

Intercepting QUIC

Max Hils

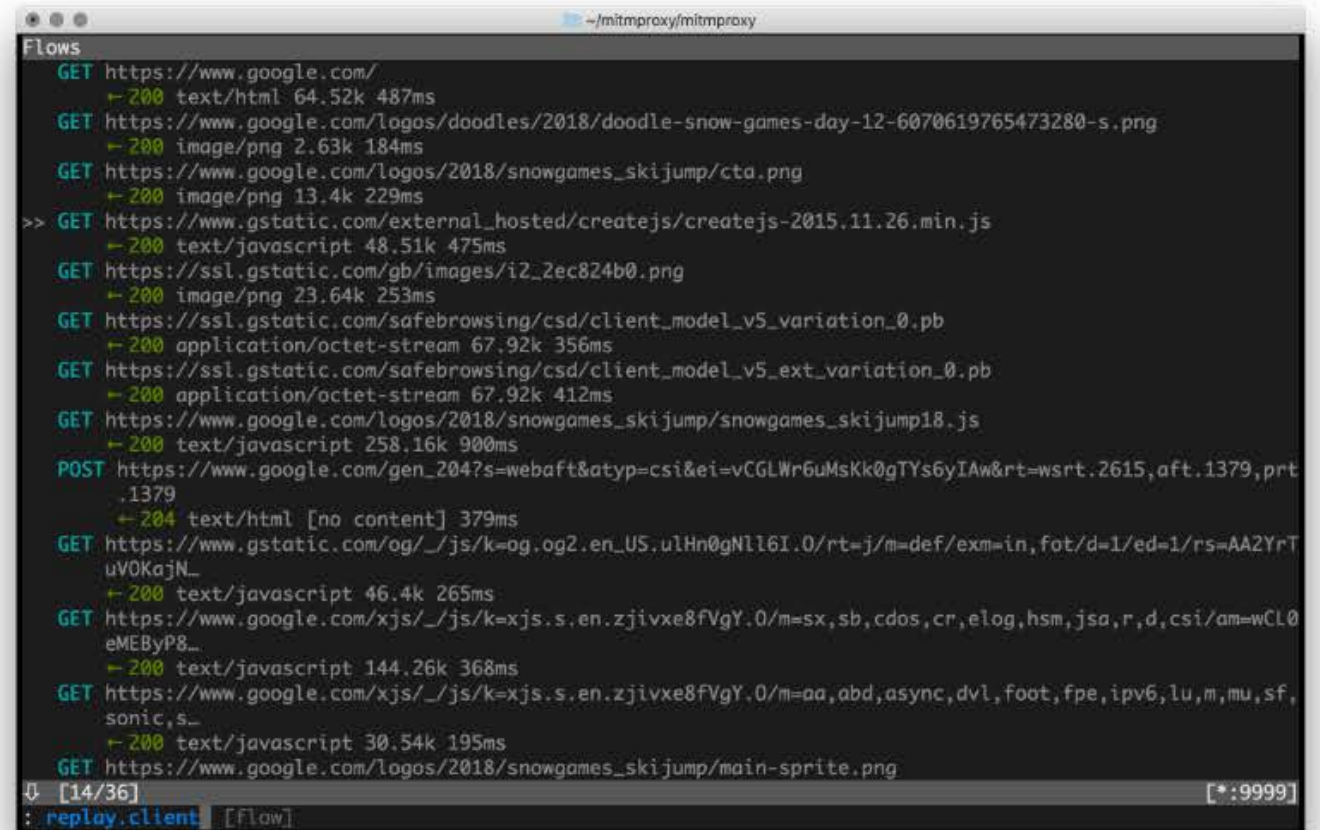
PhD Student @ Innsbruck, Austria

Lecturer @ UC Berkeley

Mitmproxy Developer



mitmproxy is a free and open source interactive HTTPS proxy.



```
~/mitmproxy/mitmproxy
Flows
GET https://www.google.com/
  ↳ 200 text/html 64.52k 487ms
GET https://www.google.com/logos/doodles/2018/doodle-snow-games-day-12-6070619765473280-s.png
  ↳ 200 image/png 2.63k 184ms
GET https://www.google.com/logos/2018/snowgames_skijump/cta.png
  ↳ 200 image/png 13.4k 229ms
>> GET https://www.gstatic.com/external_hosted/createjs/createjs-2015.11.26.min.js
  ↳ 200 text/javascript 48.51k 475ms
GET https://ssl.gstatic.com/gb/images/i2_2ec824b0.png
  ↳ 200 image/png 23.64k 253ms
GET https://ssl.gstatic.com/safebrowsing/csd/client_model_v5_variation_0.pb
  ↳ 200 application/octet-stream 67.92k 356ms
GET https://ssl.gstatic.com/safebrowsing/csd/client_model_v5_ext_variation_0.pb
  ↳ 200 application/octet-stream 67.92k 412ms
GET https://www.google.com/logos/2018/snowgames_skijump/snowgames_skijump18.js
  ↳ 200 text/javascript 258.16k 900ms
POST https://www.google.com/gen_204?s=webaft&atyp=csi&ei=vCGLWr6uMsKk0gTYs6yIAw&rt=wsrt.2615,aft.1379,prt.1379
  ↳ 204 text/html [no content] 379ms
GET https://www.gstatic.com/og/_/js/k=og.og2.en_US.u1Hn0gNl16I.0/rt=j/m=def/exm=in,fot/d=1/ed=1/rs=AA2YrT
uVOKajN_
  ↳ 200 text/javascript 46.4k 265ms
GET https://www.google.com/xjs/_/js/k=xjs.s.en.zjivxe8fVgY.0/m=sx,sb,cdos,cr,elog,hsm,jsa,r,d,csi/am=wCL0
eMEByP8_
  ↳ 200 text/javascript 144.26k 368ms
GET https://www.google.com/xjs/_/js/k=xjs.s.en.zjivxe8fVgY.0/m=aa,abd,async,dvl,foot,fpe,ipv6,lu,m,mu,sf,
sonic,s_
  ↳ 200 text/javascript 30.54k 195ms
GET https://www.google.com/logos/2018/snowgames_skijump/main-sprite.png
[14/36] [*:9999]
: replay.client [Flow]
```



Middleboxes

How to intercept TLS and sleep well at night?



- Require user consent
- Don't hide interception
- Write unoptimized Python code
- Enable privacy research

My phone is spying on me, so I decided to spy on it

Story Lab By [Simon Elvery](#)

Updated 3 Dec 2018, 7:24am

If your phone is turned on and has signal, it can be communicating — whether you've asked it to or not — with a wide variety of companies, many of which you won't have any direct relationship with.

And yes, this can happen even when you're not using it.

Your phone and other personal computing devices know an awful lot about you. They know — and often share — things like where you are and where you're going, who you're friends with, what apps you use, which websites you visit and how often you visit them, who you email and call — the list goes on.

So it's worth asking: do you know what information your apps and devices are sharing about you? And who they're sharing it with? **I thought I did, but now I'm not so sure.**

I'm an avid internet user with a good understanding of privacy. I studied IT and work as a web developer. I reckon I know how plenty of technologies work.

But that very interest in technology and privacy has me reading more and more stories with headlines like





Intercepting QUIC

Protocols in mitmproxy

- HTTP/1
 - Custom Parser
- HTTP/2
 - hyper-h2
- WebSockets
 - wsproto
- HTTP/3
 - ???

Why intercept QUIC?

- Privacy Research
 - QUIC is currently great to hide privacy violations.
- QUIC Development
 - On-the-fly frame injection API
- Security Research
 - 0-RTT replay attacks

Wrap HTTP/3 library



Replay UDP packets

Where to intercept QUIC?

