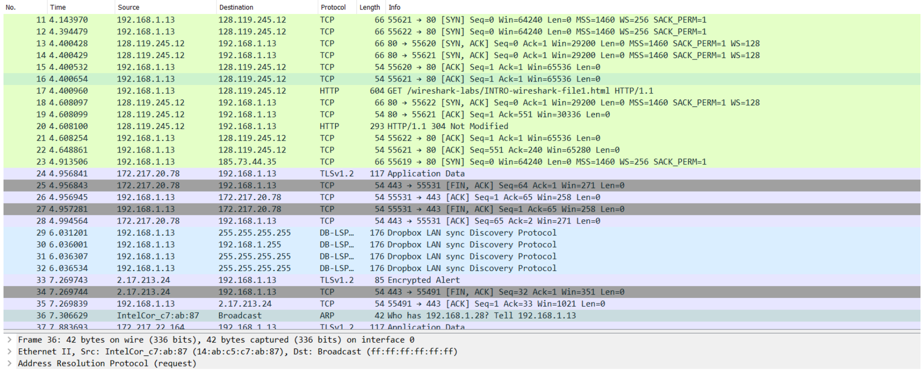
Question 1

Some of the different protocols appearing in the protocol column in the unfiltered packet-listing window is:

- TCP - Transmission Control Protocol
- HTTP - HyperText Transfer Protocol
- ARP - Address Resolution Protocol

A snapshot of the packages ”sniffed” by Wireshark is shown in fig. 1.



No.	Time	Source	Destination	Protocol	Length	Info
11	4.143970	192.168.1.13	128.119.245.12	TCP	66	55621 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
12	4.394479	192.168.1.13	128.119.245.12	TCP	66	55622 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
13	4.400428	128.119.245.12	192.168.1.13	TCP	66	80 → 55620 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
14	4.400429	128.119.245.12	192.168.1.13	TCP	66	80 → 55621 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
15	4.400532	192.168.1.13	128.119.245.12	TCP	54	55620 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
16	4.400654	192.168.1.13	128.119.245.12	TCP	54	55621 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
17	4.400960	192.168.1.13	128.119.245.12	HTTP	604	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
18	4.608097	128.119.245.12	192.168.1.13	TCP	66	80 → 55622 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
19	4.608099	128.119.245.12	192.168.1.13	TCP	54	80 → 55621 [ACK] Seq=1 Ack=551 Win=30336 Len=0
20	4.608100	128.119.245.12	192.168.1.13	HTTP	293	HTTP/1.1 304 Not Modified
21	4.608254	192.168.1.13	128.119.245.12	TCP	54	55622 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
22	4.648861	192.168.1.13	128.119.245.12	TCP	54	55621 → 80 [ACK] Seq=551 Ack=240 Win=65280 Len=0
23	4.913506	192.168.1.13	185.73.44.35	TCP	66	55619 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
24	4.956841	172.217.20.78	192.168.1.13	TLSv1.2	117	Application Data
25	4.956843	172.217.20.78	192.168.1.13	TCP	54	443 → 55531 [FIN, ACK] Seq=64 Ack=1 Win=271 Len=0
26	4.956945	192.168.1.13	172.217.20.78	TCP	54	55531 → 443 [ACK] Seq=1 Ack=65 Win=258 Len=0
27	4.957281	192.168.1.13	172.217.20.78	TCP	54	55531 → 443 [FIN, ACK] Seq=1 Ack=65 Win=258 Len=0
28	4.994564	172.217.20.78	192.168.1.13	TCP	54	443 → 55531 [ACK] Seq=65 Ack=2 Win=271 Len=0
29	6.031201	192.168.1.13	255.255.255.255	DB-LSP…	176	Dropbox LAN sync Discovery Protocol
30	6.036001	192.168.1.13	192.168.1.255	DB-LSP…	176	Dropbox LAN sync Discovery Protocol
31	6.036307	192.168.1.13	255.255.255.255	DB-LSP…	176	Dropbox LAN sync Discovery Protocol
32	6.036534	192.168.1.13	255.255.255.255	DB-LSP…	176	Dropbox LAN sync Discovery Protocol
33	7.269743	2.17.213.24	192.168.1.13	TLSv1.2	85	Encrypted Alert
34	7.269744	2.17.213.24	192.168.1.13	TCP	54	443 → 55491 [FIN, ACK] Seq=32 Ack=1 Win=351 Len=0
35	7.269839	192.168.1.13	2.17.213.24	TCP	54	55491 → 443 [ACK] Seq=1 Ack=33 Win=1021 Len=0
36	7.306629	IntelCor_c7:ab:87	Broadcast	ARP	42	Who has 192.168.1.28? Tell 192.168.1.13
37	7.883693	172.217.22.164	192.168.1.13	TLSv1.2	117	Application Data

```
> Frame 36: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: IntelCor_c7:ab:87 (14:ab:c5:c7:ab:87), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

Figure 1: Snapshot of Wireshark window after completing step 7.

Question 2

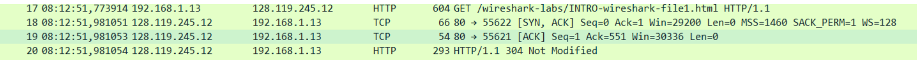
It took approximately 0.2 seconds from when the HTTP GET message was sent until the HTTP OK reply was received. The time each packket was ”sniffed” can be found in the packet-header.

Question 3

The Internet addresses are found by inspecting the packet-header window for the HTTP GET message. The Internet address of the gaia.cs.umass.edu is 128.119.245.12. The Internet address of my computer is 192.168.1.13.

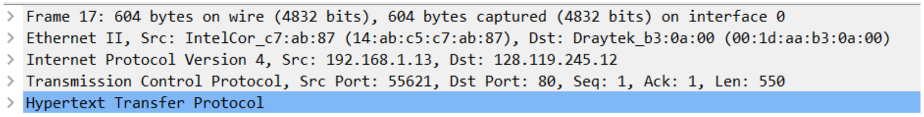
Question 4

The packet list window is shown in fig. 2. The reply was a HTTP NOT MODIFIED message instead of a HTTP OK message. This is probably due to the fact that I had accessed the web page several times before. HTTP NOT MODIFIED means that there is no need for the server to transfer a representation of the web page because my PC already had a valid representation. The packet-header for the GET message is shown in fig. 3, and the packet header for the NOT MODIFIED (OK) message is shown in fig. 4.



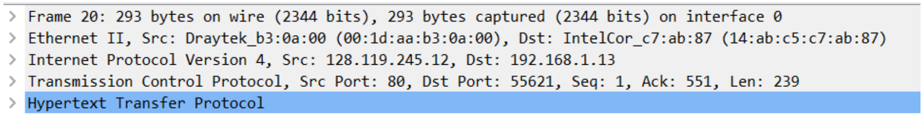
```
17 08:12:51,773914 192.168.1.13     128.119.245.12  HTTP   604 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
18 08:12:51,981051 128.119.245.12   192.168.1.13    TCP     66 80 → 55622 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
19 08:12:51,981053 128.119.245.12   192.168.1.13    TCP     54 80 → 55621 [ACK] Seq=1 Ack=551 Win=30336 Len=0
20 08:12:51,981054 128.119.245.12   192.168.1.13    HTTP   293 HTTP/1.1 304 Not Modified
```

Figure 2: Packet list including HTTP GET message and HTTP NOT MODIFIED response.



```
> Frame 17: 604 bytes on wire (4832 bits), 604 bytes captured (4832 bits) on interface 0
> Ethernet II, Src: IntelCor_c7:ab:87 (14:ab:c5:c7:ab:87), Dst: Draytek_b3:0a:00 (00:1d:aa:b3:0a:00)
> Internet Protocol Version 4, Src: 192.168.1.13, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 55621, Dst Port: 80, Seq: 1, Ack: 1, Len: 550
> Hypertext Transfer Protocol
```

Figure 3: Packet-header for GET message.



```
> Frame 20: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface 0
> Ethernet II, Src: Draytek_b3:0a:00 (00:1d:aa:b3:0a:00), Dst: IntelCor_c7:ab:87 (14:ab:c5:c7:ab:87)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.13
> Transmission Control Protocol, Src Port: 80, Dst Port: 55621, Seq: 1, Ack: 551, Len: 239
> Hypertext Transfer Protocol
```

Figure 4: Packet-header for NOT MODIFIED (OK) response.