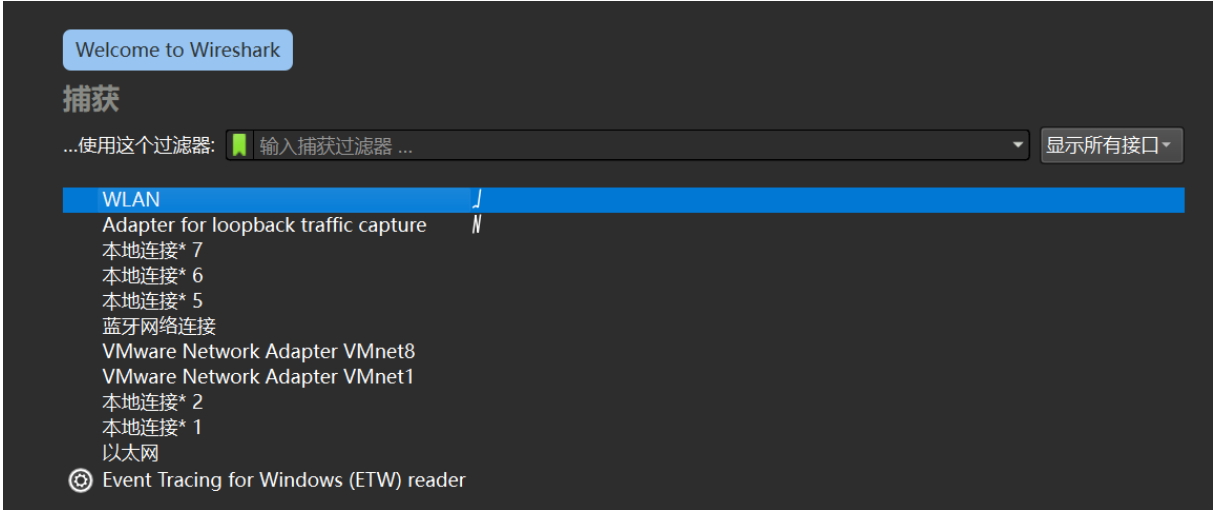


# 计算机学院 计算机网络 课程实验报告

实验题目：初步了解 WireShark1，并进行一些简单的数据包捕获和观察。		学号：202200400053
日期：2024-03-08	班级： 2 班	姓名： 王宇涵
Email：1941497679@qq. com		
<p>实验方法介绍：</p> <ol style="list-style-type: none"><li>1. 了解 WireShark 抓包的原理</li><li>2. 通过下载, 安装, 初步运行 WireShark, 了解界面的功能, 进行简单的抓包过程, 来理解数据的含义</li><li>3. 通过对数据含义的分析和理解加深对理论课学习的理解</li></ol>		
<p>实验过程描述：</p> <ol style="list-style-type: none"><li>1. 启动 WireShark，选择合适的接口，我们这里选择 WLAN</li></ol> <div></div> <ol style="list-style-type: none"><li>2. 进入抓包页面</li></ol>		

正在捕获 WLAN

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

应用显示过滤器 ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
409	1.740433	2001:250:5800:1002::...	ff02::1:ffa6:933e	ICMPv6	86	Neighbor Solicitation for 2001:250:5800:1002:a:c589...
410	1.740433	2001:250:5800:1002::...	ff02::1:ff20:1618	ICMPv6	86	Neighbor Solicitation for fe80::22:dce8:5f20:1618 f...
411	1.740433	2001:250:5800:1002::...	ff02::1:ff44:5262	ICMPv6	86	Neighbor Solicitation for fe80::10cd:33b7:4c44:5262...
412	1.840276	2001:250:5800:1002::...	ff02::1:ffa6:f460	ICMPv6	86	Neighbor Solicitation for fe80::1c42:40b3:21a6:f460...
413	1.842630	2001:250:5800:1000::...	ff02::1:ff7d:e770	ICMPv6	86	Neighbor Solicitation for 2001:250:5800:1002:c4:e1d...
414	1.842630	2001:250:5800:1002::...	ff02::1:ffdf:415d	ICMPv6	86	Neighbor Solicitation for fe80::10b6:e135:3ddf:415d...
415	2.048515	2001:250:5800:1002::...	ff02::1:ff51:103c	ICMPv6	86	Neighbor Solicitation for fe80::1c2b:af9f:5851:103c...
416	2.048515	2001:250:5800:1002::...	ff02::1:ffb1:904c	ICMPv6	86	Neighbor Solicitation for fe80::c47:982a:75b1:904c ...
417	2.048515	2001:250:5800:1002::...	ff02::1:ff63:8b16	ICMPv6	86	Neighbor Solicitation for fe80::484:553c:c663:8b16 ...
418	2.048515	2001:250:5800:1002::...	ff02::1:ff56:8e5a	ICMPv6	86	Neighbor Solicitation for fe80::c33:c1af:ee56:8e5a ...
419	2.048515	2001:250:5800:1002::...	ff02::1:ff81:a4d6	ICMPv6	86	Neighbor Solicitation for fe80::1441:2f3f:b081:a4d6...
420	2.048515	2001:250:5800:1000::...	ff02::1:ff85:7501	ICMPv6	86	Neighbor Solicitation for 2001:250:5800:1002:d:12f1...
421	2.048515	2001:250:5800:1002::...	ff02::1:ffaf:aad0	ICMPv6	86	Neighbor Solicitation for fe80::18aa:87e3:deaf:aad0...
422	2.149777	2001:250:5800:1002::...	ff02::1:ffc0:677f	ICMPv6	86	Neighbor Solicitation for fe80::44f:81e:4bc0:677f f...
423	2.228252	172.25.174.42	104.18.30.200	TLSv1.2	93	Application Data
424	2.250427	2001:250:5800:1002::...	ff02::1:fff5:dd9e	ICMPv6	86	Neighbor Solicitation for fe80::182f:614d:6ff5:dd9e...
425	2.250427	2001:250:5800:1002::...	ff02::1:ff66:37f8	ICMPv6	86	Neighbor Solicitation for fe80::c87:1af9:9b66:37f8 ...
426	2.279943	104.18.30.200	172.25.174.42	TCP	56	443 → 57646 [ACK] Seq=1 Ack=40 Win=7 Len=0
427	2.354677	2001:250:5800:1002::...	ff02::1:ffc0:be56	ICMPv6	86	Neighbor Solicitation for fe80::9c:13d9:bec0:be56 f...

Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bit) on interface wlan0  
 Ethernet II, Src: JuniperNetwo\_f6:12:a0 (28:a2:4b:f6:12:a0), Dst: ff:02::1:ffa6:933e  
 Internet Protocol Version 6, Src: 2001:250:5800:1002::1, Dst: ff02::1:ffa6:933e  
 Internet Control Message Protocol v6

WLAN: <live capture in progress> 分组: 427 · 已显示: 427 (100.0%) 配置: Default

- 分析界面：数据列从左到右依此是抓取的数据包编号，时间，发送源，到达地，协议类型，长度，详细信息
- 单击某一条数据包，即可查到详细的数据包信息，包括有关以太网帧(假设数据包是通过以太网接口发送/接收的)和包含该数据包的 IP 数据报的信息

10	0.701998	172.25.174.42	120.220.244.67	HTTP	698	GET /O8M0000eaMed3yYvDf.mgg?guid=16B2B0F0DAC71...
11	0.715950	2001:250:5800:1000::...	ff02::1:ff34:b4fb	ICMPv6	86	Neighbor Solicitation for 2001:250:5800:1002:3...
12	0.715950	2001:250:5800:1002:...	ff02::1:fff3:dd70	ICMPv6	86	Neighbor Solicitation for fe80::873:5d5e:47f3:...
13	0.717472	120.220.244.67	172.25.174.42	TCP	56	80 → 51547 [ACK] Seq=1 Ack=645 Win=4080 Len=0
14	0.718094	120.220.244.67	172.25.174.42	TCP	883	80 → 51547 [PSH, ACK] Seq=1 Ack=645 Win=4085 L...
15	0.718474	120.220.244.67	172.25.174.42	TCP	1514	[TCP Previous segment not captured] 80 → 51547...
16	0.718537	172.25.174.42	120.220.244.67	TCP	66	51547 → 80 [ACK] Seq=645 Ack=830 Win=2049 Len=...
17	0.718823	120.220.244.67	172.25.174.42	TCP	1514	80 → 51547 [ACK] Seq=8130 Ack=645 Win=4085 Len=...
18	0.718849	172.25.174.42	120.220.244.67	TCP	66	[TCP Dup ACK 16#1] 51547 → 80 [ACK] Seq=645 Ac...
19	0.720082	120.220.244.67	172.25.174.42	TCP	1514	[TCP Previous segment not captured] 80 → 51547...

Frame 10: 698 bytes on wire (5584 bits), 698 bytes captured (5584 bits) on interface 0	0000	28	a2	4b	f6	12	a0	c8	cb	9e	78	be	0a	08	00	45	00	( K ...
Ethernet II, Src: Intel_78:be:0a (c8:cb:9e:78:be:0a), Dst: Juniper_78:be:0a (08:00:06:00:00:00)	0010	02	ac	37	84	40	00	00	06	00	00	ac	19	ae	2a	78	dc	7 @ ...
Internet Protocol Version 4, Src: 172.25.174.42, Dst: 120.220.244.67	0020	f4	43	c9	5b	00	50	ac	f2	ce	a9	b9	87	dc	4a	50	18	C [ P ...
Transmission Control Protocol, Src Port: 51547, Dst Port: 80, Seq: 51547, Len: 0	0030	08	05	ca	02	00	00	47	45	54	20	2f	4f	38	4d	30	30	... G
Hypertext Transfer Protocol	0040	30	30	65	61	4d	65	64	33	79	59	76	44	66	2e	6d	67	00eaMed
	0050	67	3f	67	75	69	64	3d	31	36	42	32	42	30	46	30	44	g?guid=
	0060	41	43	37	31	45	37	39	45	38	33	30	44	43	35	31	30	AC71E79
	0070	32	36	46	46	39	46	43	26	76	6b	65	79	3d	36	37	34	26FF9FC
	0080	45	37	43	34	41	37	42	33	42	31	45	33	45	42	34	37	E7C4A7E
	0090	34	45	37	42	46	41	39	33	39	38	43	35	32	37	34	44	4E7BFA5
	00a0	41	33	44	43	38	39	36	36	34	44	43	42	46	41	42	32	A3DC89E
	00b0	37	31	33	34	34	32	38	34	31	44	32	38	30	44	44	41	7134428
	00c0	30	38	35	33	34	32	35	41	45	41	41	37	46	36	31	30	0853425
	00d0	39	35	46	38	32	33	35	38	37	30	44	39	41	30	44	35	95F8235
	00e0	32	30	39	37	42	32	44	46	31	35	42	46	30	26	75	69	2097B2C
	00f0	6e	3d	31	39	34	31	34	39	37	36	37	39	26	66	72	6f	n=19414
	0100	6d	74	61	67	3d	31	31	39	37	39	30	20	48	54	50	50	mtag=11
	0110	2f	31	2e	31	0d	0a	41	63	63	65	70	74	3a	20	2a	2f	/1.1. A
	0120	2a	0d	0a	43	6f	6e	6e	65	63	74	69	6f	6e	3a	20	4b	*. Conn
	0130	65	65	70	2d	41	6c	69	76	65	0d	0a	43	6f	6e	74	65	eep-Alli
	0140	6e	74	2d	4c	65	6e	67	74	68	3a	20	30	0d	0a	43	6f	nt-Leng

可以看出：数据包内容窗口以 ASCII 和十六进制格式显示捕获帧的全部内容

5. 进行测试：打开 Wireshark 的捕获功能，打开浏览器输入网址

<http://gaia.cs.umass.edu/Wireshark-labs/intro-Wireshark-file1.html>，显示内容

Congratulations! You've downloaded the first Wireshark lab file!

回到 Wireshark，在过滤行输入“http”：就可以查到网址的数据包

No.	Time	Source	Destination	Protocol	Length	Info
87	2.689153	172.25.174.42	120.220.244.67	HTTP	697	GET /O8M0004RN5a520keoD.mgg?guid=16B2B0F0DAC71E79E830...
527	4.615120	172.25.174.42	128.119.245.12	HTTP	659	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1...
540	4.895593	128.119.245.12	172.25.174.42	HTTP	293	HTTP/1.1 304 Not Modified
561	4.999364	172.25.174.42	128.119.245.12	HTTP	471	GET /wireshark-labs/github-markdown-css HTTP/1.1
590	5.289145	128.119.245.12	172.25.174.42	HTTP	561	HTTP/1.1 404 Not Found (text/html)
691	7.212407	2001:250:5800:1002::...	2409:8c54:1040:9::1d	HTTP	814	POST /mmtls/00006b83 HTTP/1.1
695	7.306574	2409:8c54:1040:9::1d	2001:250:5800:1002::...	HTTP	421	HTTP/1.1 200 OK
744	8.692002	172.25.174.42	120.220.244.67	HTTP	698	GET /O8M0004RN5a520keoD.mgg?guid=16B2B0F0DAC71E79E830...
1261	14.879260	172.25.174.42	120.220.244.67	HTTP	698	GET /O8M0004RN5a520keoD.mgg?guid=16B2B0F0DAC71E79E830...
1798	20.887051	172.25.174.42	120.220.244.67	HTTP	698	GET /O8M0004RN5a520keoD.mgg?guid=16B2B0F0DAC71E79E830...

6. 点击 HTTP GET 数据包，查看详细信息

Frame 527: 659 bytes on wire (5272 bits), 659 bytes captured (5272 bits) on interface \Device\NPF_{88CAC892-1425-442-8000-000000000000}	0000	02	01	d2	3f	00	00	47	45	54	20	2f	77	69	72	65	73	? GE T /wires
Ethernet II, Src: Intel_78:be:0a (c8:cb:9e:78:be:0a), Dst: JuniperNetwo_f6:12:a0 (28:a2:4b:f6:12:a0)	0010	68	61	72	6b	2d	6c	61	62	73	2f	49	4e	54	52	4f	2d	mark-lab s/INTRO-
Internet Protocol Version 4, Src: 172.25.174.42, Dst: 128.119.245.12	0020	77	69	72	65	73	68	61	72	6b	2d	66	69	66	65	31	2e	wireshark-kfile1.
Transmission Control Protocol, Src Port: 52335, Dst Port: 80, Seq: 1, Ack: 1, Len: 605	0030	68	74	6d	6c	20	48	54	54	50	2f	31	2e	31	0d	0a	48	html HTTP/1.1: H
Hypertext Transfer Protocol	0040	6f	73	74	3a	20	67	61	69	61	2e	63	73	2a	75	6d	61	ost: gai a.c.s.uma
	0050	73	73	2a	65	64	75	0d	0a	43	6f	6e	6e	65	63	74	69	ss.edu... Connecti
	0060	6f	6e	3a	20	6b	65	65	70	2d	61	6c	69	76	65	0d	0a	on: keep -alive-
	0070	43	61	63	68	65	2d	43	6f	6e	74	72	6f	6e	3a	20	6d	Cache-Co ntrol: m
	0080	61	78	2d	61	67	65	3d	30	0d	0a	55	70	67	72	61	64	ax-age=0 -Upgrad
	0090	65	2d	49	6e	73	65	63	75	72	65	2d	52	65	71	75	65	e-Insecu re-Reqe
	00a0	73	74	3a	20	31	0d	0a	55	73	65	72	2d	41	67	65	65	sts: 1-- User-Age
	00b0	6e	74	3a	20	4d	6f	7a	69	6c	6c	61	2f	35	2e	30	20	nt: Mozil lla/5.0
	00c0	28	57	69	6e	64	6f	77	78	20	4e	54	20	31	30	2e	38	(Windows NT 10.0
	00d0	3b	20	57	69	6e	36	34	3b	20	78	36	34	20	20	41	70	g Wind4; x64) Ap
	00e0	70	6c	65	57	65	62	4b	69	74	2f	35	33	37	2e	33	36	plewebKi t/537.36
	00f0	20	28	4b	48	54	4d	4c	2c	20	6c	69	6b	65	20	47	65	(KHTML, like Ge
	0100	63	6b	6f	29	20	43	68	72	6f	6d	65	2f	31	32	32	2e	cko) Chr ome/122.
	0110	30	2e	30	2e	30	20	53	61	66	61	72	69	2f	35	33	37	0.0.0 Sa fari/537
	0120	2e	33	36	0d	0a	41	63	63	65	70	74	3a	20	74	65	78	36--Acc ept: tex
	0130	74	2f	68	74	6d	6c	2c	61	70	70	6c	69	63	61	74	69	t/html,a pplicati
	0140	6f	6e	2f	78	68	74	6d	6c	2b	78	6d	6c	2c	61	70	70	on/xhtml+xml,app
	0150	6c	69	63	61	74	69	6f	6e	2f	78	6d	6c	3b	71	3d	30	lication /xml;q=0
	0160	2e	39	2c	69	6d	61	67	65	2f	61	76	69	66	2c	69	6d	.9,image /avif,im
	0170	61	67	65	2f	77	65	62	70	2c	69	6d	61	67	65	2f	61	age/webp ,image/e
	0180	70	6e	67	2c	2a	2f	2a	3b	71	3d	30	2e	38	2c	61	70	png,*/*; q=0.8,ap
	0190	70	6c	69	63	61	74	69	6f	6e	2f	73	69	67	6e	65	64	platio n/signed

7. 回答实验有关问题(见结论分析)

## 结论分析:

1. 跟踪文件中显示了下列哪个协议(例如,在 Wireshark“协议”列中列出): TCP、QUIC、HTTP、DNS、UDP、TLSv1.2?

答: http 协议

2.从发送 HTTPGET 消息到收到 HTTPOK 应答需要多长时间?(默认情况下,信息包列表窗口中 Time 列的值是自 Wireshark 跟踪开始以来的时间量(以秒为单位)。(如果要以时间格式显示 Time 字段,请选择 WiresharkView 下拉菜单,然后选择 Time Display Format,再选择 Time-of-day。)

6634	67.224447	172.25.174.42	128.119.245.12	HTTP	548 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
6647	67.570824	128.119.245.12	172.25.174.42	HTTP	492 HTTP/1.1 200 OK (text/html)

答: 时间为 0.346377s

3.Gaia.cs.umass.edu 的互联网地址(亦称为 wwwnet)。Cs.umass.edu) ? 您的计算机的 Internet 地址是什么,或者(如果您正在使用跟踪文件)发送 HTTPGET 消息的计算机的 Internet 地址是什么?

答: 172.25.174.42

4.在 Wireshark“选定包的详细信息”窗口中展开 HTTP 消息上的信息(参见上面的图 3),这样您就可以看到 HTTP GET 请求消息中的字段。什么类型的 Web 浏览器发出了 HTTP 请求? 答案显示在扩展的 HTTP 消息显示中“User-Agent:”字段后面的信息的右端。[ HTTP 消息中的这个字段值表示 Web 服务器如何了解您正在使用的浏览器类型。]Firefox, Safari, Microsoft Internet Edge, Other

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36\r\n

答: Safari

5.在 Wireshark 的“所选数据包的详细信息”窗口中展开该数据包的传输控制协议信息(参见实验室文档中的图 3),这样您就可以看到 TCP 段中携带 HTTP 消息的字段。这个 HTTP 请求被发送到的目的端口号是多少(在包含 HTTP 请求的 TCP 段的“Dest Port:”之后的数字)?

Transmission Control Protocol, Src Port: 53256, Dst Port: 80, Seq: 1, Ack: 1, Len: 494  
Source Port: 53256  
Destination Port: 80

答: 80

6.打印问题 2 中提到的两条 HTTP 消息(GET 和 OK)。要这样做,从 WiresharkFile 命令菜单中选择 Print,然后选择“Selected Packet Only”和“Print as display”径向按钮,然后单击 OK

答: 如图

No.	Time	Source	Destination	Protocol	Length	Info
6634	67.224447	172.25.174.42	128.119.245.12	HTTP	548	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Frame 6634: 548 bytes on wire (4384 bits), 548 bytes captured (4384 bits) on interface  
 \Device\NPF\_{88CAC892-1425-442F-84AB-F18E52D8913E}, id 0  
 Ethernet II, Src: Intel\_78:be:0a (c8:cb:9e:78:be:0a), Dst: JuniperNetwo\_f6:12:a0 (28:a2:4b:f6:12:a0)  
 Internet Protocol Version 4, Src: 172.25.174.42, Dst: 128.119.245.12  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 534  
 Identification: 0x0bb7 (2999)  
 010. .... = Flags: 0x2, Don't fragment  
 ...0 0000 0000 0000 = Fragment Offset: 0  
 Time to Live: 128  
 Protocol: TCP (6)  
 Header Checksum: 0x0000 [validation disabled]  
 [Header checksum status: Unverified]  
 Source Address: 172.25.174.42  
 Destination Address: 128.119.245.12  
 Transmission Control Protocol, Src Port: 53256, Dst Port: 80, Seq: 1, Ack: 1, Len: 494  
 Source Port: 53256  
 Destination Port: 80  
 [Stream index: 54]  
 [Conversation completeness: Complete, WITH\_DATA (31)]  
 [TCP Segment Len: 494]  
 Sequence Number: 1 (relative sequence number)  
 Sequence Number (raw): 4015310469  
 [Next Sequence Number: 495 (relative sequence number)]  
 Acknowledgment Number: 1 (relative ack number)  
 Acknowledgment number (raw): 833400318  
 0101 .... = Header Length: 20 bytes (5)  
 Flags: 0x018 (PSH, ACK)  
 Window: 256  
 [Calculated window size: 65536]  
 [Window size scaling factor: 256]  
 Checksum: 0xd1d0 [unverified]  
 [Checksum Status: Unverified]  
 Urgent Pointer: 0  
 [Timestamps]  
 [SEQ/ACK analysis]  
 TCP payload (494 bytes)  
 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/122.0.0.0 Safari/537.36\r\n  
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n  
 Accept-Encoding: gzip, deflate\r\n  
 Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7\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: 6647]  
 [Next request in frame: 6654]

No.	Time	Source	Destination	Protocol	Length	Info
6647	67.570824	128.119.245.12	172.25.174.42	HTTP	492	HTTP/1.1 200 OK (text/html)

Frame 6647: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface  
 \Device\NPF\_{88CAC892-1425-442F-84AB-F18E52D8913E}, id 0  
 Ethernet II, Src: JuniperNetwo\_f6:12:a0 (28:a2:4b:f6:12:a0), Dst: Intel\_78:be:0a (c8:cb:9e:78:be:0a)  
 Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.25.174.42  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 Differentiated Services Field: 0x74 (DSCP: Unknown, ECN: Not-ECT)  
 Total Length: 478  
 Identification: 0x0b6e (2926)  
 010. .... = Flags: 0x2, Don't fragment  
 ...0 0000 0000 0000 = Fragment Offset: 0  
 Time to Live: 43  
 Protocol: TCP (6)  
 Header Checksum: 0x7270 [validation disabled]  
 [Header checksum status: Unverified]  
 Source Address: 128.119.245.12  
 Destination Address: 172.25.174.42  
 Transmission Control Protocol, Src Port: 80, Dst Port: 53256, Seq: 1, Ack: 495, Len: 438  
 Source Port: 80  
 Destination Port: 53256  
 [Stream index: 54]  
 [Conversation completeness: Complete, WITH\_DATA (31)]  
 [TCP Segment Len: 438]  
 Sequence Number: 1 (relative sequence number)  
 Sequence Number (raw): 833400318  
 [Next Sequence Number: 439 (relative sequence number)]  
 Acknowledgment Number: 495 (relative ack number)  
 Acknowledgment number (raw): 4015310963  
 0101 .... = Header Length: 20 bytes (5)  
 Flags: 0x018 (PSH, ACK)  
 Window: 237  
 [Calculated window size: 30336]  
 [Window size scaling factor: 128]  
 Checksum: 0xc578 [unverified]  
 [Checksum Status: Unverified]  
 Urgent Pointer: 0  
 [Timestamps]  
 [SEQ/ACK analysis]  
 TCP payload (438 bytes)  
 Hypertext Transfer Protocol  
 HTTP/1.1 200 OK\r\n  
 Date: Sat, 09 Mar 2024 08:59:31 GMT\r\n  
 Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod\_perl/2.0.11 Perl/v5.16.3\r\n  
 Last-Modified: Sat, 09 Mar 2024 06:59:02 GMT\r\n  
 ETag: "51-61334d7edbe79"\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: 0.346377000 seconds]  
 [Request in frame: 6634]  
 [Next request in frame: 6654]  
 [Next response in frame: 6744]  
 [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)

## 结论：

本次实验是对 Wireshark 软件的初步认识，通过一个简单的抓包测试，分析 Get 和 Ok 数据包，加深了对于数据包，协议，端口等知识点的理解，也巩固了理论课的知识，让我收获良多。