

XXX 大学

《计算机网路》实验报告

专业班级： 物联网 XXXX 学号： XXXXXXXXX 姓名： 郭 XX

实验一 WireShark 安装和运行

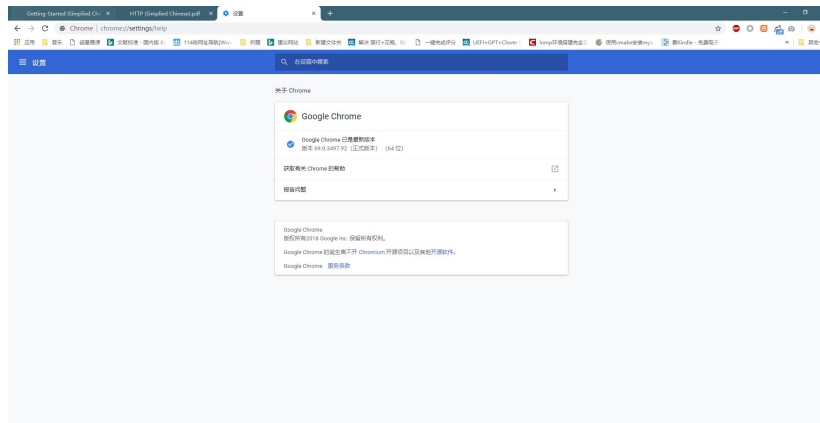
实验时间： 2018.9

【实验目的】

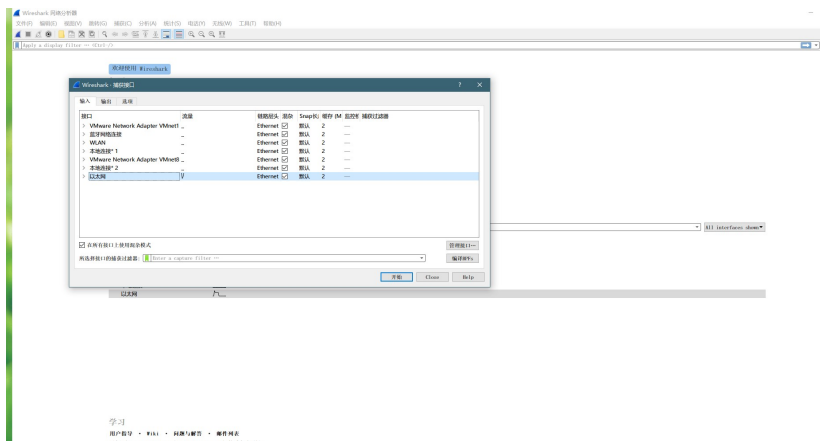
1. WireShark 的安装以及界面熟悉
2. 简单 HTTP 的抓取和过滤，结果进行分析和导出

【实验步骤】

1. 打开浏览器



2. 打开 WireShark 并且在捕获选项选择合适的网卡



Wireshark packet capture analysis of an HTTP GET request. The packet list shows a single packet (No. 12) at time 0.000000, source 172.20.10.10, and destination 128.119.245.12. The packet details pane shows the structure of the HTTP GET request, including the status bar indicating 480 bytes on wire and captured. The packet bytes pane shows the raw hex and ASCII data of the request, including the 'GET /wiresnar-lab/INTRO-wireshark-filip.html HTTP/1.1' line and various headers like 'Host: 128.119.245.12' and 'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4398.93 Safari/537.36'.

No.	Time	Source	Destination	Protocol	Length	Info
12	0.000000	172.20.10.10	128.119.245.12	HTTP	480	GET /wiresnar-lab/INTRO-wireshark-filip.html HTTP/1.1
13	0.000000	128.119.245.12	172.20.10.10	HTTP	492	HTTP/1.1 200 OK (text/html)

Frame 12: 480 bytes on wire (3840 bits), 480 bytes captured (3840 bits) on interface 0
 Ethernet II, Src: HwixpPc_F4:08:29 (18:f4:32:f4:08:29), Dst: 02:5f:45:e5:d8:64 (02:5f:45:e5:d8:64)
 Internet Protocol Version 4, Src: 172.20.10.10, Dst: 128.119.245.12
 Transmission Control Protocol, Src Port: 53765, Dst Port: 80, Seq: 1, Ack: 1, Len: 426
 Hypertext Transfer Protocol

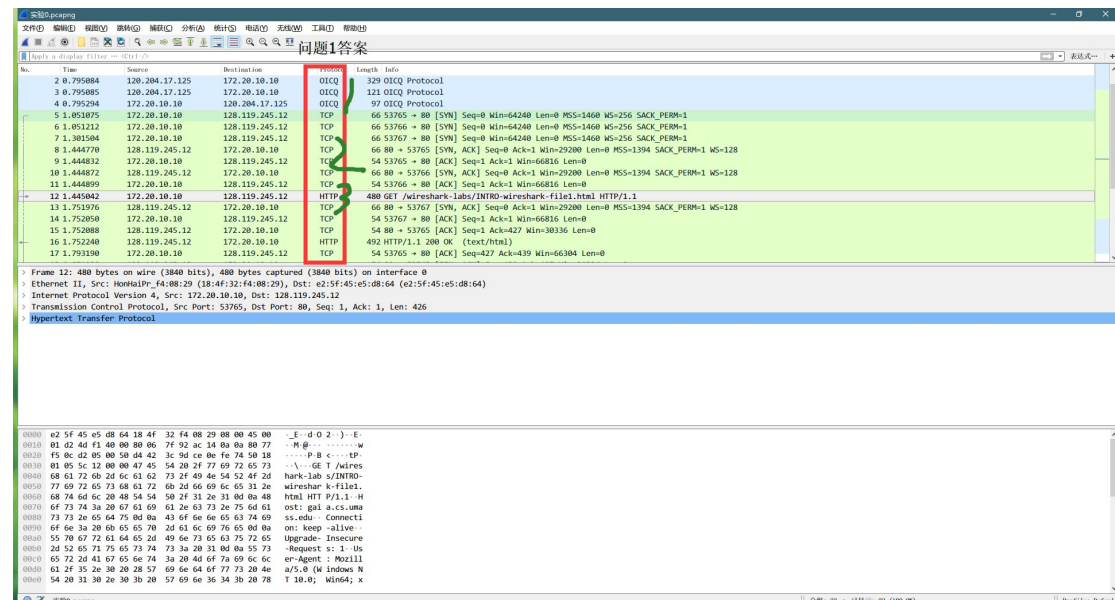
0000 02 5f 45 e5 d8 64 01 32 f4 08 29 08 00 45 00 _ E . d o 2 . : } E
 0010 61 d2 4d f1 60 00 80 06 7f 92 3c 1d 0a 80 77 - N # w
 0020 f5 0c d2 05 00 50 d4 42 3c 9d ce be f0 74 50 18 - P B TP
 0030 61 05 5c 12 00 00 4f 45 54 20 2f 7f 69 72 65 73 - \ \ - GE T / w i r e s n a r - l a b /
 0040 68 61 72 60 2d 6c 61 62 73 2f 49 4e 54 52 4f 2d h a r k - l a b / I N T R O -
 0050 77 69 72 65 73 68 61 72 69 2d 66 69 6c 65 31 2e w i r e s n a r - k - f i l i p .
 0060 68 7a 6d 6c 20 4f 54 54 50 2f 31 02 31 0d 0a 48 h t m l H T T P / 1 . 1 ;
 0070 6f 73 74 3a 20 67 61 69 61 2e 63 73 20 75 6d 61 o s t : g a i . a . c . u n a
 0080 73 73 2e 65 64 75 00 0a 43 6f 6e 0e 65 63 74 69 s s - e n e - C o n n e c t i
 0090 6f 6e 3a 20 6d 65 65 70 2d 61 6c 69 76 65 0d 0a o n : k e e p - a l i v e =
 0100 55 70 67 72 61 64 05 2d 49 6e 73 65 63 75 72 05 U p g r a d e - I n s e c u r e
 0110 2d 52 65 71 75 62 73 74 73 3a 20 31 0d 0a 55 73 R e q u e s t - s : 1 ;
 0120 65 72 2d 41 67 65 66 74 3a 20 4d 6f 7a 69 6c 6c e r - A g e n t : M o z i l l
 0130 61 2f 35 2e 30 30 28 57 69 6e 64 6f 77 73 20 4e a / 5 . 0 (W i n d o w s - N
 0140 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 30 20 78 T 1 0 . 0 ; M i n 6 4 ; x

6. 进行分析操作，请查看问题解答。

【实验结果】

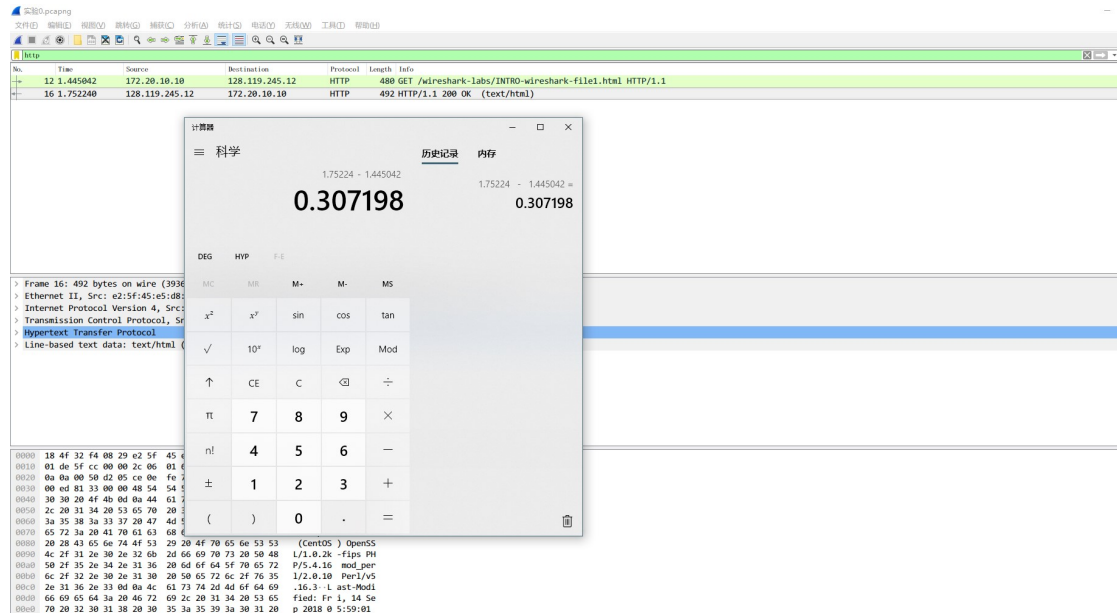
1. 列出在上面的步骤 7 中未过滤的 packet-listing window 中的协议列中出现的 3 种不同的协议。

ANS:OICQ,HTTP,TCP



2. 从发送 HTTP GET 消息到收到 HTTP OK 回复需要多长时间？

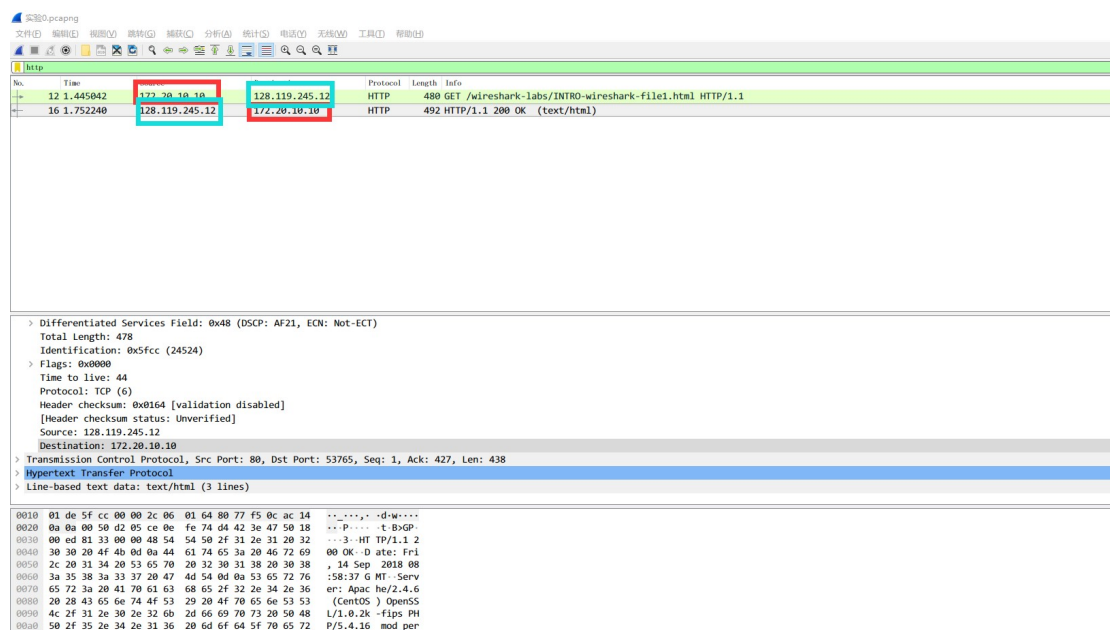
ANS=0.307198=1.752240-1.445042



3. gaia.cs.umass.edu（也称为 wwwnet.cs.umass.edu）的互联网地址是什么？ 您的计算机的 Internet 地址是什么？

ANS:我的 IP: 172.20.10.10

gaia.cs.umass.edu 的 IP: 128.119.245.12



4. Print 出上面问题 2 中提到的两条 HTTP 消息（GET 和 OK）。（参考文后附录）

【实验体会】

通过这次试验我简单了解到了 Wireshark 的使用，以及简单 HTTP 协议的抓包和分析，因为之前我也使用过 Wireshark，这次也是对它的更熟悉的过程。

继续加油！