天津大学

《计算机网络》

题目：WireShark Lab

学　院　智能与计算学部

专　业　计算机科学与技术

年　级　2019

姓　名　张明君（留学生）

学　号　6319000359

2021 年 9 月 16 日

Download Wireshark

In order to download Wireshark, you will need to have access to a computer that supports both Wireshark and the *libpcap* or *WinPCap* packet capture library. The *libpcap* software will be installed for you, if it is not installed within your operating system, when you install Wireshark.. See http://www.wireshark.org/download.html for a list of supported operating systems and download sites

Download and install the Wireshark software:

- Go to http://www.wireshark.org/download.html and download and install the Wireshark binary for your computer.
- Download the Wireshark user guide.

The Wireshark FAQ has a number of helpful hints and interesting tidbits of information, particularly if you have trouble installing or running Wireshark.

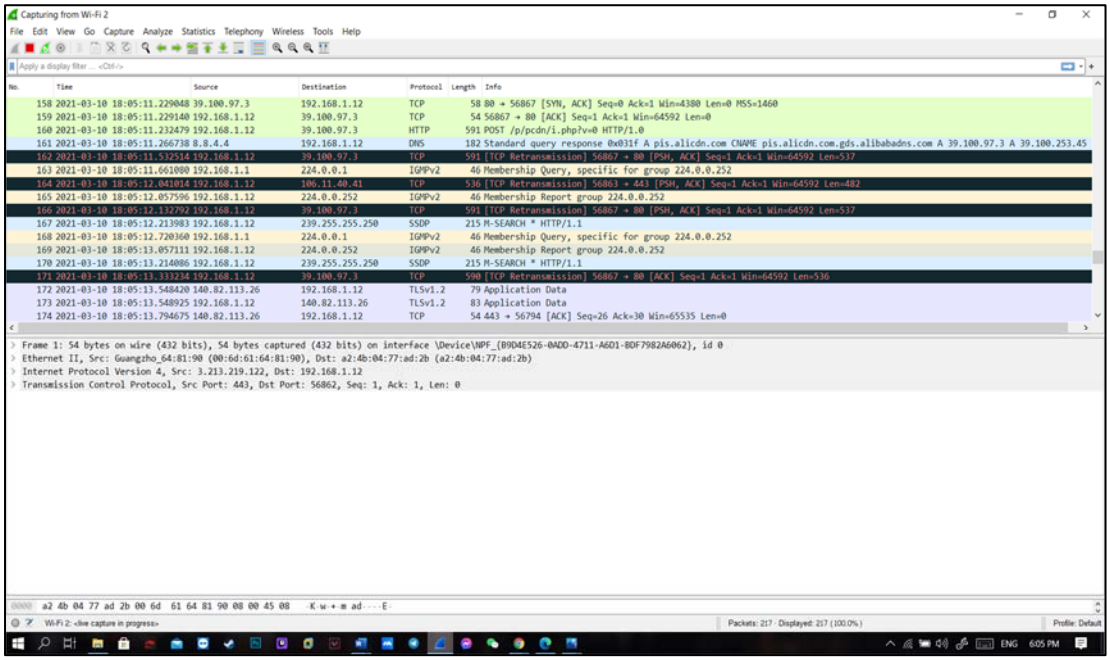
What to hand in:

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:

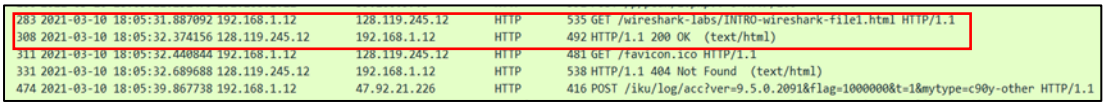
1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.
2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packetlisting window is the 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.

Answer:

1. Protocols that appear are: **DNS** ,**TLSv1.2** ,**TCP.**



2. It took approximately **0.5s** to go from HTTP GET to HTTP OK.



3. The IP address of the gaia.cs.umass.edu is **128.119.245.12** The IP of my computer is **192.168.1.12** .
4. This is the HTTP GET packet info that I have printed.

```
No.     Time                        Source                Destination           Protocol Length Info
    283 2021-03-10 18:05:31.887092  192.168.1.12          128.119.245.12        HTTP     535    GET /wireshark-labs/INTRO-wireshark-file1.html
HTTP/1.1
Frame 283: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{B9D4E526-0ADD-4711-A6D1-BDF7982A6062}, id 0
Ethernet II, Src: a2:4b:04:77:ad:2b (a2:4b:04:77:ad:2b), Dst: Guangzho_64:81:90 (00:6d:61:64:81:90)
Internet Protocol Version 4, Src: 192.168.1.12, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 56872, Dst Port: 80, Seq: 1, Ack: 1, Len: 481
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
            [GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /wireshark-labs/INTRO-wireshark-file1.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; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.72 Safari/537.36 Edg/
89.0.774.45\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;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 308]
    [Next request in frame: 311]
```

And This is the HTTP OK packet info that I have printed too.

```
No.     Time                           Source                Destination           Protocol Length Info
    308 2021-03-10 18:05:32.374156     128.119.245.12        192.168.1.12          HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 308: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{B9D4E526-0ADD-4711-A6D1-BDF7982A6062}, id 0
Ethernet II, Src: Guangzho_64:81:90 (00:6d:61:64:81:90), Dst: a2:4b:04:77:ad:2b (a2:4b:04:77:ad:2b)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.12
Transmission Control Protocol, Src Port: 80, Dst Port: 56872, Seq: 1, Ack: 482, Len: 438
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
    Date: Wed, 10 Mar 2021 10:05:30 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 10 Mar 2021 06:59:01 GMT\r\n
    ETag: "51-5bd2933a6375d"\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 1/2]
    [Time since request: 0.487064000 seconds]
    [Request in frame: 283]
    [Next request in frame: 311]
    [Next response in frame: 331]
    [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)
```

Running Wireshark

When you run the Wireshark program, the Wireshark graphical user interface shown in Figure 1 will be displayed. Initially, no data will be displayed in the various windows.

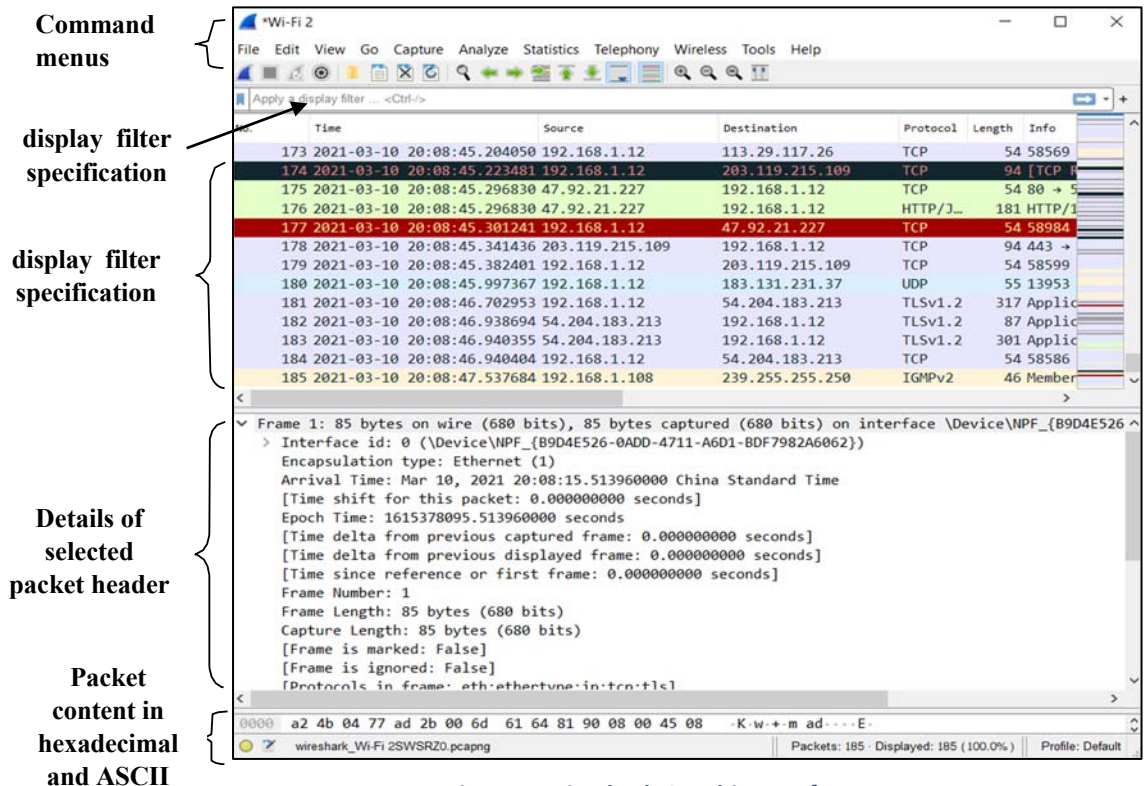


Figure 1:Wireshark Graphic Interface

Taking Wireshark for a test run

Before We start to run the Wireshark we have to connect to the internet first because we have to capture and trace the website that we would like to trace. After we connected to the internet now we have to following steps below:

1. Start up your favorite web browser (any browser that u want), which will display your selected homepage.

2. Start up the Wireshark software. You will initially see a window similar to that shown in Figure 2:

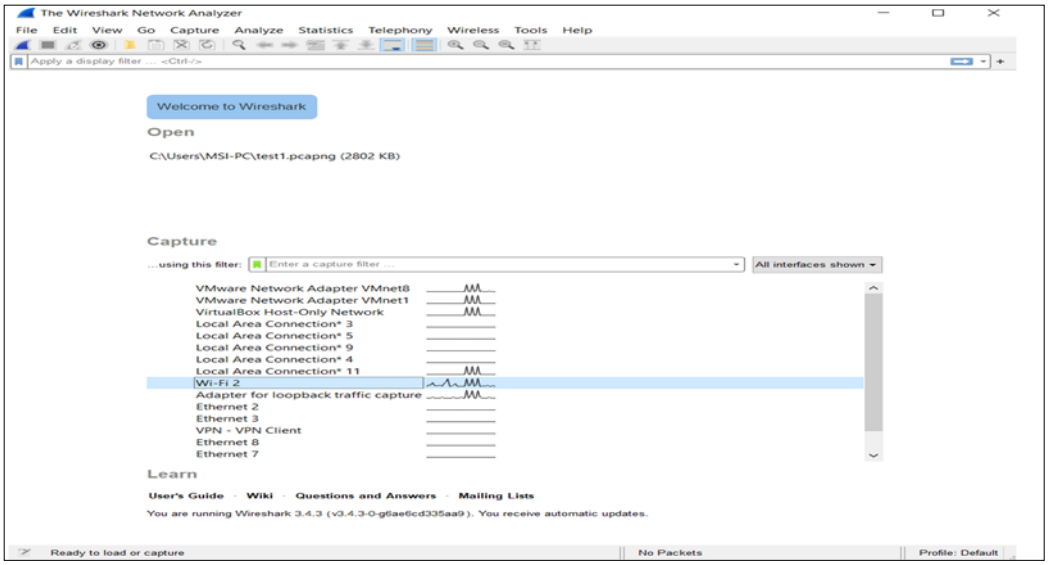


Figure 2:Wireshark interface

3. While Wireshark is running, enter the URL: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html and have that page displayed in your browser. In order to display this page, your browser will contact the HTTP server at gaia.cs.umass.edu and exchange HTTP messages with the server in order to download this page. And then you will see like the picture in figure 3 below.

Figure 3:Capture and download file

4. Type in “http” (without the quotes, and in lower case – all protocol names are in lower case in Wireshark) into the display filter specification window at the top of the main Wireshark window. Then select Apply (to the right of where you entered “http”). This will cause only HTTP message to be displayed in the packet-listing window.

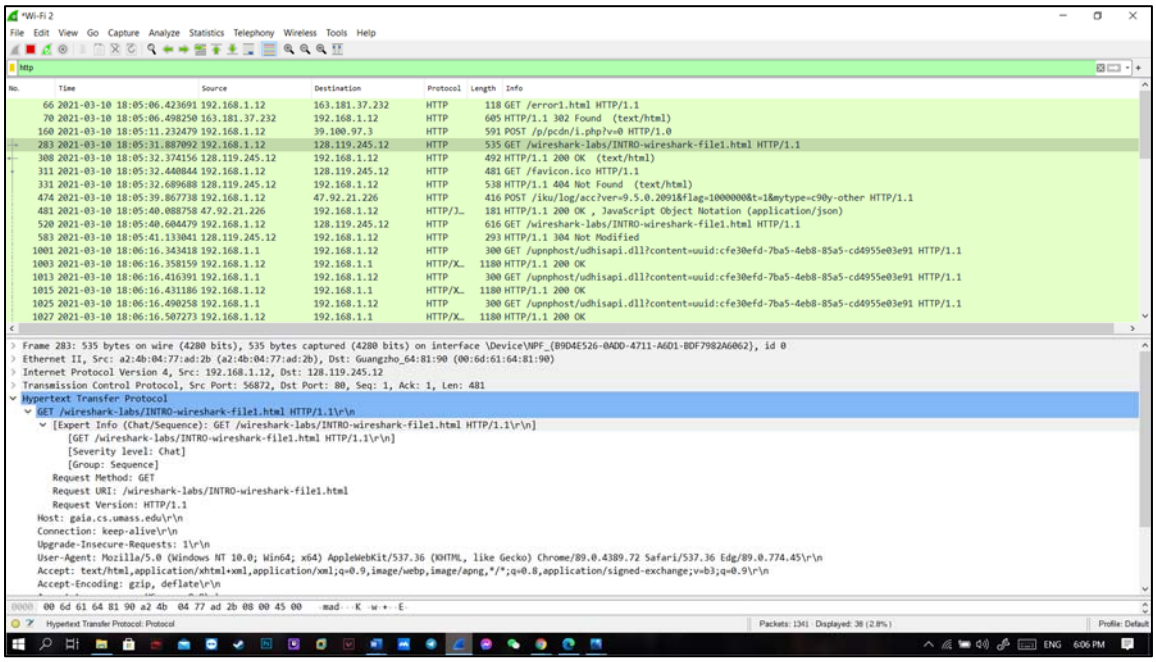


Figure 4:http trace files

5. Select the first http message shown in the packet-listing window. This should be the **HTTP GET** message that was sent from your computer to the gaia.cs.umass.edu HTTP server. When you select the **HTTP GET** message, the Ethernet frame, IP datagram, TCP segment, and HTTP message header information will be displayed in the packet-header window. By clicking plus and-minus boxes to the left side of the packet details window, minimize the amount of Frame, Ethernet, Internet Protocol, and Transmission Control Protocol information displayed. Maximize the amount information displayed about the HTTP protocol. Your Wireshark display should now look roughly as shown in Figure 5. (Note, in particular, the minimized amount of protocol information for all protocols except HTTP, and the maximized amount of protocol information for HTTP in the packet-header window).

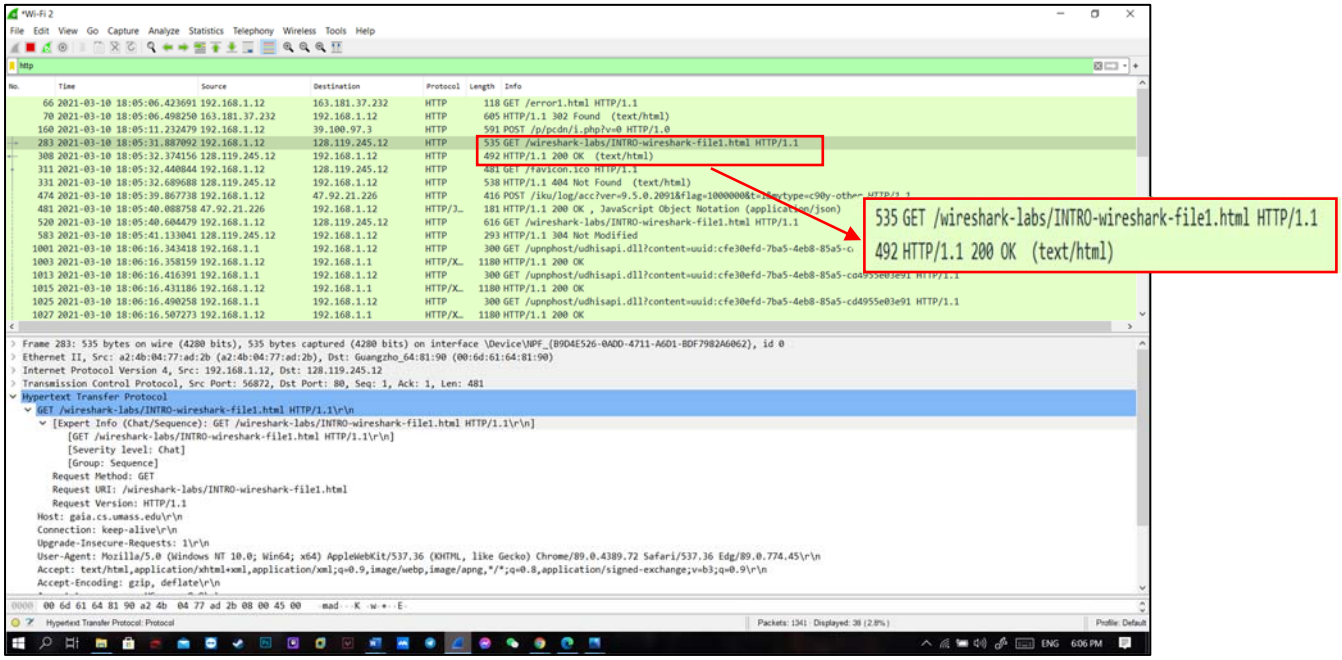


Figure 5:HTTP GET and HTTP OK information

Now we have finally completed this first Wireshark lab and I also described about the http get and http ok information in the questions above. If u have any questions you can look up for more information about it.