Kika i HTTP & HTTPS

Verktyg och strategier för att kika
i HTTP och HTTPS trafik på protokollnivå

Henrik Nordström

henrik@henriknordstrom.net

Öppen Källkod, Squid, Linux & Nätverk
sedan 1995

Vad är HTTP & HTTPS

- HTTP, MIME liknande, text
- Öppen standard, W3C
- HTTP/1.1 1998
- HTTPS, HTTP inkapslat i SSL/TLS, egen port. start_tls används inte

Metoder att komma åt trafiken

- Nätverkstrafik, t.ex. Tcpdump, wireshark
- Proxy server. Squid, mitmproxy
- Plugin i webbläsare, firebug

HTTPS

- Krypterad trafik
- Browser plugin -> OK
- Nätverksanalysatorer -> Problem
- Proxyserver -> Problem
- wireshark, ssldump -> RSA nyckel, kanske
- Proxyserver SSL Man in the middle -> OK med CA certifikat

Tcpdump, ngrep

- Väldigt låg nivå, enskilda paket
- Tidsödande
- SSL/TLS glöm det
- Ngrep, innehållsorienterad, text

Tcpdump exempel

```
17:30:13.013867 IP 130.229.158.174.46886 > 195.20.207.177.http: Flags [P.], seq
1:395, ack 1, win 115, options [nop,nop,TS val 3456774 ecr 2484994958], length 394
        0x0000:  4500 01be afe9 4000 4006 d4f6 82e5 9eae  E.....@.@.......
        0x0010:  c314 cfb1 b726 0050 0b50 10e7 da26 63f1  .....&.P.P...&c.
        0x0020:  8018 0073 0699 0000 0101 080a 0034 bf06  ...s.........4..
        0x0030:  941e 038e 4745 5420 2f20 4854 5450 2f31  ....GET./.HTTP/1
        0x0040:  2e31 0d0a 486f 7374 3a20 7777 772e 6865  .1..Host:.www.he
        0x0050:  6e72 696b 6e6f 7264 7374 726f 6d2e 6e65  nriknordstrom.ne
        0x0060:  740d 0a55 7365 722d 4167 656e 743a 204d  t..User-Agent:.M
        0x0070:  6f7a 696c 6c61 2f35 2e30 2028 5831 313b  ozilla/5.0.(X11;
        0x0080:  2055 3b20 4c69 6e75 7820 7838 365f 3634  .U;.Linux.x86_64
        0x0090:  3b20 656e 2d55 533b 2072 763a 312e 392e  ;.en-US;.rv:1.9.
        0x00a0:  322e 3133 2920 4765 636b 6f2f 3230 3131  2.13).Gecko/2011
        0x00b0:  3031 3033 2046 6564 6f72 612f 332e 362e  0103.Fedora/3.6.
        0x00c0:  3133 2d31 2e66 6331 3420 4669 7265 666f  13-1.fc14.Firefo
        0x00d0:  782f 332e 362e 3133 0d0a 4163 6365 7074  x/3.6.13..Accept
        0x00e0:  3a20 7465 7874 2f68 746d 6c2c 6170 706c  :.text/html,appl
        0x00f0:  6963 6174 696f 6e2f 7868 746d 6c2b 786d  ication/xhtml+xm
        0x0100:  6c2c 6170 706c 6963 6174 696f 6e2f 786d  l,application/xm
        0x0110:  6c3b 713d 302e 392c 2a2f 2a3b 713d 302e  l;q=0.9,*/*;q=0.
        0x0120:  380d 0a41 6363 6570 742d 4c61 6e67 7561  8..Accept-Langua
        0x0130:  6765 3a20 656e 2d75 732c 656e 3b71 3d30  ge:.en-us,en;q=0
```

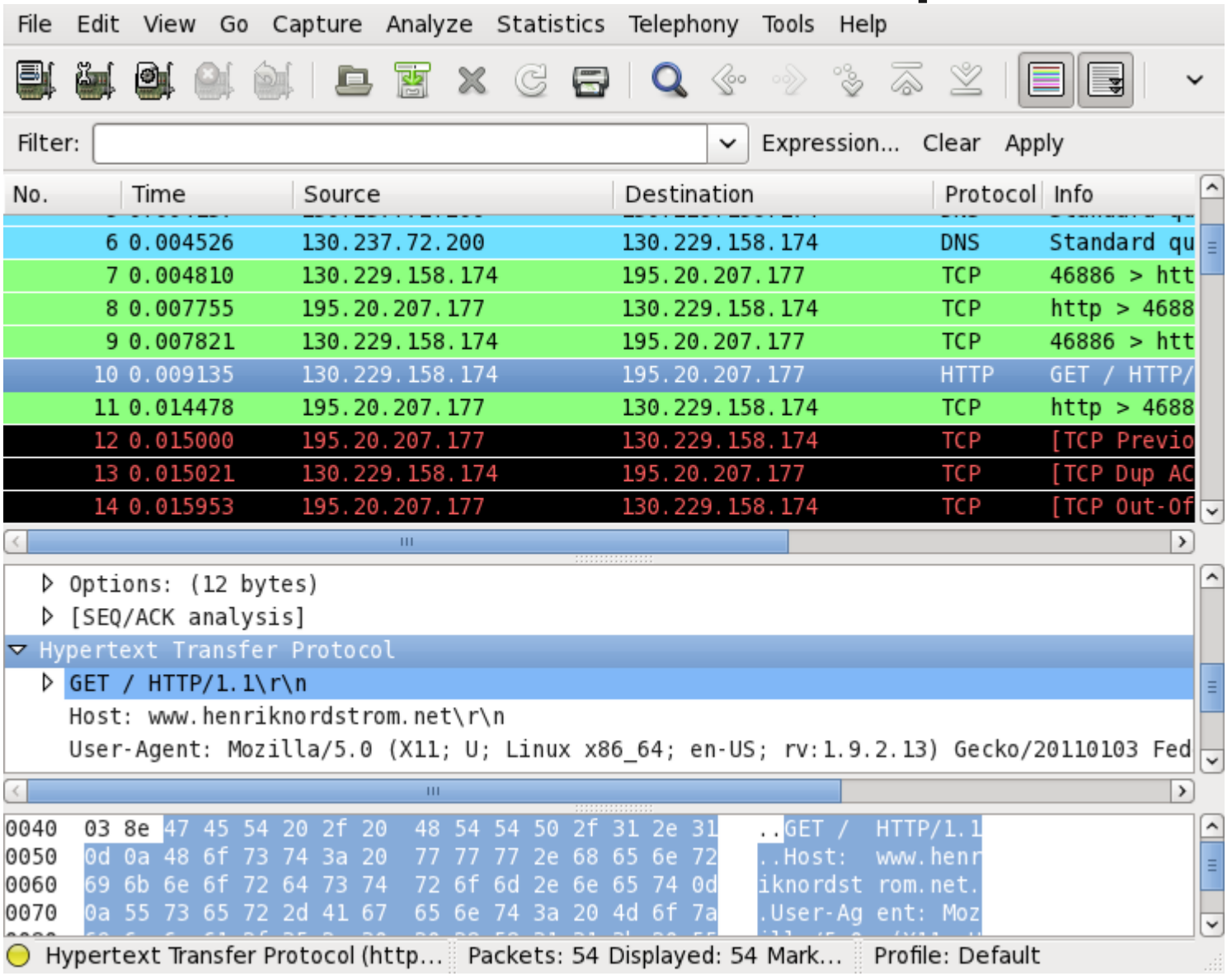
Ngrep, samma exempel

```
T 130.229.158.174:46886 -> 195.20.207.177:80 [AP]
GET / HTTP/1.1.
Host: www.henriknordstrom.net.
User-Agent: Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.2.13) Gecko/20110103
Fedora/3.6.13-1.fc14 Firefox/3.6.13.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8.
Accept-Language: en-us,en;q=0.5.
Accept-Encoding: gzip,deflate.
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7.
Keep-Alive: 115.
Connection: keep-alive.
.
```

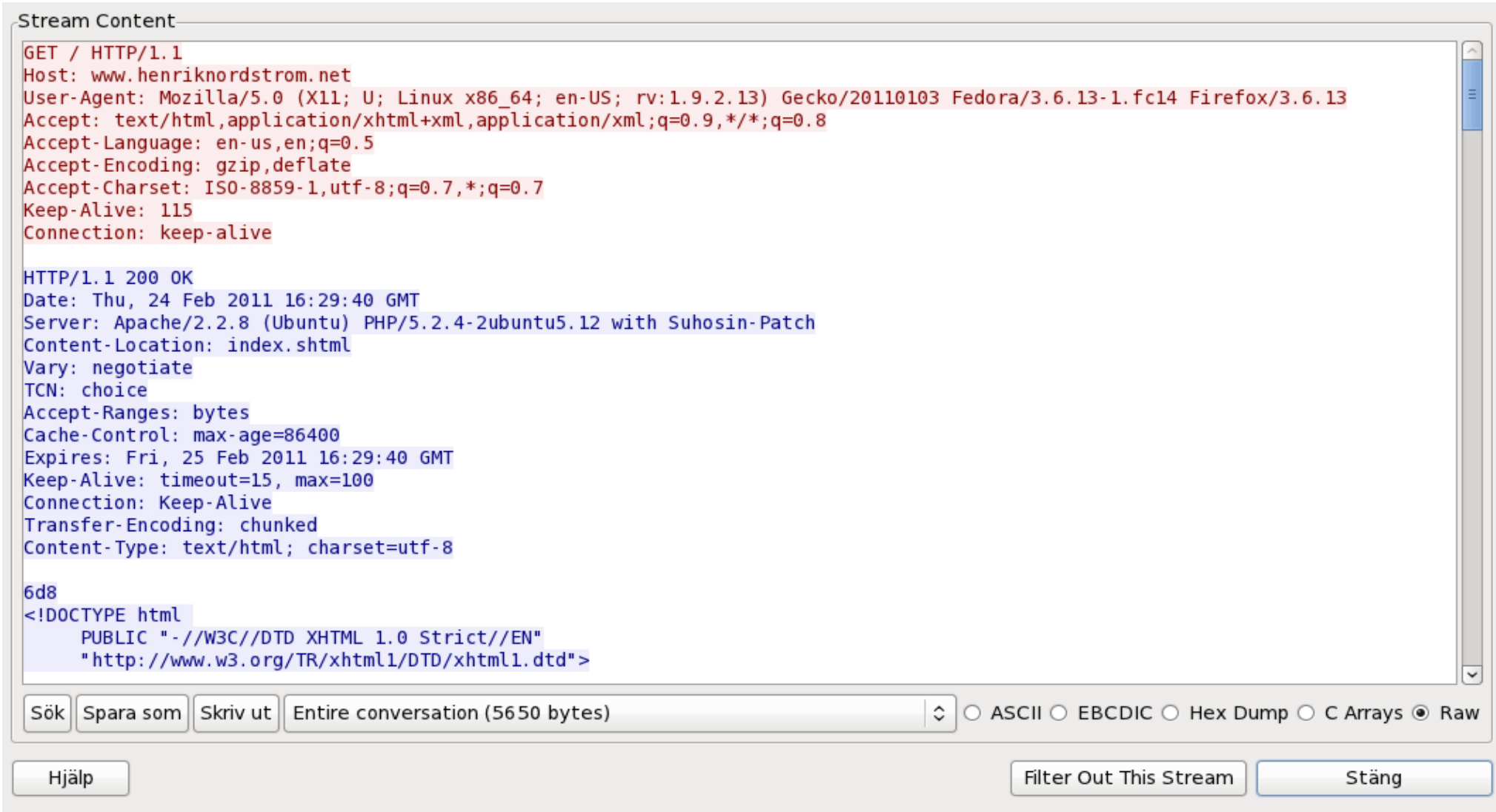
wireshark

- Kraftfull analysator av nätverkstrafik
- Paketnivå
- Tolkar de flesta protokoll
- Följer enskilda TCP strömmar
- Klarar SSL/TLS, under rätt villkor

Wireshark exempel



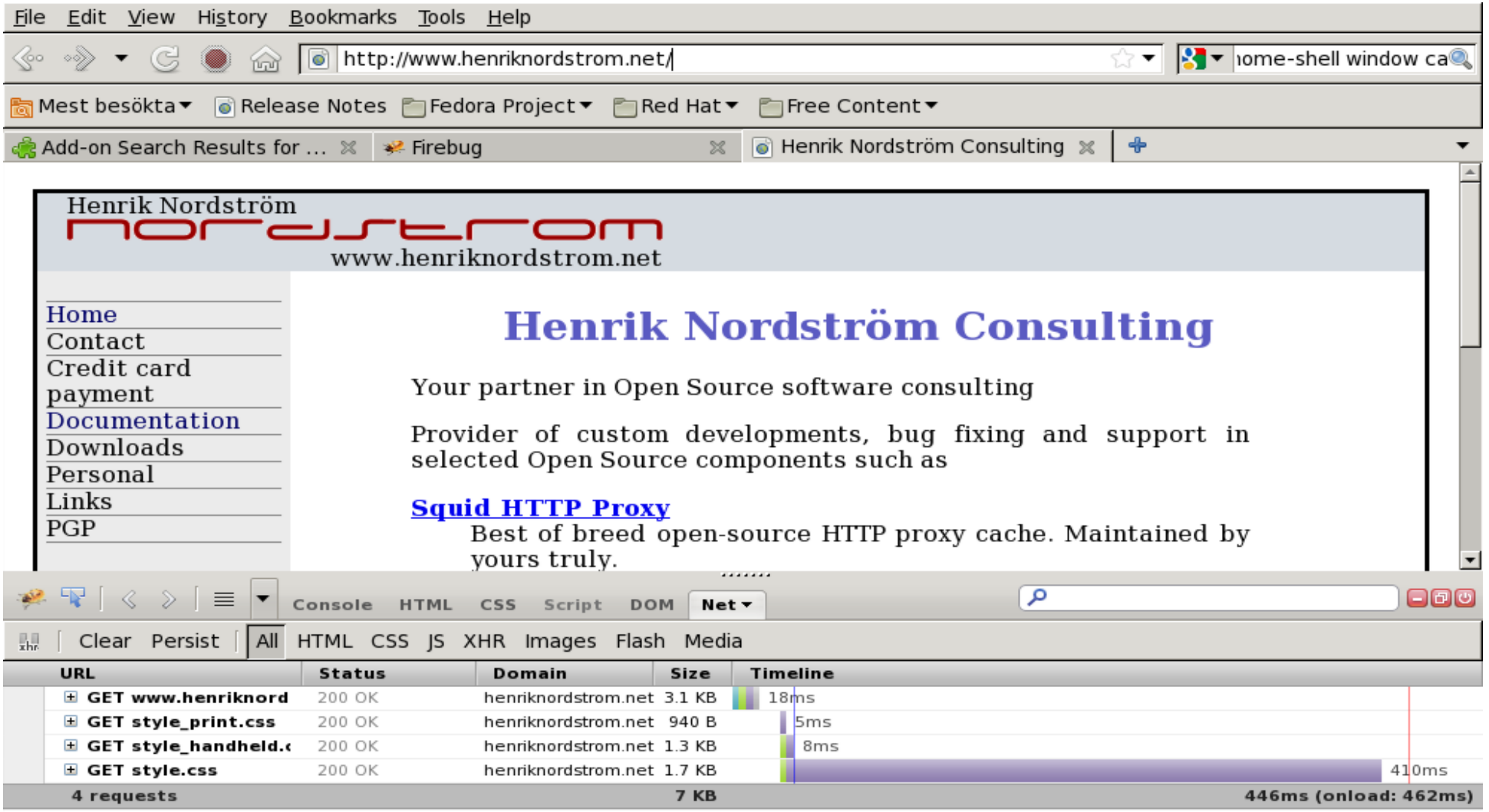
Wireshark tcp exempel



firebug

- Plugin för Firefox
- Kraftfull debugger
- HTML/CSS/Scrips/DOM/Net
- Net visar nättrafiken
- Browser trafik.
- Fångar ej Java/Flash egna klienter.

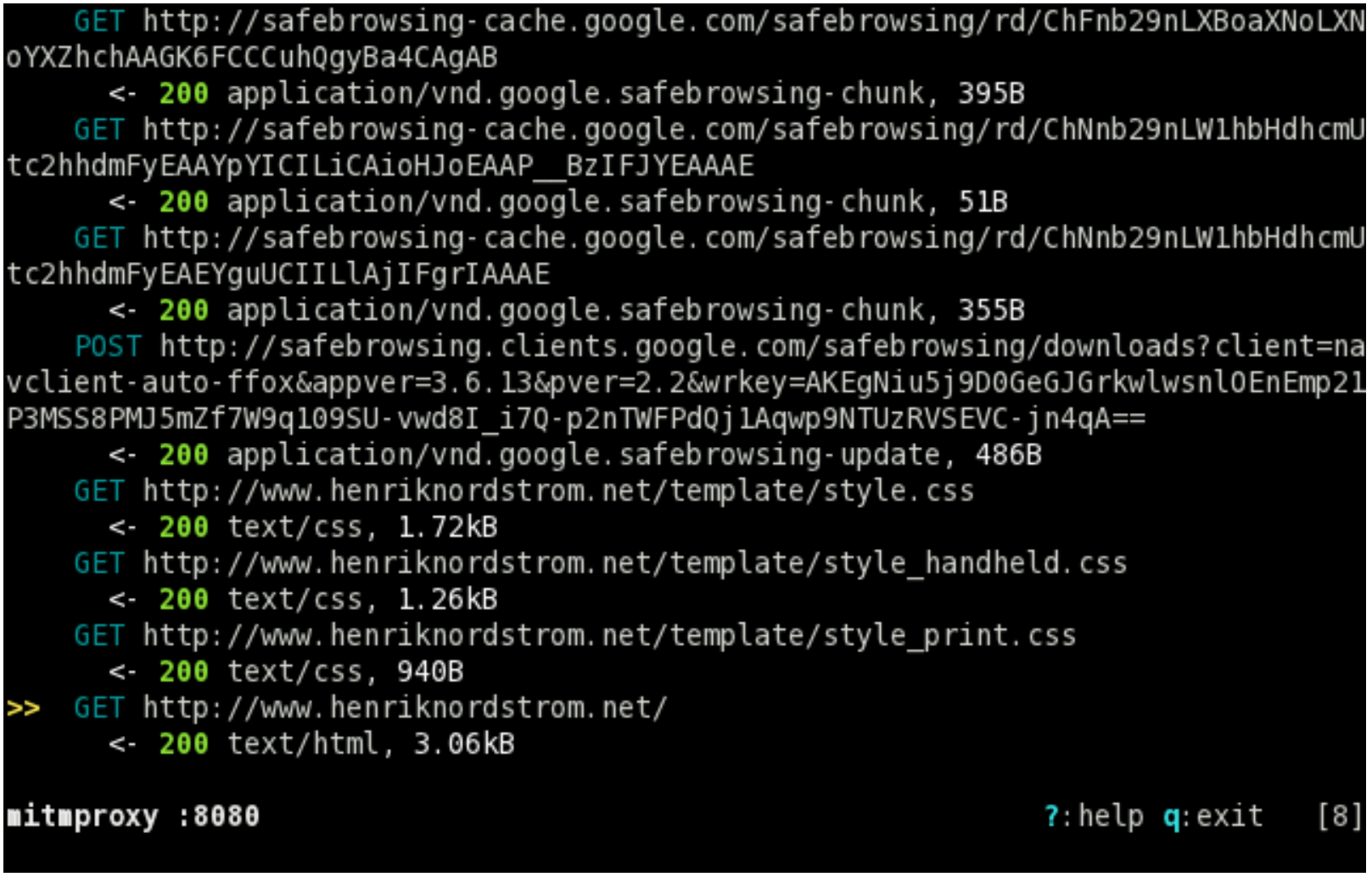
Firebug exempel



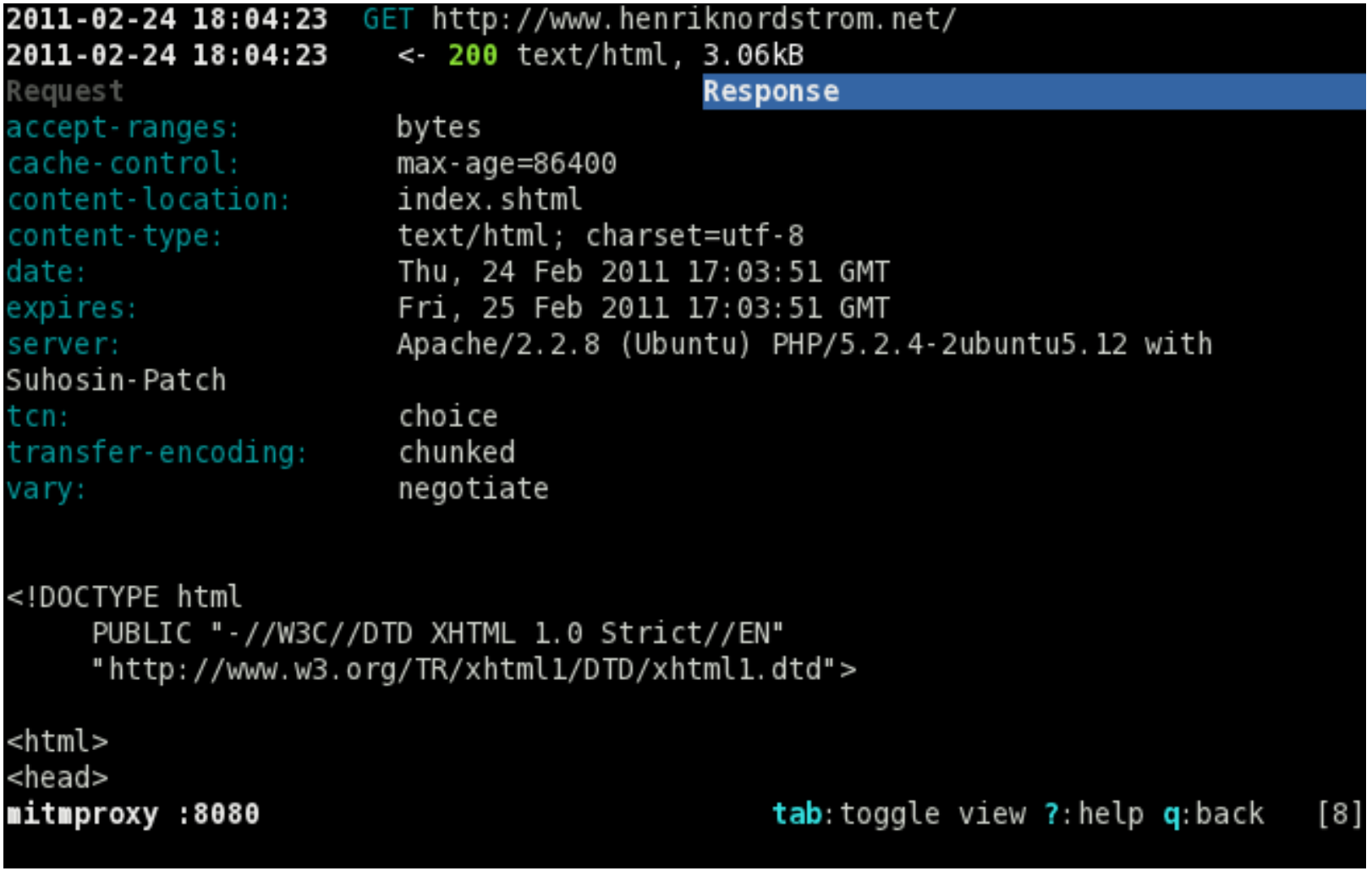
mitmproxy

- Man In The Middle Proxy server
- Specifik för HTTP/HTTPS
- Man In The Middle attack på SSL/TLS
- Fake-CA

Mitmproxy huvudbild



Mitmproxy request


2011-02-24 18:04:23 GET http://www.henriknordstrom.net/
2011-02-24 18:04:23 <- 200 text/html, 3.06kB
Request
Response
accept-ranges: bytes
cache-control: max-age=86400
content-location: index.shtml
content-type: text/html; charset=utf-8
date: Thu, 24 Feb 2011 17:03:51 GMT
expires: Fri, 25 Feb 2011 17:03:51 GMT
server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.12 with
Suhosin-Patch
tcn: choice
transfer-encoding: chunked
vary: negotiate
<!DOCTYPE html
PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1.dtd">
<html>
<head>
mitmproxy :8080
tab:toggle view ?:help q:back [8]

Tack för mig

Henrik Nordström
henrik@henriknordstrom.net

Mitmproxy
http://corte.si/projects.html
http://github.com/cortesi/mitmproxy