南昌大学实验报告

姓名：**陈华豪**

学号：**6130116238**

邮箱地址：**6130116238@email.ncu.edu.cn**

专业班级：**网络工程161班**

实验日期：**2018.10.28**

课程名称：**网络协议分析与实现**

实验项目名称

实验一：Wireshark Labs

实验目的

学习使用 Wireshark packet sniffer

实验基础

http://www-net.cs.umass.edu/wireshark-labs/

http://www-net.cs.umass.edu/wireshark-labs/Wireshark*Intro*v7.0.pdf

实验步骤

抓取一小时数据并打包分析

1. Start up your favorite web browser, 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. Wireshark has not yet begun capturing packets.
3. To begin packet capture, select the Capture pull down menu and select Interfaces. This will cause the “Wireshark: Capture Interfaces” window to be displayed, as shown in Figure 4. Figure 4: Wireshark Capture Interface Window
4. You’ll see a list of the interfaces on your computer as well as a count of the packets that have been observed on that interface so far. Click on Start for the interface on which you want to begin

packet capture (in the case, the Gigabit network Connection). Packet capture will now begin - Wireshark is now capturing all packets being sent/received from/by your computer!

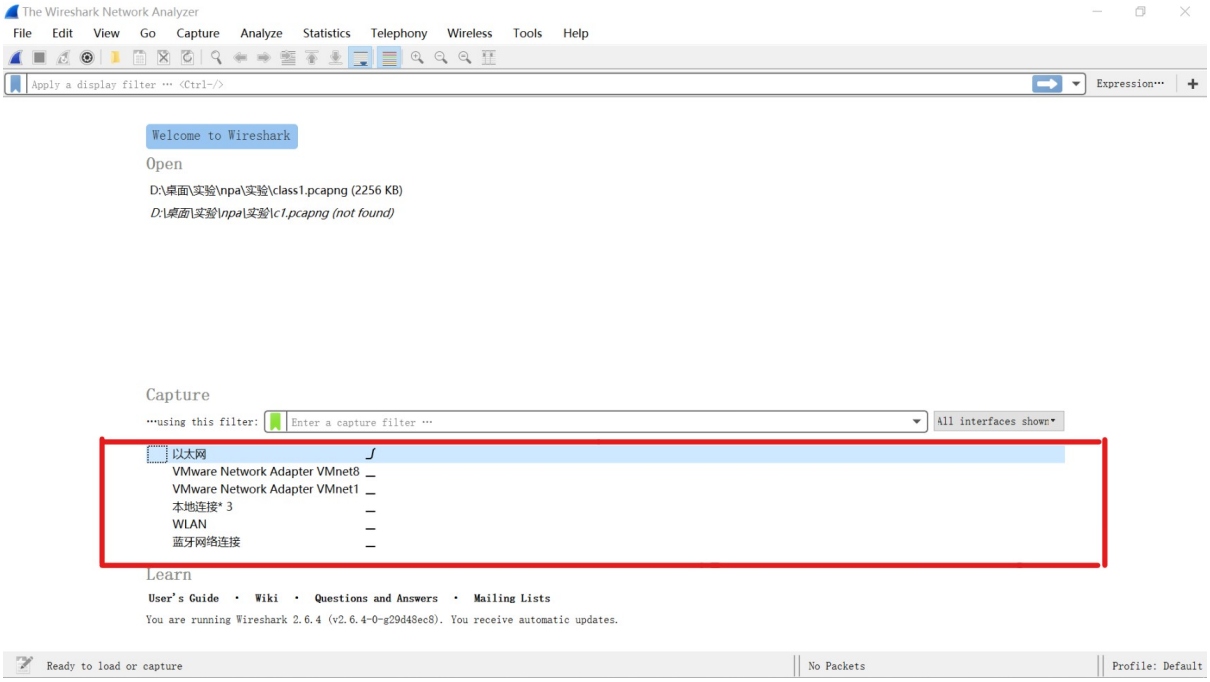
5. Once you begin packet capture, a window similar to that shown in Figure 3 will appear. This window shows the packets being captured. By selecting Capture pulldown menu and selecting Stop, you can stop packet capture. But don't stop packet capture yet. Let's capture some interesting packets first. To do so, we'll need to generate some network traffic. Let's do so using a web browser, which will use the HTTP protocol that we will study in detail in class to download content from a website.
6. 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, as discussed in section 2.2 of the text. The Ethernet frames containing these HTTP messages (as well as all other frames passing through your Ethernet adapter) will be captured by Wireshark.
7. After your browser has displayed the INTRO-wireshark-file1.html page (it is a simple one line of congratulations), stop Wireshark packet capture by selecting stop in the Wireshark capture window. The main Wireshark window should now look similar to Figure 3. You now have live packet data that contains all protocol messages exchanged between your computer and other network entities! The HTTP message exchanges with the gaia.cs.umass.edu web server should appear somewhere in the listing of packets captured. But there will be many other types of packets displayed as well (see, e.g., the many different protocol types shown in the Protocol column in Figure 3). Even though the only action you took was to download a web page, there were evidently many other protocols running on your computer that are unseen by the user. We'll learn much more about these protocols as we progress through the text! For now, you should just be aware that there is often much more going on than "meet's the eye"!
8. 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.
9. Find the HTTP GET message that was sent from your computer to the gaia.cs.umass.edu HTTP server. (Look for an HTTP GET message in the "listing of captured packets" portion of the Wireshark window (see Figure 3) that shows "GET" followed by the gaia.cs.umass.edu URL that you entered. 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 window2 . By clicking on '+' and '-' right-pointing and down-pointing arrowheads 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).

10. Exit Wireshark

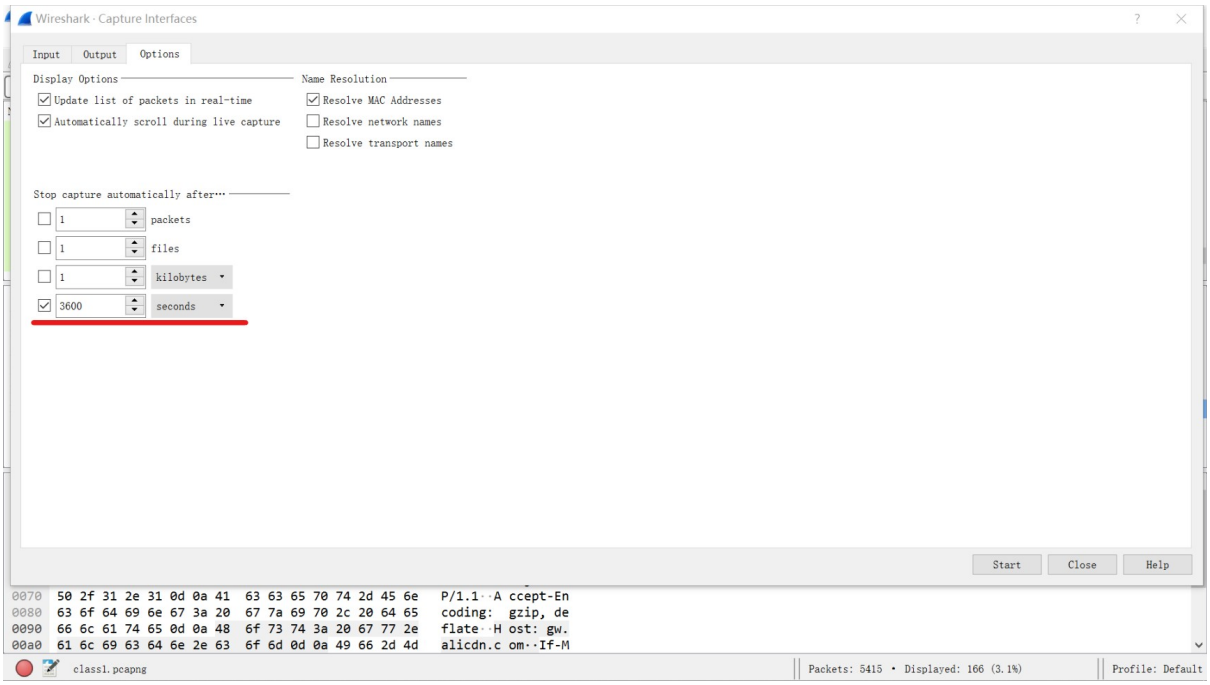
抓取一小时数据并打包分析

实验数据或结果

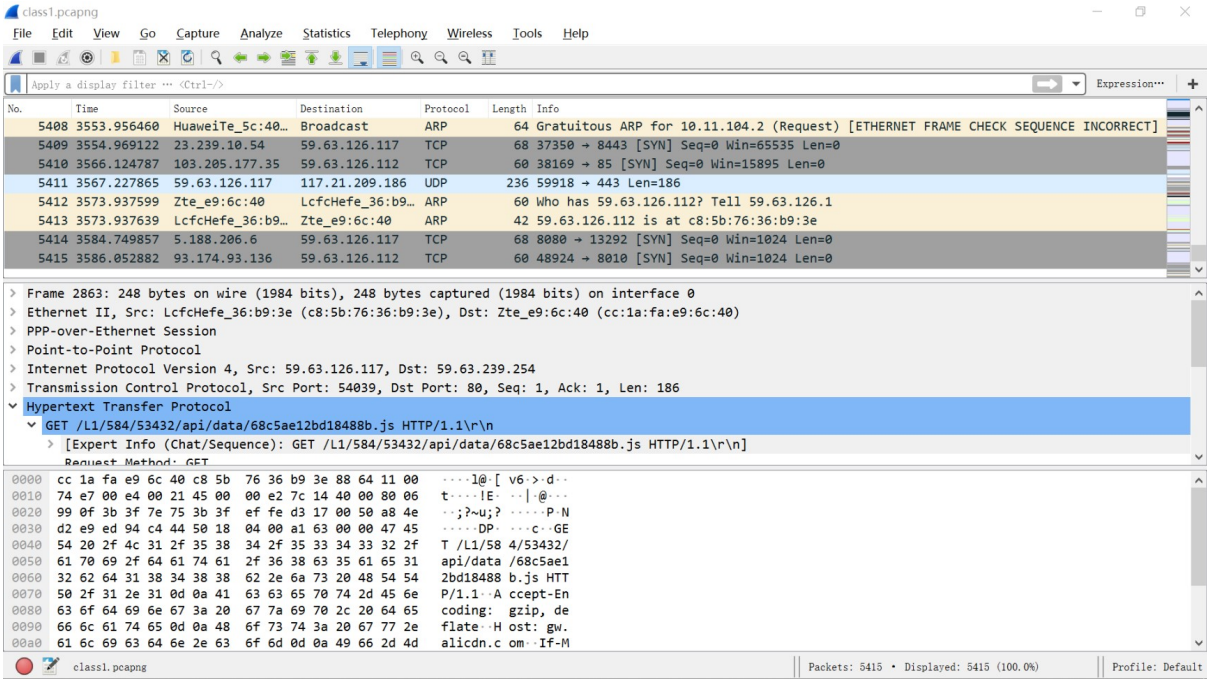
- **开始： (红线标注位置为可选择的接口)**



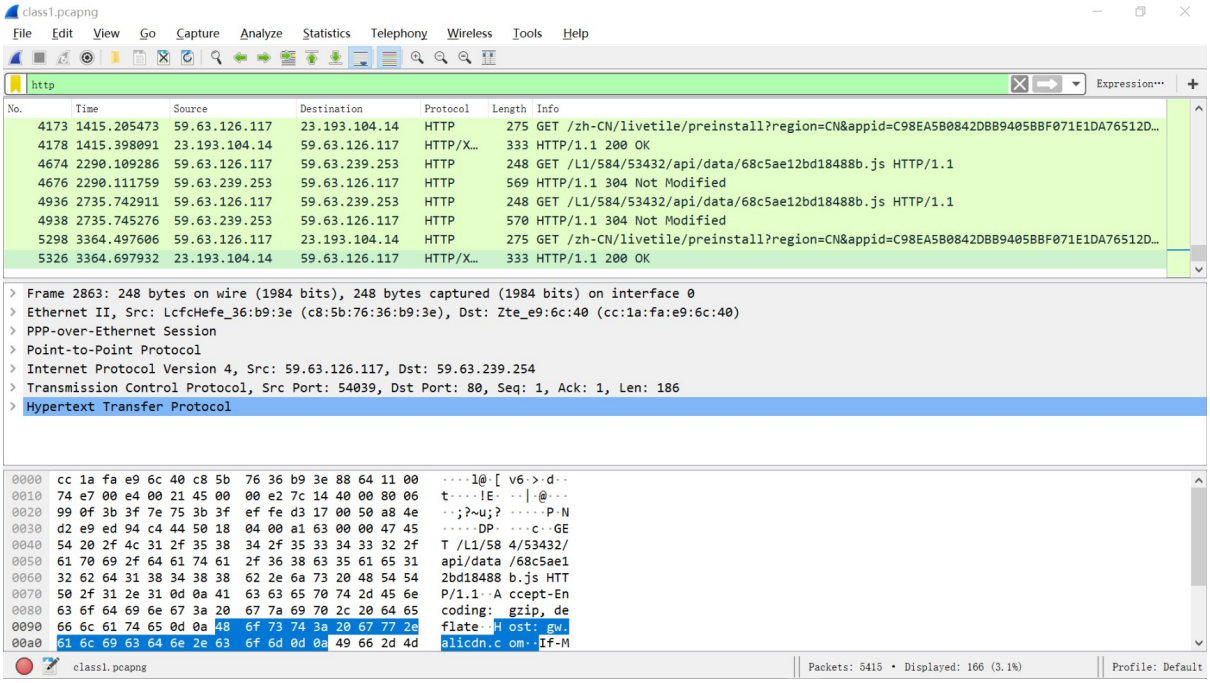
- **定时：一小时**



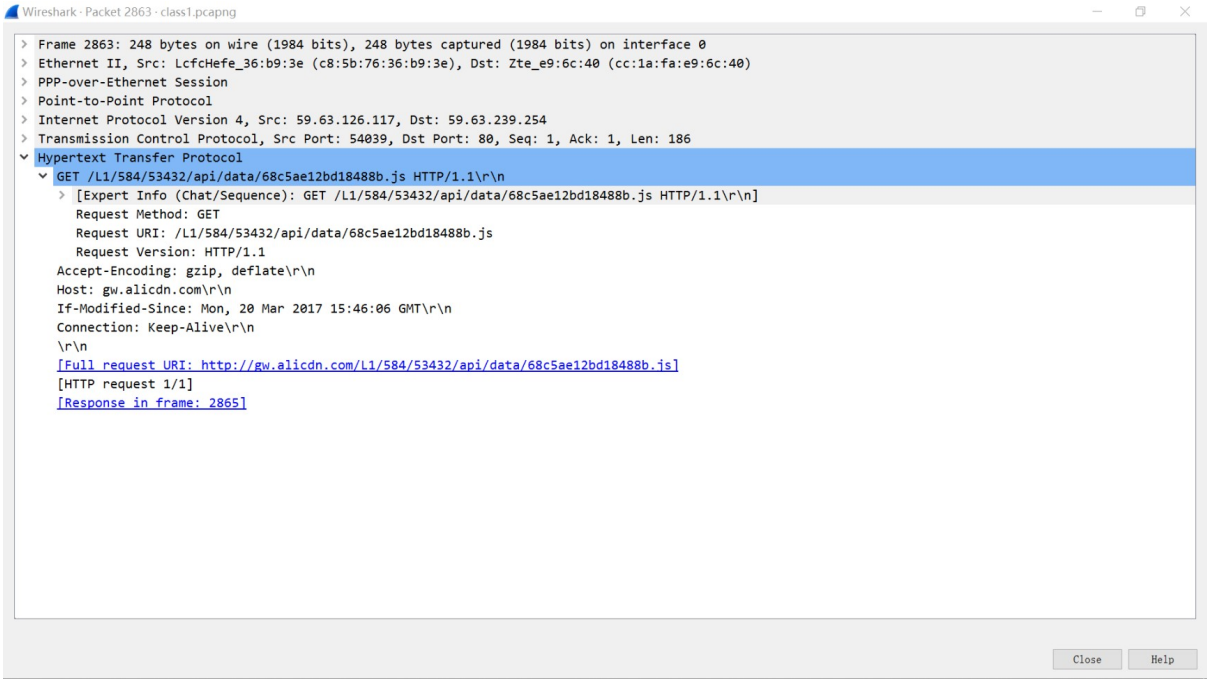
- **抓取**


class1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ··· <Ctrl-/>
Expression···
No. Time Source Destination Protocol Length Info
5408 3553.956460 HuaweiTe_5c:40… Broadcast ARP 64 Gratuitous ARP for 10.11.104.2 (Request) [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
5409 3554.969122 23.239.10.54 59.63.126.117 TCP 68 37350 → 8443 [SYN] Seq=0 Win=65535 Len=0
5410 3566.124787 103.205.177.35 59.63.126.112 TCP 60 38169 → 85 [SYN] Seq=0 Win=15895 Len=0
5411 3567.227865 59.63.126.117 117.21.209.186 UDP 236 59918 → 443 Len=186
5412 3573.937599 Zte_e9:6c:40 LcfcHefe_36:b9… ARP 60 Who has 59.63.126.112? Tell 59.63.126.1
5413 3573.937639 LcfcHefe_36:b9… Zte_e9:6c:40 ARP 42 59.63.126.112 is at c8:5b:76:36:b9:3e
5414 3584.749857 5.188.206.6 59.63.126.117 TCP 68 8080 → 13292 [SYN] Seq=0 Win=1024 Len=0
5415 3586.052882 93.174.93.136 59.63.126.112 TCP 60 48924 → 8010 [SYN] Seq=0 Win=1024 Len=0
Frame 2863: 248 bytes on wire (1984 bits), 248 bytes captured (1984 bits) on interface 0
Ethernet II, Src: LcfcHefe_36:b9:3e (c8:5b:76:36:b9:3e), Dst: Zte_e9:6c:40 (cc:1a:fa:e9:6c:40)
PPP-over-Ethernet Session
Point-to-Point Protocol
Internet Protocol Version 4, Src: 59.63.126.117, Dst: 59.63.239.254
Transmission Control Protocol, Src Port: 54039, Dst Port: 80, Seq: 1, Ack: 1, Len: 186
Hypertext Transfer Protocol
GET /L1/584/53432/api/data/68c5ae12bd18488b.js HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /L1/584/53432/api/data/68c5ae12bd18488b.js HTTP/1.1\r\n]
Request Method: GET
0000 cc 1a fa e9 6c 40 c8 5b 76 36 b9 3e 88 64 11 00 ····l@·[v6·>·d··
0010 74 e7 00 e4 00 21 45 00 00 e2 7c 14 40 00 80 06 t····!E· ··|·@···
0020 99 0f 3b 3f 7e 75 3b 3f ef fe d3 17 00 50 a8 4e ··;?~u;? ·····P·N
0030 d2 e9 ed 94 c4 44 50 18 04 00 a1 63 00 00 47 45 ·····DP· ···c··GE
0040 54 20 2f 4c 31 2f 35 38 34 2f 35 33 34 33 32 2f T /L1/58 4/53432/
0050 61 70 69 2f 64 61 74 61 2f 36 38 63 35 61 65 31 api/data /68c5ae1
0060 32 62 64 31 38 34 38 38 62 2e 6a 73 20 48 54 54 2bd18488 b.js HTT
0070 50 2f 31 2e 31 0d 0a 41 63 63 65 70 74 2d 45 6e P/1.1··A ccept-En
0080 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 coding: gzip, de
0090 66 6c 61 74 65 0d 0a 48 6f 73 74 3a 20 67 77 2e flate··H ost: gw.
00a0 61 6c 69 63 64 6e 2e 63 6f 6d 0d 0a 49 66 2d 4d alicdn.c om··If-M
class1.pcapng
Packets: 5415 · Displayed: 5415 (100.0%)
Profile: Default

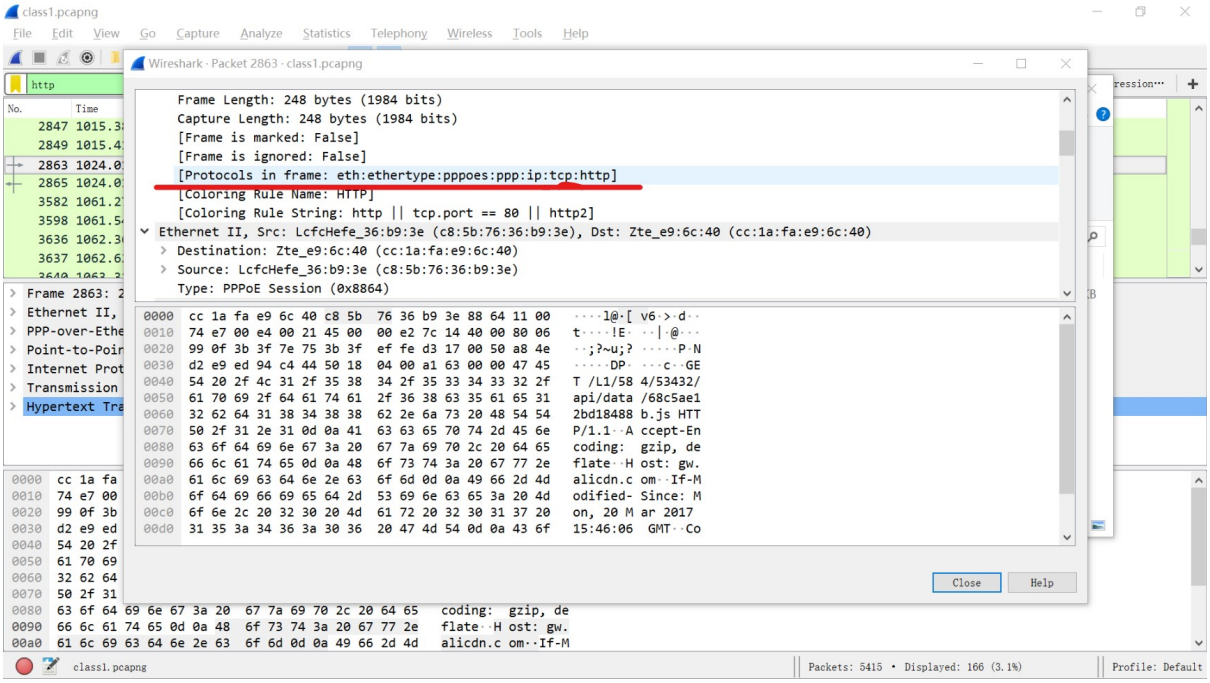
- **筛选 特定 http**


class1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression···
No. Time Source Destination Protocol Length Info
4173 1415.205473 59.63.126.117 23.193.104.14 HTTP 275 GET /zh-CN/livetile/preinstall?region=CN&appid=C98EA5B0842DBB9405BBF071E1DA76512D…
4178 1415.398091 23.193.104.14 59.63.126.117 HTTP/X… 333 HTTP/1.1 200 OK
4674 2290.109286 59.63.126.117 59.63.239.253 HTTP 248 GET /L1/584/53432/api/data/68c5ae12bd18488b.js HTTP/1.1
4676 2290.111759 59.63.239.253 59.63.126.117 HTTP 569 HTTP/1.1 304 Not Modified
4936 2735.742911 59.63.126.117 59.63.239.253 HTTP 248 GET /L1/584/53432/api/data/68c5ae12bd18488b.js HTTP/1.1
4938 2735.745276 59.63.239.253 59.63.126.117 HTTP 570 HTTP/1.1 304 Not Modified
5298 3364.497606 59.63.126.117 23.193.104.14 HTTP 275 GET /zh-CN/livetile/preinstall?region=CN&appid=C98EA5B0842DBB9405BBF071E1DA76512D…
5326 3364.697932 23.193.104.14 59.63.126.117 HTTP/X… 333 HTTP/1.1 200 OK
Frame 2863: 248 bytes on wire (1984 bits), 248 bytes captured (1984 bits) on interface 0
Ethernet II, Src: LcfcHefe_36:b9:3e (c8:5b:76:36:b9:3e), Dst: Zte_e9:6c:40 (cc:1a:fa:e9:6c:40)
PPP-over-Ethernet Session
Point-to-Point Protocol
Internet Protocol Version 4, Src: 59.63.126.117, Dst: 59.63.239.254
Transmission Control Protocol, Src Port: 54039, Dst Port: 80, Seq: 1, Ack: 1, Len: 186
Hypertext Transfer Protocol
0000 cc 1a fa e9 6c 40 c8 5b 76 36 b9 3e 88 64 11 00 ····l@·[v6·>·d··
0010 74 e7 00 e4 00 21 45 00 00 e2 7c 14 40 00 80 06 t····!E· ··|·@···
0020 99 0f 3b 3f 7e 75 3b 3f ef fe d3 17 00 50 a8 4e ··;?~u;? ·····P·N
0030 d2 e9 ed 94 c4 44 50 18 04 00 a1 63 00 00 47 45 ·····DP· ···c··GE
0040 54 20 2f 4c 31 2f 35 38 34 2f 35 33 34 33 32 2f T /L1/58 4/53432/
0050 61 70 69 2f 64 61 74 61 2f 36 38 63 35 61 65 31 api/data /68c5ae1
0060 32 62 64 31 38 34 38 38 62 2e 6a 73 20 48 54 54 2bd18488 b.js HTT
0070 50 2f 31 2e 31 0d 0a 41 63 63 65 70 74 2d 45 6e P/1.1··A ccept-En
0080 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 coding: gzip, de
0090 66 6c 61 74 65 0d 0a 48 6f 73 74 3a 20 67 77 2e flate··H ost: gw.
00a0 61 6c 69 63 64 6e 2e 63 6f 6d 0d 0a 49 66 2d 4d alicdn.c om··If-M
class1.pcapng
Packets: 5415 · Displayed: 166 (3.1%)
Profile: Default

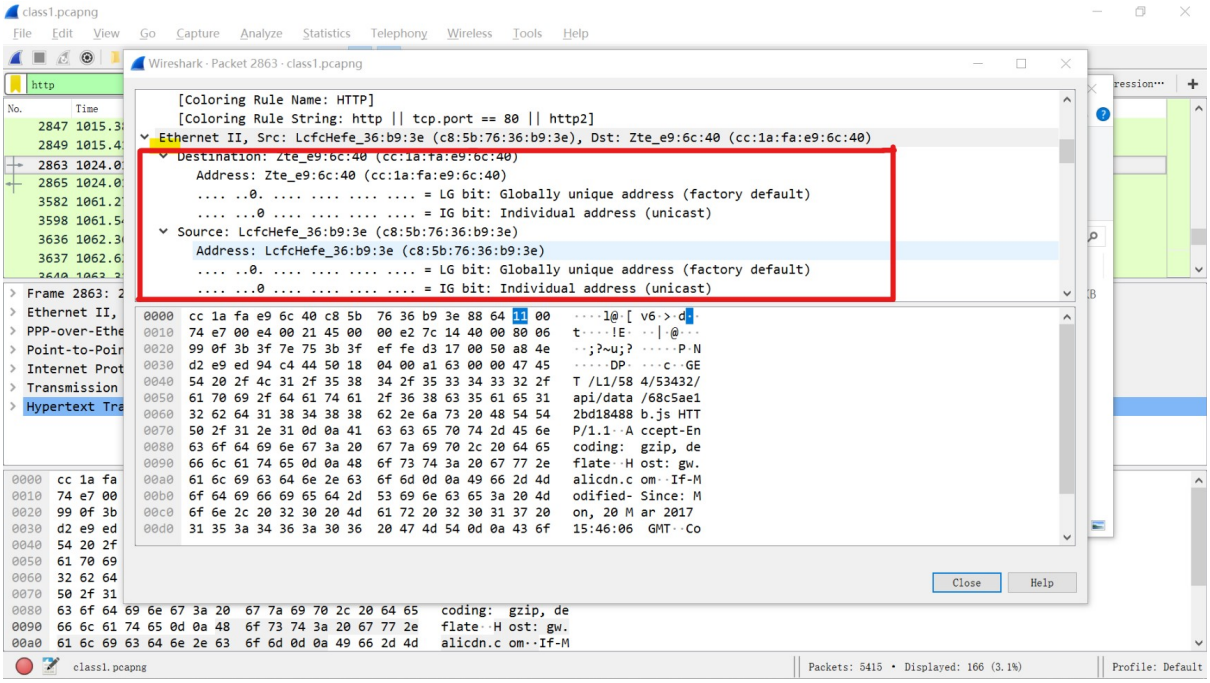
- **特定 http 包详情**



- **协议**



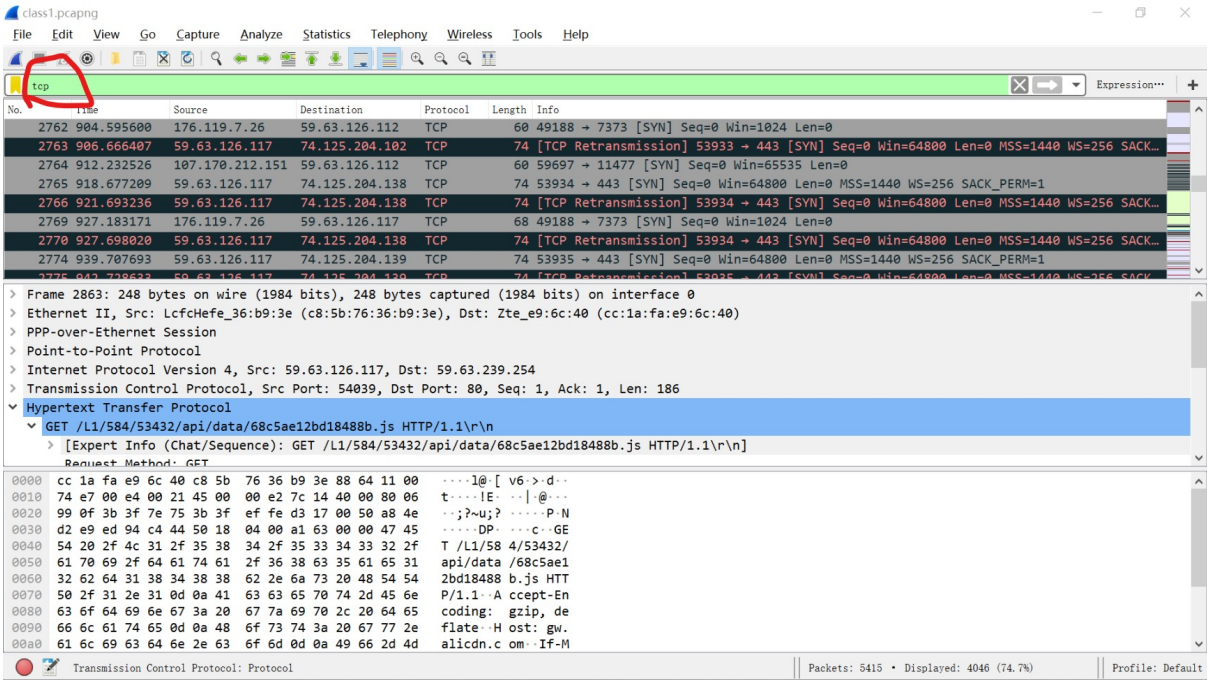
- **地址**



- **存活时间**

```
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: 128
Protocol: TCP (6)
Header checksum: 0x990f [validation disabled]
[Header checksum status: Unverified]
Source: 59.63.126.117
Destination: 59.63.239.254
```

- **筛选 tcp**



实验思考

四个问题：

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.

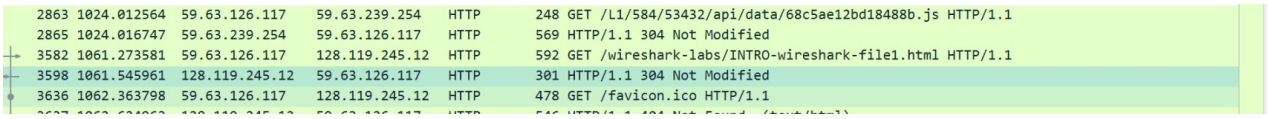
回答：

1.

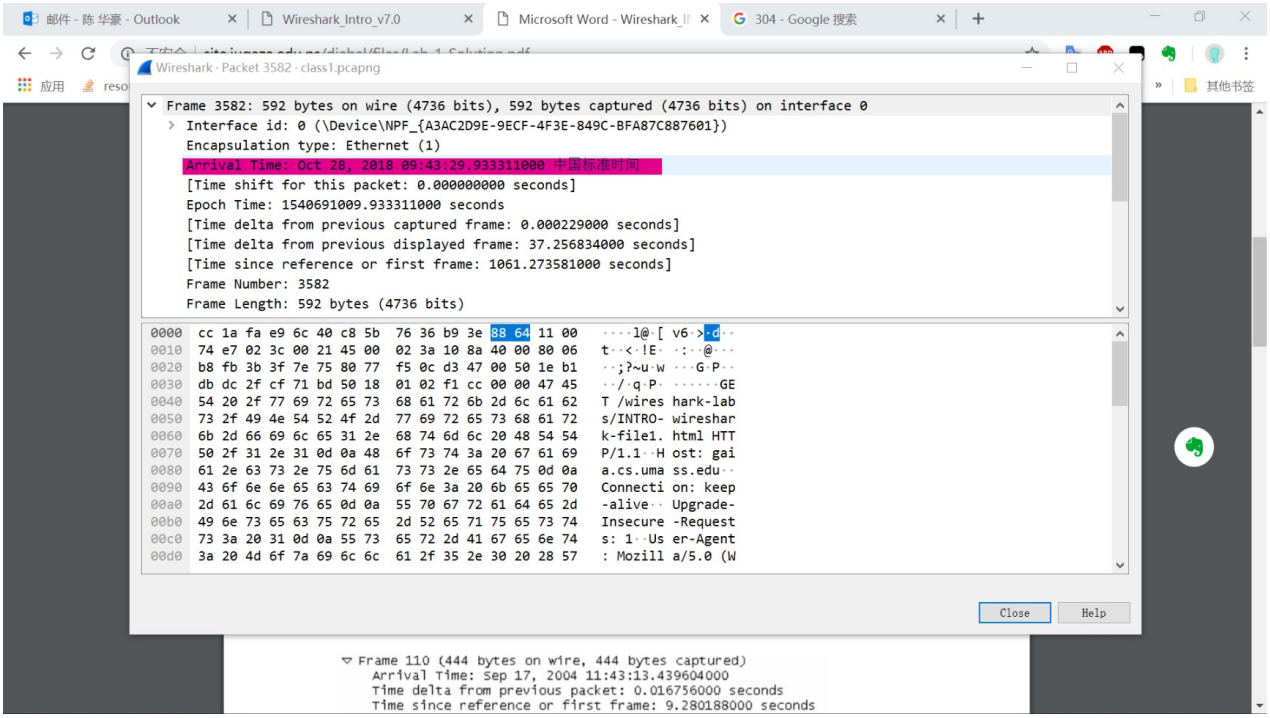
```
- TCP
- UDP
- DNS
```

2. 下载此网页 http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

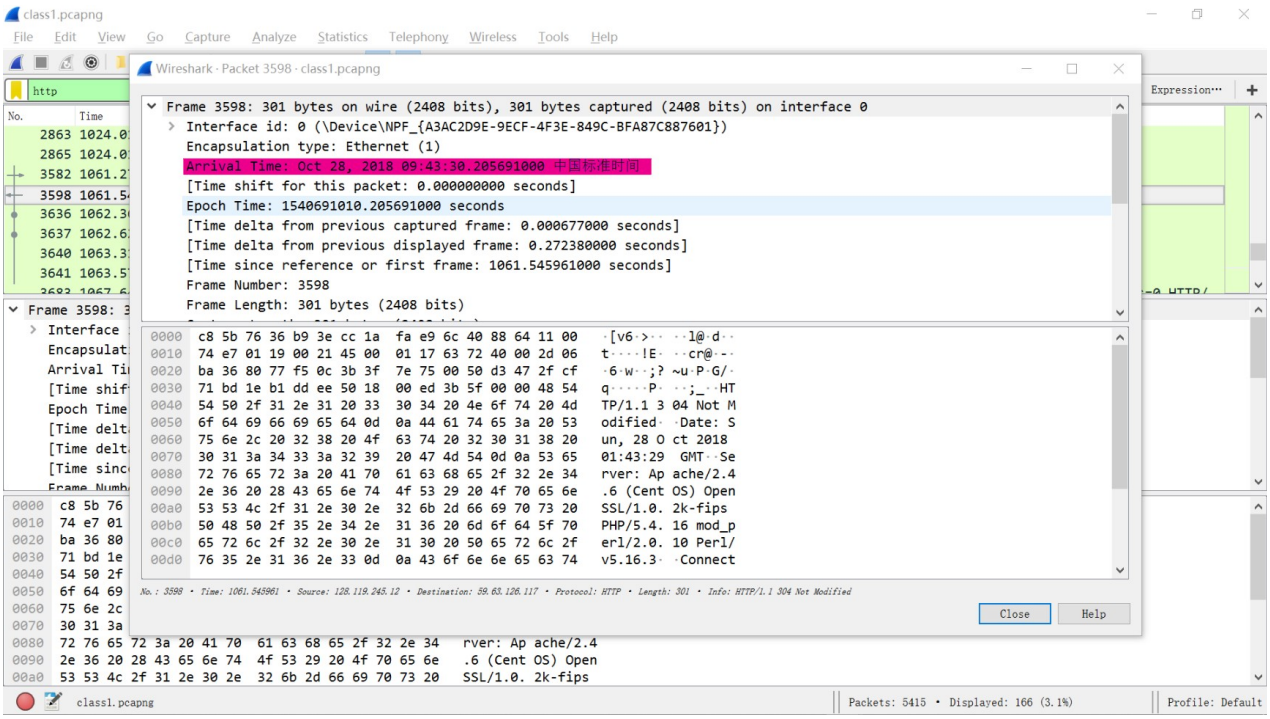
```
get-ok
```




```
到达时间：
```



回复时间：



Arrival Time: Oct 28, 2018 09:43:29.933311000 中国标准时间

Arrival Time: Oct 28, 2018 09:43:30.205691000 中国标准时间

相减得 0.27238s

3. 查看IPv4部分详情：

```
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 59.63.126.117
> Transmission Control Protocol, Src Port: 80, Dst Port: 54087, Seq: 1, Ack: 531, Len: 239
> Hypertext Transfer Protocol
```

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 59.63.126.117

本机地址为：128.119.245.12

网页服务器地址为：59.63.126.117

4. 打印结果如下：

```
No.     Time           Source                Destination           Protocol Length Info
   3582 1061.273581    59.63.126.117         128.119.245.12        HTTP     592    GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 3582: 592 bytes on wire (4736 bits), 592 bytes captured (4736 bits) on interface 0
Ethernet II, Src: LcfcHefe_36:b9:3e (c8:5b:76:36:b9:3e), Dst: Zte_e9:6c:40 (cc:1a:fa:e9:6c:40)
PPP-over-Ethernet Session
Point-to-Point Protocol
Internet Protocol Version 4, Src: 59.63.126.117, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 54087, Dst Port: 80, Seq: 1, Ack: 1, Len: 530
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; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100
Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,pl;q=0.7\r\n
    If-None-Match: "51-5792f8858d0ef"\r\n
    If-Modified-Since: Sat, 27 Oct 2018 05:59:01 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/3]
    [Response in frame: 3598]
    [Next request in frame: 3636]
No.     Time           Source                Destination           Protocol Length Info
   3598 1061.545961    128.119.245.12        59.63.126.117         HTTP     301    HTTP/1.1 304 Not Modified
Frame 3598: 301 bytes on wire (2408 bits), 301 bytes captured (2408 bits) on interface 0
Ethernet II, Src: Zte_e9:6c:40 (cc:1a:fa:e9:6c:40), Dst: LcfcHefe_36:b9:3e (c8:5b:76:36:b9:3e)
PPP-over-Ethernet Session
Point-to-Point Protocol
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 59.63.126.117
Transmission Control Protocol, Src Port: 80, Dst Port: 54087, Seq: 1, Ack: 531, Len: 239
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
    Date: Sun, 28 Oct 2018 01:43:29 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
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "51-5792f8858d0ef"\r\n
    \r\n
    [HTTP response 1/3]
    [Time since request: 0.272380000 seconds]
```

参考资料

- http://www-net.cs.umass.edu/wireshark-labs/

- http://www-net.cs.umass.edu/wireshark-labs/Wireshark*Intro*v7.0.pdf
- Computer Networking: A Top-Down Approach, Kurose and Ross