Bro Practial Session

What is NetFlow?

- Exported by routers via UDP
- Received by Bro as DataSrc
- Describes traffic flows
- Flow most commonly: 5-tuple
  - Src-IP, Dst-IP, Src-Port, Dst-Port, Protocol
- Statistics: byte counts, pkt counts, flags, timestamps
- Flow export happens
  - On RST and FIN flags
  - After timeout

=> We want to restitch flows in Bro

HTTP Reminder

```
GET / HTTP/1.1
Host: www.example.com
User-Agent: Mozilla/5.0 (Machintosh; …
Accept-Encoding: gzip,deflate
Connection: keep-alive

HTTP/1.1 200 OK
Date: Fri, 28 Jul 2000 22:03:40 GMT
Server: Apache/1.3.12 (Unix) mod_ssl/…
Last-Modified: Fri, 28 Jul 2000 18:56:12 GMT
Content-Length: 123
Connection: Keep-Alive
Content-Type: text/html

<html>…
```