

復旦大學

实验一 WireShark 的安装和运行

专业班级：信息安全_ 学号：22307130049_ 姓名：李思全_

【实验目的】

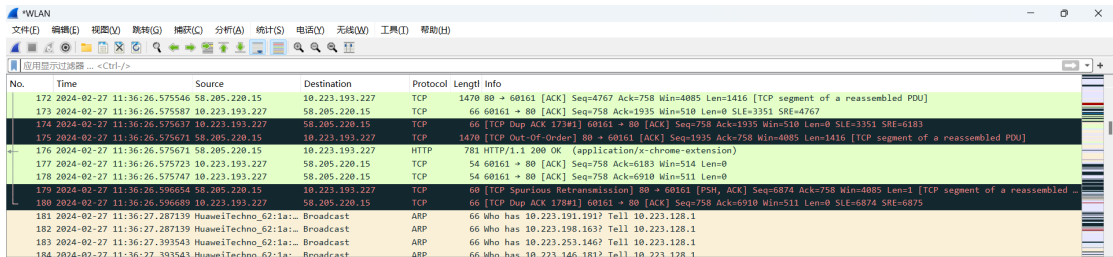
1. WireShark 的安装以及界面熟悉
2. 简单 HTTP 的抓取和过滤，结果进行分析和导出

【实验步骤】

1. 下载 WireShark 并安装
2. 打开接口列表并选择要抓取的接口，由于本电脑流量主要经过 WLAN，选择“WLAN”
3. 在浏览器中打开网页 <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>
4. 停止捕获，观察到抓取的包的协议
5. 利用筛选器筛选出 http 协议的包
6. 找到 HTTP GET，记录 GET 和 OK 消息的时间，Internet 地址，详细信息等
7. 关闭 WireShark，完成实验

【实验结果】

1. 在步骤 4 中，我们观察到抓取的包里除了 HTTP 协议外，还有 TCP 协议，DNS 协议，ARP 协议等其他协议



No.	Time	Source	Destination	Protocol	Length	Info
172	2024-02-27 11:36:26.575546	58.205.220.15	10.223.193.227	TCP	1470	80 → 60161 [ACK] Seq=4767 Ack=758 Win=4085 Len=1416 [TCP segment of a reassembled PDU]
173	2024-02-27 11:36:26.575587	10.223.193.227	58.205.220.15	TCP	66	60161 → 80 [ACK] Seq=758 Ack=1935 Win=510 Len=0 SLE=3351 SRE=4767
174	2024-02-27 11:36:26.575637	10.223.193.227	58.205.220.15	TCP	66	[TCP Dup ACK 173#1] 60161 → 80 [ACK] Seq=758 Ack=1935 Win=510 Len=0 SLE=3351 SRE=6183
175	2024-02-27 11:36:26.575671	58.205.220.15	10.223.193.227	TCP	1470	[TCP Out-Of-Order] 80 → 60161 [ACK] Seq=1935 Ack=758 Win=4085 Len=1416 [TCP segment of a reassembled PDU]
176	2024-02-27 11:36:26.575671	58.205.220.15	10.223.193.227	HTTP	781	HTTP/1.1 200 OK (application/x-chrome-extension)
177	2024-02-27 11:36:26.575723	10.223.193.227	58.205.220.15	TCP	54	60161 → 80 [ACK] Seq=758 Ack=6183 Win=514 Len=0
178	2024-02-27 11:36:26.575747	10.223.193.227	58.205.220.15	TCP	54	60161 → 80 [ACK] Seq=758 Ack=6210 Win=511 Len=0
179	2024-02-27 11:36:26.596054	58.205.220.15	10.223.193.227	TCP	60	[TCP Spurious Retransmission] 80 → 60161 [PSH, ACK] Seq=6874 Ack=758 Win=4085 Len=1 [TCP segment of a reassembled PDU]
180	2024-02-27 11:36:26.596089	10.223.193.227	58.205.220.15	TCP	66	[TCP Dup ACK 178#1] 60161 → 80 [ACK] Seq=758 Ack=6910 Win=511 Len=0 SLE=6874 SRE=6875
181	2024-02-27 11:36:27.287139	HuaweiTechno_62:1a:...	Broadcast	ARP	66	Who has 10.223.193.191? Tell 10.223.128.1
182	2024-02-27 11:36:27.287139	HuaweiTechno_62:1a:...	Broadcast	ARP	66	Who has 10.223.198.163? Tell 10.223.128.1
183	2024-02-27 11:36:27.393543	HuaweiTechno_62:1a:...	Broadcast	ARP	66	Who has 10.223.253.146? Tell 10.223.128.1
184	2024-02-27 11:36:27.393543	HuaweiTechno_62:1a:...	Broadcast	ARP	66	Who has 10.223.146.1812. Tell 10.223.128.1

No.	Time	Source	Destination	Protocol	Length	Info
157	2024-02-27 11:36:26.537557	2620:1ec:12::239	24bc::c791:2:807:bcd::	TCP	74	443 → 60149 [ACK] Seq=399 Ack=1664 Win=16385 Len=0
158	2024-02-27 11:36:26.522437	58.205.220.15	10.223.193.227	TCP	60	[TCP Spurious Retransmission] 80 → 60161 [PSH, ACK] Seq=940 Ack=354 Win=4085 Len=1
159	2024-02-27 11:36:26.522467	10.223.193.227	58.205.220.15	TCP	66	[TCP Dup ACK 156#1] 60161 → 80 [ACK] Seq=354 Ack=968 Win=514 Len=0 SLE=940 SRE=941
160	2024-02-27 11:36:26.528978	58.205.220.15	10.223.193.227	TCP	60	[TCP Spurious Retransmission] 80 → 60161 [PSH, ACK] Seq=938 Ack=354 Win=4085 Len=1
161	2024-02-27 11:36:26.528979	10.223.193.227	58.205.220.15	TCP	66	[TCP Dup ACK 156#2] 60161 → 80 [ACK] Seq=354 Ack=968 Win=514 Len=0 SLE=938 SRE=939
162	2024-02-27 11:36:26.530111	240c::c791:2:807:bcd::	2001:da8:8001:2::250::	DNS	121	Standard query 0x8266 AAAA wsedge.b.tlu.dl.delivery.mp.microsoft.com
163	2024-02-27 11:36:26.535562	2001:da8:8001:2::250::	240c::c791:2:807:bcd::	DNS	338	Standard query response 0x8266 AAAA wsedge.b.tlu.dl.delivery.mp.microsoft.com CNAME cdp-tlu-shim.trafficmanager.net
164	2024-02-27 11:36:26.537032	58.205.220.15	10.223.193.227	TCP	60	[TCP Spurious Retransmission] 80 → 60161 [PSH, ACK] Seq=936 Ack=354 Win=4085 Len=1
165	2024-02-27 11:36:26.537063	10.223.193.227	58.205.220.15	TCP	66	[TCP Dup ACK 156#1] 60161 → 80 [ACK] Seq=354 Ack=968 Win=514 Len=0 SLE=936 SRE=937
166	2024-02-27 11:36:26.537569	10.223.193.227	58.205.220.15	HTTP	458	GET /filestreamingservice/files/22bd2c3f-162f-4ed8-934e-97de224b15777P1=17096028498P2=4048P3=28P4=K5Ikeep4N1Ruee3Fx5oG2V...
167	2024-02-27 11:36:26.540613	58.205.220.15	10.223.193.227	TCP	60	[TCP Spurious Retransmission] 80 → 60161 [PSH, ACK] Seq=934 Ack=354 Win=4085 Len=1
168	2024-02-27 11:36:26.545107	10.223.193.227	58.205.220.15	TCP	66	[TCP Dup ACK 156#4] 60161 → 80 [ACK] Seq=354 Ack=968 Win=514 Len=0 SLE=934 SRE=935
169	2024-02-27 11:36:26.574127	58.205.220.15	10.223.193.227	TCP	60	80 → 60161 [ACK] Seq=968 Ack=758 Win=4082 Len=0

2. 通过筛选后 GET 消息与 OK 消息中记录的时间， 2024-02-27 11:36:26.537569 与 2024-02-27 11:36:26.575671 ， 计算得 回复时间为 0.038102 秒

147	2024-02-27 11:36:26.461978	10.223.193.227	58.205.220.15	HTTP	407	HEAD /filestreamingservice/files/22bd2c3f-162f-4ed8-934e-97de224b15777P1=17096028498P2=4048P3=28P4=K5Ikeep4N1Ruee3Fx5oG2V...
154	2024-02-27 11:36:26.507625	58.205.220.15	10.223.193.227	HTTP	1021	HTTP/1.1 200 OK
166	2024-02-27 11:36:26.537569	10.223.193.227	58.205.220.15	HTTP	458	GET /filestreamingservice/files/22bd2c3f-162f-4ed8-934e-97de224b15777P1=17096028498P2=4048P3=28P4=K5Ikeep4N1Ruee3Fx5oG2V...
176	2024-02-27 11:36:26.575671	58.205.220.15	10.223.193.227	HTTP	781	HTTP/1.1 200 OK (application/x-chrome-extension)

3. 我的计算机的 Internet 地址为 10.223.193.227, gaia.cs.umass.edu 的 Internet 地址为 58.205.220.15

No.	Time	Source	Destination	Protocol	Length	Info
147	2024-02-27 11:36:26.461978	10.223.193.227	58.205.220.15	HTTP	407	HEAD /filestreamingservice/files/22bd2c3f-162f-4ed8-934e-97de224b15777P1=17096028498P2=4048P3=28P4=K5Ikeep4N1Ruee3Fx5oG2V...
154	2024-02-27 11:36:26.507625	58.205.220.15	10.223.193.227	HTTP	1021	HTTP/1.1 200 OK
166	2024-02-27 11:36:26.537569	10.223.193.227	58.205.220.15	HTTP	458	GET /filestreamingservice/files/22bd2c3f-162f-4ed8-934e-97de224b15777P1=17096028498P2=4048P3=28P4=K5Ikeep4N1Ruee3Fx5oG2V...
176	2024-02-27 11:36:26.575671	58.205.220.15	10.223.193.227	HTTP	781	HTTP/1.1 200 OK (application/x-chrome-extension)

> Frame 166: 458 bytes on wire (3664 bits)	0000	e0 4b a6 62 1a 1d f4 26	79 72 06 23 08 00 45 00	.K b . & y r # : E
> Ethernet II, Src: Intel72:06:23 (f4:2	0010	01 bc f6 0a 40 00 40 06	00 00 0a ff c1 e3 3a rd	... @ ... : :
> Internet Protocol Version 4, Src: 10.2	0020	dc 0f eb 01 00 50 9a 3f	e6 c5 50 d3 3d 61 50 18 P ? : P : aP
> Transmission Control Protocol, Src Por	0030	02 02 e5 4d 00 00 47 45	54 20 2f 66 69 6c 65 73	... M GET / /files
> Hypertext Transfer Protocol	0040	74 72 63 18 f5 08 10 6e	67 73 65 72 70 69 63 65 2f	streamingservice/
	0050	66 69 6c 65 73 2f 32 32	62 64 32 63 33 66 2d 31	files/22 bd2c3f-1
	0060	36 32 66 2d 34 65 64 38	2d 39 33 34 65 2d 39 37	62f-4ed8 -934e-97
	0070	64 65 32 34 62 21 35	37 3f 50 31 3d 31 37	de224b15 777P1=17
	0080	30 39 36 30 32 38 34 39	26 50 32 3d 34 30 34 26	09602849 8P2=4048
	0090	60 33 3d 32 26 50 34 3d	4b 35 49 6b 65 65 70 34	P3=28P4= K5Ikeep4
	00a0	4a 69 52 55 65 65 33 46	78 35 6f 47 32 56 5a 66	N1Ruee3F x5oG2V...
	00b0	62 34 53 61 74 62 62 50	5a 5a 4a 39 5a 36 43 55	b4SatbBP 27N976C0
	00c0	31 75 55 48 38 73 7a 4c	52 4f 78 7a 56 78 63 68	luU8StL R0x1vach
	00d0	5a 6c 39 32 75 6f 68 39	6f 74 70 44 44 25 32 66	2192noh0 o1p00RT4
	00e0	36 77 6a 62 42 59 51 25	32 62 43 5a 64 70 4d 39	6wJBbVQk 2bC2d4p0
	00f0	37 41 25 33 64 25 33 64	20 48 54 54 50 2f 31 26	7A53dR3M HTTP/1
	0100	11 0a 00 43 6f 6e 6e 65	63 74 69 6f 6e 3a 20 4b	L: connec tion: K
	0110	65 65 70 2d 41 6c 69 76	65 0d 0a 41 63 63 65 70	keep-Alive e-Accep
	0120	74 3a 20 2a 2f 2a 0d 0a	41 63 63 65 70 74 2d 45	t: */*: Accept-E
	0130	6e 63 6f 64 69 6e 67 3a	20 69 64 65 6e 74 69 74	ncoding: identiti
	0140	79 0d 0a 49 66 2d 55 6e	6d 6f 64 69 69 69 65 64	y-:If-Un modified
	0150	2d 53 69 6e 63 65 3a 20	53 61 74 2c 20 30 36 20	-Since: Sat, 06
	0160	4a 61 6e 20 32 30 32 34	20 31 38 3a 32 38 3a 31	Jan 2024, 18:28:11
	0170	31 20 47 4d 54 0d 0a 55	73 65 72 2d 41 67 65 6e	1 GMT--U ser-Agen
	0180	74 3a 20 4d 69 63 72 6f	73 6f 66 74 20 42 49 54	t: Micro soft BIT
	0190	53 2f 37 2e 38 0d 0a 48	6f 73 74 3a 20 6d 73 65	5/7,0-H ost: msa
	01a0	64 67 65 2e 62 2e 7a 6c	75 2a 64 6c 2e 64 65 6c	dge.b.tl u.dl.del
	01b0	69 76 65 72 79 2e 6d 70	2e 6d 69 63 72 6f 73 6f	ivery.mp .microso
	01c0	66 74 2e 63 6f 6d 0d 0a	bd 0a	ft.com:...

4. Text item (text), 205 byte(s) | 分信: 732 · 已显示: 4 (0.5%) · 已丢弃: 0 (0.0%) | 配置: Default

WULAN
文件(F) 编辑(E) 视图(V) 传输(T) 捕获(C) 统计(S) 电话(T) 无线(W) 工具(I) 帮助(H)

http
⏮ ⏪ ⏩ ⏭ 🔍 🔄

No.	Time	Source	Destination	Protocol	Length	Info
147	2024-02-27 11:36:26.461978	10.223.193.227	58.205.220.15	HTTP	407	HEAD /filestreamingservice/files/22bd2c3f-162f-4ed8-934e-97de224b15777P1-17096028498P2-4048P3=28P4=KS1keep4NIIRue3FxF5oG2...
154	2024-02-27 11:36:26.507625	58.205.220.15	10.223.193.227	HTTP	302	HTTP/1.1 200 OK
164	2024-02-27 11:36:26.537695	10.223.193.227	58.205.220.15	HTTP	458	GET /filestreamingservice/files/22bd2c3f-162f-4ed8-934e-97de224b15777P1-17096028498P2-4048P3=28P4=KS1keep4NIIRue3FxF5oG2...
176	2024-02-27 11:36:26.575671	58.205.220.15	10.223.193.227	HTTP	783	HTTP/1.1 200 OK (application/x-chrome-extension)

> Frame 176: 781 bytes on wire (6248 bits)

> Ethernet II, Src: HuaweiTechno_62:1a:1e

> Internet Protocol Version 4, Src: 58.205.220.15

> Transmission Control Protocol, Src Port: 58205

> [Reassembled TCP Segments (5942 bytes)]

> **Hypertext Transfer Protocol**

> Media Type

```

0000  f4 26 79 72 06 23 e0 ab a6 62 1a 1d 08 00 45 00  8yp # K b ---E-
0010  02 ff ef fe 40 00 34 06 74 5b 3a cd cf 0f 0a df  ...@ 4 [1:---
0020  c1 e3 00 50 eb 01 50 d3 51 c0 9a 3f 8b 59 50 18  ...P Q ? ?YP-
0030  0f fe 43 00 00 72 2d c5 5d 47 97 43 4c 4b 5d  ...F fe 43 00 00 72 2d c5 5d 47 97 43 4c 4b 5d
0040  9f bc cc 44 08 f6 72 47 48 8e fc d5 b0 e6 2e 67  ...D rw H ---g
0050  12 89 32 51 84 30 18 db 21 a9 58 81 80 2a 2d a6  ...2Q 0 - 1 X ---
0060  3b 3d c2 1d 2d c2 ce 91 ba 08 3b 4a 3c 6d 76 e7  ...@ - R
0070  93 01 2e ac f7 91 d7 e1 8d 87 f0 ad 19 5a 92 52  ...P -9 dle- I
0080  f5 a7 88 3c 50 b3 c1 39 11 64 ac 31 65 8b b6 49  ...- - - - -
0090  4c 95 98 26 3a 6a 75 c5 5c 02 56 78 c8 c2 0c c1  ...- - - - -
00a0  7c f3 cd e9 f9 24 8a ce 9d bd ad 31 f3 db c8 00  ...- - - - -
00b0  71 d7 5d b1 56 74 3d 2c cf 4f 79 34 a6 79 f2 89  ...q ] Vtr- 0yd y-
00c0  bc a9 59 c6 80 b6 05 88 be 9f ba 33 46 bd 08 54  ...Y --- - - - -
00d0  fd 20 35 71 79 74 f0 64 f7 90 ed d1 94 1c 00 c5  ...Sag d - - - -
00e0  f5 a0 9e 13 34 1a 64 aa fe 0c 36 26 fa d8 31 9f 5a  ...-3 jD -> 8- 1 Z
00f0  c6 00 b0 e4 ead 74 21 bc b5 a6 b1 64 fa c8 4b 08  ...- - - - -
0100  d1 f1 73 71 6c 57 8f 11 8a 9b 30 f1 13 f7 fe ed  ...- - - - -
0110  cb b7 6f 5f be 03 50 4b 01 02 3f 00 14 00 00 00  ...- - - - -
0120  08 00 14 75 94 57 8f 68 54 aa 1e 03 00 00 16 06  ...- - - - -
0130  00 00 00 00 24 00 00 00 00 00 00 00 00 00 00  ...- - - - -
0140  00 00 00 00 4c 49 43 45 4e 53 45 0a 00 20 00 00  ...- - - - -
0150  00 00 00 01 00 18 00 00 79 67 8b 52 33 da 01 42  ...- - - - -
0160  a9 c6 9e cb 40 da 01 42 a9 c6 9e cb 40 da 01 50  ...- - - - -
0170  4b 01 02 3f 00 14 00 00 00 00 01 14 75 94 57 a1  ...K - - - - -
0180  2f 14 36 51 00 00 00 56 00 00 00 00 24 00 00 00  .../ - - - - -
0190  00 00 00 00 00 00 00 00 43 03 00 00 6d 61 6e  ...- - - - -
01a0  69 66 65 73 74 2a 6a 73 67 6a 0a 00 20 00 00 00  ...lfeet.js on
01b0  00 00 01 00 18 00 00 79 67 8b 52 33 da 01 42 a9  ...- - - - -
01c0  c6 8e cb 40 da 01 42 a9 c6 8e cb 40 da 01 50 4b  ...- - - - -
01d0  01 02 3f 00 14 00 00 00 00 00 1d 75 94 57 8b 57  ...- - - - -
01e0  cc db 5c 03 00 00 e2 0f 00 00 09 24 00 00 00 00  ...- - - - -
01f0  00 00 00 00 80 00 00 00 bf 03 00 00 73 65 74 73  ...- - - - -
0200  2a 6a 73 7f 6e 0a 00 20 00 00 00 00 01 01 18  ...- - - - -
0210  00 00 79 67 8b 52 33 da 01 93 43 c4 8e cb 40 da  ...yg R3 - - - @-
  
```

Frame (781 bytes) Reassembled TCP (5942 bytes)

 统计: 732 - 已显示: 4 (0.5%) - 已丢弃: 0 (0.0%)

Hypertext Transfer Protocol
配置: Default