Project1 2019.9.24

Name:潘盛琪
Student number:3170105737
Partner:毕铁锴

PART A

1. **(0.5 pts) List up to 10 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.**
   UDP SSDP ICMPv6 ARP TCP MDNS LLMNR LSD OSPF DHCPv6

	Destination	Protocol	Length	Info
.7	10.110.33.255	UDP	305	54915 → 54915 Le
65	239.255.255.250	SSDP	216	M-SEARCH * HTTP/
.216	239.255.255.250	UDP	698	54240 → ws-disc
.20	10.110.29.255	UDP	305	54915 → 54915 Le
e000:1a05:…	ff02::1:ffcb:8730	ICMPv6	86	Neighbor Solicit
.62	10.110.33.255	UDP	305	54915 → 54915 Le
.63	10.110.33.255	UDP	82	59980 → sentinel
.229	10.110.33.255	UDP	305	54915 → 54915 Le
.216	10.110.33.255	UDP	305	54915 → 54915 Le
a:e1c0:6f6…	ff02::c	UDP	718	54241 → ws-disc

Destination	Protocol	Length	Info
10.110.33.255	UDP	305	54915 → 54915 L
239.255.255.250	SSDP	318	NOTIFY * HTTP/1
10.110.33.255	UDP	305	54915 → 54915 L
Broadcast	ARP	60	Who has 10.110.
ff02::16	ICMPv6	90	Multicast Liste
ff02::1:ffcb:4130	ICMPv6	78	Neighbor Solici
ff02::2	ICMPv6	62	Router Solicita
239.255.255.250	SSDP	216	M-SEARCH * HTTP
2404:6800:4008:801:…	TCP	86	64354 → https(4
10.110.29.255	UDP	305	54915 → 54915 L

	Destination	Protocol	Length	Info
:887f:30c…	ff02::1:3	LLMNR	95	Standard query 0x6eb2 AN
:887f:30c…	ff02::16	ICMPv6	90	Multicast Listener Repor
:887f:30c…	ff02::16	ICMPv6	90	Multicast Listener Repor
:887f:30c…	ff02::fb	MDNS	101	Standard query 0x0000 AN
:887f:30c…	ff02::fb	MDNS	235	Standard query response
:887f:30c…	ff02::1:3	LLMNR	95	Standard query 0x1696 AN
:887f:30c…	ff02::16	ICMPv6	90	Multicast Listener Repor
:887f:30c…	ff02::16	ICMPv6	90	Multicast Listener Repor
:887f:30c…	ff02::16	ICMPv6	90	Multicast Listener Repor
:887f:30c…	ff02::16	ICMPv6	90	Multicast Listener Repor

	Destination	Protocol	Length	Info
	255.255.255.255	UDP	155	49468 → 61
…	2404:6800:4008:800:…	TCP	86	64344 → ht
	239.192.152.143	LSD	161	
	10.110.29.255	UDP	305	54915 → 54
	Broadcast	0x9001	64	Ethernet I
…	2404:6800:4008:800:…	TCP	86	64345 → ht
	10.110.33.255	UDP	305	54915 → 54
	224.0.0.5	OSPF	78	Hello Pack
	10.110.33.255	UDP	305	54915 → 54
…	ff02::1:2	DHCPv6	157	Solicit XI

2. **(1 pt) 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.)**

0.276666s

→	67	01:11:18.202804	222.205.4.167
←	75	01:11:18.479470	128.119.245.12

3. **(1 pt) Print the two HTTP messages displayed above. To do so, select Print from the Wireshark File command menu, and select "Selected Packet Only" and "Print as displayed" and select "output to a file", and then click OK. Copy the text to your final PDF document for submission.**

Request message

```
No.     Time              Source                Destination           Protocol Length Info
     67 01:11:18.202804   222.205.4.167         128.119.245.12        HTTP     549    GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 67: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits) on interface 0
Ethernet II, Src: Dell_f2:fd:99 (f4:8e:38:f2:fd:99), Dst: Hangzhou_00:95:03 (5c:dd:70:00:95:03)
Internet Protocol Version 4, Src: 10.110.33.41, Dst: 10.0.2.3
User Datagram Protocol, Src Port: 12f (1701), Dst Port: 12f (1701)
Layer 2 Tunneling Protocol
Point-to-Point Protocol
Internet Protocol Version 4, Src: 222.205.4.167, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 52371 (52371), Dst Port: http (80), Seq: 1, Ack: 1, Len: 455
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 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
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 75]
```

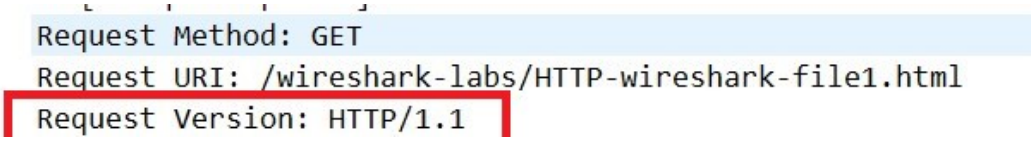
Response message

```
No.     Time              Source                Destination           Protocol Length Info
     75 01:11:18.479470    128.119.245.12        222.205.4.167         HTTP     530    HTTP/1.1 200 OK  (text/html)
Frame 75: 530 bytes on wire (4240 bits), 530 bytes captured (4240 bits) on interface 0
Ethernet II, Src: Hangzhou_00:95:03 (5c:dd:70:00:95:03), Dst: Dell_f2:fd:99 (f4:8e:38:f2:fd:99)
Internet Protocol Version 4, Src: 10.0.2.3, Dst: 10.110.33.41
User Datagram Protocol, Src Port: 12f (1701), Dst Port: 12f (1701)
Layer 2 Tunneling Protocol
Point-to-Point Protocol
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 222.205.4.167
Transmission Control Protocol, Src Port: http (80), Dst Port: 52371 (52371), Seq: 1, Ack: 456, Len: 438
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Mon, 07 Oct 2019 17:11:17 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Mon, 07 Oct 2019 05:59:01 GMT\r\n
    ETag: "51-5944bbf9d0260"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 81\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.276666000 seconds]
    [Request in frame: 67]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    File Data: 81 bytes
Line-based text data: text/html (3 lines)
```

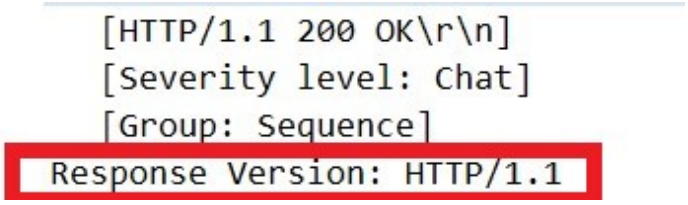
PART B

1. **(1pt) Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?**

   HTTP version1.1.

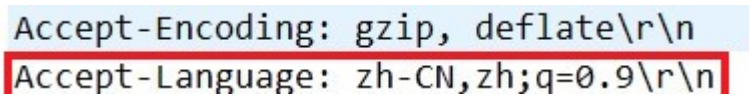


   The server is also running HTTP version 1.1.



2. **(0.5pts) What languages (if any) does your browser indicate that it can accept to the server?**

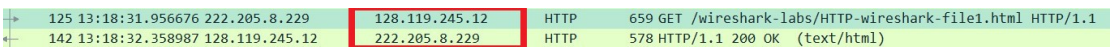
   Zh-CN(简体中文)



3. **(1 pt) What is the IP address of your computer? Of the gaia.cs.umass.edu server?**

   The IP address of my computer is 222.205.8.229.

   The IP address of the server is 128.119.245.12.



```
Internet Protocol Version 4, Src: 222.205.8.229, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 494
    Identification: 0xb832 (47154)
    Flags: 0x4000, Don't fragment
        0... .... .... .... = Reserved bit: Not set
        .1.. .... .... .... = Don't fragment: Set
        ..0. .... .... .... = More fragments: Not set
        ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0x23a1 [validation disabled]
    [Header checksum status: Unverified]
    Source: 222.205.8.229
    Destination: 128.119.245.12
```

4. **(0.5pt) What is the status code returned from the server to your browser?**

   200 It means succeeding.

```
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
            [HTTP/1.1 200 OK\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
```

5. **(0.5pt) When was the HTML file that you are retrieving last modified at the server?**

   Thu, 26 Sep 2018 05:59:02 GMT

```
Date: Fri, 27 Sep 2019 04:58:45 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
Last-Modified: Thu, 26 Sep 2019 05:59:02 GMT\r\n
ETag: "80-5936e77606bbc"\r\n
Accept-Ranges: bytes\r\n
```

6. **(0.5pt) How many bytes of content are being returned to your browser?**

   128 bytes.

```
Accept-Ranges: bytes\r\n
Content-Length: 128\r\n
    [Content length: 128]
```

7. **(0.5pts) Inspect the contents of the first HTTP GET request from your browser to the** server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?

   No

8. **(1pt) Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?**

   Yes

```
    File Data: 371 bytes
Line-based text data: text/html (10 lines)
    \n
    <html>\n
    \n
    Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
    This file's last modification date will not change.  <p>\n
    Thus  if you download this multiple times on your browser, a complete copy <br>\n
    will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n
```

```
1
2  <html>
3
4  Congratulations again!  Now you've downloaded the file lab2-2.html. <br>
5  This file's last modification date will not change.  <p>
6  Thus  if you download this multiple times on your browser, a complete copy <br>
7  will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>
8  field in your browser's HTTP GET request to the server.
9
10 </html>
11
```

The same with source codes of the web page.

9. **(0.5pts) Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?**

   Yes

   ```
   If-None-Match: "173-59382513e615b"\r\n
   If-Modified-Since: Fri, 27 Sep 2019 05:40:01 GMT\r\n
   ```

   The time when the web was modified last time.

10. **(1pt) What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.**

    304 Not Modified

    ```
    Hypertext Transfer Protocol
        HTTP/1.1 304 Not Modified\r\n
    ```

    No

    Because the file has not been modified.

11. **(0.5pts) How many HTTP GET request messages were sent by your browser?**

    Only one.

```
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
            [GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /wireshark-labs/HTTP-wireshark-file3.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 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
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
    [HTTP request 1/1]
    [Response in frame: 79]
```

12. **(0.5pts) How many data-containing TCP segments were needed to carry the single HTTP response?**

    Four.

```
[4 Reassembled TCP Segments (4861 bytes): #75(1360), #76(1360), #78(1360), #79(781)]
    [Frame: 75, payload: 0-1359 (1360 bytes)]
    [Frame: 76, payload: 1360-2719 (1360 bytes)]
    [Frame: 78, payload: 2720-4079 (1360 bytes)]
    [Frame: 79, payload: 4080-4860 (781 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2046…]
```

13. **(0.5pts) What is the status code and phrase associated with the response to the HTTP GET request?**

    200 OK

```
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
            [HTTP/1.1 200 OK\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
```

14. **(0.5pts) Are there any HTTP status lines in the transmitted data associated with a TCP-induced "Continuation"?**

    No

15. **(1pt) How many HTTP GET request messages were sent by your browser? To which Internet addresses (IP addresses) were these GET requests sent?**

    Three

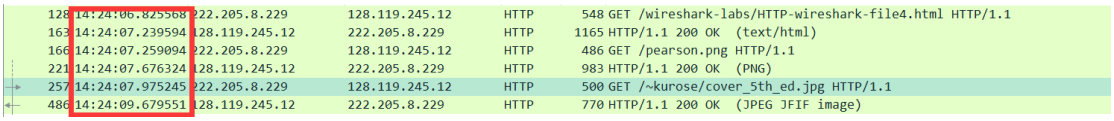
```
128 14:24:06.825568 222.205.8.229   128.119.245.12   HTTP   548 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
163 14:24:07.239594 128.119.245.12  222.205.8.229    HTTP  1165 HTTP/1.1 200 OK  (text/html)
166 14:24:07.259094 222.205.8.229   128.119.245.12   HTTP   486 GET /pearson.png HTTP/1.1
221 14:24:07.676324 128.119.245.12  222.205.8.229    HTTP   983 HTTP/1.1 200 OK  (PNG)
257 14:24:07.975245 222.205.8.229   128.119.245.12   HTTP   500 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
486 14:24:09.679551 128.119.245.12  222.205.8.229    HTTP   770 HTTP/1.1 200 OK  (JPEG JFIF image)
```

    128.119.245.12

16. **(0.5pt) Can you tell whether your browser downloaded the two images serially, or**

whether they were downloaded from the two web sites in parallel? Explain.

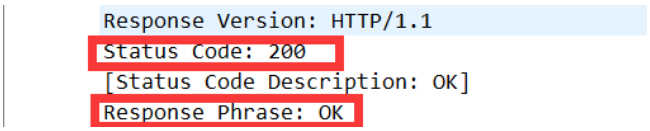
Serially



The time is different.

17. **(0.5pts) What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?**

200 OK.



18. **(0.5pts)When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?**

Upgrate-Insecure-Requests and Accept.