

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.

The image shows a Wireshark packet capture window. The top pane displays the packet list, with packet 520 selected. The middle pane shows the details of the selected packet, which is an HTTP GET request. The bottom pane shows the raw packet data in hexadecimal and ASCII. The details pane is expanded to show the Hypertext Transfer Protocol section, which includes the request method (GET), request URI (/servicejs/components/auframe/? HTTP/1.1), request version (HTTP/1.1), host (secure.mycouponsmartmac.com), connection (keep-alive), upgrade-insecure-requests (1), 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), accept (text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3), referer (http://darjansclass.info/cnit106/), accept-encoding (gzip, deflate), accept-language (en-US,en;q=0.9,fy;q=0.8), and cookies (cfduid=d15750cb1d4894dce8eade9bdf548ccd01571702575; X-Mapping-fjhppo=9852B125DE0E682EF080951802052203; wt-first-init=true).

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
[Expert Info (Chat/Sequence): GET /servicejs/components/auframe/? HTTP/1.1
Request Method: GET
Request URI: /servicejs/components/auframe/?
Request Version: HTTP/1.1
Host: secure.mycouponsmartmac.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
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
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://darjansclass.info/cnit106/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,fy;q=0.8
Cookie: cfduid=d15750cb1d4894dce8eade9bdf548ccd01571702575; X-Mapping-fjhppo=9852B125DE0E682EF080951802052203; wt-first-init=true
[Full request URI: http://secure.mycouponsmartmac.com/servicejs/components/auframe/?]
[HTTP request 2/2]
[Prev request in frame: 490]
[Response in frame: 525]

0160 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c n/xtml+ xml,appl
0170 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e ication/ xml;q=0.
0180 39 2c 69 6d 61 67 65 2f 77 65 62 70 2c 69 6d 61 9,image/ webp,ima
0190 67 65 2f 61 70 6e 67 2c 2a 2f 2a 3b 71 3d 30 2e ge/apng, /*;q=0.
01a0 38 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 73 69 8,applic ation/si
01b0 67 6e 65 64 2d 65 78 63 68 61 6e 67 65 3b 76 3d gned-exc hange;v=
01c0 62 33 0d 0a 52 65 66 65 72 65 72 3a 20 68 74 74 b3-Refere r: htt
01d0 70 3a 2f 2f 64 61 72 69 61 6e 73 63 6c 61 73 73 p://dari ansclass
01e0 2e 69 6e 66 6f 2f 63 6e 69 74 31 30 36 2f 0d 0a .info/cn it106/..
01f0 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a Accept-E ncoding:
0200 28 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a gzip, d eflate..
0210 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a Accept-L anguage:
0220 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 39 2c en-US, e n;q=0.9,
0230 66 79 3b 71 3d 30 2e 38 0d 0a 43 6f 6f 6b 69 65 fy;q=0.8 ..Cookie
0240 3a 20 5f 5f 63 66 64 75 69 64 3d 64 31 35 37 35 : cfdu id=d1575
0250 30 63 62 31 64 34 38 39 34 64 63 65 38 65 61 64 0cb1d489 4dce8ead
0260 65 39 62 64 66 35 34 38 63 63 64 30 31 35 37 31 e9bd548 ccd01571
0270 37 30 32 35 37 35 3b 20 58 2d 4d 61 70 70 69 6e 702575; X-Mappin
0280 67 2d 66 6a 68 70 70 6f 66 6b 3d 39 38 35 32 42 g-fjhppo fk=9852B
0290 31 32 35 44 45 30 45 36 38 32 45 46 30 38 44 39 125DE0E6 82EF0809
02a0 35 31 38 30 32 30 35 32 32 44 33 3b 20 77 74 2d 51802052 203; wt-
02b0 66 69 72 73 74 2d 69 6e 69 74 3d 74 72 75 65 0d first-in it=true
02c0 0a 0d 0a

No.: 520 - Time: 19:00:34.475097 - Source: 10.12.14.225 - Destination: 104.25.231.10 - Protocol: HTTP - Length: 707 - Info: GET /servicejs/components/auframe/? HTTP/1.1

Help Close

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: 0.004138000 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 00 00 45 02E:
0010 00 2d 7a 98 40 00 37 06 61 20 68 19 e7 0a 0a 0c ...z.@7: a h:..
0020 0e e1 00 50 c3 75 20 ef 42 54 be 3c fe 57 50 18 ...P.u BT< WP..
0030 00 1f 1f e0 00 00 3d 0d 0a 0d 0a 000:.....

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

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=46group=U2lsWC9VdmZKvmt6am9CbHNGVHB1Zz09 H
474	19:00:34.346632	10.12.14.225	104.25.231.10	HTTP	630	GET /servicejs/components/js/?key=plugin&source=upd-1942&isn=46group=U2lsWC9VdmZKvmt6am9CbHNGVHB1Z
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=46group=U2lsWC9VdmZKvmt6am9CbHNGVHB1Zz0
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=46group=U2lsWC9VdmZKvmt6am9CbHNGVHB1Zz096co
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=46group=U2lsWC9VdmZKvmt6am9CbHNGVHB1Zz
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=46group=U2lsWC9VdmZKvmt6am9CbHNGVHB1Zz09 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?_dt=event&channel=0000-0000&m=26056_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?ip=YtE4nZM2MTc4Njh43Hc81ptHuXs9sXHp0ETAGvzRWry462HfoeWzp9u2a3C8BVNC05VtmPorxQXqykpZ9fB16EQ

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/cnt186/\r\n

Accept-Encoding: gzip, deflate\r\n

Accept-Language: en-US,en;q=0.9,fy;q=0.8\r\n

Cookie: _cfduid=d15758cbid4894dce8eade9bdf548ccd01571702575; X-Mapping-fjhpfok=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

Wi-Fi: en0: <live capture in progress>

Packets: 40917 - Displayed: 35 (0.1%)

Profile: Default

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=plugin&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=U2lsWC9VdmZKVmt6am9CbHNGVHBLZz096co
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	190.189.255.156	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?_dt=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=YTE4NzMTc4Njh43Hc81pthuXs9sXmp0ETAGvzRmry462HfoeWzp9pU2a3C8BVNC05VtmPorxQXqyJkpZ9F816EQ

▶ 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)