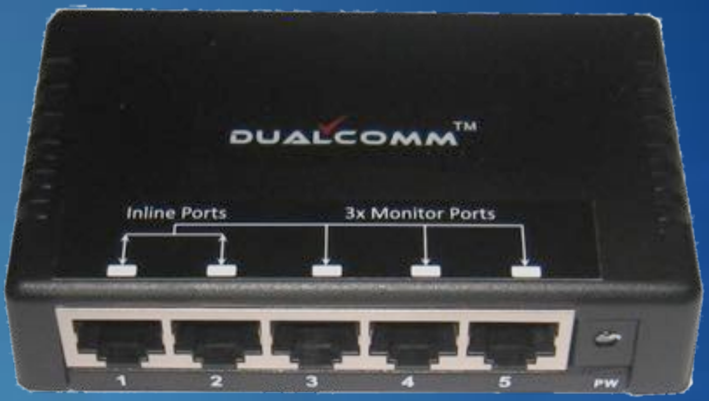


Phil’s Tap House

Episode 0x00 v2
HTTP/2 and You

Welcome to the Tap House

Network Forensics

- Talk about new, cool, or otherwise notable developments in the general domain of network forensics
- We monitor networks with a tap

Craft Beer

- Talk about (US) craft beer industry, craft breweries, and good craft beers
- We get beer from a tap

Links relevant to this presentation:

`http://for572.com/taphouse`

Tagged with the episode number (`0x00`)

Phil Hagen

- SANS Certified Instructor, FOR572 Course lead
- Evangelist, Red Canary (Managed Threat Detection)
- Forensic/infosec consultant: LE, DoD, IC, commercial
- Craft Beer fan (Hopeful homebrewer someday)

HTTP Through the Ages

- Protocol History:
  - HTTP/0.9: 1991 (should never be seen)
  - HTTP/1.0: 1996 (rare but not unheard of)
  - HTTP/1.1: 1997 (most common today)
  - HTTP/2: 2015 (highly optimized via multiplexing)

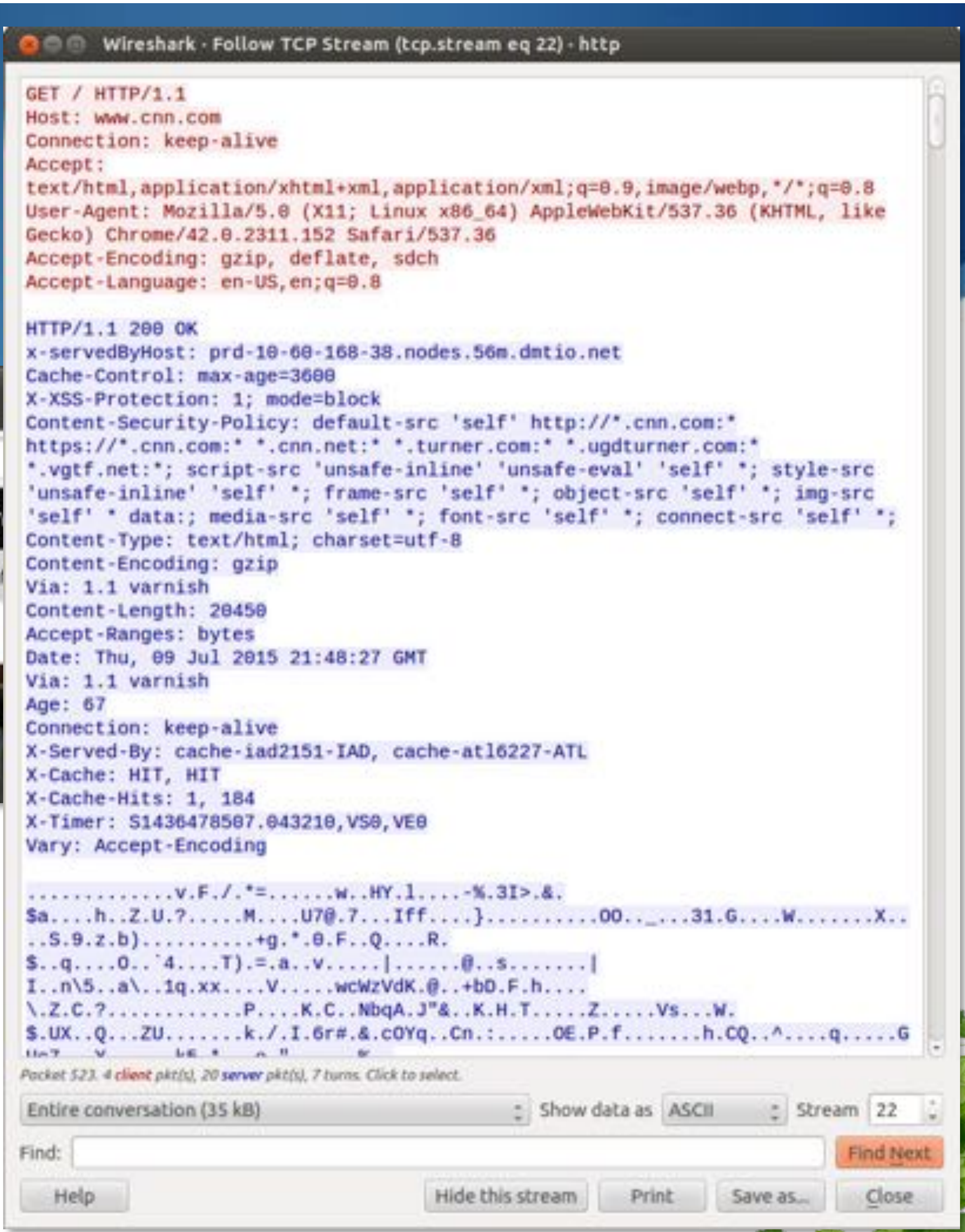
<= HTTP/1.1 is Straightforward

- Request/response protocol
- ASCII-based
- Standard layout between headers and object
- >1 request/response per TCP socket with Keep-Alive
- Encoding and compression for objects…

  …but headers are ALWAYS plain old ASCII

Let's go look at some http/1.1 traffic in Wireshark!

HTTP/1.1…



```
GET / HTTP/1.1
Host: www.cnn.com
Connection: keep-alive
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/42.0.2311.152 Safari/537.36
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8

HTTP/1.1 200 OK
x-servedByHost: prd-10-60-168-38.nodes.56m.dmtio.net
Cache-Control: max-age=3600
X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'self' http://*.cnn.com:*
https://*.cnn.com:* *.cnn.net:* *.turner.com:* *.ugdturner.com:*
*.vgtf.net:*; script-src 'unsafe-inline' 'unsafe-eval' 'self' *; style-src
'unsafe-inline' 'self' *; frame-src 'self' *; object-src 'self' *; img-src
'self' * data:; media-src 'self' *; font-src 'self' *; connect-src 'self' *;
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Via: 1.1 varnish
Content-Length: 20450
Accept-Ranges: bytes
Date: Thu, 09 Jul 2015 21:48:27 GMT
Via: 1.1 varnish
Age: 67
Connection: keep-alive
X-Served-By: cache-iad2151-IAD, cache-atl6227-ATL
X-Cache: HIT, HIT
X-Cache-Hits: 1, 184
X-Timer: S1436478507.043210,VS0,VE0
Vary: Accept-Encoding

..............v.F./.*=......w..HY.l....-%.3I>.&.
$a....h..Z.U.?.....M....U7@.7...Iff....}..........OO.._...31.G....W.......X..
..S.9.z.b)..........+g.*.0.F..Q....R.
$..q....O..`4....T).=.a..v.....|......@..s.......|
I..n\5..a\..1q.xx....V.....wcWzVdK.@..+bD.F.h....
\.Z.C.?............P....K.C..NbqA.J"&..K.H.T.....Z.....Vs...W.
$.UX..Q...ZU.......k./.I.6r#.&.cOYq..Cn.:.....OE.P.f.......h.CQ..^....q.....G
```

Packet 523. 4 client pkt(s), 20 server pkt(s), 7 turns. Click to select.
Entire conversation (35 kB)
Show data as
ASCII
Stream
22
Find:
Find Next
Help
Hide this stream
Print
Save as...
Close

Craft Beer Knowledge (1)

- Craft Brewery Definition
  - **Small**: <6M barrels/year
  - **Independent**: <25% ownership by non-craft
  - **Traditional**: Majority of alcohol from traditional or innovative ingredients
  - Note: “microbrewery”= <15k bls, 75% off-site sales
- Craft beer is 11% of beer market
- Currently over 3,400 breweries in the US
  - Dozens of beer styles – find something you enjoy!

Craft Beer Knowledge (2)

- No US macro brewery is US-owned
  - AB-INBEV (Belgium)
  - SAB-MILLER-COORS (UK)

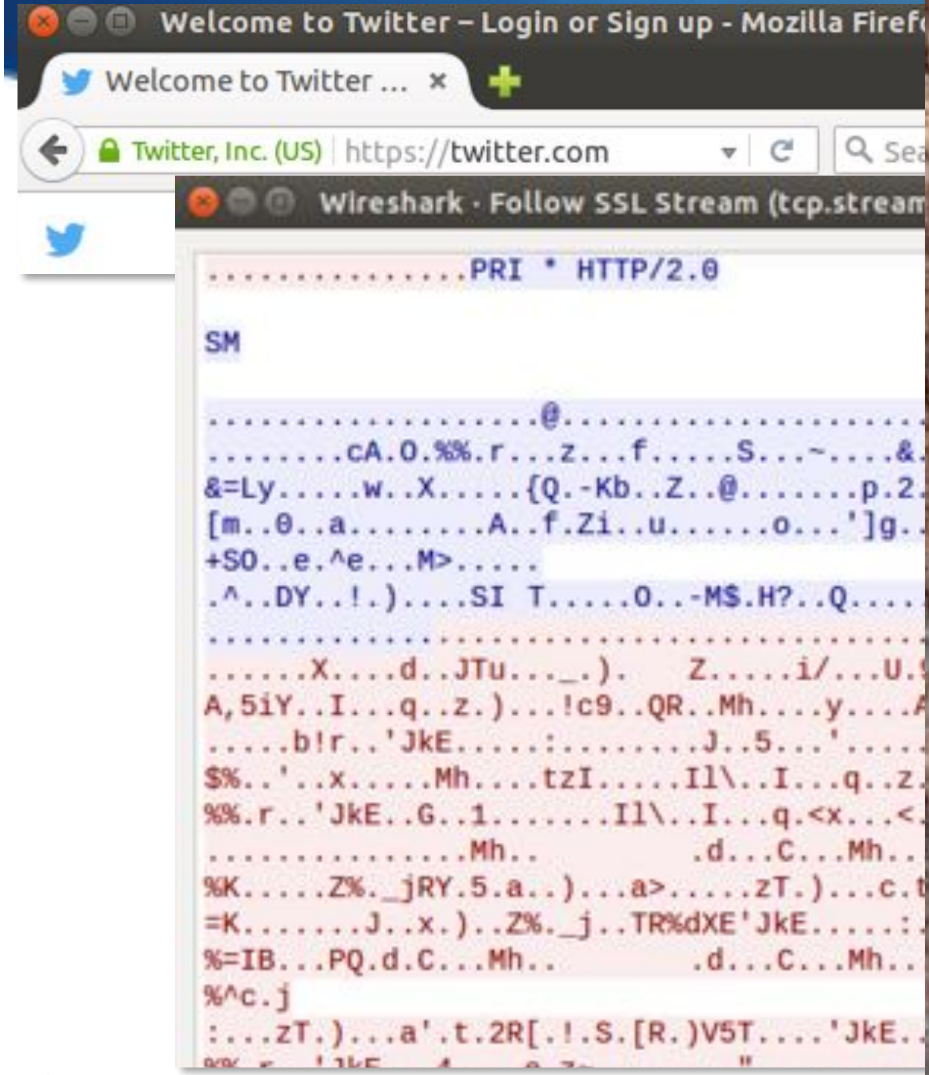
AB InBev took over SAB-Miller-Coors for US$ 106B

- Macro brewers do good job creating consistent product with natural ingredients

- **Craft brewers do a great job creating good beers with natural ingredients**
  - Creativity encouraged – no ingredient restrictions

Now, let's go look at some http/2 traffic in Wireshark!

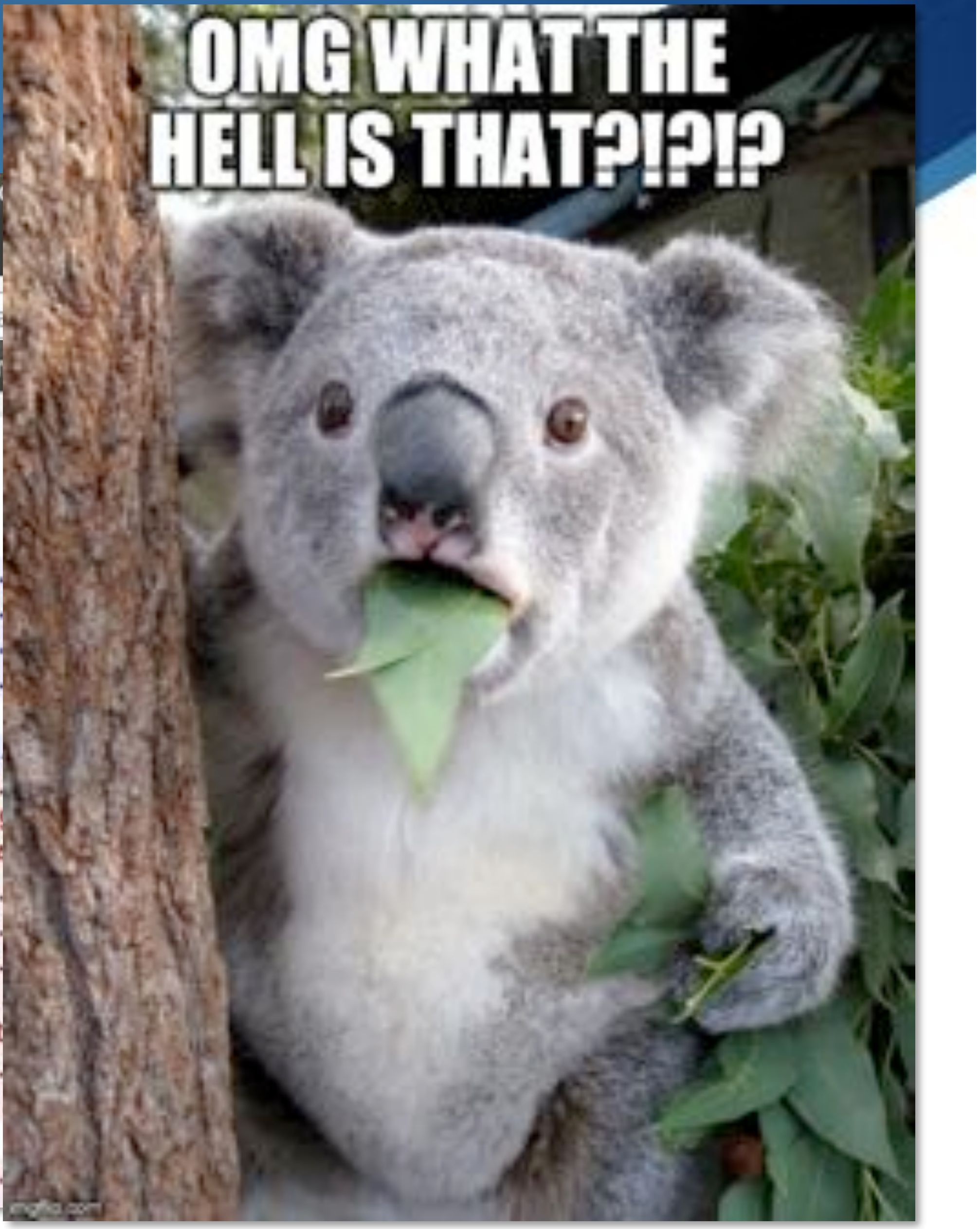
HTTP/2…


Welcome to Twitter – Login or Sign up - Mozilla Firef
Welcome to Twitter …
Twitter, Inc. (US)
https://twitter.com
Sea
Wireshark · Follow SSL Stream (tcp.stream

```
...............PRI * HTTP/2.0

SM

...................@.....................
........cA.O.%%.r...z...f.....S...~....&.
&=Ly.....w..X.....{Q.-Kb..Z..@.......p.2.
[m..0..a........A..f.Zi..u......o...']g..
+SO..e.^e...M>.....
.^..DY..!.)....SI T.....O..-M$.H?..Q.....
.........................................
......X....d..JTu..._.).   Z.....i/...U.
A,5iY..I...q..z.)...!c9..QR..Mh....y....A
.....b!r..'JkE....:.........J..5...'.....
$%..'..x.....Mh....tzI.....Il\..I...q..z.
%%.r..'JkE..G..1.......Il\..I...q.<x...<.
...............Mh..        .d...C...Mh...
%K.....Z%._jRY.5.a..)...a>.....zT.)...c.t
=K.......J..x.)..Z%._j..TR%dXE'JkE.....:.
%=IB...PQ.d.C...Mh..       .d...C...Mh...
%^c.j
:...zT.)...a'.t.2R[.!.S.[R.)V5T....'JkE..
```

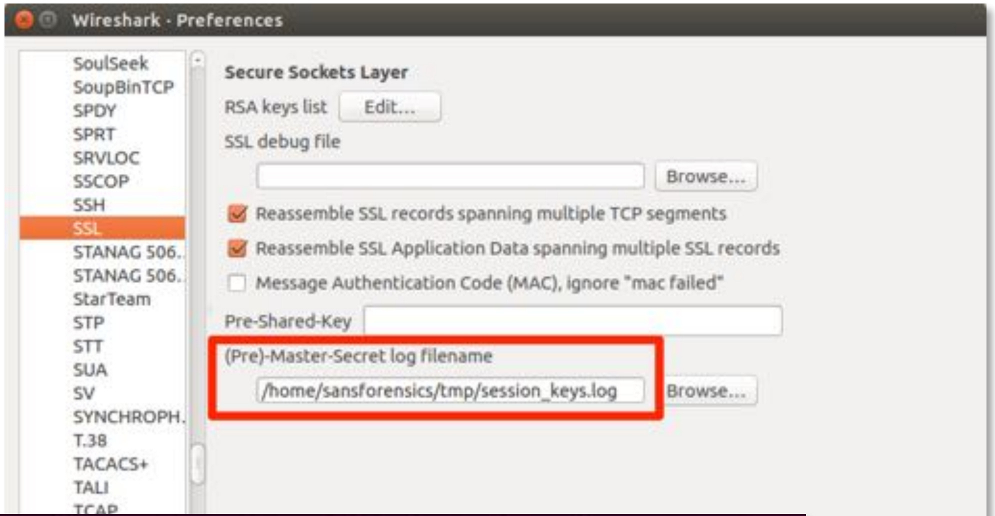


HTTP/2 Changes Things… A Lot (1)

- Binary w/ header compression
- Today, most often used with SSL (and PFS), but not req'd
  - Bet you didn't know you were using it already!
- Connection can "upgrade" from HTTP/1.1 to HTTP/2
- Tagged objects complicates Wireshark analysis
  - "`tshark -T fields`" dead for HTTP/2 traffic (for now?) ☹
  - Common HTTP conveniences (related packets, etc) not implemented (yet)

How to Access for Analysis?

- Debug settings for Chrome/ Firefox
- Debug settings to log session keys (including PFS)
- See Sally Vandeven's SANS Gold Paper for detailed steps



Secure Sockets Layer

RSA keys list

SSL debug file

☑ Reassemble SSL records spanning multiple TCP segments

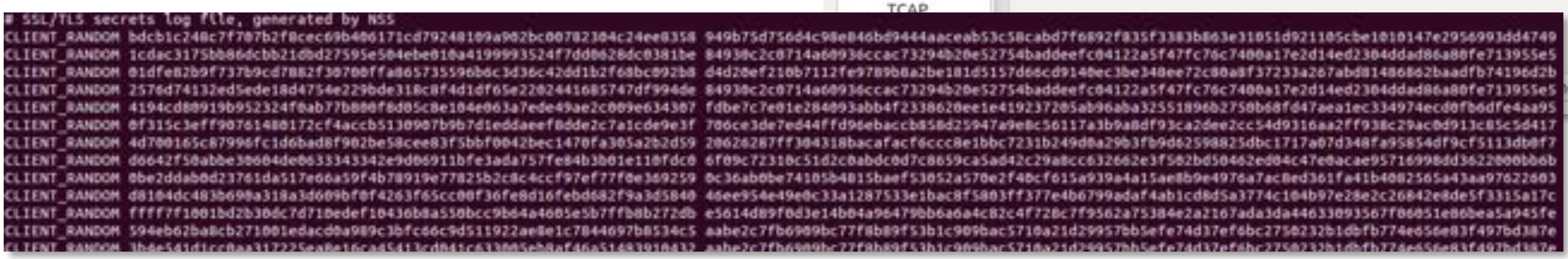
☑ Reassemble SSL Application Data spanning multiple SSL records

☐ Message Authentication Code (MAC), ignore "mac failed"

Pre-Shared-Key

(Pre)-Master-Secret log filename

/home/sansforensics/tmp/session_keys.log



```
# SSL/TLS secrets log file, generated by NSS
CLIENT_RANDOM bdcb1c248c7f707b2f8cec69b406171cd79248109a902bc00782304c24ee8358 949b75d756d4c98e046bd9444aaceab53c58cabd7f6892f835f3383b863e31051d921105cbe1010147e2956993dd4749
CLIENT_RANDOM 1cdac3175b086dcbb21dbd27595e504ebe010a4199993524f7dd0628dc0381be 84930c2c0714a60936ccac73294b20e52754baddeefc04122a5f47fc76c7400a17e2d14ed2304ddad86a80fe713955e5
CLIENT_RANDOM 01dfe82b9f737b9cd7882f30700ffa865735596b6c3d36c42dd1b2f68bc092b8 d4d20ef210b7112fe9789b8a2be181d5157d66cd9140ec3be340ee72c80a8f37233a267abd81486862baadfb74196d2b
CLIENT_RANDOM 2576d74132ed5ede18d4754e229bde318c8f4d1df65e2202441685747df994de 84930c2c0714a60936ccac73294b20e52754baddeefc04122a5f47fc76c7400a17e2d14ed2304ddad86a80fe713955e5
CLIENT_RANDOM 4194cd00919b952324f0ab77b880f8d05c8e104e063a7ede49ae2c009e634307 fdbe7c7e01e284093abb4f2338620ee1e419237205ab96aba32551896b2750b68fd47aea1ec334974ecd0fb6dfe4aa95
CLIENT_RANDOM 0f315c3eff90761480172cf4accb5130907b9b7d1eddaeef0dde2c7a1cde9e3f 706ce3de7ed44ffd96ebaccb858d25947a9e8c56117a3b9a8df93ca2dee2cc54d9316aa2ff938c29ac0d913c85c5d417
CLIENT_RANDOM 4d700165c87996fc1d6bad8f902be58cee83f5bbf0042bec1470fa305a2b2d59 20626287ff304318bacafacf6ccc8e1bbc7231b249d0a29b3fb9d62598825dbc1717a07d348fa95854df9cf5113db0f7
CLIENT_RANDOM d6642f50abbe30604de0633343342e9d06911bfe3ada757fe84b3b01e110fdc0 6f09c72310c51d2c0abdc0d7c8659ca5ad42c29a8cc632662e3f502bd50462ed04c47e0acae95716998dd3622000bb6b
CLIENT_RANDOM 0be2ddab0d23761da517e66a59f4b78919e77825b2c8c4ccf97ef77f0e369259 0c36ab0be74105b4015baef53052a570e2f40cf615a939a4a15ae8b9e4976a7ac8ed361fa41b4082565a43aa97622603
CLIENT_RANDOM d8104dc483b690a318a3d609bf0f4263f65cc00f36fe8d16febd682f9a3d5840 46ee954e49e0c33a1287533e1bac8f5803ff377e4b6799adaf4ab1cd8d5a3774c104b97e28e2c26842e8de5f3315a17c
CLIENT_RANDOM ffff7f1001bd2b30dc7d710edef10436b8a550bcc9b64a4605e5b7ffb0b272db e5614d89f0d3e14b04a96479bb6a6a4c82c4f728c7f9562a75384e2a2167ada3da44633093567f06051e06bea5a945fe
CLIENT_RANDOM 594eb62ba8cb271001edacd0a989c3bfc66c9d511922ae0e1c7844697b8534c5 aabe2c7fb6909bc77f8b89f53b1c909bac5710a21d29957bb5efe74d37ef6bc2750232b1dbfb774e656e83f497bd387e
CLIENT_RANDOM 3b4e541d1cc0aa317225ea0e16ca45413cd041c633005eb0af46a51403910432 aabe2c7fb6909bc77f8b89f53b1c909bac5710a21d29957bb5efe74d37ef6bc2750232b1dbfb774e656e83f497bd387e
```

HTTP/2 Changes Things… A Lot (2)

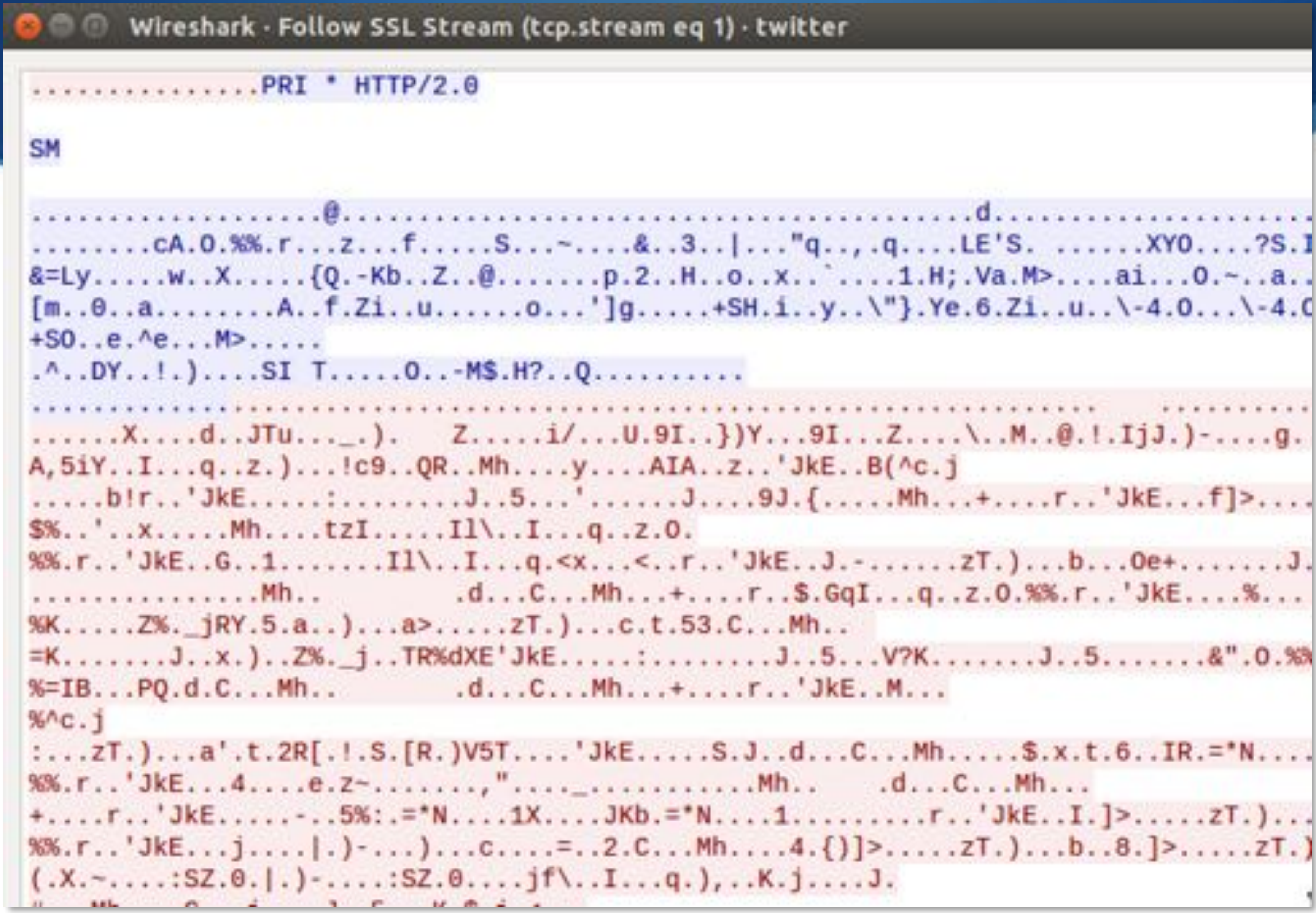
- Multiplexed data streams
  - Including stream dependencies and prioritization
  - Each stream can be RST independently of others
  - Entire connection can be closed via GOAWAY frame
- **Servers can proactively "push" responses into client caches**

Let's Explore A Brewery

- Dogfish Head Craft Brewed Ales: Delaware
  - 1995: 1st brewery in the First State
  - Today: Craft leader
  - Recent 15% stake investment
- Typically high ABV, creative beers (30+/yr)
  - IPAs: 60min, 90min, 120min, Sixty One
  - Ancient Ales: Midas Touch, Theobroma, Chateau Jiahu
  - Music: Faithfull, American Beauty, Miles Davis Bitches Brew, Positive Contact
  - Wood aging program: Burton Baton, Palo Santo Marron
  - Distilled spirits: Rum, Vodka, Gin

Basic HTTP/2 Process

- TCP 3-way handshake [SSL negotiation]
- Server setup via SETTINGS frame
- Client “Magic”, request via SETTINGS, HEADER frames
    - Typical HTTP/1.1 request fields part of HTTP/2 HEADERs
- Server response via SETTINGS, HEADER, DATA frames



```
...............PRI * HTTP/2.0

SM

...................@.........................................d.....................
........cA.O.%%.r...z...f.....S...~....&..3..|..."q..,.q....LE'S. ......XYO....?S.I
&=Ly.....w..X.....{Q.-Kb..Z..@.......p.2..H..o..x..`....1.H;.Va.M>....ai...O.~..a..
[m..0..a........A..f.Zi..u......o...']g.....+SH.i..y..\"}.Ye.6.Zi..u..\-4.O...\-4.C
+SO..e.^e...M>.....
.^..DY..!.)....SI T.....O..-M$.H?..Q.........
....................................................................    ..........
......X....d..JTu..._.).   Z.....i/...U.9I..})Y...9I...Z....\..M..@.!.IjJ.)-....g.
A,5iY..I...q..z.)...!c9..QR..Mh....y....AIA..z..'JkE..B(^c.j
.....b!r..'JkE....:........J..5...'......J....9J.{.....Mh...+....r..'JkE...f]>....
$%..'..x.....Mh....tzI.....Il\..I...q..z.O.
%%.r..'JkE..G..1.......Il\..I...q.<x...<..r..'JkE..J.-......zT.)...b...Oe+.......J.
...............Mh..        .d...C...Mh...+....r..$.GqI...q..z.O.%%.r..'JkE....%...
%K.....Z%._jRY.5.a..)...a>.....zT.)...c.t.53.C...Mh..
=K.......J..x.)..Z%._j..TR%dXE'JkE....:........J..5...V?K.......J..5.......&".O.%%
%=IB...PQ.d.C...Mh..       .d...C...Mh...+....r..'JkE..M...
%^c.j
:...zT.)...a'.t.2R[.!.S.[R.)V5T....'JkE.....S.J..d...C...Mh.....$.x.t.6..IR.=*N....
%%.r..'JkE...4....e.z~.......,"..._...........Mh..    .d...C...Mh...
+....r..'JkE.....-..5%:.=*N....1X....JKb.=*N....1.........r..'JkE..I.]>.....zT.)...
%%.r..'JkE...j....|.)-...)...c....=..2.C...Mh....4.{)]>.....zT.)...b..8.]>.....zT.)
(.X.~....:SZ.0.|.)-.....:SZ.0....jf\..I...q.),..K.j....J.
```

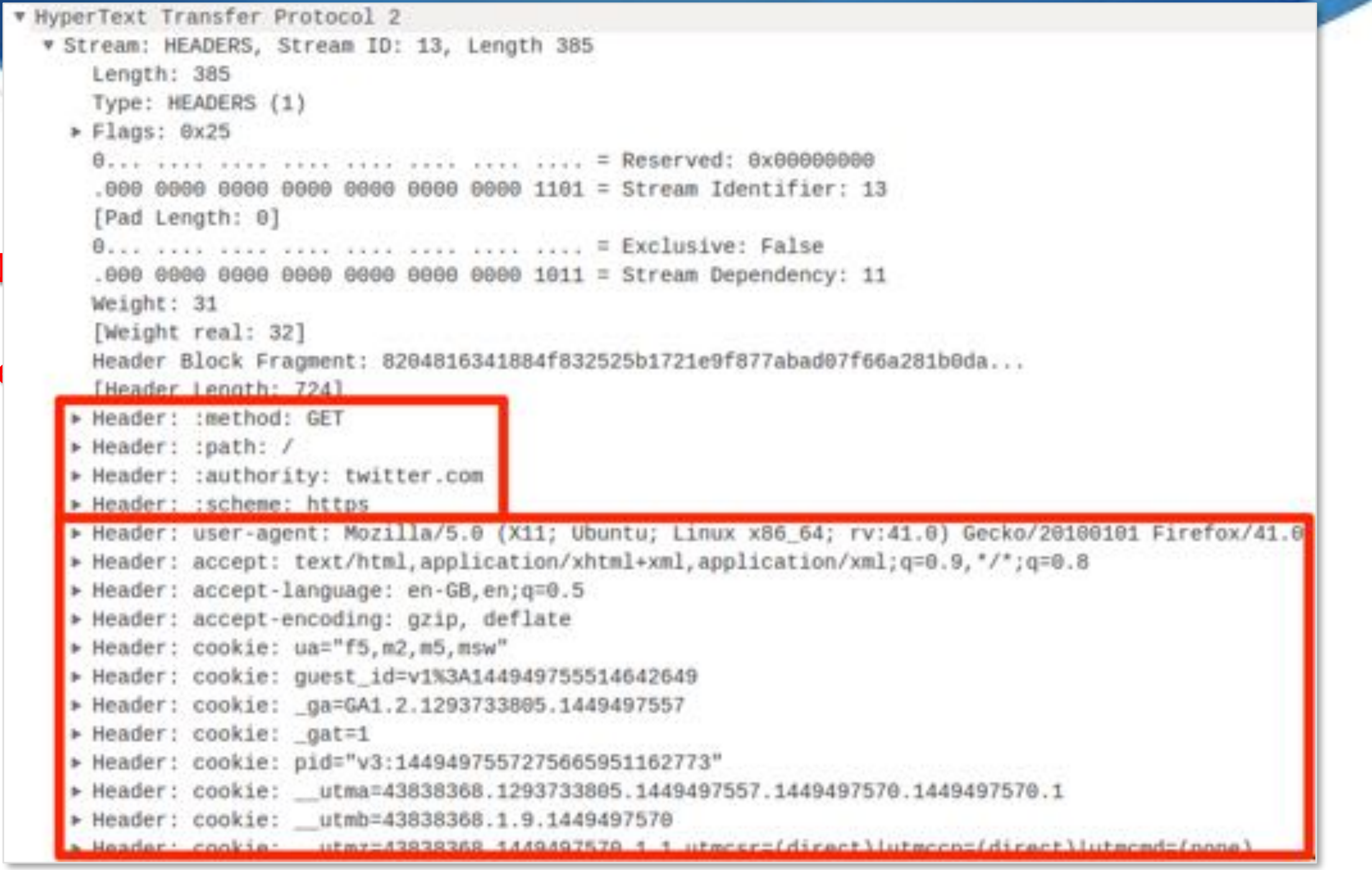
©2015 Lewes Technology Consulting, LLC

HTTP/2 Request

GI

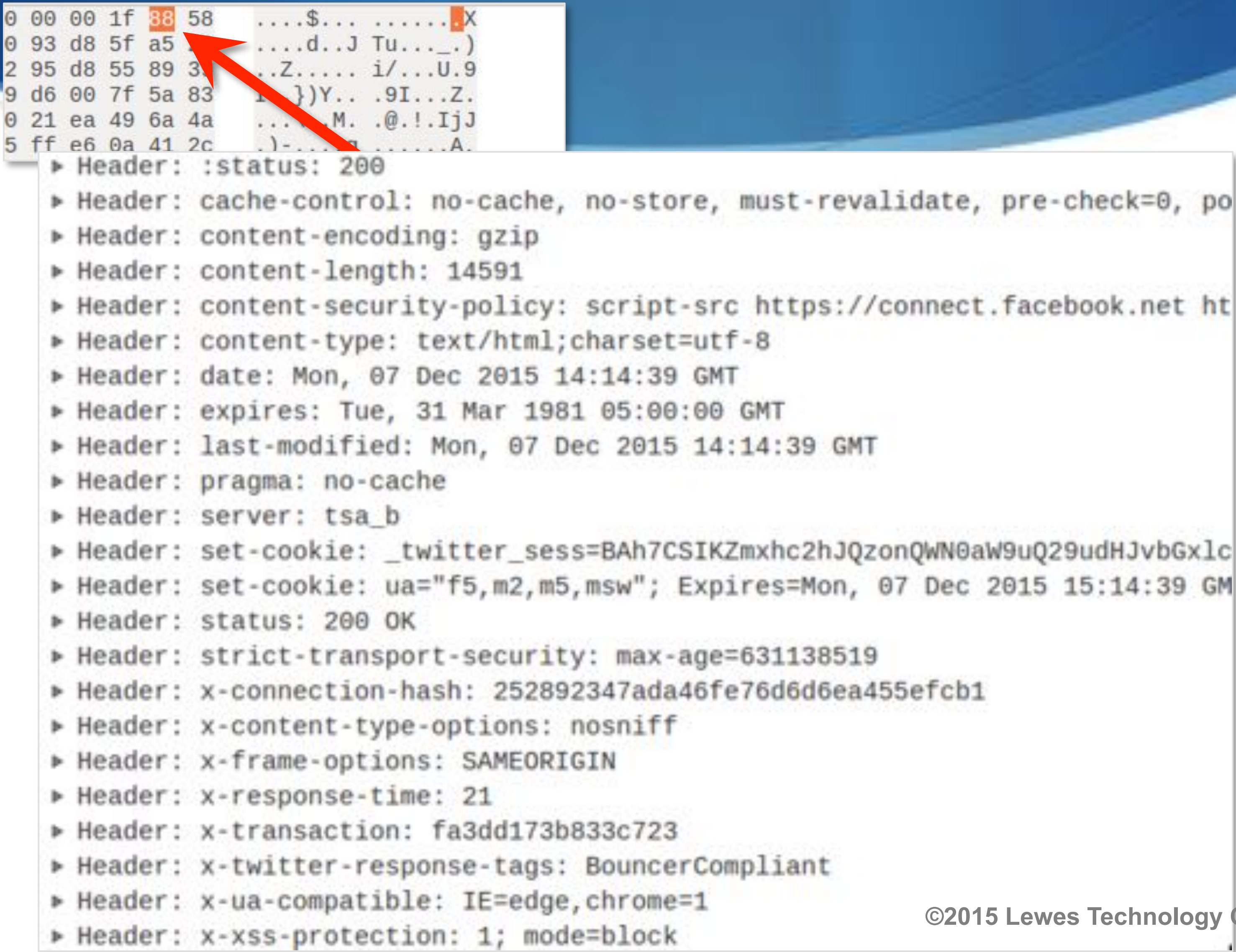
He

•



```
▾ HyperText Transfer Protocol 2
  ▾ Stream: HEADERS, Stream ID: 13, Length 385
      Length: 385
      Type: HEADERS (1)
    ▸ Flags: 0x25
      0... .... .... .... .... .... .... .... = Reserved: 0x00000000
      .000 0000 0000 0000 0000 0000 0000 1101 = Stream Identifier: 13
      [Pad Length: 0]
      0... .... .... .... .... .... .... .... = Exclusive: False
      .000 0000 0000 0000 0000 0000 0000 1011 = Stream Dependency: 11
      Weight: 31
      [Weight real: 32]
      Header Block Fragment: 8204816341884f832525b1721e9f877abad07f66a281b0da...
      [Header Length: 724]
    ▸ Header: :method: GET
    ▸ Header: :path: /
    ▸ Header: :authority: twitter.com
    ▸ Header: :scheme: https
    ▸ Header: user-agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:41.0) Gecko/20100101 Firefox/41.0
    ▸ Header: accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
    ▸ Header: accept-language: en-GB,en;q=0.5
    ▸ Header: accept-encoding: gzip, deflate
    ▸ Header: cookie: ua="f5,m2,m5,msw"
    ▸ Header: cookie: guest_id=v1%3A144949755514642649
    ▸ Header: cookie: _ga=GA1.2.1293733805.1449497557
    ▸ Header: cookie: _gat=1
    ▸ Header: cookie: pid="v3:1449497557275665951162773"
    ▸ Header: cookie: __utma=43838368.1293733805.1449497557.1449497570.1449497570.1
    ▸ Header: cookie: __utmb=43838368.1.9.1449497570
    ▸ Header: cookie: __utmz=43838368.1449497570.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
```

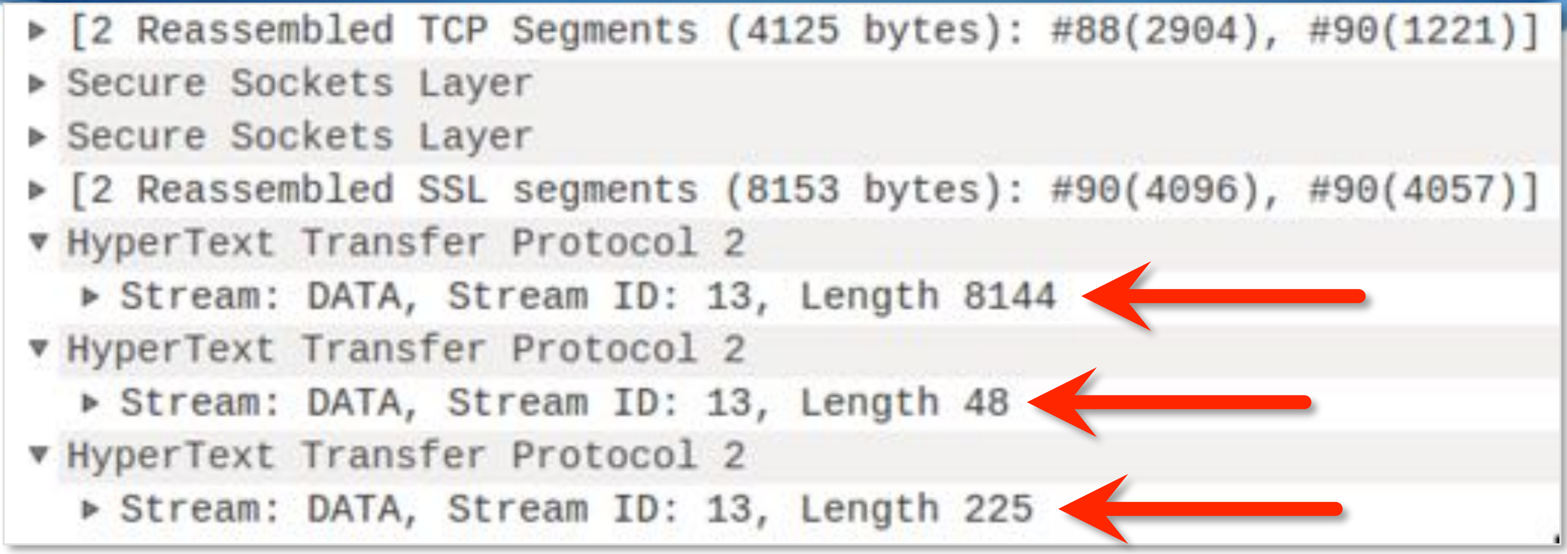
HTTP/2 Response Headers



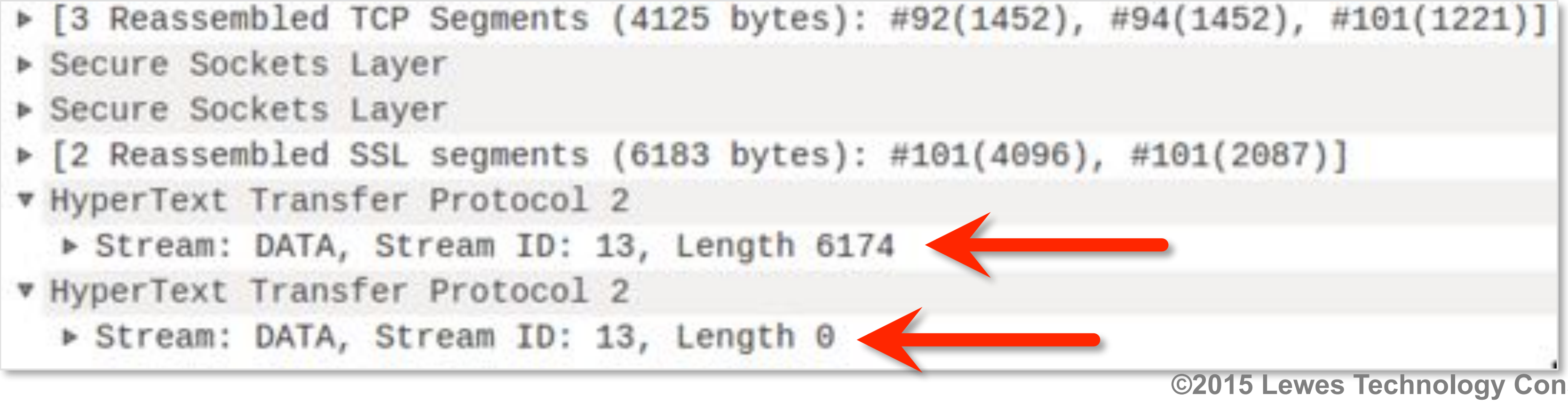
```
0 00 00 1f 88 58    ....$... ......X
0 93 d8 5f a5       ....d..J Tu..._.)
2 95 d8 55 89 3     ..Z..... i/...U.9
9 d6 00 7f 5a 83     ..})Y.. .9I...Z.
0 21 ea 49 6a 4a    ... ..M. .@.!.IjJ
5 ff e6 0a 41 2c    .)-... ......A.
```

```
▸ Header: :status: 200
▸ Header: cache-control: no-cache, no-store, must-revalidate, pre-check=0, po
▸ Header: content-encoding: gzip
▸ Header: content-length: 14591
▸ Header: content-security-policy: script-src https://connect.facebook.net ht
▸ Header: content-type: text/html;charset=utf-8
▸ Header: date: Mon, 07 Dec 2015 14:14:39 GMT
▸ Header: expires: Tue, 31 Mar 1981 05:00:00 GMT
▸ Header: last-modified: Mon, 07 Dec 2015 14:14:39 GMT
▸ Header: pragma: no-cache
▸ Header: server: tsa_b
▸ Header: set-cookie: _twitter_sess=BAh7CSIKZmxhc2hJQzonQWN0aW9uQ29udHJvbGxlc
▸ Header: set-cookie: ua="f5,m2,m5,msw"; Expires=Mon, 07 Dec 2015 15:14:39 GM
▸ Header: status: 200 OK
▸ Header: strict-transport-security: max-age=631138519
▸ Header: x-connection-hash: 252892347ada46fe76d6d6ea455efcb1
▸ Header: x-content-type-options: nosniff
▸ Header: x-frame-options: SAMEORIGIN
▸ Header: x-response-time: 21
▸ Header: x-transaction: fa3dd173b833c723
▸ Header: x-twitter-response-tags: BouncerCompliant
▸ Header: x-ua-compatible: IE=edge,chrome=1
▸ Header: x-xss-protection: 1; mode=block
```

HTTP/2 Response Body

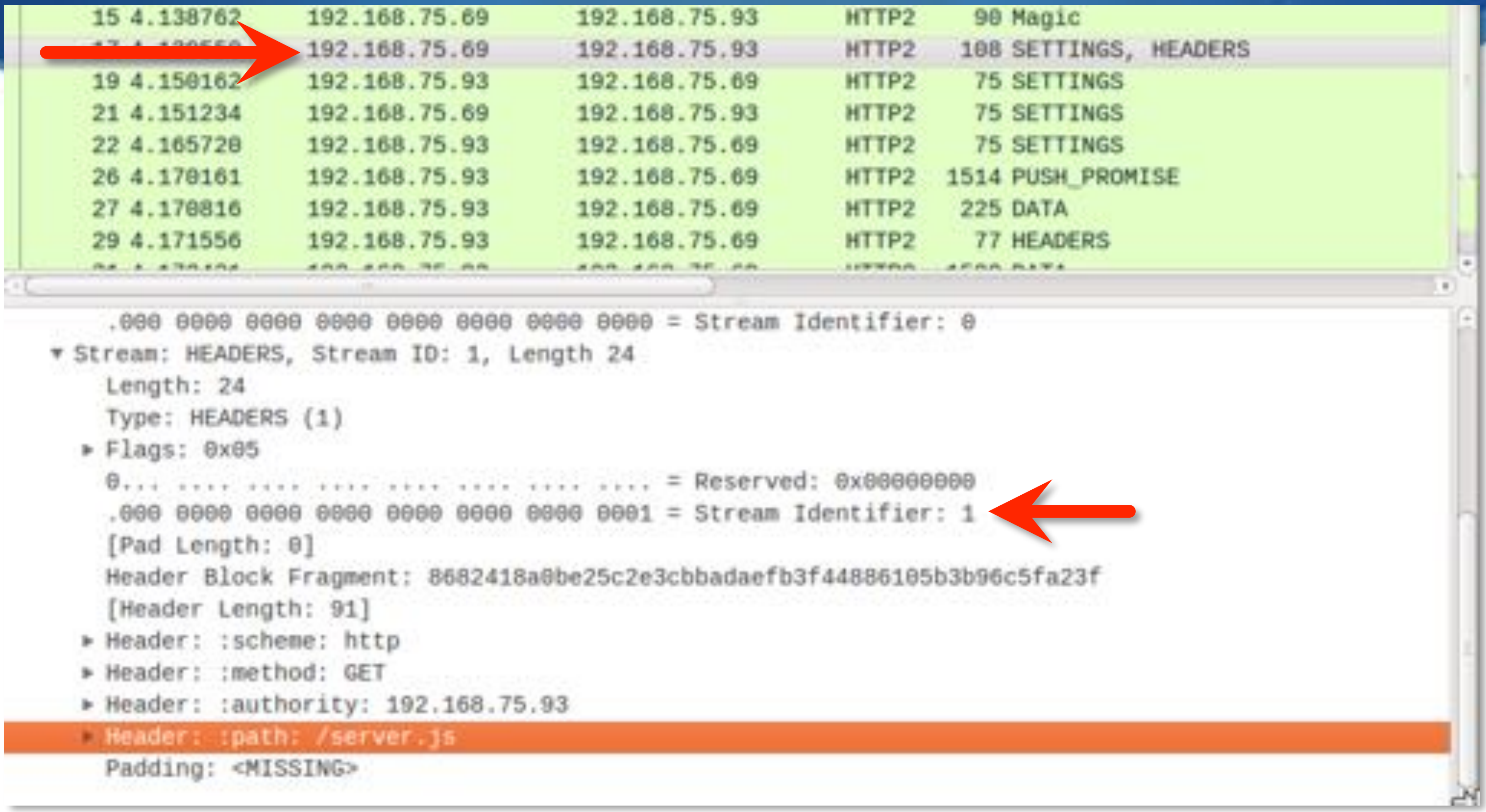


```
▶ [2 Reassembled TCP Segments (4125 bytes): #88(2904), #90(1221)]
▶ Secure Sockets Layer
▶ Secure Sockets Layer
▶ [2 Reassembled SSL segments (8153 bytes): #90(4096), #90(4057)]
▼ HyperText Transfer Protocol 2
  ▶ Stream: DATA, Stream ID: 13, Length 8144
▼ HyperText Transfer Protocol 2
  ▶ Stream: DATA, Stream ID: 13, Length 48
▼ HyperText Transfer Protocol 2
  ▶ Stream: DATA, Stream ID: 13, Length 225
```



```
▶ [3 Reassembled TCP Segments (4125 bytes): #92(1452), #94(1452), #101(1221)]
▶ Secure Sockets Layer
▶ Secure Sockets Layer
▶ [2 Reassembled SSL segments (6183 bytes): #101(4096), #101(2087)]
▼ HyperText Transfer Protocol 2
  ▶ Stream: DATA, Stream ID: 13, Length 6174
▼ HyperText Transfer Protocol 2
  ▶ Stream: DATA, Stream ID: 13, Length 0
```

Single HTTP/2 Request… ?

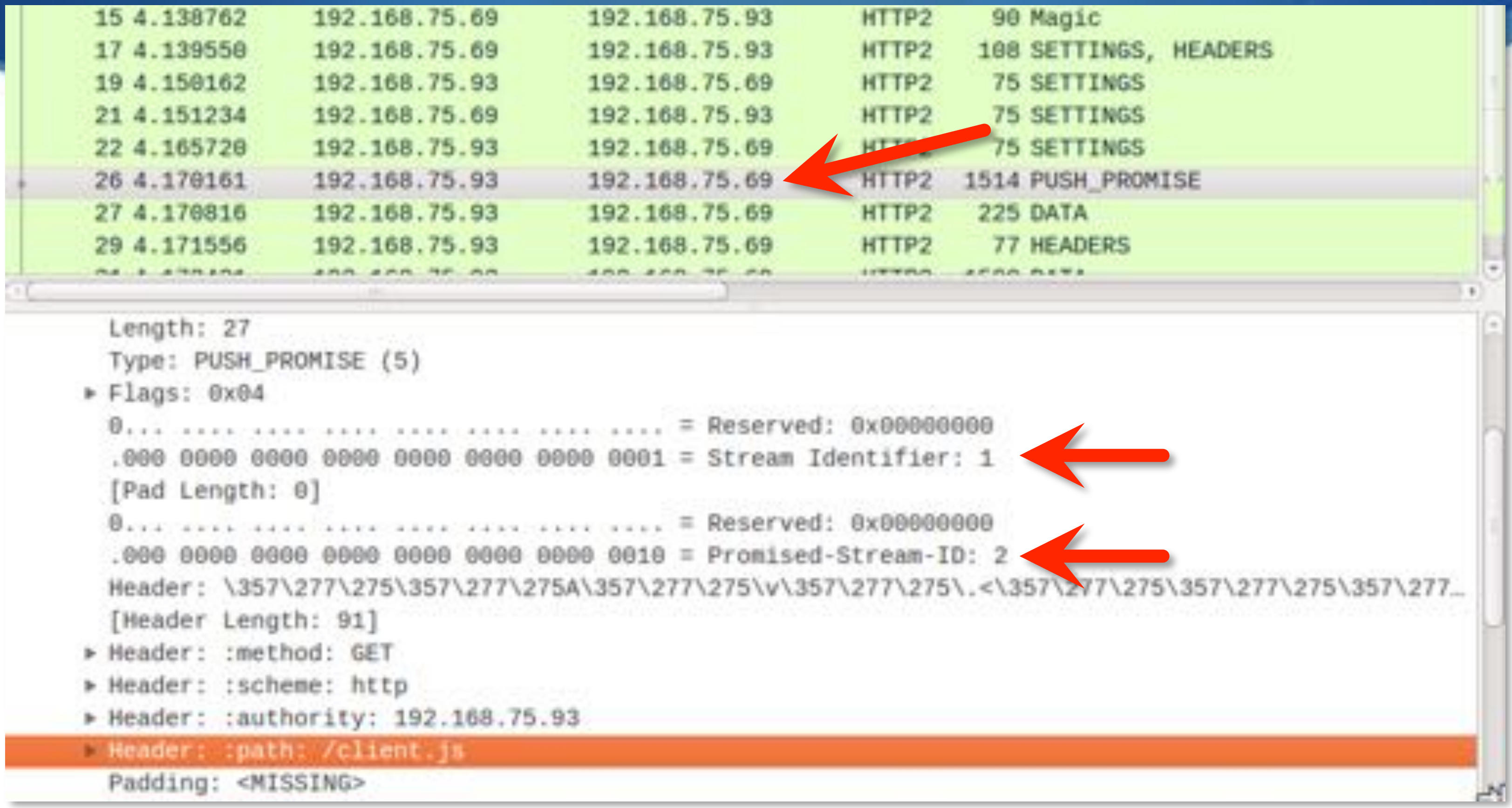


```
15 4.138762    192.168.75.69    192.168.75.93    HTTP2     90 Magic
[illegible]    192.168.75.69    192.168.75.93    HTTP2    108 SETTINGS, HEADERS
19 4.150162    192.168.75.93    192.168.75.69    HTTP2     75 SETTINGS
21 4.151234    192.168.75.69    192.168.75.93    HTTP2     75 SETTINGS
22 4.165728    192.168.75.93    192.168.75.69    HTTP2     75 SETTINGS
26 4.170161    192.168.75.93    192.168.75.69    HTTP2   1514 PUSH_PROMISE
27 4.170816    192.168.75.93    192.168.75.69    HTTP2    225 DATA
29 4.171556    192.168.75.93    192.168.75.69    HTTP2     77 HEADERS
```

```
    .000 0000 0000 0000 0000 0000 0000 0000 = Stream Identifier: 0
▾ Stream: HEADERS, Stream ID: 1, Length 24
    Length: 24
    Type: HEADERS (1)
  ▸ Flags: 0x05
    0... .... .... .... .... .... .... .... = Reserved: 0x00000000
    .000 0000 0000 0000 0000 0000 0000 0001 = Stream Identifier: 1
    [Pad Length: 0]
    Header Block Fragment: 8682418a0be25c2e3cbbadaefb3f44886105b3b96c5fa23f
    [Header Length: 91]
  ▸ Header: :scheme: http
  ▸ Header: :method: GET
  ▸ Header: :authority: 192.168.75.93
  ▸ Header: :path: /server.js
    Padding: <MISSING>
```

Stream ID 1: `http://192.168.75.93:8080/server.js`

HTTP/2 Server Push (1)

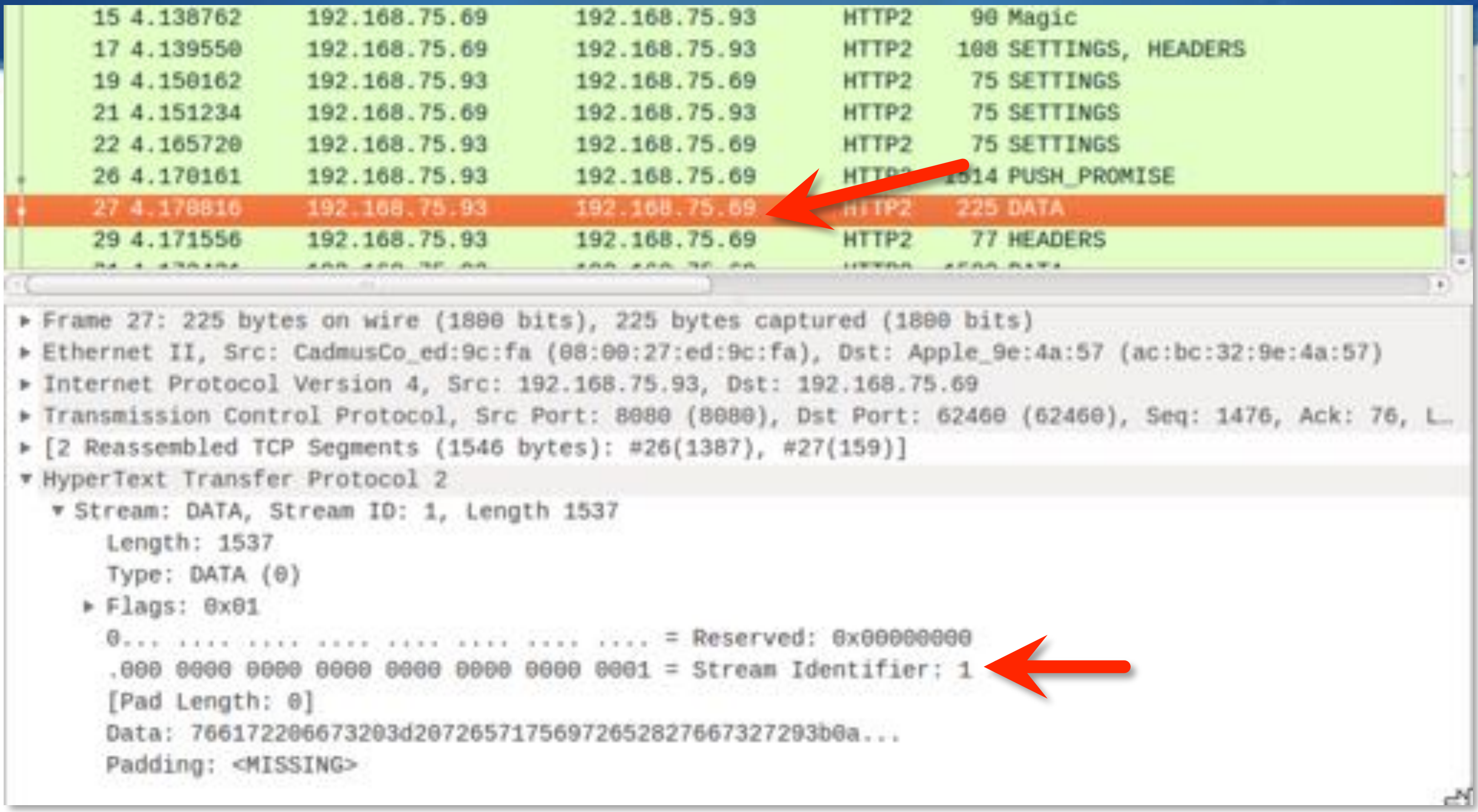


```
15 4.138762    192.168.75.69    192.168.75.93    HTTP2     90 Magic
17 4.139550    192.168.75.69    192.168.75.93    HTTP2    108 SETTINGS, HEADERS
19 4.150162    192.168.75.93    192.168.75.69    HTTP2     75 SETTINGS
21 4.151234    192.168.75.69    192.168.75.93    HTTP2     75 SETTINGS
22 4.165720    192.168.75.93    192.168.75.69    HTTP2     75 SETTINGS
26 4.170161    192.168.75.93    192.168.75.69    HTTP2   1514 PUSH_PROMISE
27 4.170816    192.168.75.93    192.168.75.69    HTTP2    225 DATA
29 4.171556    192.168.75.93    192.168.75.69    HTTP2     77 HEADERS
```

```
   Length: 27
   Type: PUSH_PROMISE (5)
 ▸ Flags: 0x04
   0... .... .... .... .... .... .... .... = Reserved: 0x00000000
   .000 0000 0000 0000 0000 0000 0000 0001 = Stream Identifier: 1
   [Pad Length: 0]
   0... .... .... .... .... .... .... .... = Reserved: 0x00000000
   .000 0000 0000 0000 0000 0000 0000 0010 = Promised-Stream-ID: 2
   Header: \357\277\275\357\277\275A\357\277\275\v\357\277\275\.<\357\277\275\357\277\275\357\277…
   [Header Length: 91]
 ▸ Header: :method: GET
 ▸ Header: :scheme: http
 ▸ Header: :authority: 192.168.75.93
 ▸ Header: :path: /client.js
   Padding: <MISSING>
```

NEW Stream ID 2: **`http://192.168.75.93:8080/client.js`**

HTTP/2 Response (Expected)

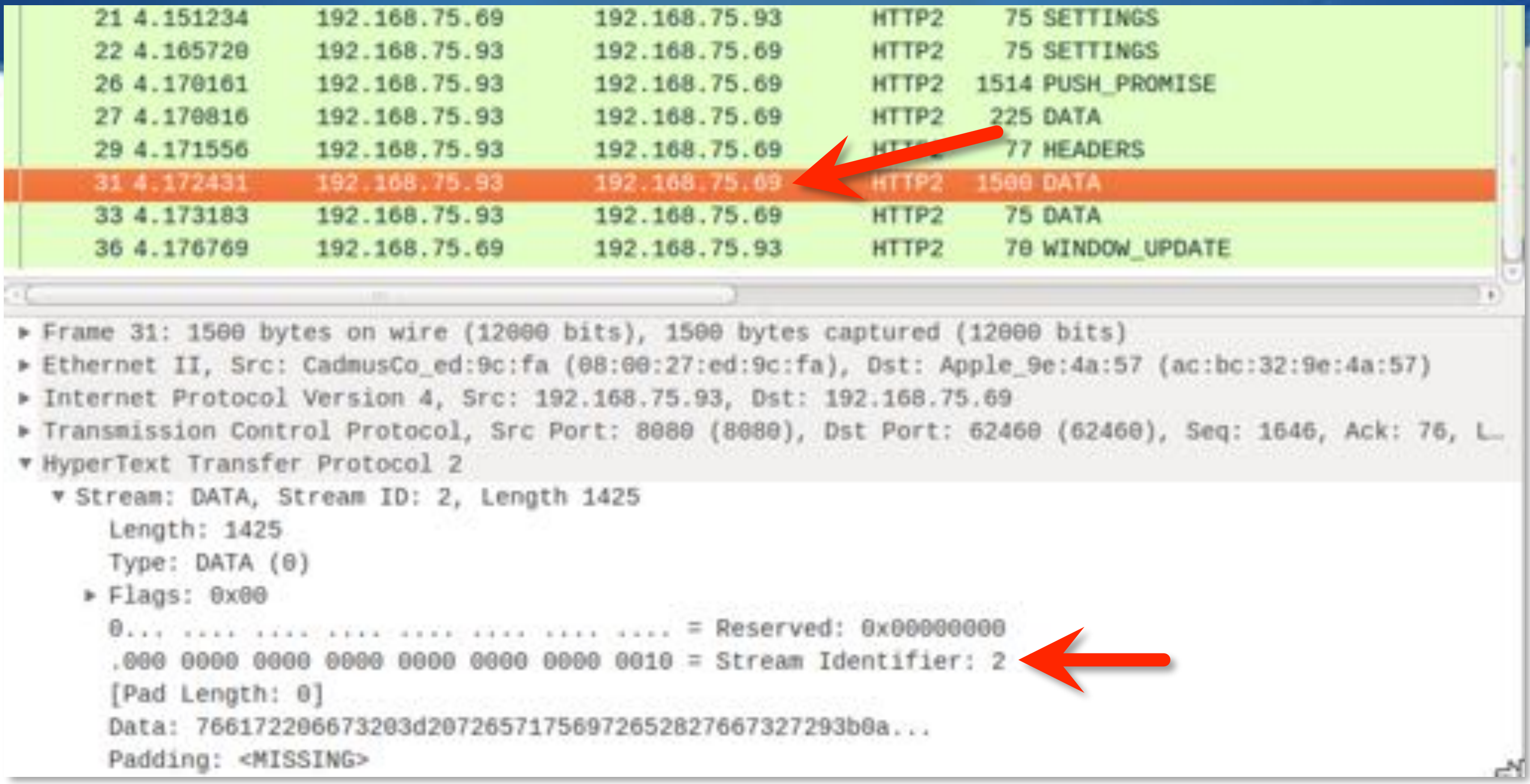


```
15 4.138762    192.168.75.69    192.168.75.93    HTTP2     90 Magic
17 4.139550    192.168.75.69    192.168.75.93    HTTP2    108 SETTINGS, HEADERS
19 4.150162    192.168.75.93    192.168.75.69    HTTP2     75 SETTINGS
21 4.151234    192.168.75.69    192.168.75.93    HTTP2     75 SETTINGS
22 4.165720    192.168.75.93    192.168.75.69    HTTP2     75 SETTINGS
26 4.170161    192.168.75.93    192.168.75.69    HTTP2   1514 PUSH_PROMISE
27 4.170816    192.168.75.93    192.168.75.69    HTTP2    225 DATA
29 4.171556    192.168.75.93    192.168.75.69    HTTP2     77 HEADERS
```

```
▸ Frame 27: 225 bytes on wire (1800 bits), 225 bytes captured (1800 bits)
▸ Ethernet II, Src: CadmusCo_ed:9c:fa (08:00:27:ed:9c:fa), Dst: Apple_9e:4a:57 (ac:bc:32:9e:4a:57)
▸ Internet Protocol Version 4, Src: 192.168.75.93, Dst: 192.168.75.69
▸ Transmission Control Protocol, Src Port: 8080 (8080), Dst Port: 62460 (62460), Seq: 1476, Ack: 76, L…
▸ [2 Reassembled TCP Segments (1546 bytes): #26(1387), #27(159)]
▾ HyperText Transfer Protocol 2
  ▾ Stream: DATA, Stream ID: 1, Length 1537
      Length: 1537
      Type: DATA (0)
    ▸ Flags: 0x01
      0... .... .... .... .... .... .... .... = Reserved: 0x00000000
      .000 0000 0000 0000 0000 0000 0000 0001 = Stream Identifier: 1
      [Pad Length: 0]
      Data: 766172206673203d207265717569726528276673272930a...
      Padding: <MISSING>
```

Stream ID 1: **`http://192.168.75.93:8080/server.js`**

HTTP/2 Response (Pushed)



```
   21 4.151234    192.168.75.69    192.168.75.93    HTTP2     75 SETTINGS
   22 4.165720    192.168.75.93    192.168.75.69    HTTP2     75 SETTINGS
   26 4.170161    192.168.75.93    192.168.75.69    HTTP2   1514 PUSH_PROMISE
   27 4.170816    192.168.75.93    192.168.75.69    HTTP2    225 DATA
   29 4.171556    192.168.75.93    192.168.75.69    HTTP2     77 HEADERS
   31 4.172431    192.168.75.93    192.168.75.69    HTTP2   1500 DATA
   33 4.173183    192.168.75.93    192.168.75.69    HTTP2     75 DATA
   36 4.176769    192.168.75.69    192.168.75.93    HTTP2     70 WINDOW_UPDATE
```

```
▸ Frame 31: 1500 bytes on wire (12000 bits), 1500 bytes captured (12000 bits)
▸ Ethernet II, Src: CadmusCo_ed:9c:fa (08:00:27:ed:9c:fa), Dst: Apple_9e:4a:57 (ac:bc:32:9e:4a:57)
▸ Internet Protocol Version 4, Src: 192.168.75.93, Dst: 192.168.75.69
▸ Transmission Control Protocol, Src Port: 8080 (8080), Dst Port: 62460 (62460), Seq: 1646, Ack: 76, L…
▾ HyperText Transfer Protocol 2
  ▾ Stream: DATA, Stream ID: 2, Length 1425
      Length: 1425
      Type: DATA (0)
    ▸ Flags: 0x00
      0... .... .... .... .... .... .... .... = Reserved: 0x00000000
      .000 0000 0000 0000 0000 0000 0000 0010 = Stream Identifier: 2
      [Pad Length: 0]
      Data: 766172206673203d20726571756972652827667327293b0a...
      Padding: <MISSING>
```

Stream ID 2: **`http://192.168.75.93:8080/client.js`**

Current Status

- Browsers/servers/sites using HTTP/2
  - Chrome, Firefox, MS ~~IE~~ Edge, Safari 9+, Opera, curl…
  - Apache, nginx, IIS…
  - Twitter, Google
- Wireshark analysis via exported client ephemeral keys (often TLS and PFS) (See Sally's paper in Evernote)
- Squid 4 will fully handle HTTP/2
- **Layer 7 logs are best chance for continued visibility**

Beer Spotlight

- Dogfish Head 90min IPA
  - "Perhaps the best IPA in America" –Esquire Mag
  - "The best IPA I know" –Phil
  - 9% ABV, 90 IBU
  - **Continuously hopped**
  - Available year round: AZ, CA, CO, CT, DC, DE, FL, GA, IL, KY, MA, MD, ME, MI, NC, NH, NJ, NV, NY, OH, OR, PA, SC, TX, VA, VT, WA

Questions

`phil@lewestech.com | @PhilHagen`

Links relevant to this presentation:

`http://for572.com/taphouse`

Tagged with the episode number (`0x00`)