

Assignment 5.2 Network Analysis

Shashank Mondrati

Dominik Gonzales

Connor Carroll

William Zhang

The image shows a Wireshark network analysis tool window titled "http-pcapmnet101.pcapng". The main display area shows a list of captured packets. The selected packet is an HTTP GET request from 24.6.173.220 to 209.133.32.69. The details pane shows the following information:

- Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
- Internet Protocol Version 4, Src: 24.6.173.220, Dst: 209.133.32.69
- Transmission Control Protocol, Src Port: 21213, Dst Port: 80, Seq: 1, Ack: 1, Len: 287
 - Source Port: 21213
 - Destination Port: 80
 - [Stream index: 0]
 - [Conversation completeness: Complete, WITH_DATA (31)]
 - [TCP Segment Len: 287]
 - Sequence Number: 1 (relative sequence number)
 - Sequence Number (raw): 1288438180
 - [Next Sequence Number: 288 (relative sequence number)]
 - Acknowledgment Number: 1 (relative seq. number)
- Hypertext Transfer Protocol: Protocol

The packet bytes pane shows the raw data of the HTTP request, including the status line "200 OK (text/html)" and the "GET /static/script/browse.js?1351033873262 HTTP/1.1" line.

HTTP: HyperText Transfer Protocol

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	24.6.173.220	75.75.75.75	DNS	73	Standard query 0xc3bf A www.pcapr.net
2	0.021485	75.75.75.75	24.6.173.220	DNS	89	Standard query response 0xc3bf A www.pcapr.net A 209.133.32.69
3	0.023115	24.6.173.220	75.75.75.75	DNS	73	Standard query 0x406e AAAA www.pcapr.net
4	0.048477	75.75.75.75	24.6.173.220	DNS	146	Standard query response 0x406e AAAA www.pcapr.net SOA pdns1.ultradns.net
23	1.940425	24.6.173.220	75.75.75.75	DNS	80	Standard query 0xe7b3 A pcapr.googlecode.com
24	1.941671	24.6.173.220	75.75.75.75	DNS	83	Standard query 0x8d8f A jqueryjs.googlecode.com
25	1.943350	24.6.173.220	75.75.75.75	DNS	84	Standard query 0x9946 A jquery-ui.googlecode.com
31	1.957246	75.75.75.75	24.6.173.220	DNS	144	Standard query response 0x8d8f A jqueryjs.googlecode.com CNAME googlecode.l.googleusercontent.com A 74.125...
32	1.958156	75.75.75.75	24.6.173.220	DNS	145	Standard query response 0x9946 A jquery-ui.googlecode.com CNAME googlecode.l.googleusercontent.com A 74.125...
33	1.958325	24.6.173.220	75.75.75.75	DNS	83	Standard query 0x858f AAAA jqueryjs.googlecode.com
34	1.959216	24.6.173.220	75.75.75.75	DNS	84	Standard query 0x9a1e AAAA jquery-ui.googlecode.com
40	1.971823	75.75.75.75	24.6.173.220	DNS	156	Standard query response 0x858f AAAA jqueryjs.googlecode.com CNAME googlecode.l.googleusercontent.com AAAA 2...
41	1.972676	75.75.75.75	24.6.173.220	DNS	157	Standard query response 0x9a1e AAAA jquery-ui.googlecode.com CNAME googlecode.l.googleusercontent.com AAAA 2...
45	1.978718	75.75.75.75	24.6.173.220	DNS	141	Standard query response 0xe7b3 A pcapr.googlecode.com CNAME googlecode.l.googleusercontent.com A 173.194.79...
46	1.979477	24.6.173.220	75.75.75.75	DNS	80	Standard query 0xe40b AAAA pcapr.googlecode.com
55	1.994049	75.75.75.75	24.6.173.220	DNS	153	Standard query response 0xe40b AAAA pcapr.googlecode.com CNAME googlecode.l.googleusercontent.com AAAA 2607...

> Frame 4: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface \Device\NPF{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}, id 0

> Ethernet II, Src: Cadant_31:bb:c1 (00:01:5c:31:bb:c1), Dst: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3)

> Internet Protocol Version 4, Src: 75.75.75.75, Dst: 24.6.173.220

> User Datagram Protocol, Src Port: 53, Dst Port: 51612

> Domain Name System (response)

```

0000  d4 85 64 a7 bf a3 00 01 5c 31 bb c1 08 00 45 40  ..d....\....E@
0010  00 84 00 00 40 00 3b 11 e2 b0 4b 4b 4b 08 06  ....@;....KKKK..
0020  ad dc 00 35 c9 00 70 8f 90 40 6e 61 00 00 01  ...$...p...@....
0030  00 00 00 01 00 00 03 77 77 05 70 63 61 70 72  ....w.w.w.pcapr
0040  03 6e 65 74 00 00 1c 00 01 c0 10 00 06 00 01 00  .net.....
0050  00 0e 10 00 3d 05 70 64 6e 73 31 08 75 6c 74 72  ....pd ns1.ultr
0060  61 64 6e 73 c0 16 0a 68 6f 73 74 6d 61 73 74 65  adns...hostmaste
0070  72 07 73 70 69 72 65 6e 74 03 63 6f 6d 00 77 ed  nspirin t:com-w
0080  cc 8e 00 00 2a 30 00 00 07 08 00 09 3a 08 00 01  ....*0.....

```

Domain Name System: Protocol

Packets: 487 · Displayed: 68 (14.0%)

Profile: Default

DNS: DOnain Naming Server, displays the IP

No.	Time	Source	Destination	Protocol	Length	Info
8	0.071372	24.6.173.220	209.133.32.69	HTTP	341	GET / HTTP/1.1
18	0.126044	24.6.173.220	209.133.32.69	HTTP	387	GET /home HTTP/1.1
44	1.975884	24.6.173.220	209.133.32.69	HTTP	396	GET /static/script/browse.js?1351033873262 HTTP/1.1
77	2.026058	24.6.173.220	209.133.32.69	HTTP	410	GET /static/image/apps.png HTTP/1.1
78	2.026279	24.6.173.220	209.133.32.69	HTTP	412	GET /static/image/studio.png HTTP/1.1
81	2.030584	24.6.173.220	173.194.79.82	HTTP	363	GET /svn/trunk/style/page.css HTTP/1.1
84	2.035403	24.6.173.220	173.194.79.82	HTTP	355	GET /svn/trunk/script/jquery.form.js HTTP/1.1
87	2.036304	24.6.173.220	173.194.79.82	HTTP	361	GET /svn/trunk/script/jquery.dimensions.js HTTP/1.1
94	2.040261	24.6.173.220	173.194.79.82	HTTP	355	GET /svn/trunk/script/jquery.menu.js HTTP/1.1
99	2.041102	24.6.173.220	173.194.79.82	HTTP	366	GET /svn/trunk/style/pmagick.css HTTP/1.1
100	2.041460	24.6.173.220	173.194.79.82	HTTP	373	GET /svn/trunk/style/jquery.suggest.css HTTP/1.1
145	2.090448	24.6.173.220	173.194.79.82	HTTP	363	GET /svn/trunk/script/jquery.suggest.pack.js HTTP/1.1
167	2.111942	24.6.173.220	173.194.79.82	HTTP	375	GET /svn/trunk/image/favicon.ico HTTP/1.1
169	2.112768	24.6.173.220	173.194.79.82	HTTP	379	GET /svn/trunk/image/blank.png HTTP/1.1
189	2.118700	24.6.173.220	173.194.79.82	HTTP	377	GET /svn/trunk/image/rss.png HTTP/1.1
204	2.123926	24.6.173.220	173.194.79.82	HTTP	391	GET /svn/trunk/image/apps/drafts_small.png HTTP/1.1

> Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)

> Internet Protocol Version 4, Src: 24.6.173.220, Dst: 209.133.32.69

> Transmission Control Protocol, Src Port: 21213, Dst Port: 80, Seq: 1, Ack: 1, Len: 287

Source Port: 21213

Destination Port: 80

[Stream index: 0]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 287]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 1288438180

[Next Sequence Number: 288 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

```

0020  20 45 52 dd 00 50 4c cc 01 a4 04 ea 62 2d 50 18  ER...PL...b-P-
0030  40 29 b8 e6 00 00 47 45 54 20 2f 20 48 54 54 50  @)....GE T / HTTP
0040  2f 31 2e 31 0d 0a 4b 6f 73 74 3a 20 77 77 77 2e  /1.1..Ho st: ww.
0050  70 63 61 70 72 2e 6e 65 74 0d 0a 55 73 65 72 2d  pcapr.ne t: User-
0060  41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35  Agent: M orilla/5
0070  2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 36  .0 (Wind ows NT 6
0080  2e 31 3b 20 57 4f 57 36 34 3b 20 72 76 3a 31 36  .1; WOW6 4; rv:16
0090  2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 30 30 31  .0) Geck o/201001
00a0  30 31 20 46 69 72 65 66 6f 78 2f 31 36 2e 30 0d  01 Fire ox/16.0-

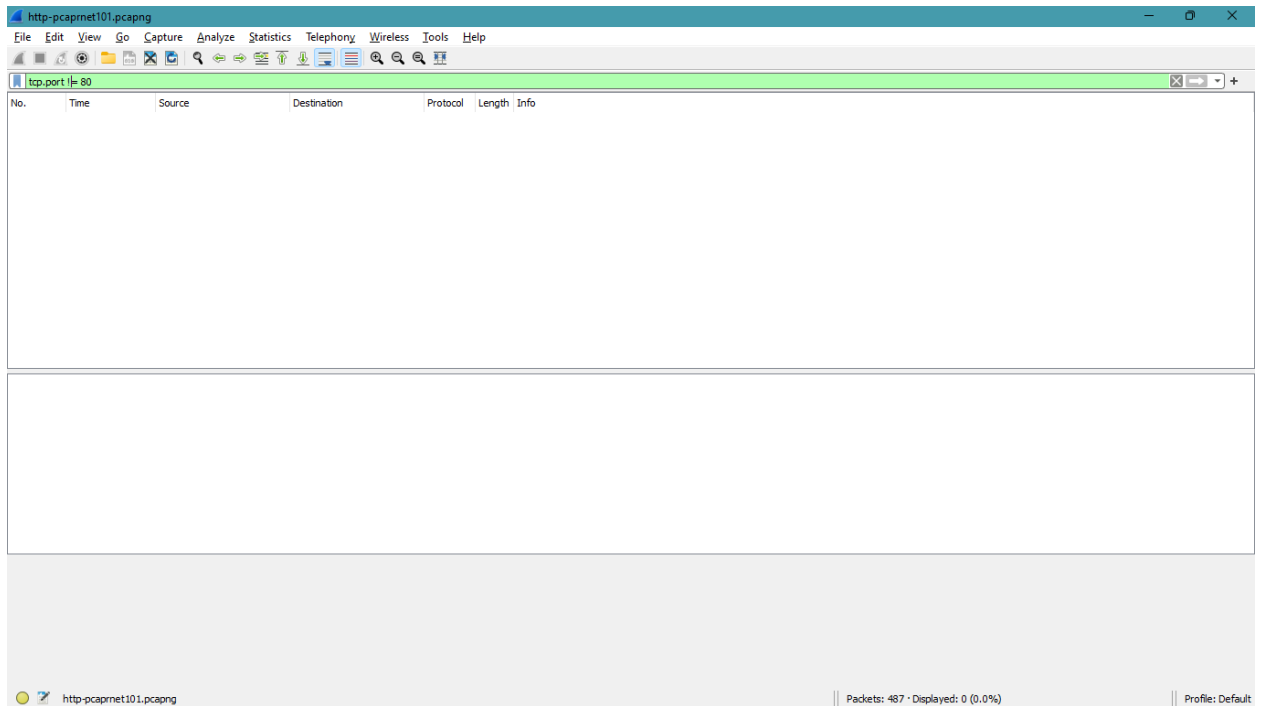
```

Request Method: Character string

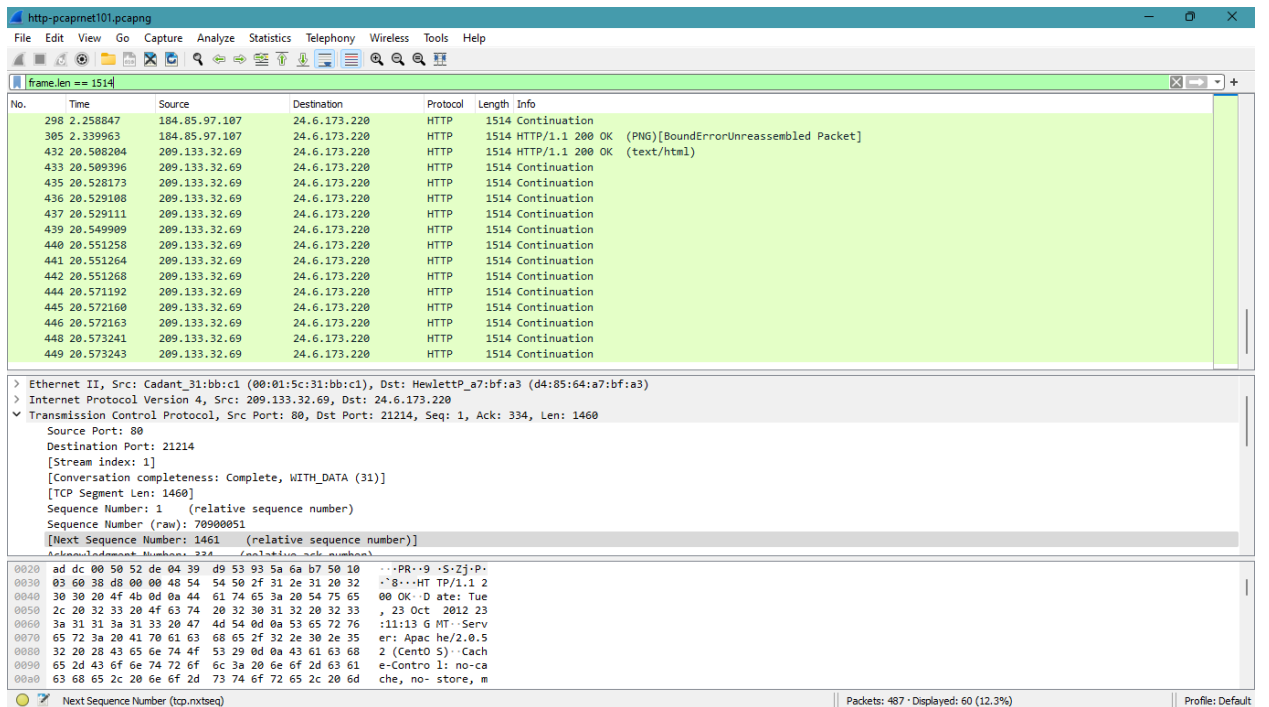
Packets: 487 · Displayed: 37 (7.6%)

Profile: Default

481 Frames are included in http.request.method



I used `tcp.port != 80`.



I used `frame.len == 1514` to get 449 frames.

http-pcapnet101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request

No.	Time	Source	Destination	Protocol	Length	Info
258	2.208081	24.6.173.220	173.194.79.82	HTTP	391	GET /svn/trunk/image/musl/architecture.jpg HTTP/1.1
263	2.209435	24.6.173.220	173.194.79.82	HTTP	403	GET /svn/trunk/image/bg.png HTTP/1.1
265	2.214115	24.6.173.220	173.194.79.82	HTTP	411	GET /svn/trunk/image/pcapr-logo.png HTTP/1.1
278	2.239156	24.6.173.220	184.85.97.107	HTTP	347	GET /javascripts/widgets/tab.js HTTP/1.1
302	2.324882	24.6.173.220	184.85.97.107	HTTP	391	GET /images/widgets/en/feedback_tab_white.png HTTP/1.1
303	2.325331	24.6.173.220	173.194.79.82	HTTP	411	GET /svn/trunk/image/btn-search.png HTTP/1.1
304	2.325674	24.6.173.220	173.194.79.82	HTTP	412	GET /svn/trunk/image/status-info.png HTTP/1.1
410	13.216496	24.6.173.220	209.133.32.69	HTTP	657	GET /browse/suggest?_1351033897626&q=sip HTTP/1.1
420	18.585700	24.6.173.220	209.133.32.69	HTTP	624	GET /browse?q=sip HTTP/1.1
425	19.062454	24.6.173.220	209.133.32.69	HTTP	657	GET /browse/suggest?_1351033903473&q=sip HTTP/1.1
457	20.603099	24.6.173.220	209.133.32.69	HTTP	647	GET /static/script/browse.js?1351033873262 HTTP/1.1
458	20.611551	24.6.173.220	173.194.79.82	HTTP	390	GET /svn/trunk/image/throbber.gif HTTP/1.1
469	20.674695	24.6.173.220	173.194.79.82	HTTP	418	GET /svn/trunk/image/16x16/FullSize.png HTTP/1.1
470	20.675046	24.6.173.220	173.194.79.82	HTTP	411	GET /svn/trunk/image/16x16/User.png HTTP/1.1
471	20.675453	24.6.173.220	173.194.79.82	HTTP	409	GET /svn/trunk/image/p-expand.gif HTTP/1.1
481	22.807434	24.6.173.220	209.133.32.69	HTTP	665	GET /browse/suggest?_1351033907216&q=sip HTTP/1.1

> Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
> Internet Protocol Version 4, Src: 24.6.173.220, Dst: 209.133.32.69
v Transmission Control Protocol, Src Port: 21214, Dst Port: 80, Seq: 1, Ack: 1, Len: 333
Source Port: 21214
Destination Port: 80
[Stream index: 1]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 333]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 2472175978
[Next Sequence Number: 334 (relative sequence number)]
[Acknowledgment Number: 1 (relative ack number)]

0020 20 45 52 de 00 50 93 5a 69 6a 04 39 d9 53 50 18 ER..P.Z ij.9.SP.
0030 40 29 b9 14 00 00 47 45 54 20 2f 68 6f 6d 65 20 @....GE T /home
0040 40 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 HTTP/1.1 ..Host:
0050 77 77 77 2e 70 63 61 70 72 2e 6e 65 74 0d 0a 55 www.pcap.r.net..U
0060 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c ser-Agen t: Mozil
0070 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 la/5.0 (Windows
0080 4e 54 20 36 2e 31 3b 20 57 4f 57 36 34 3b 20 72 NT 6.1; WOW64; r
0090 76 3a 31 36 2e 30 29 20 47 65 63 6b 6f 2f 32 30 v:16.0) Gecko/20
00a0 31 30 30 31 30 31 20 46 69 72 65 66 6f 78 2f 31 100101 F irefox/1

Stream index (tcp.stream) Packets: 487 · Displayed: 37 (7.6%) Profile: Default

Used http.request to get 481 GET Requests

/a display filter ... <Ctrl>

Source	Destination	Protocol	Length	Info	HTTP host
72 24.6.173.220	209.133.32.69	HTTP	341	GET / HTTP/1.1	✓
44 24.6.173.220	209.133.32.69	HTTP	387	GET /home HTTP/1.1	✓
84 24.6.173.220	209.133.32.69	HTTP	396	GET /static/script/browse.js?1351033873262 HTTP/1.1	✓
58 24.6.173.220	209.133.32.69	HTTP	410	GET /static/image/apps.png HTTP/1.1	✓
79 24.6.173.220	209.133.32.69	HTTP	412	GET /static/image/studio.png HTTP/1.1	✓
84 24.6.173.220	173.194.79.82	HTTP	363	GET /svn/trunk/style/page.css HTTP/1.1	✓
83 24.6.173.220	173.194.79.82	HTTP	355	GET /svn/trunk/script/jquery.form.js HTTP/1.1	✓
94 24.6.173.220	173.194.79.82	HTTP	361	GET /svn/trunk/script/jquery.dimensions.js HTTP/1.1	✓
61 24.6.173.220	173.194.79.82	HTTP	355	GET /svn/trunk/script/jquery.menu.js HTTP/1.1	✓
82 24.6.173.220	173.194.79.82	HTTP	366	GET /svn/trunk/style/pmagick.css HTTP/1.1	✓
60 24.6.173.220	173.194.79.82	HTTP	373	GET /svn/trunk/style/jquery.suggest.css HTTP/1.1	✓

[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.071372000 seconds]
Frame Number: 8
Frame Length: 341 bytes (2728 bits)
Capture Length: 341 bytes (2728 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
ernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
Destination: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
Address: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)

00 01 5c 31 bb c1 d4 85 64 a7 bf a3 00 00 45 00 ..1....d....E-
01 47 6a 4e 40 00 80 06 00 00 18 06 ad dc d1 85 -GJ)@.....
20 45 52 dd 00 50 4c cc 01 a4 04 ea 62 2d 50 18 ER..PL....b-P-
40 29 b8 e6 00 00 47 45 54 20 2f 20 48 54 50 20 @....GE T / HTTP
2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e /1.1..Ho st: www.
70 63 61 70 72 2e 6e 65 74 0d 0a 55 73 65 72 2d pcapr.ne t: User-
41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 Agent: M ozilla/5
2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 36 .0 (Wind ows NT 6
2e 31 3b 20 57 4f 57 36 34 3b 20 72 76 3a 31 36 .1; WOW6 4; rv:16
2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 30 30 31 .0) Geck o/201001
30 31 20 46 69 72 65 66 6f 78 2f 31 36 2e 30 0d 01 Firef ox/16.0.

Wireshark							
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help							
http.request							
No.	Time	Source	Destination	Protocol	Length	Info	HTTP Host
8	0.071372	24.6.173.220	209.133.32.69	HTTP	341	GET / HTTP/1.1	✓
18	0.126044	24.6.173.220	209.133.32.69	HTTP	387	GET /home HTTP/1.1	✓
44	1.975884	24.6.173.220	209.133.32.69	HTTP	396	GET /static/script/browse.js?1351033873262 HTTP/1.1	✓
77	2.026058	24.6.173.220	209.133.32.69	HTTP	410	GET /static/image/apps.png HTTP/1.1	✓
78	2.026279	24.6.173.220	209.133.32.69	HTTP	412	GET /static/image/studio.png HTTP/1.1	✓
81	2.030584	24.6.173.220	173.194.79.82	HTTP	363	GET /svn/trunk/style/page.css HTTP/1.1	✓
84	2.035403	24.6.173.220	173.194.79.82	HTTP	355	GET /svn/trunk/script/jquery.form.js HTTP/1.1	✓
87	2.036304	24.6.173.220	173.194.79.82	HTTP	361	GET /svn/trunk/script/jquery.dimensions.js HTTP/1.1	✓
94	2.040261	24.6.173.220	173.194.79.82	HTTP	355	GET /svn/trunk/script/jquery.menu.js HTTP/1.1	✓
99	2.041102	24.6.173.220	173.194.79.82	HTTP	366	GET /svn/trunk/style/pmagick.css HTTP/1.1	✓
100	2.041460	24.6.173.220	173.194.79.82	HTTP	373	GET /svn/trunk/style/jquery.suggest.css HTTP/1.1	✓
145	2.090448	24.6.173.220	173.194.79.82	HTTP	363	GET /svn/trunk/script/jquery.suggest.pack.js HTTP/1.1	✓
167	2.111942	24.6.173.220	173.194.79.82	HTTP	375	GET /svn/trunk/image/favicon.ico HTTP/1.1	✓
169	2.112768	24.6.173.220	173.194.79.82	HTTP	379	GET /svn/trunk/image/blank.png HTTP/1.1	✓
189	2.118700	24.6.173.220	173.194.79.82	HTTP	377	GET /svn/trunk/image/rss.png HTTP/1.1	✓
204	2.123926	24.6.173.220	173.194.79.82	HTTP	391	GET /svn/trunk/image/apps/drafts_small.png HTTP/1.1	✓
315	3.123447	24.6.173.220	173.194.79.82	HTTP	202	GET /svn/trunk/image/apps/drafts_small.png HTTP/1.1	✓
<p>> Frame 8: 341 bytes on wire (2728 bits), 341 bytes captured (2728 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EFF300A0B9F}, id 0</p> <p>> Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)</p> <p>> Internet Protocol Version 4, Src: 24.6.173.220, Dst: 209.133.32.69</p> <p>> Transmission Control Protocol, Src Port: 21213, Dst Port: 80, Seq: 1, Ack: 1, Len: 287</p> <p>> Hypertext Transfer Protocol</p> <p>> GET / HTTP/1.1\r\n</p> <p>Host: www.pcapr.net\r\n</p> <p>User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0\r\n</p> <p>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n</p> <p>Accept-Language: en-US,en;q=0.5\r\n</p> <p>Accept-Encoding: gzip, deflate\r\n</p> <p>Connection: keep-alive\r\n</p>							
0020	20 45 52 dd	00 50 4c cc 01 a4 04 ea 62 2d 50 18	ER:PL.....b-P-				
0030	40 29 b8 e6 00 00 47 45	54 20 2f 20 48 54 54 50	@)....GE T / HTTP				
0040	2f 31 2e 31 0d 0a 40 6f	73 74 3a 20 77 77 72 e	/1.1..Ho st: www.				
0050	70 63 61 70 72 2e 6e 65	74 0d 0a 55 73 65 72 2d	pcapr.net:User-				
0060	41 67 65 6e 74 3a 20 4d	6f 7a 69 6c 6c 61 2f 35	Agent: Mozilla/5				
0070	2e 30 20 28 57 69 6e 64	6f 77 73 20 4e 54 20 36	.0 (Wind ows NT 6				
0080	2e 31 3b 20 57 4f 57 36	34 3b 20 72 76 3a 31 36	.1; WOW6 4; rv:16				
0090	2e 30 29 20 47 65 63 6b	6f 2f 32 30 31 30 30 31	.0) Geck o/201001				
00a0	30 31 20 46 69 72 65 66	6f 78 2f 31 36 2e 30 0d	01 Fire ox/16.0-				
Stream index (tcp.stream)				Packets: 487 · Displayed: 37 (7.6%)		Profile: Default	

6 and 7. Application Layer: HyperText Transfer Protocol

Transport Layer Protocol: TCP (6)

Source IP: 24.6.173.220

Destination IP: 209.133.32.69.