

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.
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 packetlisting 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.)
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?
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.

1. different protocols:

ARP, EAP, ICMPv6, TCP, UDP

The screenshot shows the Wireshark interface with a packet capture in progress. The packet list pane displays the following packets:

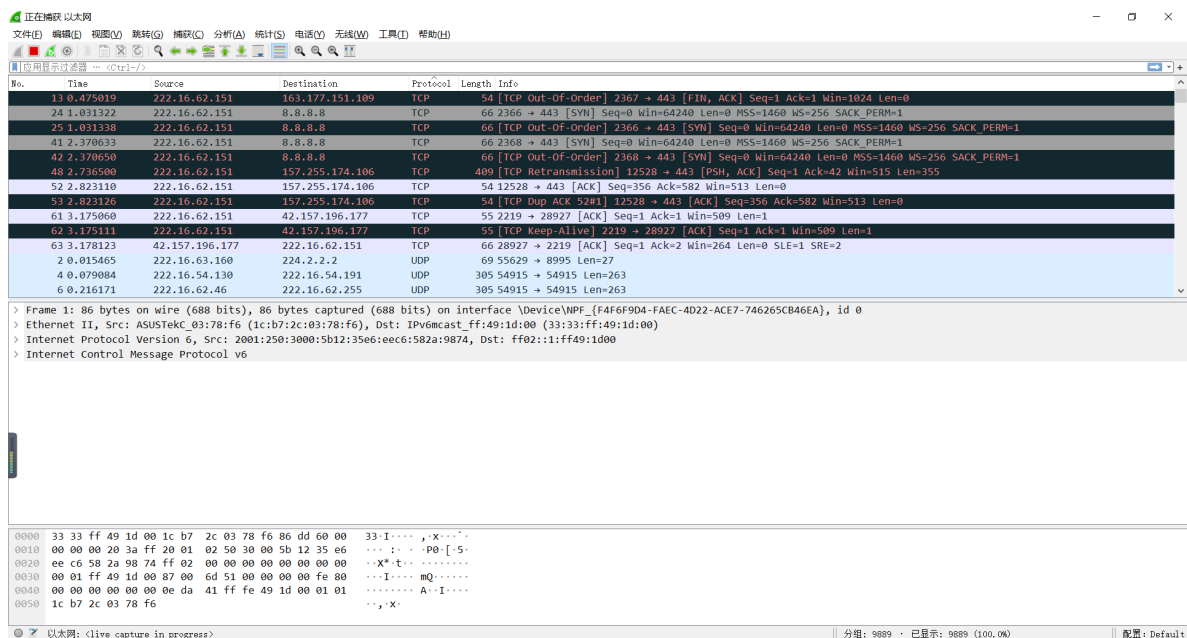
No.	Time	Source	Destination	Protocol	Length	Info
20	0.896039	LCFCHFe_11:9b:80	Broadcast	ARP	60	who has 169.254.255.255? Tell 222.16.62.46
37	2.219845	LCFCHFe_11:9b:80	Broadcast	ARP	60	who has 169.254.255.255? Tell 222.16.62.46
55	2.867017	LCFCHFe_11:9b:80	Broadcast	ARP	60	who has 169.254.255.255? Tell 222.16.62.46
45	2.640898	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xfcd055c
40	2.284288	Hangzhou_f1:0e:63	LCFCHFe_54:b0:06	EAP	64	Request, Identity
49	2.745729	LCFCHFe_54:b0:06	Hangzhou_f1:0e:63	EAP	96	Response, Identity
50	2.745743	LCFCHFe_54:b0:06	Hangzhou_f1:0e:63	EAP	96	Response, Identity
10	0.000000	2001:250:3000:5b12::...	ff02::1:ff49:1d00	ICMPv6	86	Neighbor Solicitation for fe80::eda:41ff:fe49:1d00 from 1c:b7:2c:03:78:f6
5	0.169877	2001:250:3000:5b12::...	ff02::1:ff49:1d00	ICMPv6	86	Neighbor Solicitation for fe80::eda:41ff:fe49:1d00 from 80:fa:5b:41:fe:ec
14	0.527757	2001:250:3000:5b12::...	ff02::1:ffec:6cce	ICMPv6	86	Neighbor Solicitation for 2001:250:3000:5b12:51:dadc:67ec:6cce from b4:a9:fc:48:c5:05
16	0.794820	2001:250:3000:5b12::...	ff02::1:ffec:6cce	ICMPv6	86	Neighbor Solicitation for 2001:250:3000:5b12:51:dadc:67ec:6cce from 10:7b:44:db:ae:4d
18	0.817717	2001:250:3000:5b12::...	ff02::1:ffec:6cce	ICMPv6	86	Neighbor Solicitation for 2001:250:3000:5b12:51:dadc:67ec:6cce from ac:e2:d3:54:a5:fa
8	0.252317	222.16.62.1	222.16.62.255	NNNS	92	Name query NB WPAD<00>
17	0.809741	220.249.245.141	222.16.62.151	OICQ	129	OICQ Protocol

The packet details pane for the selected packet (No. 10) shows:

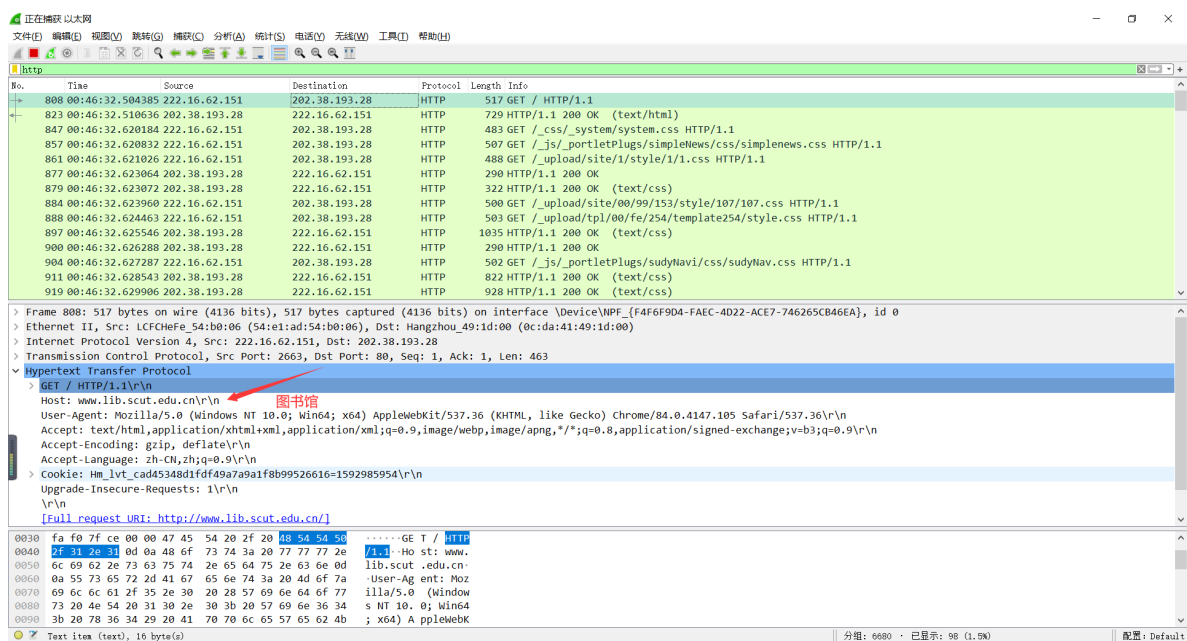
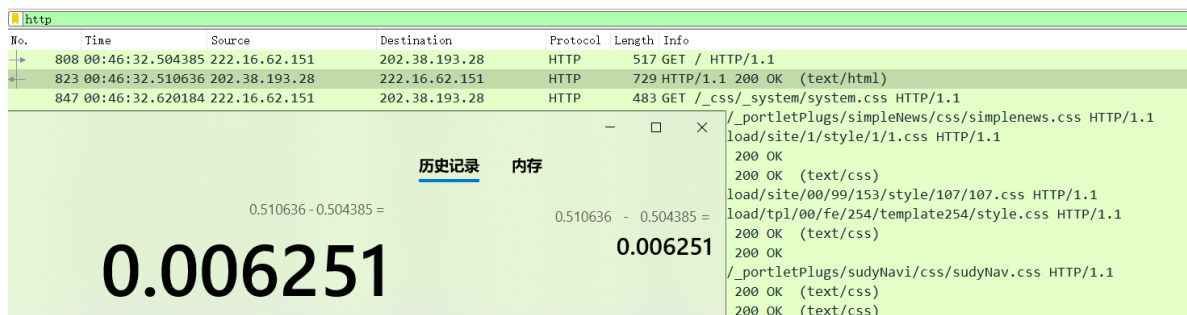
- Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{F4F6F9D4-FAEC-4D22-ACE7-746265CB46EA}, id 0
- Ethernet II, Src: ASUSTek_03:78:f6 (1c:b7:2c:03:78:f6), Dst: IPv6mcast_ff49:1d:00 (33:33:ff:49:1d:00)
- Internet Protocol Version 6, Src: 2001:250:3000:5b12:35e6:ee6:582a:9874, Dst: ff02::1:ff49:1d00
- Internet Control Message Protocol v6

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000  33 33 ff 49 1d 00 1c b7 2c 03 78 f6 86 dd 60 00  33:I.....,X.....
0010  00 00 00 20 3a ff 20 01 02 50 30 00 5b 12 35 a6  ..:..:..P0[.5.
0020  ee c6 58 2a 98 74 ff 02 00 00 00 00 00 00 00  ..X*.t.....
0030  00 01 ff 49 1d 00 87 00 6d 51 00 00 00 00 fe 80  ...I.....mQ.....
0040  00 00 00 00 00 00 0e da 41 ff fe 49 1d 00 01 01  ....A..I....
0050  1c b7 2c 03 78 f6  ....X.
```



2. the time between HTTP GET message was sent and the HTTP OK reply was received



3. the Internet address of the school library

