What to hand in

The goal of this first lab was primarily to introduce you to Wireshark. The following questions will demonstrate that you've been able to get Wireshark up and running, and have explored some of its capabilities. Answer the following questions, based on your Wireshark experimentation:

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

- Hypertext Transfer Protocol
- Transmission Control Protocol
- Internet Protocol

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)

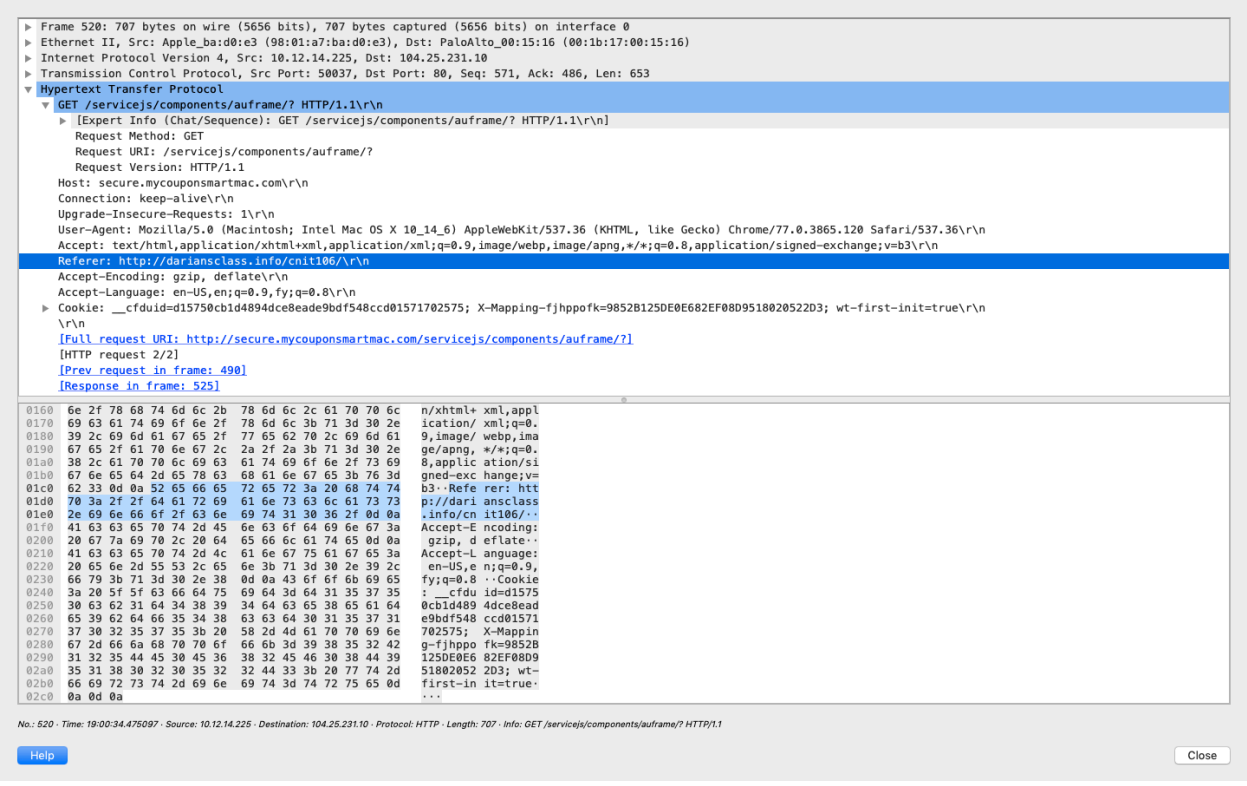
- HTTP GET message was sent - Value of Time Column in packet listing: 23.172841 seconds - Time of Day: 19:00:34.475097
- HTTP OK reply was received - Value of Time Column in packet listing: 23.256979 seconds - Time of Day: 19:00:34.559235

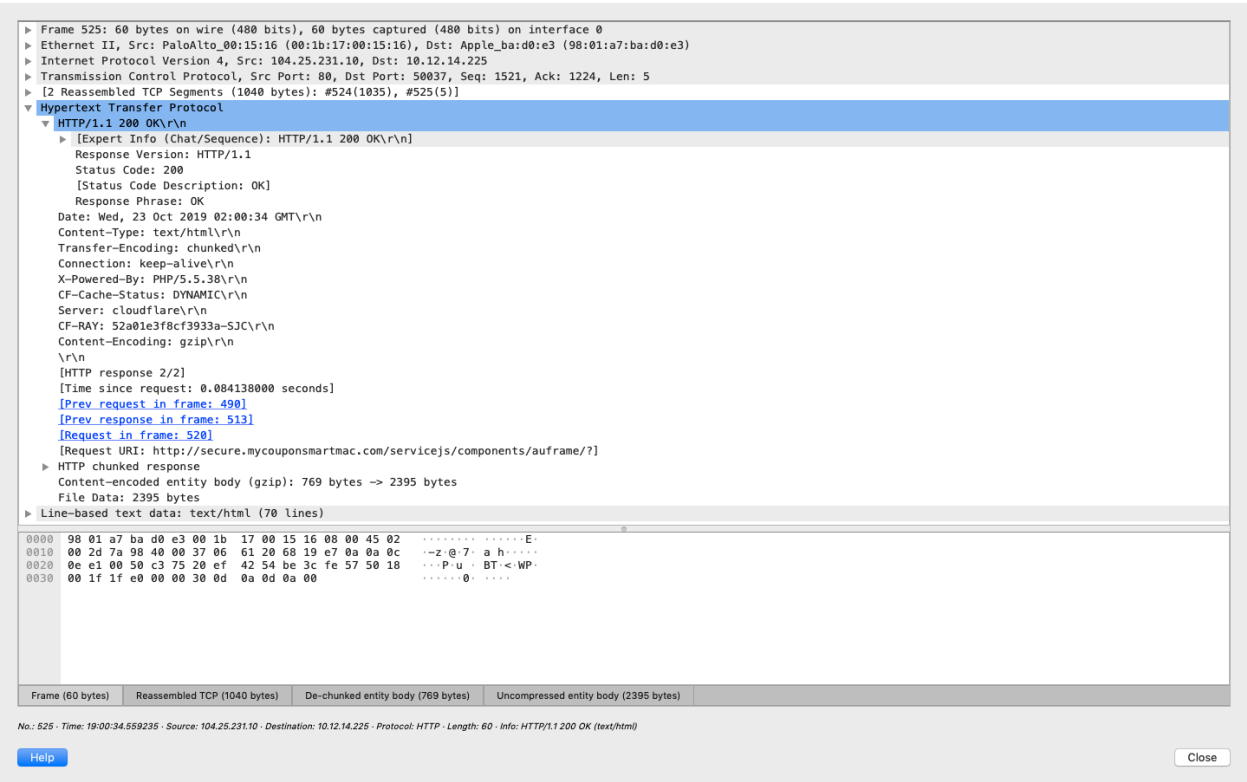
3. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the Internet address of your computer?

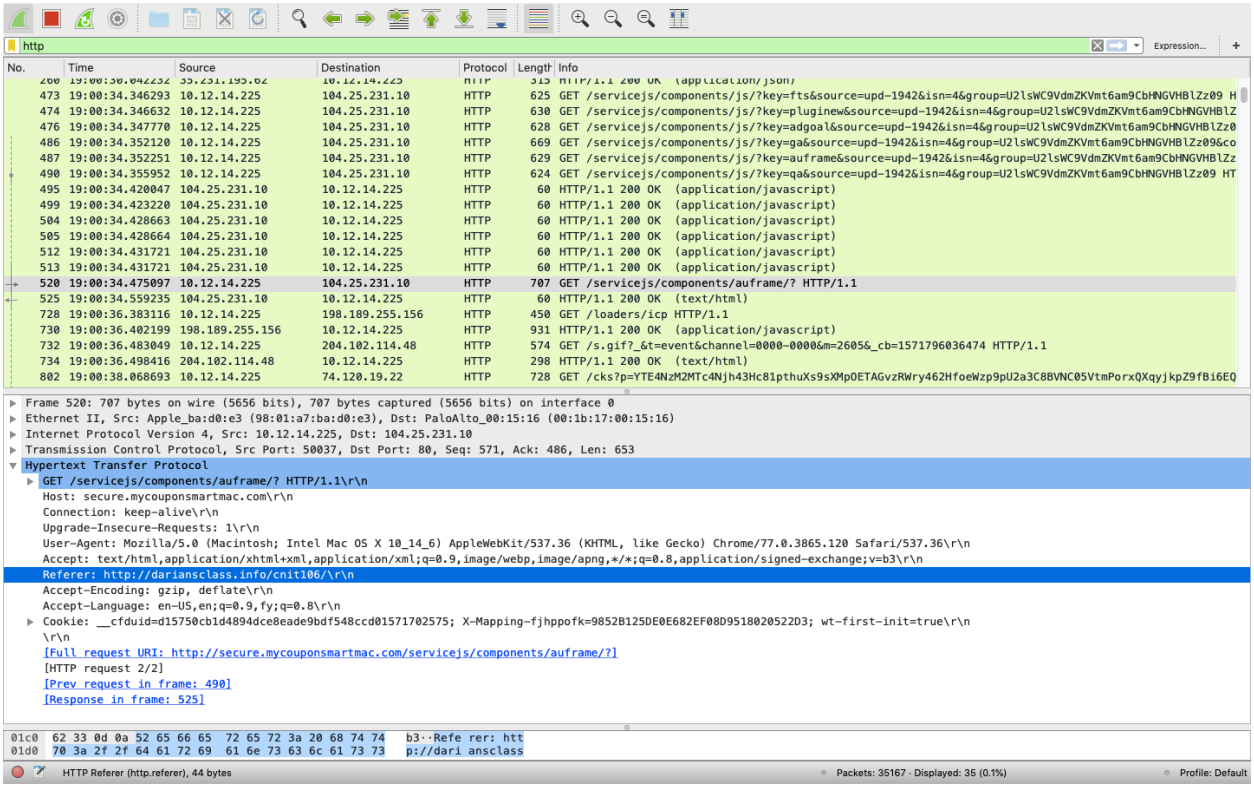
http://gaia.cs.umass.edu/

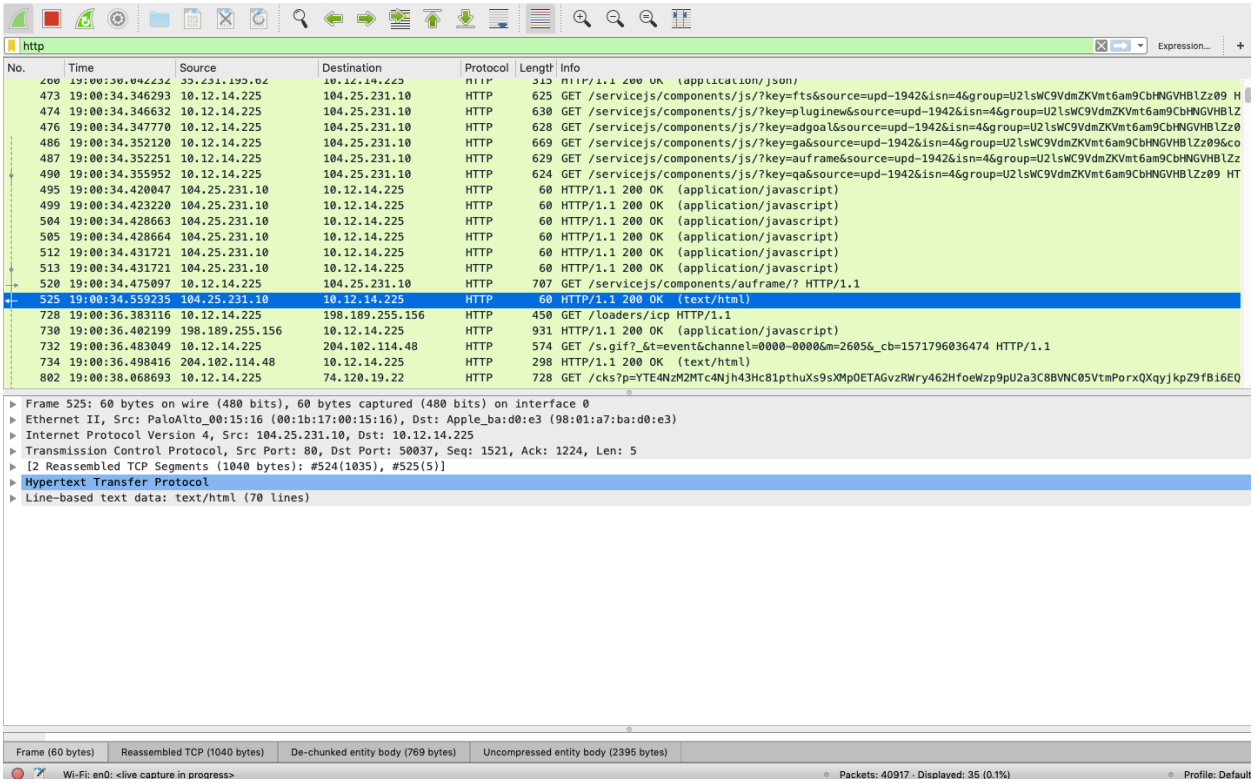
GET_HTTP Messages:
- Source Address: 10.12.14.225 - From computer
- Destination Address: 104.25.230.10 - To gaia.cs.umass.edu

4. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the "Selected Packet Only" and "Print as displayed" radial buttons, and then click OK.




▶ Frame 525: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▶ Ethernet II, Src: PaloAlto_00:15:16 (00:1b:17:00:15:16), Dst: Apple_ba:d0:e3 (98:01:a7:ba:d0:e3)
▶ Internet Protocol Version 4, Src: 104.25.231.10, Dst: 10.12.14.225
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 50037, Seq: 1521, Ack: 1224, Len: 5
▶ [2 Reassembled TCP Segments (1040 bytes): #524(1035), #525(5)]
▼ Hypertext Transfer Protocol
▼ HTTP/1.1 200 OK\r\n
▶ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Wed, 23 Oct 2019 02:00:34 GMT\r\n
Content-Type: text/html\r\n
Transfer-Encoding: chunked\r\n
Connection: keep-alive\r\n
X-Powered-By: PHP/5.5.38\r\n
CF-Cache-Status: DYNAMIC\r\n
Server: cloudflare\r\n
CF-RAY: 52a01e3f8cf3933a-SJC\r\n
Content-Encoding: gzip\r\n
\r\n
[HTTP response 2/2]
[Time since request: 0.084138000 seconds]
[Prev request in frame: 490]
[Prev response in frame: 513]
[Request in frame: 520]
[Request URI: http://secure.mycouponsmartmac.com/servicejs/components/auframe/?]
▶ HTTP chunked response
Content-encoded entity body (gzip): 769 bytes -> 2395 bytes
File Data: 2395 bytes
▶ Line-based text data: text/html (70 lines)
0000 98 01 a7 ba d0 e3 00 1b 17 00 15 16 08 00 45 02
0010 00 2d 7a 98 40 00 37 06 61 20 68 19 e7 0a 0a 0c
0020 0e e1 00 50 c3 75 20 ef 42 54 be 3c fe 57 50 18
0030 00 1f 1f e0 00 00 30 0d 0a 0d 0a 00
Frame (60 bytes)
Reassembled TCP (1040 bytes)
De-chunked entity body (769 bytes)
Uncompressed entity body (2395 bytes)
No.: 525 · Time: 19:00:34.559235 · Source: 104.25.231.10 · Destination: 10.12.14.225 · Protocol: HTTP · Length: 60 · Info: HTTP/1.1 200 OK (text/html)
Help
Close


http
Expression...
No. Time Source Destination Protocol Length Info
473 19:00:34.346293 10.12.14.225 104.25.231.10 HTTP 625 GET /servicejs/components/js/?key=fts&source=upd-1942&isn=4&group=U2lsWC9VdmZKVmt6am9CbHNGVHBlZz09 H
474 19:00:34.346632 10.12.14.225 104.25.231.10 HTTP 630 GET /servicejs/components/js/?key=pluginew&source=upd-1942&isn=4&group=U2lsWC9VdmZKVmt6am9CbHNGVHBlZ
476 19:00:34.347770 10.12.14.225 104.25.231.10 HTTP 628 GET /servicejs/components/js/?key=adgoal&source=upd-1942&isn=4&group=U2lsWC9VdmZKVmt6am9CbHNGVHBlZz0
486 19:00:34.352120 10.12.14.225 104.25.231.10 HTTP 669 GET /servicejs/components/js/?key=ga&source=upd-1942&isn=4&group=U2lsWC9VdmZKVmt6am9CbHNGVHBlZz09&co
487 19:00:34.352251 10.12.14.225 104.25.231.10 HTTP 629 GET /servicejs/components/js/?key=auframe&source=upd-1942&isn=4&group=U2lsWC9VdmZKVmt6am9CbHNGVHBlZz
490 19:00:34.355952 10.12.14.225 104.25.231.10 HTTP 624 GET /servicejs/components/js/?key=qa&source=upd-1942&isn=4&group=U2lsWC9VdmZKVmt6am9CbHNGVHBlZz09 HT
495 19:00:34.420047 104.25.231.10 10.12.14.225 HTTP 60 HTTP/1.1 200 OK (application/javascript)
499 19:00:34.423220 104.25.231.10 10.12.14.225 HTTP 60 HTTP/1.1 200 OK (application/javascript)
504 19:00:34.428663 104.25.231.10 10.12.14.225 HTTP 60 HTTP/1.1 200 OK (application/javascript)
505 19:00:34.428664 104.25.231.10 10.12.14.225 HTTP 60 HTTP/1.1 200 OK (application/javascript)
512 19:00:34.431721 104.25.231.10 10.12.14.225 HTTP 60 HTTP/1.1 200 OK (application/javascript)
513 19:00:34.431721 104.25.231.10 10.12.14.225 HTTP 60 HTTP/1.1 200 OK (application/javascript)
520 19:00:34.475097 10.12.14.225 104.25.231.10 HTTP 707 GET /servicejs/components/auframe/? HTTP/1.1
525 19:00:34.559235 104.25.231.10 10.12.14.225 HTTP 60 HTTP/1.1 200 OK (text/html)
728 19:00:36.383116 10.12.14.225 198.189.255.156 HTTP 450 GET /loaders/icp HTTP/1.1
730 19:00:36.402199 198.189.255.156 10.12.14.225 HTTP 931 HTTP/1.1 200 OK (application/javascript)
732 19:00:36.483049 10.12.14.225 204.102.114.48 HTTP 574 GET /s.gif?_&t=event&channel=0000-0000&m=2605&_cb=1571796036474 HTTP/1.1
734 19:00:36.498416 204.102.114.48 10.12.14.225 HTTP 298 HTTP/1.1 200 OK (text/html)
802 19:00:38.068693 10.12.14.225 74.120.19.22 HTTP 728 GET /cks?p=YTE4NzM2MTc4Njh43Hc81pthuXs9sXMpOETAGvzRWry462HfoeWzp9pU2a3C8BVNC05VtmPorxQXqyjkpZ9fBi6EQ
▶ Frame 520: 707 bytes on wire (5656 bits), 707 bytes captured (5656 bits) on interface 0
▶ Ethernet II, Src: Apple_ba:d0:e3 (98:01:a7:ba:d0:e3), Dst: PaloAlto_00:15:16 (00:1b:17:00:15:16)
▶ Internet Protocol Version 4, Src: 10.12.14.225, Dst: 104.25.231.10
▶ Transmission Control Protocol, Src Port: 50037, Dst Port: 80, Seq: 571, Ack: 486, Len: 653
▼ Hypertext Transfer Protocol
▶ GET /servicejs/components/auframe/? HTTP/1.1\r\n
Host: secure.mycouponsmartmac.com\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.120 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
Referer: http://dariansclass.info/cnit106/\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9,fy;q=0.8\r\n
▶ Cookie: __cfduid=d15750cb1d4894dce8eade9bdf548ccd01571702575; X-Mapping-fjhppofk=9852B125DE0E682EF08D9518020522D3; wt-first-init=true\r\n
\r\n
[Full request URI: http://secure.mycouponsmartmac.com/servicejs/components/auframe/?]
[HTTP request 2/2]
[Prev request in frame: 490]
[Response in frame: 525]
01c0 62 33 0d 0a 52 65 66 65 72 65 72 3a 20 68 74 74 b3··Refe rer: htt
01d0 70 3a 2f 2f 64 61 72 69 61 6e 73 63 6c 61 73 73 p://dari ansclass
HTTP Referer (http.referer), 44 bytes
Packets: 35167 · Displayed: 35 (0.1%)
Profile: Default


http
Expression...
No. Time Source Destination Protocol Length Info
473 19:00:34.346293 10.12.14.225 104.25.231.10 HTTP 625 GET /servicejs/components/js/?key=fts&source=upd-1942&isn=4&group=U2lsWC9VdmZKVmt6am9CbHNGVHBlZz09 H
474 19:00:34.346632 10.12.14.225 104.25.231.10 HTTP 630 GET /servicejs/components/js/?key=pluginew&source=upd-1942&isn=4&group=U2lsWC9VdmZKVmt6am9CbHNGVHBlZ
476 19:00:34.347770 10.12.14.225 104.25.231.10 HTTP 628 GET /servicejs/components/js/?key=adgoal&source=upd-1942&isn=4&group=U2lsWC9VdmZKVmt6am9CbHNGVHBlZz0
486 19:00:34.352120 10.12.14.225 104.25.231.10 HTTP 669 GET /servicejs/components/js/?key=ga&source=upd-1942&isn=4&group=U2lsWC9VdmZKVmt6am9CbHNGVHBlZz09&co
487 19:00:34.352251 10.12.14.225 104.25.231.10 HTTP 629 GET /servicejs/components/js/?key=auframe&source=upd-1942&isn=4&group=U2lsWC9VdmZKVmt6am9CbHNGVHBlZz
490 19:00:34.355952 10.12.14.225 104.25.231.10 HTTP 624 GET /servicejs/components/js/?key=qa&source=upd-1942&isn=4&group=U2lsWC9VdmZKVmt6am9CbHNGVHBlZz09 HT
495 19:00:34.420047 104.25.231.10 10.12.14.225 HTTP 60 HTTP/1.1 200 OK (application/javascript)
499 19:00:34.423220 104.25.231.10 10.12.14.225 HTTP 60 HTTP/1.1 200 OK (application/javascript)
504 19:00:34.428663 104.25.231.10 10.12.14.225 HTTP 60 HTTP/1.1 200 OK (application/javascript)
505 19:00:34.428664 104.25.231.10 10.12.14.225 HTTP 60 HTTP/1.1 200 OK (application/javascript)
512 19:00:34.431721 104.25.231.10 10.12.14.225 HTTP 60 HTTP/1.1 200 OK (application/javascript)
513 19:00:34.431721 104.25.231.10 10.12.14.225 HTTP 60 HTTP/1.1 200 OK (application/javascript)
520 19:00:34.475097 10.12.14.225 104.25.231.10 HTTP 707 GET /servicejs/components/auframe/? HTTP/1.1
525 19:00:34.559235 104.25.231.10 10.12.14.225 HTTP 60 HTTP/1.1 200 OK (text/html)
728 19:00:36.383116 10.12.14.225 198.189.255.156 HTTP 450 GET /loaders/icp HTTP/1.1
730 19:00:36.402199 198.189.255.156 10.12.14.225 HTTP 931 HTTP/1.1 200 OK (application/javascript)
732 19:00:36.483049 10.12.14.225 204.102.114.48 HTTP 574 GET /s.gif?_&t=event&channel=0000-0000&m=2605&_cb=1571796036474 HTTP/1.1
734 19:00:36.498416 204.102.114.48 10.12.14.225 HTTP 298 HTTP/1.1 200 OK (text/html)
802 19:00:38.068693 10.12.14.225 74.120.19.22 HTTP 728 GET /cks?p=YTE4NzM2MTc4Njh43Hc81pthuXs9sXMpOETAGvzRWry462HfoeWzp9pU2a3C8BVNC05VtmPorxQXqyjkpZ9fBi6EQ
Frame 525: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: PaloAlto_00:15:16 (00:1b:17:00:15:16), Dst: Apple_ba:d0:e3 (98:01:a7:ba:d0:e3)
Internet Protocol Version 4, Src: 104.25.231.10, Dst: 10.12.14.225
Transmission Control Protocol, Src Port: 80, Dst Port: 50037, Seq: 1521, Ack: 1224, Len: 5
[2 Reassembled TCP Segments (1040 bytes): #524(1035), #525(5)]
Hypertext Transfer Protocol
Line-based text data: text/html (70 lines)
Frame (60 bytes)
Reassembled TCP (1040 bytes)
De-chunked entity body (769 bytes)
Uncompressed entity body (2395 bytes)
Wi-Fi: en0: <live capture in progress>
Packets: 40917 · Displayed: 35 (0.1%)
Profile: Default