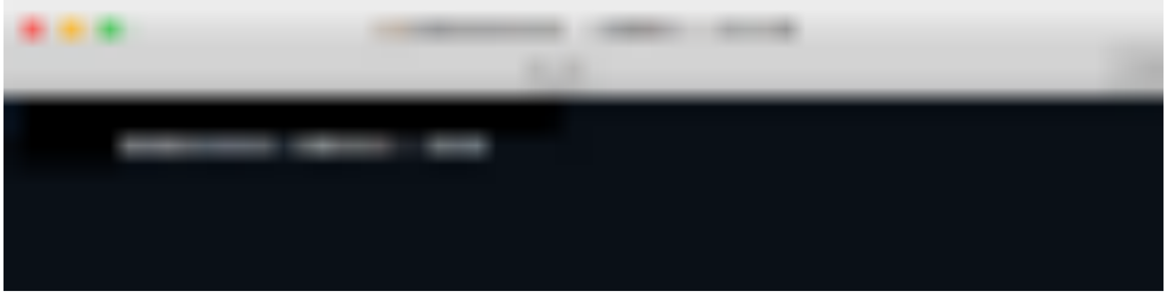
Finally you can download Mitmproxy by going to your Terminal application and typing:

```
pip install mitmproxy
```

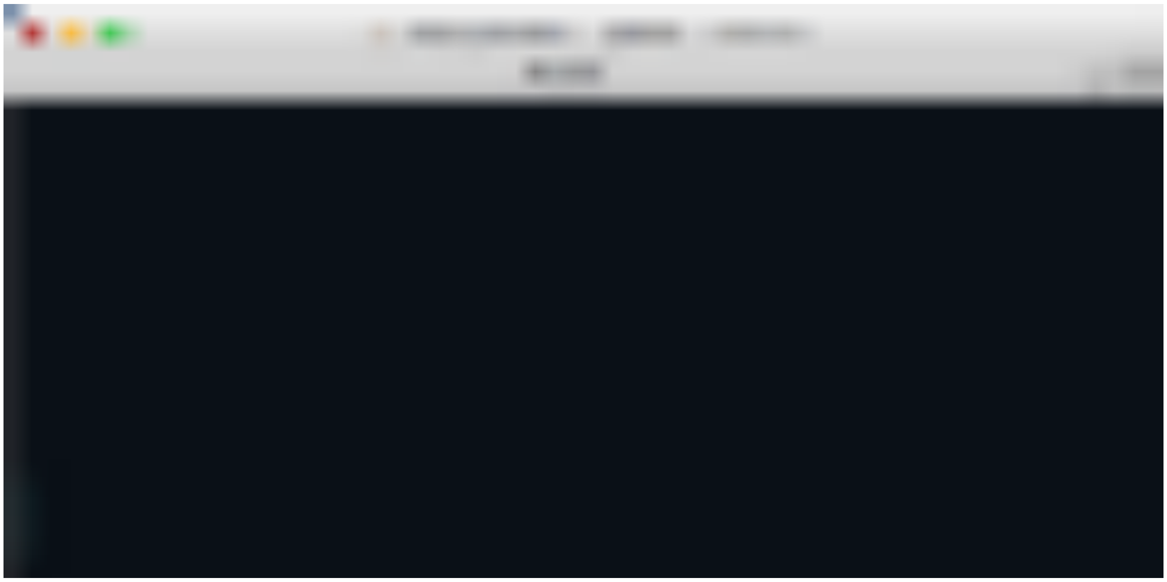
And then hit enter. Note the lowercase “m.” Know that capital letters matter in coding so do not type any capitals in the above command.

To check to make sure it worked, now type into Terminal,

```
mitmproxy --host
```



That is two dashes before “host.” Then hit enter. Note the lowercase “m.” Ignore the stuff on the screenshot that is not “mitmproxy --host” (poppyrivera is just the name of my computer). You should see something that looks like this:



A blank Mitmproxy screen

Now type "q" followed by "y" to quit Mitmproxy.

Other Set Up Option:

If this gets too confusing or for some reason does not work, you can try the following steps:

1. On the mitmproxy website (mitmproxy.org), click the link next to the big apple logo, which reads, "OSX (Mountain Lion and later)".

2. It should drop a file into your "Downloads" directory, which is probably the icon on your desktop dock next to your trash can. Click that icon.

3. Double click the file you just downloaded. It'll be called something like "osx-mitmproxy-0.13.0.tar.gz", although the version numbers may vary.

4. Now the mitmproxy file is ready to go on your computer, but it only "works" if run from the Downloads folder, lets make it runnable from any folder. Open up your Terminal application and type

```
mdfind mitmproxy
```

And hit enter. You should see a few lines spit out. One of them is the file path to where mitmproxy lives. It should start with "/Users" and end with "mitmproxy" and look something like:

```
/Users/YourName/Downloads/SomeStuff/osx-mitmproxy-
0.13/mitmproxy
```

Whatever it is, copy that whole line. Then type into Terminal

```
cd /usr/local/bin
```

And hit enter. Now type (and paste the file path where I write FILEPATH)

```
sudo cp FILEPATH .
```

Notice the "." at the end after a space. And hit enter. Then enter your password and hit enter. This copies mitmproxy into the base of your computer such that now you can use mitmproxy anywhere! Now type

```
cd
```

and hit enter. This gets you back to your regular Terminal starting point. Now type

```
./mitmproxy
```

and then enter.

5. You should be running mitmproxy. It should look like the picture above^. Now type "q" followed by "y" to quit Mitmproxy.

Heads up: In all of the following steps, instead of typing "mitmproxy --host" into Terminal you'll need to type "./mitmproxy"

Continue if you have a Linux Computer or skip to the Phone Set Up section

---

Linux Computer Installation:

On your Konsole type

```
sudo apt-get install python-pyasn1 python-flask python-urwid
python-dev libxml2-dev libxslt-dev libffi-dev
```

Hit enter and wait until completion. You might have to type in your computer password which is just your computer asking if you are okay with downloading some new stuff. Then type

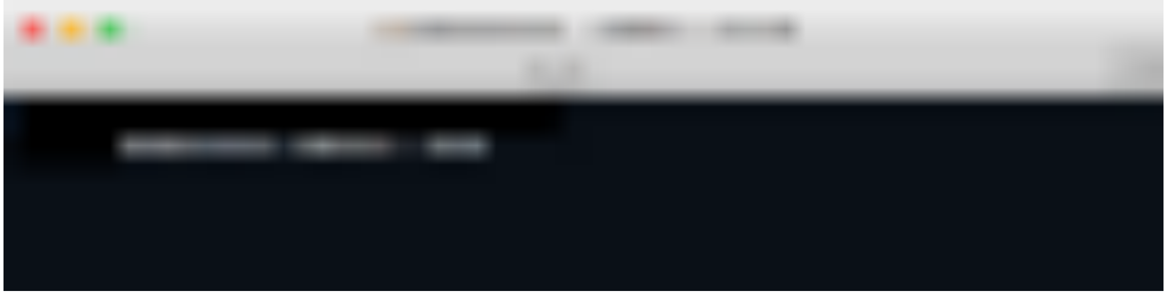
```
sudo pip install mitmproxy
```

Hit enter and wait until completion. Note the lowercase "m."

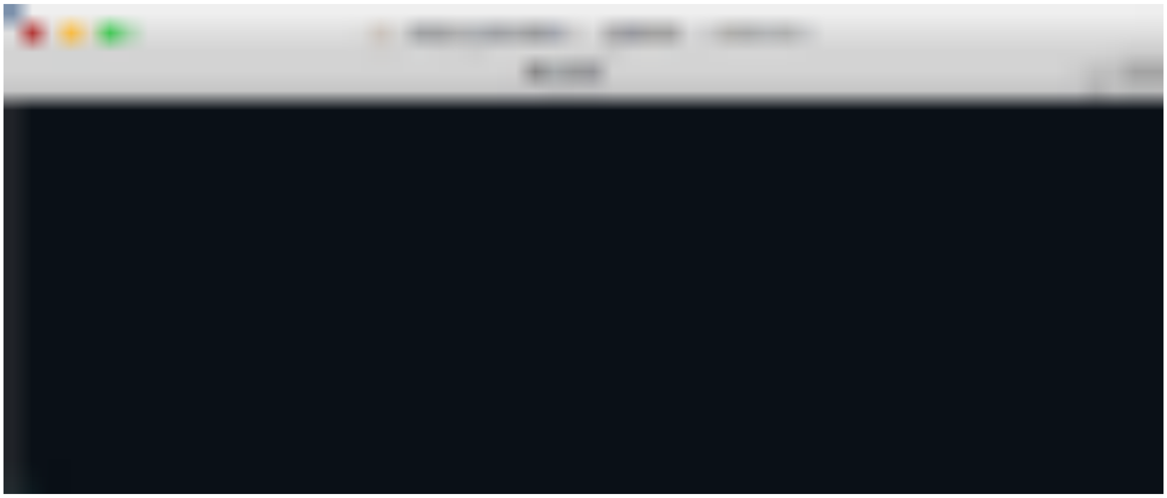
This will download a few other dependencies if you don't have them like Python and Pip.

To check to make sure it worked, now type into Terminal,

```
mitmproxy --host
```



That is two dashes before "host." Then hit enter. Note the lowercase "m." Ignore the stuff on the screenshot that is not "mitmproxy --host" You should see something that looks like this:



A blank Mitmproxy screen

Now type "q" followed by "y" to quit Mitmproxy.

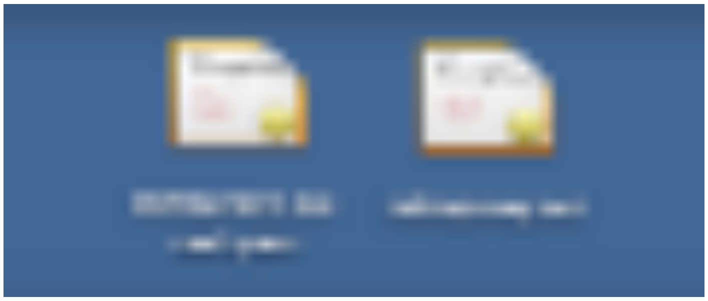
We now have Mitmproxy installed on our computer. Mitmproxy can now see 1 of 2 of the types of channels we want to see: HTTP. To enable our computer to trust Mitmproxy enough to allow it see HTTPS connections we need to install a certificate. First type into Terminal/Konsole,

```
mitmproxy --host
```

Mitmproxy needs to be running for the certificate to work. Note the lowercase "m." Then from your browser on your computer (Chrome, Safari, etc), visit `http://mitm.it`. (This won't send you to an Italian webpage; Mitmproxy intercepts the request and sends you its own content instead.) and click on the Apple logo for Mac or the Other logo for Linux.

What you should see on mitm.it

Follow the instructions to install the certificate. If for some reason that is not working, go to this link and follow the instructions.



What a certificate looks like if on your desktop

You can now in Terminal/Konsole type “q” followed by “y” to quit Mitmproxy.

Now our computer will trust Mitmproxy. Now we can open our browser and start to surf the web. At this point I highly recommend downloading a new browser (Firefox is great if you use something else currently. Get Chrome if you use Firefox) so that you can search the web normally on one, and use Mitmproxy on the other. Otherwise you will have to revert the settings back and forth on your browser to go between regular use and Mitmproxy use.

The following is how you configure Firefox and Chrome to work for Mitmproxy. The process is the same for both browsers– instead of telling our browser to send HTTP and HTTPS information to our router and the internet at large, we are going to send the HTTP and HTTPS traffic to a channel, called a port, that Mitmproxy will intercept, show you what you want to see, and then Mitmproxy will cast out the information to the internet at large.

Continue if you are going to use Firefox to browse Mitmproxy or* *skip to the Chrome section

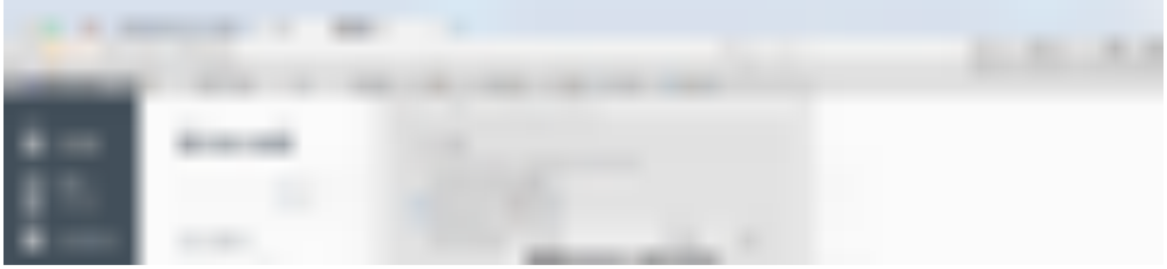
Firefox Mitmproxy Settings

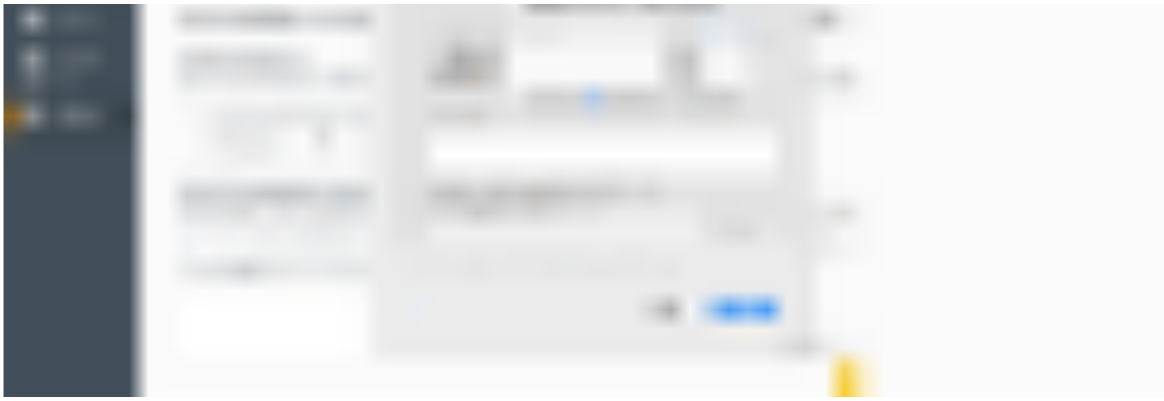
If you haven't already, make sure to download that certificate on mitm.it using Firefox.

In the top right of Firefox look for the three horizontal lines, called a menu bar, click it and then click Preferences.

A typical Firefox browser on launch

On the left click Advanced, in the middle click Network, on the right click Settings and then click "Manual Proxy Configuration." Under HTTP Proxy type 127.0.0.1 in the first field, and 8080 under Port. Now under SSL Proxy type 127.0.0.1 in the first field, and 8080 under Port. Then hit OK.





Advanced settings for Firefox

You are now directing all HTTP and SSL encrypted HTTPS traffic from your browser to Mitmproxy, who is listening on your local host (127.0.0.1) on port 8080. Now type into Terminal/Konsole,

```
mitmproxy --host
```

In Firefox type www.google.com in the URL bar and hit Enter. You should see something like this in Terminal/Konsole:

Mitmproxy capturing HTTP and HTTPS packets

Which should show HTTP and HTTPS packets. I will explain later exactly what the heck you're looking at. If it does not show this or your browser says it is not trusted, navigate to some other sites and see if simply any HTTP packets show up. No HTTPS means you have problems with your certificate installation and no packets at all could indicate a problem with your Firefox settings. You might have to delete the Certificate and try again. Under Advanced > Certificates > View Certificates > Authorities and scroll down and delete the Mitmproxy certificate. Go to mitm.it and try again.

You can now in Terminal/Konsole type "q" followed by "y" to quit Mitmproxy.

A picture of what you should see when quitting Mitmproxy

How to reset your Firefox settings to browse normally

Later, when you're finished with Mitmproxy switch Firefox back by clicking No Proxy and then OK.

By using two browsers, you could just always leave the Firefox settings to save hassle in future sessions.

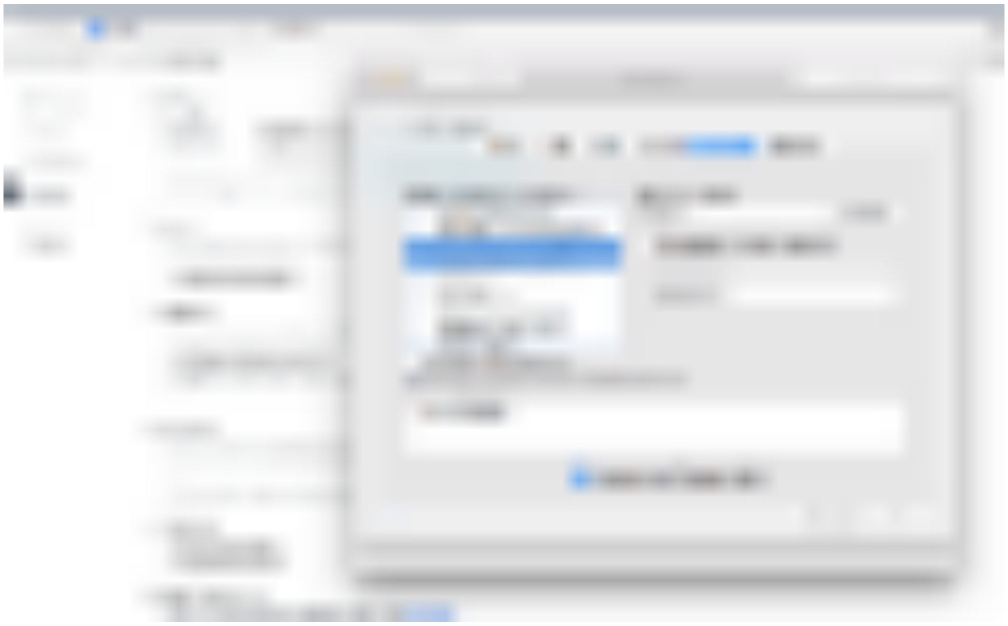
Chrome Mitmproxy Settings

If you haven't already, make sure to download that certification on mitm.it using Chrome.

Open Chrome and where the three bars (for Menu) are on the right hand side click "Settings" and then scroll down to the bottom and click "Show Advanced Settings"

A typical Chrome Settings page

Then about halfway down click on "Network Settings" this should open up your Network Preferences, click on HTTP and set the first field to the left of the colon to be 127.0.0.1 and the field on the right of the colon to be 8080. Then click on HTTPS and set the first field to the left of the colon to be 127.0.0.1 and the field on the right of the colon to be 8080. Make sure you do this for both.



Changing proxy settings on Chrome via Network Settings for Mac

Click "OK" and then click "Apply."

You are now directing all HTTP and SSL encrypted HTTPS traffic to Mitmproxy, who is listening on your local host (127.0.0.1) on port 8080. Quit Chrome and reopen it just in case to make sure it saves the settings.

Now type into Terminal/Konsole:

```
mitmproxy --host
```

In Chrome type www.google.com in the URL bar. You should see something like this on Chrome and Terminal/Konsole:

Mitmproxy capturing HTTP and HTTPS packets via Chrome

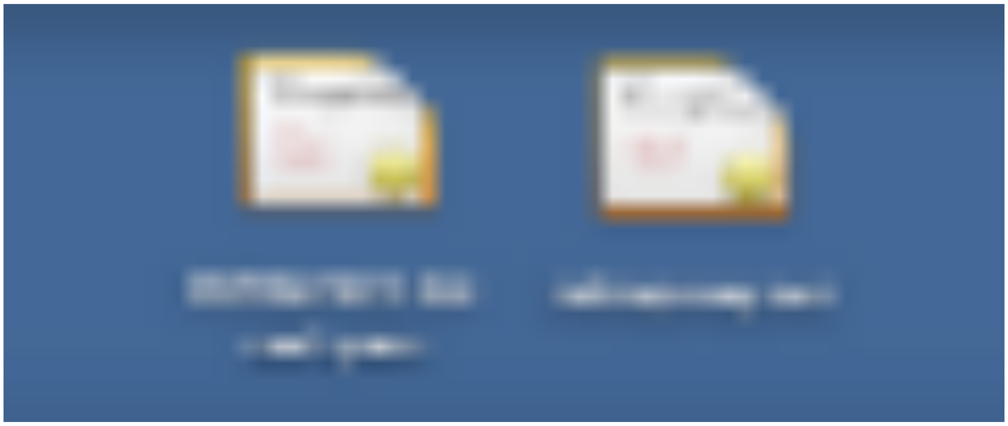
Which should show HTTP and HTTPS packets. I will explain later exactly what the heck you're looking at. If it does not show this or your browser says it is not trusted, navigate to some other sites and see if simply any HTTP packets show up. No HTTPS means you have problems with your certificate installation and no packets at all could indicate a problem with your Chrome settings.

You can now in Terminal/Konsole type "q" followed by "y" to quit Mitmproxy.

A picture of what you should see when quitting Mitmproxy

Later, when you're finished with Mitmproxy switch back by navigating back to Network Settings and unclicking the HTTP and HTTPS field. Make sure to click Apply afterwards. By using a different browser than Chrome, you could just always leave the other browsers settings like this to save hassle in future sessions because Chrome changes your computer settings.

Now we will do a similar process for your phone so Mitmproxy can record the behind the scenes stuff from your mobile applications. We need to set up a certificate on the phone and then configure the phone to send information to your computer where Mitmproxy is living.

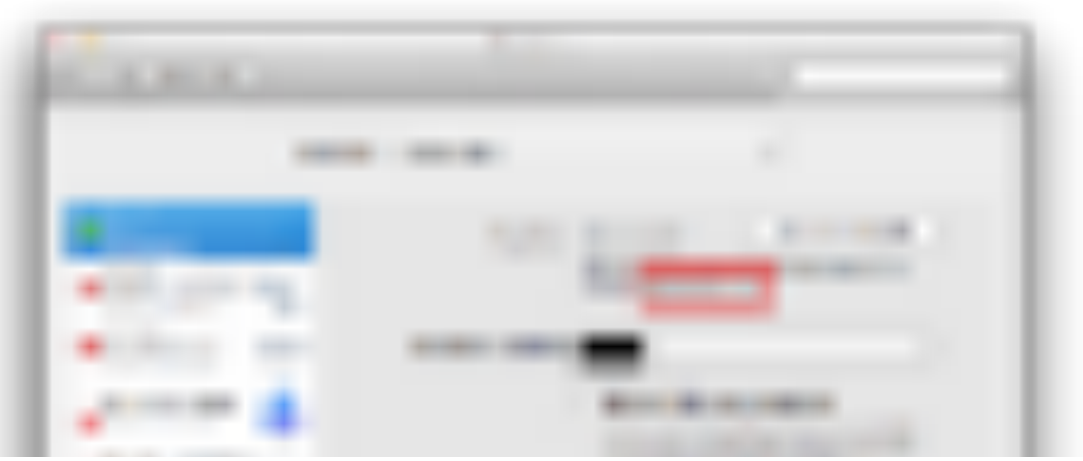


What a certificate looks like if on your desktop

From your computer find the certificate you installed for your browser in the Downloads section. It should say something like "mitmproxy-ca-cert.pem" and drag this to your desktop. Then email yourself with the certificate as an attachment. If you can't find it, Google "mitmproxy-ca-cert download" and get it.

Next you will need to find your local IP address of your computer.

On a Mac go to System Preferences, then Network and look for the number here. If you're using Ethernet and not Wi-Fi, jump to the Ethernet section or unplug, connect to Wi-Fi and try again to go here to see your IP Address. Here is mine:



Network Settings on Mac with the red box indicating a typical IP Address

On a Linux type into Konsole "ifconfig" and get your IP Address to the right of the field "inet" on the correct Wi-Fi that you're using. Or Google it.

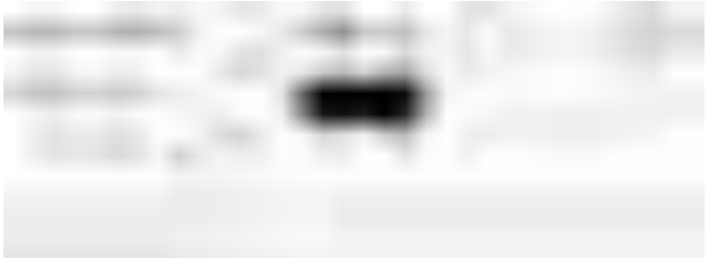
Now we will need to get our phones to trust Mitmproxy by configuring our phone network settings and then installing a certificate on our phone.

Continue if you have an iPhone or skip to the Android or Ethernet section

---

iPhone

First we tell our phone to send information to our computer by going to Settings, then Wi-Fi, then click on the little blue "i" next to your Wi-Fi name.



Changing the HTTP Proxy Settings on your iPhone Wi-Fi network to direct traffic to Mitmproxy with your computer's IP Address

Scroll down set HTTP PROXY to Manual. Then under Server enter the IP Address that you found before for your computer, and under Port enter 8080. This sends HTTP (and now HTTPS because of the certificate) traffic to Mitmproxy on our computer, where Mitmproxy is listening on port 8080.

You can reset this to make your phone work normally later by either turning Wi-Fi off and then on or by clicking Off on HTTP PROXY.

Now open the Mail app (not another email app like Gmail) and install the certificate by clicking on the certificate from the email and clicking Install. Follow the instructions. This tells our phone to trust Mitmproxy.

Screenshots from the Mail app on iPhone to download Mitmproxy certificate on your phone

What you should see on mitm.it on mobile

If this doesn't work. From your browser on your phone (Chrome, Safari, etc), visit mitm.it. (This won't send you to an Italian webpage; mitmproxy intercepts the request and sends you its own content instead.) and click on the Apple logo for iPhone and follow the instructions.

If for some reason this doesn't work you'll need to install the certificate manually. This can be done here under the heading for manual install.

Now type into Terminal/Konsole on your computer:

```
mitmproxy --host
```

On your phone quit all of your apps and then go open up one app (I opened the App Store). You should see something like this on your computer and phone:

Mitmproxy capturing HTTP and HTTPS packets from an iPhone

Which should show HTTP and HTTPS packets. We will explain later exactly what the heck you're looking at. If it does not show this or the application is acting weird, navigate to some other apps and see if simply any HTTP packets show up. No HTTPS means you have problems with your certificate installation and no packets at all could indicate a problem with your network settings. If you're getting one or two packets to show up, it is possible that this app that you are looking at is using certificate pinning. Quit this app and try another — to break certificate pinning you need to install SSL Kill Switch for iPhone.

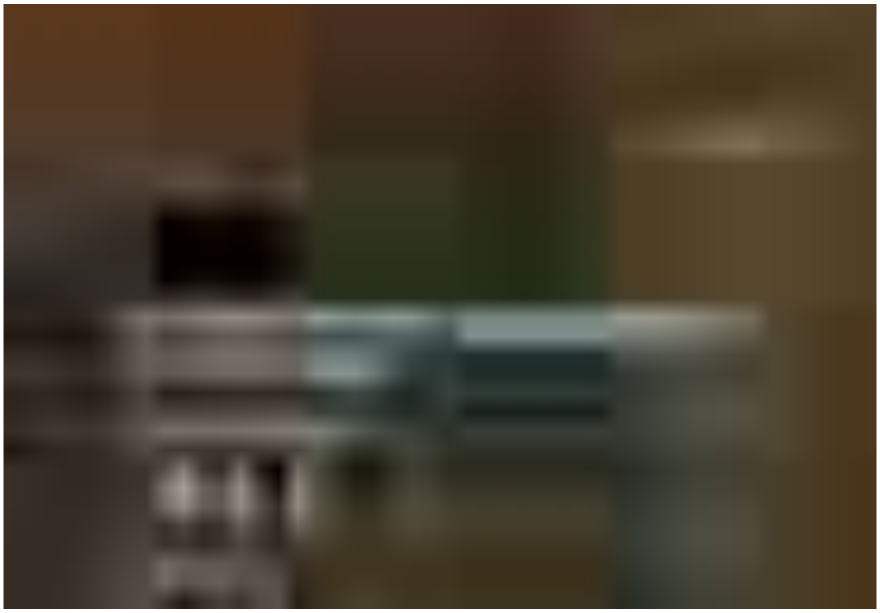
You can now in Terminal/Konsole type "q" followed by "y" to quit Mitmproxy.

Continue if you have an Android or skip to the Ethernet section

---

Android

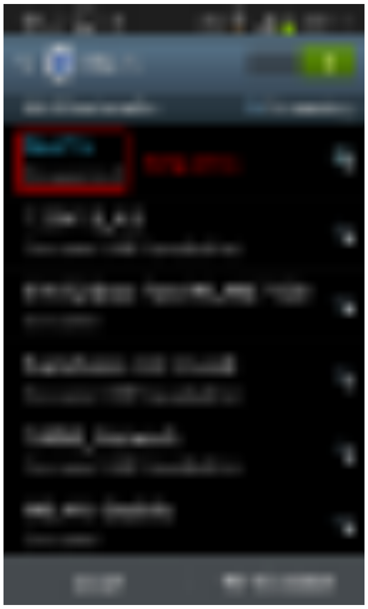
First we configure the network settings. Go to "Settings," "Wi-Fi" and **long-press** on your connected network. Choose "Modify network config.”

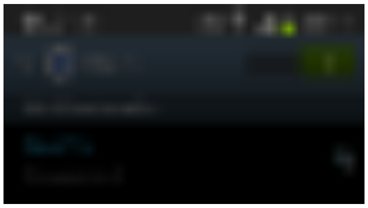


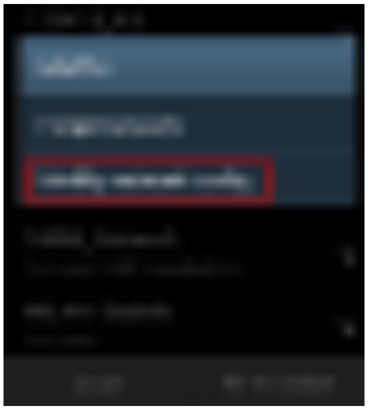
Screenshots from Network Settings on Android to direct traffic to Mitmproxy on your computer's IP Address

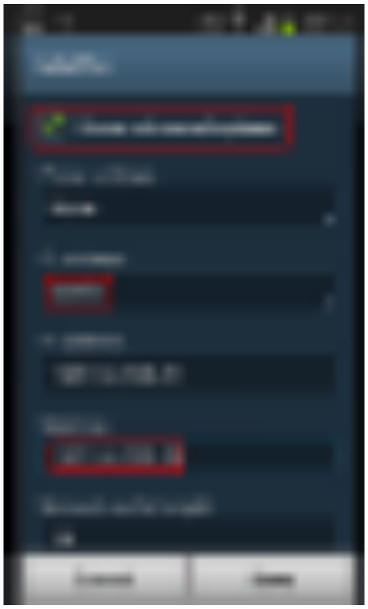
Click "Show Advanced Options" and change the Proxy settings to manual. Then change the Proxy Hostname to your IP Address that we found before, and the port to 8080.

If you do not have those options on your Android Phone, try this:









Screenshots from Network Settings on Android to direct traffic to Mitmproxy on your computer's IP Address

1. Go to Settings, Wi-Fi and **long-press** on your connected network.

2. Choose "Modify network config."

3. Check "Show advanced options", set IP settings to "Static" and (after writing down the gateway address for when you change it back) manually change the Gateway address to the IP Address that you found before on your computer, and under Port enter 8080. This sends HTTP (and now HTTPS because of the certificate) traffic to Mitmproxy on our computer, where

Mitmproxy is listening on port 8080. Click "Save"

To undo this you will need either turn Wi-Fi off and then on or change "Static" back to "DHCP" and the Gateway address to what was before.

Now open the email in Mail (not another mail app like Gmail) and click "view." Under Name put "mitmproxy-ca-cert".

Screenshots from the Mail app on Android to download Mitmproxy certificate on your phone

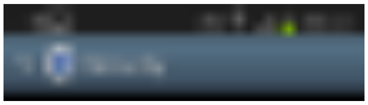
Then it should be installed. To check this, go to Settings, then Security, then Trusted Credentials and select the User Tab and you should see Mitmproxy. If this does not work:

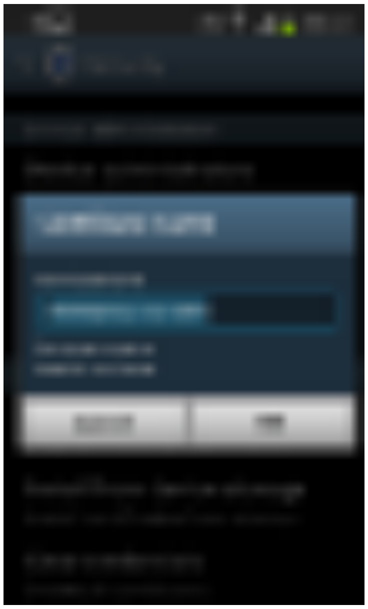
1. Upload the /sdcard/Download/ section of your Android device.

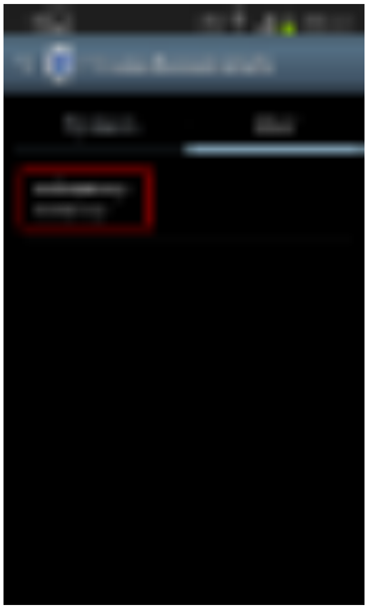
2. Go to Settings, Security and click “Install from device storage”

3. Enter “mitmproxy-ca-cert” (no suffix!) and click “OK”

4. Now click on “Trusted credentials” and select the “User” tab. The certificate should now appear in the list.







Screenshots from Network Settings on Android to direct traffic to Mitmproxy on your computer's IP Address

If this doesn't work then from your browser on your phone (Chrome, Safari, etc), visit mitm.it. (This won't send you to an Italian webpage; mitmproxy intercepts the request and sends you its own content instead.) and click on the Android logo for Android and follow the instructions.

If for some reason even this doesn't work you'll need to install the certificate manually. This can be done here under the heading for manual install or here. Now type into Terminal/Konsole on your computer,

```
mitmproxy --host
```

On your phone quit all of your apps (I opened the play store) and then go open up one app. You should see something like this on your phone and computer:

Mitmproxy capturing HTTP and HTTPS packets on your computer from your Android Phone

Which should show HTTP and HTTPS packets. I will explain later exactly what the heck you're looking at. If it does not show this or the app is malfunctioning, navigate to some other apps and see if simply any HTTP packets show up. No HTTPS means you have problems with your certificate installation and no packets at all could indicate a problem with your network settings. If you're getting one or two packets to show up, it is possible that this app that you are looking at is using certificate pinning. Quit this app and try another — to break certificate pinning you need to install SSL-Trust Killer for Android after Rooting your phone.

You can now in Terminal/Konsole type "q" followed by "y" to quit Mitmproxy.

Continue if you are using Ethernet or skip to the conclusion section

---

Ethernet (no Wi-Fi)

If you have Ethernet, connect your computer to the Ethernet cable and then you can create a fake Wi-Fi for your phone to connect to called an Adhoc Network. Create one on Mac using this link and on Linux using this link:

Then connect your phone to the "Wi-Fi" (Adhoc Network) that you create. Now type into Terminal/Konsole on your computer:

```
mitmproxy --host
```

On your phone quit all of your apps (I opened up the Play Store) and then go open up one app. You should see something like this:

Mitmproxy capturing HTTP and HTTPS packets on your computer from Ethernet from your Android Phone

Which should show HTTP and HTTPS packets. I will explain later exactly what the heck you're looking at. If it does not show this or the app is malfunctioning, navigate to some other apps and see if simply any HTTP packets show up. No HTTPS means you have problems with your certificate installation and no packets at all could indicate a problem with your network settings. If you're getting one or two packets to show up, it is possible that this app that you are looking at is using certificate pinning. Quit this app and try another — to break certificate pinning you need to install

SSL-Trust Killer for Android after Rooting your phone or SSL Kill Switch for iPhone.

You can now in Terminal/Konsole type "q" followed by "y" to quit Mitmproxy.

Congratulations on completing your setup of Mitmproxy! Now that you have that headache out of the way it will only take you 30 seconds to boot up Mitmproxy to work on your computer or phone. Remember to configure your browser settings on your computer to local host and your HTTP proxy settings on your phone to point to your computer's IP address. Simply change them back to revert back to normal functionality.

Now that you have the setup complete, go to Part 2: How To Analyze Mitmproxy to learn how to analyze the data that you are looking at to catch companies red handed.

Questions, concerns or somethings not working? E-mail me at maxpg@princeton.edu.
