

Lab Exercise

- How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill of Rights?

The top screenshot shows the Google Chrome settings page under Privacy and security, specifically the 'Delete browsing data' section. It displays options for deleting browsing history, cookies, and cached images. The bottom screenshot shows a Wireshark capture of an HTTP session between two hosts. The GET request for the Bill of Rights is highlighted in blue, showing its details: Source 192.168.100.162, Destination 128.119.245.12, Protocol HTTP, Length 492, and Info GET /wir... file3.html HTTP/1.1. The response packet (packet #542) shows a 200 OK status code and text containing the Bill of Rights.

- Answer:**

- 1 HTTP GET request was sent.**
- The packet containing the GET request is packet #536.**

- Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

Answer:

- The packet containing the status code and phrase is packet #542.**

- What is the status code and phrase in the response?

- Answer:**

- Status Code: 200 OK**
- This indicates the request was successful, and the file is being sent.**

- How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

No.	Time	Source	Destination	Protocol	Length	Info
527	41.717342	2a03:2880:f267:c5:face...	2400:0:0:0:388d:3:500:0:4e...	TCP	347	5222 → 53455 [PSH, ACK] Seq=6087 Ack=479 Win=1083 Len=201 TStamp=2073773064 TSect=4257850732 [TCP PDU reassembled in 527]
528	41.717345	2a03:2880:f267:c5:face...	2406:d0:0:aaa:c300:64e...	TCP	193	5222 → 53455 [PSH, ACK] Seq=6348 Ack=479 Win=1083 Len=187 TStamp=2073775651 TSect=4257850732 [TCP PDU reassembled in 528]
529	41.717758	2a06:d0:0:aaa:c300:64e...	2a03:2880:f267:c5:face...	TCP	86	53455 → 5222 [ACK] Seq=479 Ack=6455 Win=2042 Len=0 TStamp=4257850949 TSect=2073775651
530	41.734244	51.159.221.14	192.168.100.162	TLSv1.2	252	Application Data
531	41.734354	192.168.100.162	51.159.221.14	TCP	66	50095 → 18333 [ACK] Seq=6462 Ack=3837 Win=2045 Len=0 TStamp=433707159 TSect=708459150
532	41.736142	192.168.100.162	51.159.221.14	TLSv1.2	123	Application Data
533	41.736174	51.159.221.14	192.168.100.162	TCP	66	18333 → 50095 [ACK] Seq=3837 Ack=6519 Win=581 Len=0 TStamp=708459306 TSect=433707161
534	41.736196	128.119.245.12	192.168.100.162	TCP	74	88 → 55241 [SYN, ACK] Seq=1 Ack=1 Win=20968 Len=0 MSS=1412 SACN_PERN TStamp=1933658279 TSect=224381389 WS=128
535	41.737696	192.168.100.162	128.119.245.12	TCP	66	55241 → 88 [ACK] Seq=1 Ack=1 Win=31384 Len=0 TStamp=224381610 TSect=1933658279
536	41.737613	192.168.100.162	128.119.245.12	HTTP	403	GET /4.4.1/ HTTP/1.1
537	42.209618	128.119.245.12	192.168.100.162	TCP	66	88 → 55241 [ACK] Seq=1 Ack=427 Win=30800 Len=0 TStamp=1933658501 TSect=224381612
538	42.209621	128.119.245.12	192.168.100.162	TCP	1466	88 → 55241 [ACK] Seq=1 Ack=427 Win=30800 Len=1400 TStamp=1933658501 TSect=224381612 [TCP PDU reassembled in 542]
539	42.209625	128.119.245.12	192.168.100.162	TCP	1466	88 → 55241 [ACK] Seq=1401 Ack=427 Win=30800 Len=1400 TStamp=1933658501 TSect=224381612 [TCP PDU reassembled in 542]
540	42.209627	128.119.245.12	192.168.100.162	TCP	1466	88 → 55241 [ACK] Seq=2801 Ack=427 Win=30800 Len=1400 TStamp=1933658501 TSect=224381612 [TCP PDU reassembled in 542]
541	42.297884	192.168.100.162	128.119.245.12	TCP	66	55241 → 88 [ACK] Seq=427 Ack=4201 Win=31072 Len=0 TStamp=224381982 TSect=1933658501
542	42.298987	128.119.245.12	192.168.100.162	HTTP	727	HTTP/1.1 200 OK (text/html)
543	42.298333	192.168.100.162	128.119.245.12	TCP	66	55241 → 88 [ACK] Seq=427 Ack=4862 Win=130368 Len=0 TStamp=224381983 TSect=1933658501
544	43.767847	192.168.100.162	51.159.221.44	TCP	54	50063 → 19317 [ACK] Seq=1 Ack=1 Win=2048 Len=0
545	43.769257	51.159.221.44	192.168.100.162	TCP	66	[TCP ACKED Unseen segment] 19317 → 50063 [ACK] Seq=1 Ack=2 Win=581 Len=0 TStamp=2760071229 TSect=4171646460
546	45.266810	fe80::18e2:6dde:336a:3...	fe80::1	ICMPv6	86	Neighbor Solicitation for fe80::1 from fa:f5:2b:68:27:0a
547	45.279418	fe80::1	fe80::18e2:6dde:336a:3...	ICMPv6	78	Neighbor Advertisement fe80::1 (rtr, sol)
548	47.222321	128.119.245.12	192.168.100.162	TCP	66	88 → 55241 [FIN, ACK] Seq=4862 Ack=427 Win=30800 Len=0 TStamp=1933663586 TSect=224381983
549	47.222602	192.168.100.162	128.119.245.12	TCP	66	55241 → 88 [ACK] Seq=427 Ack=4863 Win=31072 Len=0 TStamp=224386908 TSect=1933663586
550	47.222797	192.168.100.162	128.119.245.12	TCP	66	55241 → 88 [FIN, ACK] Seq=427 Ack=4863 Win=31072 Len=0 TStamp=224386908 TSect=1933663586
551	47.528223	128.119.245.12	192.168.100.162	TCP	66	88 → 55241 [ACK] Seq=4863 Ack=428 Win=30800 Len=0 TStamp=1933663799 TSect=224386908
552	48.114663	192.168.100.162	51.159.221.14	TLSv1.2	326	Application Data
						0020 64 a2 00 50 5d c9 e0 73 0030 00 eb e7 ce 00 00 01 01 0040 c8 ac 6d 6f 6e 20 6e 0050 3e 3c 70 3e 3c 61 20 6e 0060 2f 73 74 72 6f 6e 00 7e 0070 64 6d 6f 6e 20 61 6e 49 0080 2f 73 74 72 6f 6e 37 3e 0090 3e 3c 2f 70 3e 3c 70 3e 00a0 65 20 62 61 69 6c 20 73 00b0 28 62 65 20 72 65 71 75 00c0 72 75 65 6c 20 61 6e 64 00d0 73 69 6d 70 6f 73 65 00e0 72 75 65 6c 20 61 6e 64 00f0 28 70 75 6e 69 73 68 6d 0100 6c 69 63 74 65 64 2e 0a 0110 3c 61 20 6e 61 65 6d 3d 0120 6f 6e 67 3e 3c 68 63 3e

- 4 data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights.

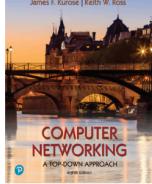
Lab Exercise

- How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?



Pearson

This little HTML file is being served by gaia.cs.umass.edu. It contains two embedded images. The image above, also served from the gaia.cs.umass.edu web site, is the logo of our publisher, Pearson. The image of our 8th edition book cover below is stored at, and served from, a WWW server kurose.csplash.net in France:



And while we have your attention, you might want to take time to check out the available open resources for this book at http://gaia.cs.umass.edu/kurose_ross.

No.	Time	Source	Destination	Protocol	Length	Info
119	24.189187	192.168.100.162	128.119.245.12	HTTP	492	GET /wreshark-labs/HTTP-wreshark-file4.html HTTP/1.1
122	24.189188	128.119.245.12	192.168.100.162	HTTP	1367	HTTP/1.1 200 OK (text/html)
123	24.189189	192.168.100.162	128.119.245.12	HTTP	571	HTTP/1.1 200 OK (image/png)
133	24.619243	128.119.245.12	192.168.100.162	HTTP	877	HTTP/1.1 200 OK (PNG)
146	25.616293	192.168.100.162	128.79.137.154	HTTP	537	GET /8E_cover_small.jpg HTTP/1.1
149	25.949694	128.79.137.154	192.168.100.162	HTTP	237	HTTP/1.1 302 Moved Permanently
						> Frame 119: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface en0, id 0 > Ethernet II, Src: HuaweiTech_40:1e:be (34:b3:54:40:1e:be), Dst: fa:f5:2b:68:27:0a (fa:f5:2b:68:27:0a) > Internet Protocol Version 4, Src: 192.168.100.162, Dst: 128.119.245.12 > Transmission Control Protocol, Src Port: 80, Dst Port: 5142, Seq: 4201, Ack: 427, Len: 661 > Hypertext Transfer Protocol > Request Method: GET > Request URI: /wreshark-labs/HTTP-wreshark-file4.html > Host: gaia.cs.umass.edu\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X_10_7_) AppleWebKit/655.15 (KHTML, like Gecko) Version/10.1.1 Safari/655.1.15\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\nAccept-Language: en-us,en;q=0.8;q=0.7\nAccept-Encoding: gzip, deflate\nAccept-Charset: utf-8\nConnection: keep-alive\n\n<html>\n<head>\n<title>HTTP-wreshark-labs</title>\n</head>\n<body>\n<h1>HTTP-wreshark-labs</h1>\n<pre>GET /8E_cover_small.jpg HTTP/1.1\nHost: gaia.cs.umass.edu\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X_10_7_) AppleWebKit/655.15 (KHTML, like Gecko) Version/10.1.1 Safari/655.1.15\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\nAccept-Language: en-us,en;q=0.8;q=0.7\nAccept-Encoding: gzip, deflate\nAccept-Charset: utf-8\nConnection: keep-alive\n\n</pre>\n\n</body>\n</html>\n\n<pre>HTTP/1.1 200 OK\nContent-Type: image/png\nContent-Length: 3936\n\n[Binary data]\n</pre>

1. **Packet 119:**
 - Destination IP: 128.119.245.12 (gaia.cs.umass.edu).
2. **Packet 124:**
 - Destination IP: 128.119.245.12 (gaia.cs.umass.edu).
3. **Packet 146:**
 - Destination IP: 178.79.137.164 (a different server).

2. **Total GET requests: 3.**

3. The requests were sent to:

1. 128.119.245.12 (for the HTML file and pearson.png).
2. 178.79.137.164 (for 85_cover_small.jpg).

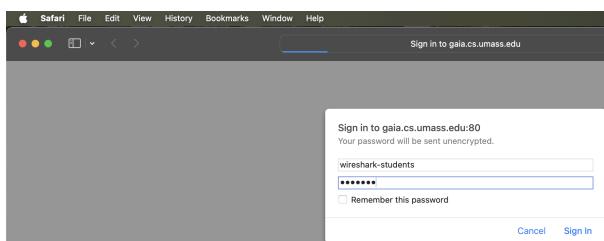
2. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

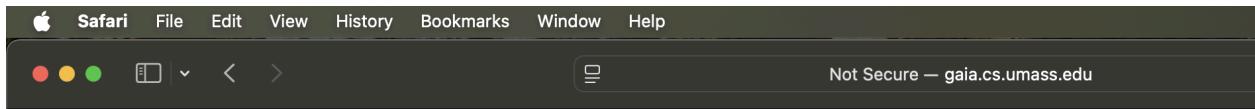
No.	Time	Source	Destination	Protocol	Length	Info
124	24.335015	192.168.100.162	128.119.245.12	HTTP	570	GET /pearson.png HTTP/1.1
125	24.336876	fe80::18e2:6dde:336a:3...	fe80::1	DNS	97	Standard query 0x1e8d HTTPS kurose.csslash.net
126	24.337080	fe80::18e2:6dde:336a:3...	fe80::1	DNS	97	Standard query 0x5085 AAAA kurose.csslash.net
127	24.337219	fe80::18e2:6dde:336a:3...	fe80::1	DNS	97	Standard query 0x4680 A kurose.csslash.net
128	24.340578	128.119.245.12	192.168.100.162	TCP	74	80 → 55243 [SYN, ACK] Seq=0 Ack=1 Win=28968 Len=0 MSS=1412 SACK_PERM TStamp=1935406768 TSect=3308923991 WS=128
129	24.340958	192.168.100.162	128.119.245.12	TCP	66	55243 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TStamp=3308924220 TSect=1935406768
130	24.610788	128.119.245.12	192.168.100.162	TCP	1466	80 → 55242 [ACK] Seq=1302 Ack=93 Win=31104 Len=1408 TStamp=1935406982 TSect=2759558586 [TCP PDU reassembled in 133]
131	24.610793	128.119.245.12	192.168.100.162	TCP	1466	80 → 55242 [ACK] Seq=2702 Ack=93 Win=31104 Len=1408 TStamp=1935406982 TSect=2759558586 [TCP PDU reassembled in 133]
132	24.611684	192.168.100.162	128.119.245.12	TCP	66	55242 → 80 [ACK] Seq=931 Ack=4108 Win=131072 Len=0 TStamp=2759558862 TSect=1935406982
133	24.619243	128.119.245.12	192.168.100.162	HTTP	877	HTTP/1.1 200 OK (PNG)
134	24.619467	192.168.100.162	128.119.245.12	TCP	66	55242 → 80 [ACK] Seq=931 Ack=4913 Win=130240 Len=0 TStamp=2759558871 TSect=1935406982
135	25.126466	fe80::18e2:6dde:336a:3...	fe80::1	DNS	459	Standard query response 0x5085 AAAA kurose.csslash.net CNAME csslash.net AAAA 2a01:fe80::f03c:91ff:fe70:4c18 NS ns2...
136	25.126465	fe80::1	fe80::18e2:6dde:336a:3...	DNS	447	Standard query response 0x5085 AAAA kurose.csslash.net CNAME csslash.net A 178.79.137.164 NS ns3.linode.com NS ns2.linode...
137	25.126468	fe80::18e2:6dde:336a:3...	fe80::1	DNS	173	Standard query response 0x4680 A kurose.csslash.net CNAME csslash.net 50A ns1.linode.com
138	25.128521	fe80::18e2:6dde:336a:3...	fe80::1	DNS	98	Standard query 0x45f7 HTTPS csslash.net
139	25.142183	fe80::1	fe80::18e2:6dde:336a:3...	DNS	152	Standard query response 0x45f7 HTTPS csslash.net 50A ns1.linode.com
140	25.145782	2406:0:aaaa:c300:64e:...	2a01:7e00::f03c:91ff:f...	TCP	98	53693 → 80 [SYN, ECE, CMRJ] Seq=0 Win=65535 Len=0 MSS=1412 WS=64 TStamp=1361692204 TSect=0 SACK_PERM
141	25.398889	192.168.100.162	178.79.137.164	TCP	78	55244 → 80 [SYN] Seq=0 Win=65525 Len=0 MSS=1460 WS=64 TStamp=3942286931 TSect=0 SACK_PERM
142	25.419836	7a01:7e00::f03c:91ff:f...	2406:0:aaaa:c300:64e:...	TCP	74	80 → 53693 [RST, ACK] Seq=1 Ack=1 Win=0
143	25.482776	192.168.100.162	51.159.221.14	TCP	54	58284 → 18333 [ACK] Seq=1 Ack=1 Win=2848 Len=0
144	25.613746	178.79.137.164	192.168.100.162	TCP	74	80 → 55244 [SYN, ACK] Seq=0 Ack=1 Win=65168 Len=0 MSS=1412 SACK_PERM TStamp=3906935499 TSect=3942286931 WS=128
145	25.616284	192.168.100.162	178.79.137.164	TCP	66	55244 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TStamp=3942287146 TSect=3906935499
146	25.616293	192.168.100.162	178.79.137.164	HTTP	537	GET /8E_cover_small.jpg HTTP/1.1
147	25.732415	51.159.221.14	192.168.100.162	TCP	66	[TCP ACKed unseen segment] 18333 → 50204 [ACK] Seq=1 Ack=2 Win=6945 Len=0 TStamp=710209143 TSect=1410206613
148	25.934242	178.79.137.164	192.168.100.162	TCP	66	80 → 55244 [ACK] Seq=1 Ack=472 Win=64788 Len=0 TStamp=3906935777 TSect=3942287149
149	25.949694	178.79.137.164	192.168.100.162	HTTP	237	HTTP/1.1 301 Moved Permanently

- In this case, the request for 85_cover_small.jpg starts at **25.616293 seconds**, which is **after** the first image (pearson.png) has finished downloading at **24.619243 seconds**.
- The two image requests do **not overlap** in time.
- This indicates that the images were downloaded **serially** (one after the other).

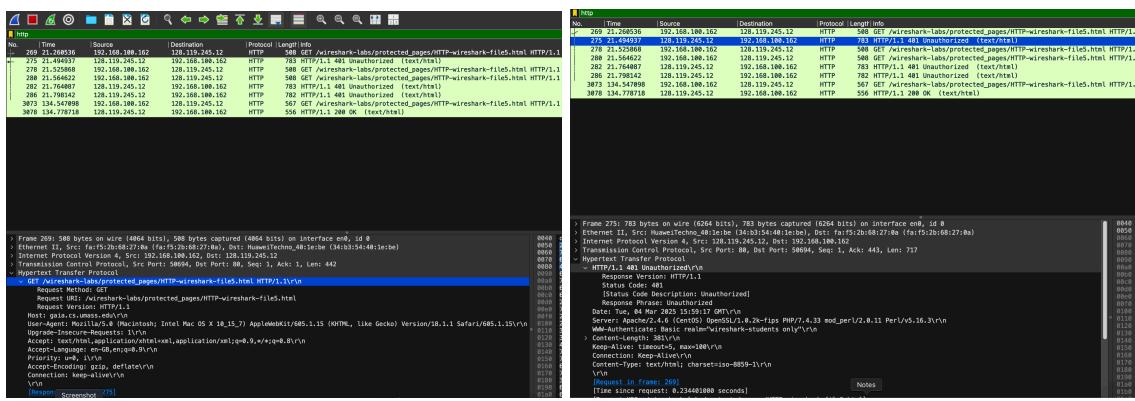
Lab Exercise

1. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?





This page is password protected! If you're seeing this, you've downloaded the page correctly
Congratulations!



Initial HTTP GET Request:

- This is packet #269 in the trace.

the Server's Response:

- for corresponding HTTP response from the server.
- This is packet #275 in the trace.
- The status code and phrase indicate the result of the request.
- For the initial request, the server responds with **401 Unauthorized** because the client has not provided valid credentials.
- The server's response to the initial HTTP GET message is:
 - Status Code: 401 Unauthorized**
 - Phrase: Unauthorized**

- When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

No.	Time	Source	Description	Protocol	Length	Info
269	21.265836	192.158.180.152	192.158.180.152	HTTP	588	GET /wireshark-labs/protected_pages/http-wireshark-files.html HTTP/1.1
275	21.494937	192.158.180.152	192.158.180.152	HTTP	783	HTTP/1.1.1.401 Unauthorized (text/html)
281	21.500000	192.158.180.152	192.158.180.152	HTTP	588	GET /wireshark-labs/protected_pages/http-wireshark-files.html HTTP/1.1
282	21.564682	192.158.180.152	192.158.180.152	HTTP	588	GET /wireshark-labs/protected_pages/http-wireshark-files.html HTTP/1.1
288	21.565000	192.158.180.152	192.158.180.152	HTTP	588	GET /wireshark-labs/protected_pages/http-wireshark-files.html HTTP/1.1
290	21.565000	192.158.180.152	192.158.180.152	HTTP	588	GET /wireshark-labs/protected_pages/http-wireshark-files.html HTTP/1.1
3873	24.547898	192.158.180.152	192.158.180.152	HTTP	567	GET /wireshark-labs/protected_pages/http-wireshark-files.html HTTP/1.1
3878	24.777118	192.158.180.152	192.158.180.152	HTTP	556	HTTP/1.1.200 OK (text/html)

Http	Time	Source	Destination	Protocol	Length	Info
269	21.126.98.170	192.168.190.162	128.119.245.12	HTTP	589	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
275	21.126.98.170	192.168.190.162	128.119.245.12	HTTP	589	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
276	21.126.98.170	192.168.190.162	128.119.245.12	HTTP	589	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
288	21.556462	192.168.190.162	128.119.245.12	HTTP	589	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
289	21.556462	192.168.190.162	128.119.245.12	HTTP	589	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
288	21.798142	192.168.190.162	128.119.245.12	HTTP	783	HTTP/1.1 401 Unauthorized (text/html)
387	21.134.547988	192.168.190.162	128.119.245.12	HTTP	567	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
3910	21.134.71978	192.168.190.162	158.108.198.102	HTTP	556	HTTP/1.1 200 OK (text/html)

No.	Time	Source	Destination	Protocol	Length/Info	
269	21.11.2016 192.168.100.162	128.119.245.12	HTTP	568 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html	HTTP/1.1	
270	21.11.2016 192.168.100.162	128.119.245.12	HTTP	781 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html	HTTP/1.1	
278	21.11.2016 192.168.100.162	128.119.245.12	HTTP	781 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html	HTTP/1.1	
280	21.11.2016 192.168.100.162	128.119.245.12	HTTP	568 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html	HTTP/1.1	
282	21.11.2016 192.168.100.162	128.119.245.12	HTTP	781 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html	HTTP/1.1	
284	21.11.2016 192.168.100.162	128.119.245.12	HTTP	781 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html	HTTP/1.1	
3873	134.547988	192.168.100.162	128.119.245.12	HTTP	567 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html	HTTP/1.1
3878	134.547988	128.119.245.12	HTTP	556 GET / HTTP/1.1.200 OK	(text/html)	

From 3878: 556 bytes on wire (4448 bits), 556 bytes captured (4448 bits) on interface wlo, link layer type Ethernet II, Src: Huwelschen_4c:b1:b0 (34:01:54:4c:b1:b0), Dst: Fa:f5:2b:0d:27:fa (7a:02:5b:0d:27:fa) at 2016-11-21T19:54:45.011Z (0.000000000s ago)
Transmission Control Protocol Src Port: 54608 Dst Port: 54608 Seq: 1 Ack: 562 Len: 498
HyperText Transfer Protocol
Response Version: HTTP/1.1
HTTP/1.1 200 OK
[Status Code Description: OK]
Content-Type: text/html

When the browser sends the HTTP GET message for the next time, the new field

included is:

- **Authorization**
 - **This field contains the Base64-encoded credentials (username and password).**

Lab Exercise

1. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to `gaia.cs.umass.edu`? To answer this question, it's probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the "details of the selected packet header window".

No.	Time	Source	Destination	Protocol	Length	Info
198	5.297257	128.119.245.12	192.168.1.102	TCP	68	80 - 1161 [ACK] Seq=1 Ack=159389 Win=62788 Len=0
199	5.297341	192.168.1.102	128.119.245.12	HTTP	184	POST /ethereal-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
200	5.389471	128.119.245.12	192.168.1.102	TCP	68	80 - 1161 [ACK] Seq=1 Ack=162389 Win=62788 Len=0

> Frame 199: 184 bytes on wire (832 bits), 184 bytes captured (832 bits)
> Ethernet II, Src: ActiontecElc_0a:70:1a (00:0c:9a:0a:70:1a), Dst: LinksysGroup_da:af:73 (00:0e:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 164841, Ack: 1, Len: 50
Source Port: 1161
Destination Port: 80
[Stream index: 0]
> (Conversation completeness: Incomplete, DATA (15))
> (TCP Segment Len: 50)
Sequence Number: 164841 (relative sequence number)
Sequence Number (raw): 232293053
[Next Sequence Number: 164891 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 883061786
@0x1 -> header Length: 20 bytes (5)
@0x1 -> payload Length: 20 bytes (5)
@0x1 -> flags: 0x018 (PSH, ACK)
Window: 17520
[Calculated window size: 17520]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x9f0f (unverified)
[Checksum Status: Unverified]
Urgent Pointer: 0
@0x1 -> payload Length: 20 bytes (5)
> [SACK Block Analysis]
> TCP payload (50 bytes)
TCP segment data (50 bytes)
> [122 Reassembled TCP Segments (164098 bytes): #4(565), #5(1460), #7(1460), #8(1460), #10(1460), #11(1460), #13(147), #18(1460), #19(1460), #20(1460), #21(1460), #22(1460), #23(802), #30(1460), #31(1460), #32(1460), #33(1460), #34(1460),]
> Hypertext Transfer Protocol
> MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "-----265001916915724"

1. The provided trace shows Frame 203, which is an HTTP response from the server (128.119.245.12) to the client (192.168.1.102). The HTTP response has a status code of 200 OK, indicating a successful request.

2. Determine the Client's IP Address and Port:

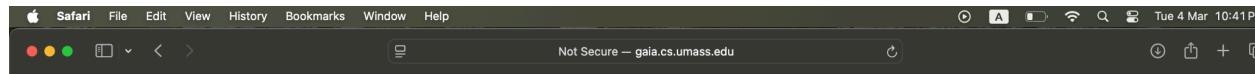
- **The client is the destination of the HTTP response.**
- **Destination IP Address: 192.168.1.102 (client IP).**
- **Destination Port: 1161 (client port).**

2. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

- **The server is the source of the HTTP response.**
- **Source IP Address: 128.119.245.12 (server IP, gaia.cs.umass.edu).**
- **Source Port: 80 (server port, HTTP).**

If you have been able to create your own trace, answer the following question:

3. What is the IP address and TCP port number used by your client computer (source) to transfer the file to `gaia.cs.umass.edu`?



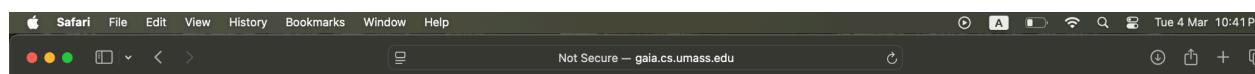
Upload page for TCP Wireshark Lab
Computer Networking: A Top Down Approach, 6th edition
Copyright 2012 J.F. Kurose and K.W. Ross, All Rights Reserved

If you have followed the instructions for the TCP Wireshark Lab, you have already downloaded an ASCII copy of Alice and Wonderland from <http://gaia.cs.umass.edu/wireshark-labs/alice.txt> and you also already have the Wireshark packet sniffer running and capturing packets on your computer.

Click on the Browse button below to select the directory/file name for the copy of `alice.txt` that is stored on your computer.

hello.txt

Once you have selected the file, click on the "Upload alice.txt file" button below. This will cause your browser to send a copy of `alice.txt` over an HTTP connection (using TCP) to the web server at `gaia.cs.umass.edu`. After clicking on the button, wait until a short message is displayed indicating the the upload is complete. Then stop your Wireshark packet sniffer - you're ready to begin analyzing the TCP transfer of `alice.txt` from your computer to `gaia.cs.umass.edu`!!



No.	Time	Source	Destination	Protocol	Length	Info
86	7.057436	192.168.100.162	128.119.245.12	HTTP	491	GET /wireshark-labs/TCP-wireshark-file1.html HTTP/1.1
90	7.380909	128.119.245.12	192.168.100.162	HTTP	860	HTTP/1.1 200 OK (text/html)
+ 2520	137.734656	192.168.100.162	128.119.245.12	HTTP	646	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
- 2523	138.018414	128.119.245.12	192.168.100.162	HTTP	843	HTTP/1.1 200 OK (text/html)

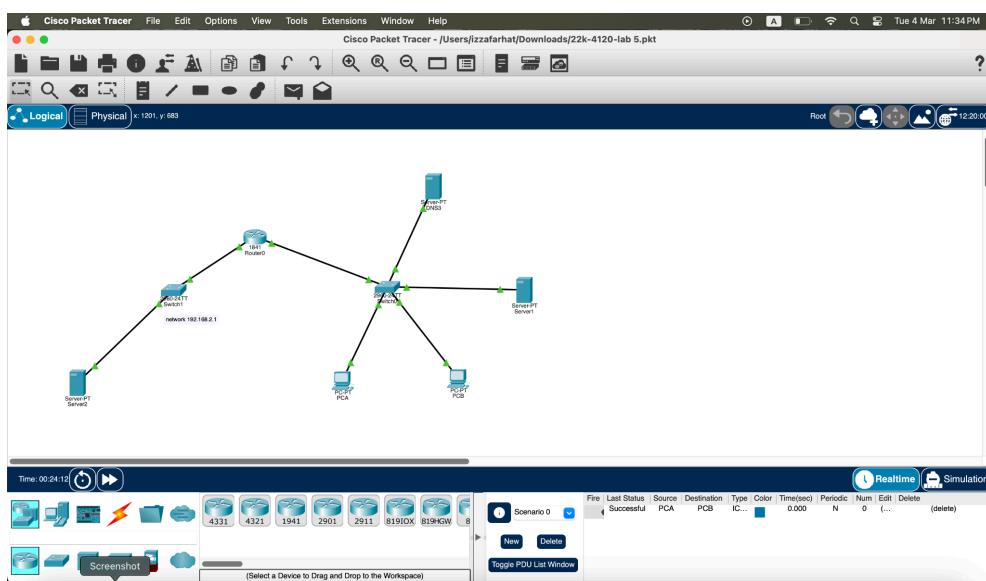
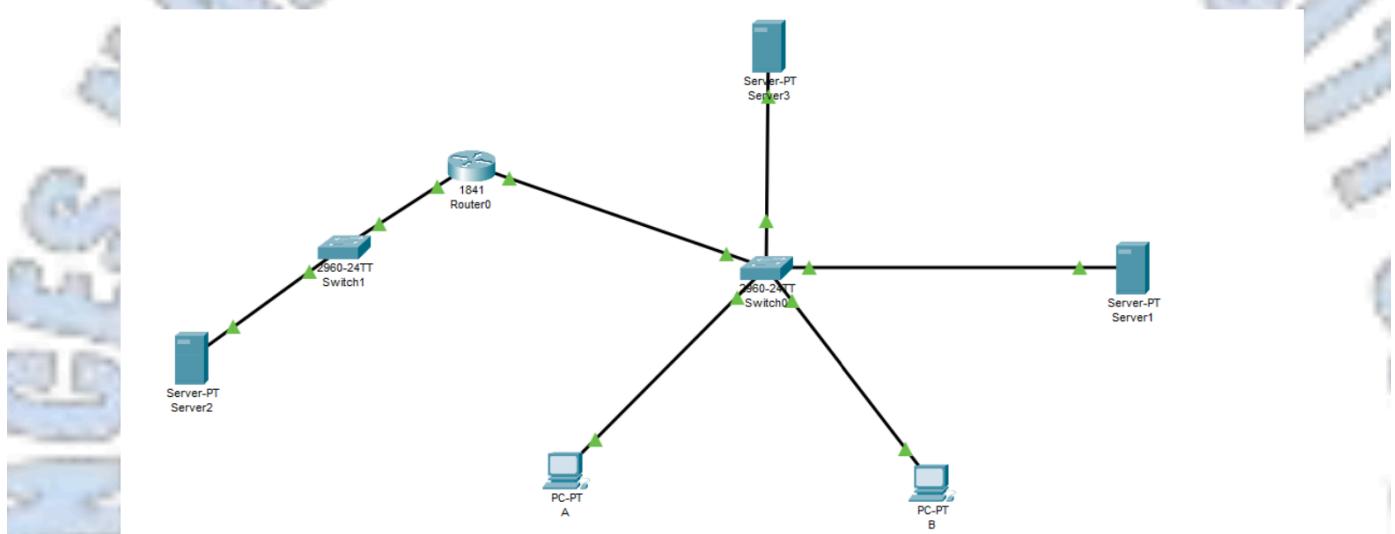
> Frame 2520: 646 bytes on wire (5168 bits), 646 bytes captured (5168 bits) on interface en0, id 0
> Ethernet II, Src: fa:f5:2b:68:27:0a (fa:f5:2b:68:27:0a), Dst: HuaweiTechno_40:1e:be (34:b3:54:40:1e:be)
> Internet Protocol Version 4, Src: 192.168.100.162, Dst: 128.119.245.12
▼ Transmission Control Protocol, Src Port: 50761, Dst Port: 80, Seq: 633, Ack: 1, Len: 580
 Source Port: 50761
 Destination Port: 80
 [Stream index: 17]
 > [Conversation completeness: Complete, WITH_DATA (31)]
 [TCP Segment Len: 580]
 Sequence Number: 633 (relative sequence number)
 Sequence Number (raw): 1725025048
 [Next Sequence Number: 1213 (relative sequence number)]
 Acknowledgment Number: 1 (relative ack number)
 Acknowledgment number (raw): 2785499337
 1000 = Header Length: 32 bytes (8)
 > Flags: 0x018 (PSH, ACK)
 Window: 2056
 [Calculated window size: 131584]
 [Window size scaling factor: 64]
 Checksum: 0xdb40 [unverified]
 [Checksum Status: Unverified]
 Urgent Pointer: 0
 > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
 > [Timestamps]
 > [SEQ/ACK analysis]
 TCP payload (580 bytes)
 TCP segment data (580 bytes)
> [2 Reassembled TCP Segments (1212 bytes): #2519(632), #2520(580)]
> Hypertext Transfer Protocol
> MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "----WebKitFormBoundaryPK2svCtz0UQCmRlr"

- **Source IP Address: 192.168.100.162 (client IP).**
- **Source Port: 50761 (client port).**
- **Destination IP Address: 128.119.245.12 (server IP, gaia.cs.umass.edu).**
- **Destination Port: 80 (HTTP port).**

Lab Exercises

- Let's suppose your organization need to create it's own small server (for provide some services) based network. With below mentioned topology and instructions:

- Configure SMTP (create account with your last name along with last 3 digits roll number) send mail from PC A to PC-B.
- PC A should be configured to have the SMTP account of Server 2 while PC B should be having an account of Server 1.
- Configure FTP server create account with your first name, password with your roll number and filename with your last name (.bin extension) show all connection results. The FTP Server should be established on both Server 2 and Server 3.



Server2

Physical Config Services Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL**
- FTP
- IoT
- VM Management
- Radius EAP

EMAIL

SMTP Service ON OFF

POP3 Service ON OFF

Domain Name: server2.com

User Setup

User	izza	Password	123
izza			

+

Server2

Physical Config Services Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL**
- FTP**
- IoT
- VM Management
- Radius EAP

FTP

Service On Off

User Setup

Username Password
 Write Read Delete Rename List

	Username	Password	Permission
1	cisco	cisco	RWDNL
2	izza	4120	RW

Add Save Remove

Server1

Physical Config Services Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL**
- FTP
- IoT
- VM Management
- Radius EAP

EMAIL

SMTP Service ON OFF

POP3 Service ON OFF

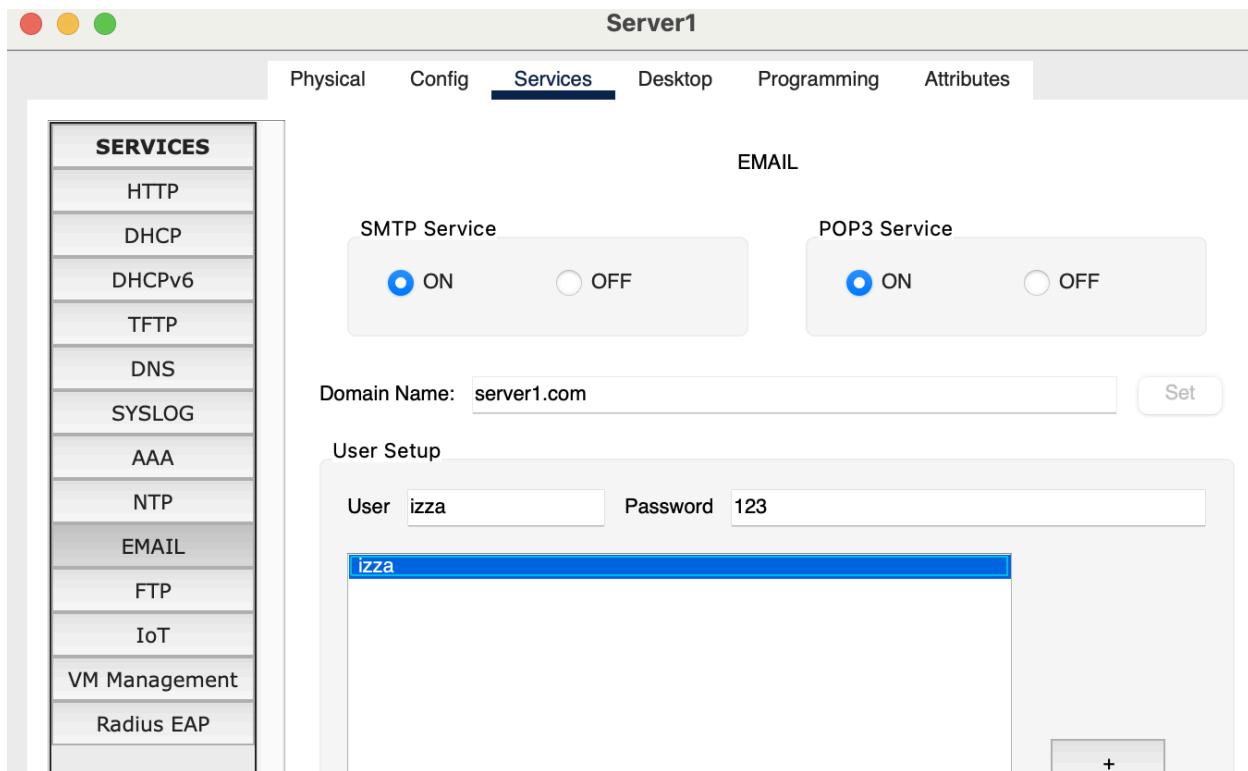
Domain Name: server1.com Set

User Setup

User izza Password 123

izza

+



DNS3

Physical Config Services Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS**
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DNS

DNS Service On Off

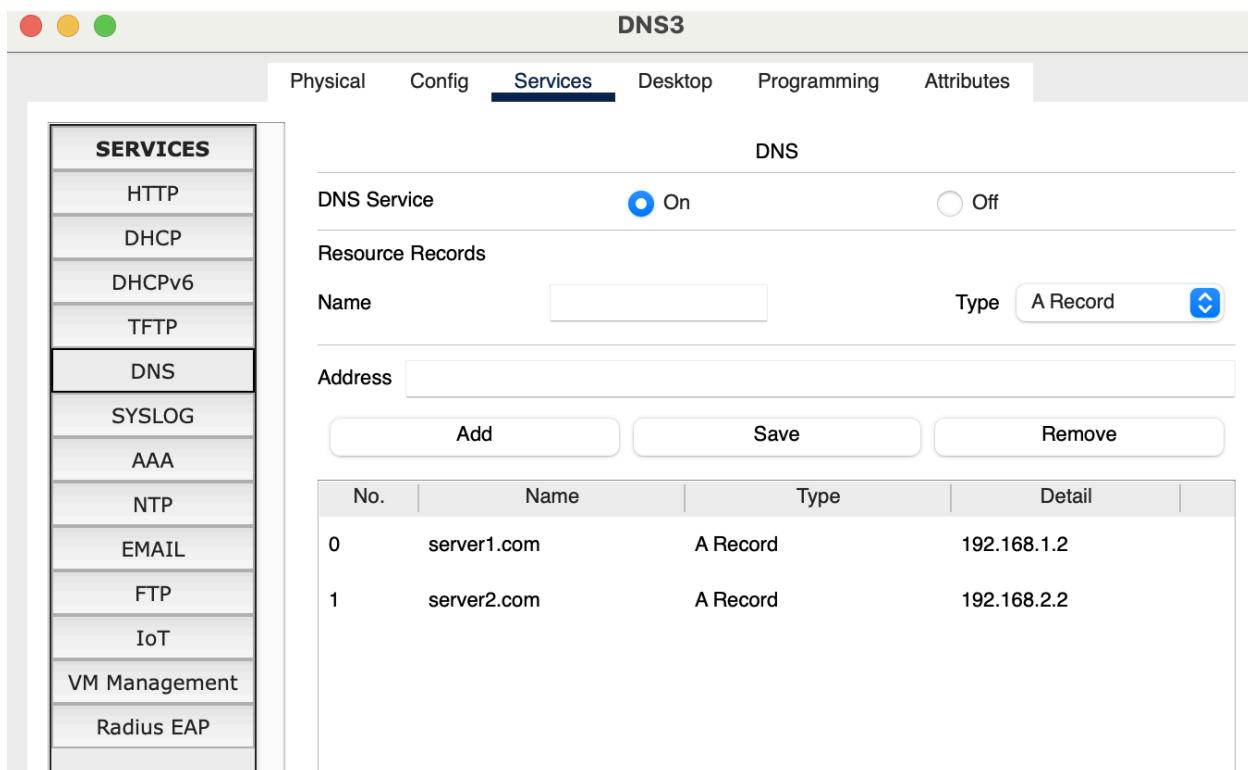
Resource Records

Name Type **A Record**

Address

Add Save Remove

No.	Name	Type	Detail
0	server1.com	A Record	192.168.1.2
1	server2.com	A Record	192.168.2.2



DNS3

Physical Config Services Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL**
- FTP
- IoT
- VM Management
- Radius EAP

EMAIL

SMTP Service ON OFF

POP3 Service ON OFF

Domain Name: Set

User Setup

User Password

+

DNS3

Physical Config Services Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL**
- FTP**
- IoT
- VM Management
- Radius EAP

FTP

Service On Off

User Setup

Username Password
 Write Read Delete Rename List

	Username	Password	Permission
1	cisco	cisco	RWDNL
2	izza	4120	RWDL

Add Save Remove

DNS3

Physical Config Services Desktop Programming Attributes

GLOBAL

Settings Algorithm Settings

INTERFACE

FastEthernet0

FastEthernet0

Port Status On

Bandwidth 100 Mbps 10 Mbps Auto

Duplex Half Duplex Full Duplex Auto

MAC Address 0005.5EEB.64CA

IP Configuration Static DHCP

IPv4 Address 192.168.1.3

Subnet Mask 255.255.255.0

IPv6 Configuration Automatic Static

IPv6 Address /

Link Local Address: FE80::205:5EFF:FE6B:64CA

Server1

Physical Config Services Desktop Programming Attributes

GLOBAL

Settings Algorithm Settings

INTERFACE

FastEthernet0

FastEthernet0

Port Status On

Bandwidth 100 Mbps 10 Mbps Auto

Duplex Half Duplex Full Duplex Auto

MAC Address 00E0.F774.8E26

IP Configuration Static DHCP

IPv4 Address 192.168.1.2

Subnet Mask 255.255.255.0

IPv6 Configuration Automatic Static

IPv6 Address /

Link Local Address: FE80::2E0:F7FF:FE74:8E26

