

学号：	姓名：	班级：
实验题目： 实验一		
实验学时：2h	实验日期：2023.02.27	
实验目的： 熟悉 Wireshark 的使用		
硬件环境： Windows10 家庭版		
软件环境： Wireshark		
实验步骤与内容： 实验内容： <ol style="list-style-type: none"> 熟悉 Wireshark 的使用 打开 Wireshark 并开始抓包 查看 Wireshark 中 HTTP GET 消息 完成相应的实验习题 实验步骤： 先是下载 Wireshark 软件，然后开始使用 Wireshark 进行抓包，其中下面为随机测试的抓包信息：		

No.	Time	Source	Destination	Protocol	Length	Info
43	2023-02-27 14:54:48.821106	120.220.179.64	172.25.163.122	TLSv1.3	341	Application Data
44	2023-02-27 14:54:48.821106	120.220.158.226	172.25.163.122	TCP	56	[TCP Spurious Retransmission] 443 → 14992 [PSH, ACK] Seq=149 AcK=518 Win=523648 Len=1
45	2023-02-27 14:54:48.821106	120.220.179.64	172.25.163.122	TCP	56	[TCP Out-Of-Order] 443 → 14991 [PSH, ACK] Seq=536 AcK=702 Win=525440 Len=1
46	2023-02-27 14:54:48.82168	172.25.163.122	120.220.158.226	TCP	66	[TCP Dup ACK 4141] 14992 → 443 [ACK] Seq=569 AcK=151 Win=131072 Len=0 SLE=149 SRE=150
47	2023-02-27 14:54:48.821354	172.25.163.122	120.220.179.64	TCP	66	14991 → 443 [ACK] Seq=702 AcK=542 Win=130816 Len=0 SLE=536 SRE=537
48	2023-02-27 14:54:48.820339	120.220.158.226	172.25.163.122	TCP	56	[TCP Spurious Retransmission] 443 → 14992 [PSH, ACK] Seq=149 AcK=518 Win=523648 Len=1
49	2023-02-27 14:54:48.820339	120.220.179.64	172.25.163.122	TCP	56	[TCP Spurious Retransmission] 443 → 14991 [PSH, ACK] Seq=534 AcK=702 Win=525440 Len=1
50	2023-02-27 14:54:48.820414	172.25.163.122	120.220.158.226	TCP	66	[TCP Dup ACK 4142] 14992 → 443 [ACK] Seq=569 AcK=151 Win=131072 Len=0 SLE=147 SRE=148
51	2023-02-27 14:54:48.820500	172.25.163.122	120.220.179.64	TCP	66	[TCP Dup ACK 4741] 14991 → 443 [ACK] Seq=702 AcK=542 Win=130816 Len=0 SLE=534 SRE=535
52	2023-02-27 14:54:48.833685	120.220.158.226	172.25.163.122	TCP	56	[TCP Spurious Retransmission] 443 → 14992 [PSH, ACK] Seq=145 AcK=518 Win=523648 Len=1
53	2023-02-27 14:54:48.833685	120.220.179.64	172.25.163.122	TCP	56	[TCP Spurious Retransmission] 443 → 14991 [PSH, ACK] Seq=532 AcK=702 Win=525440 Len=1

```

> Frame 71: 632 bytes on wire (5056 bits), 632 bytes captured (5056 bits) on interface \Device\
> Ethernet II, Src: Liteontef_1f:d7:61 (14:5a:fc:1f:d7:61), Dst: Juniperf_f6:12:a0 (28:a2:4b:f6:
> Internet Protocol Version 4, Src: 172.25.163.122, Dst: 103.74.50.106
> Transmission Control Protocol, Src Port: 14993, Dst Port: 80, Seq: 1, Ack: 1, Len: 566
  > Hypertext Transfer Protocol
    > [truncated]GET /apps/updates/dictupdate.xml?ver=1720&-1677480889171&client-deskdic&id=5
      > [truncated]Expert Info (Chat/Sequence): GET /apps/updates/dictupdate.xml?ver=1720&-16
        Request Method: GET
        Request URI: [truncated]: /apps/updates/dictupdate.xml?ver=1720&-1677480889171&client-deskd
          Request Version: HTTP/1.1
        Accept: */*\r\n
        Accept-Encoding: gzip\r\n
        User-Agent: Youdao Desktop Dict (Windows NT 10.0)\r\n
        Host: cidian.youdao.com\r\n
        Connection: Keep-Alive\r\n
      > Cookie: OUTFOX_SEARCH_USER_ID=-1563872273@10.105.137.204; DESKDICT_VENDOR=webdict_default;
        \r\n
        [Full request URI [truncated]: http://cidian.youdao.com/apps/updates/dictupdate.xml?ver=17
        [HTTP request 1/1]
        [Response in frame 74]
    
```

后我们用 Wireshark 抓取想要的封包，并查看其中 HTTP GET 消息

Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
71	2023-02-27 14:54:49.202978	172.25.163.122	103.74.50.106	HTTP	632	GET /apps/update5/dictupdate.xml?ver=1720&_=-1677480889171&lient=deskdickt&id=5d330e5a75968
74	2023-02-27 14:54:49.276113	103.74.50.106	172.25.163.122	HTTP/X	737	HTTP/1.1 200 OK

> Frame 71: 632 bytes on wire (5056 bits), 632 bytes captured (5056 bits) on interface \Device\NPF{...}

> Ethernet II, Src: LiteonTe_1f:d7:61 (14:5a:fc:1f:d7:61), Dst: JuniperM_f6:12:a0 (28:a2:4b:f6:12:a0)

> Internet Protocol Version 4, Src: 172.25.163.122, Dst: 103.74.50.106

> Transmission Control Protocol, Src Port: 14993, Dst Port: 80, Seq: 1, Ack: 1, Len: 566

> Hypertext Transfer Protocol

> [truncated] GET /apps/update5/dictupdate.xml?ver=1720&_=-1677480889171&lient=deskdickt&id=5d330e5a75968

> [truncated] Expert Info (chat/Sequence): GET /apps/update5/dictupdate.xml?ver=1720&_=-1677480889171&lient=deskdickt&id=5d330e5a75968

> Request Method: GET

> Request URI [truncated]: /apps/update5/dictupdate.xml?ver=1720&_=-1677480889171&lient=deskdickt&id=5d330e5a75968

> Request Version: HTTP/1.1

> Accept: */*\r\n

> Accept-Encoding: gzip\r\n

> User-Agent: Youdao Desktop Dict (Windows NT 10.0)\r\n

> Host: cidian.youdao.com\r\n

> Connection: Keep-Alive\r\n

> Cookie: OUTFOX_SEARCH_USER_ID=-1563872273@10.105.137.204; DESKDICTIONARY_VENDOR=webdict_default\r\n

> [Full request URI [truncated]: http://cidian.youdao.com/apps/update5/dictupdate.xml?ver=1720&_=-1677480889171&lient=deskdickt&id=5d330e5a75968]

> [Response in frame: 74]

0000 28 a2 4b f6 12 a0 14 5a fc 1f d7 61 08 00 45 00 (.K....Z...a..E..

0010 02 6a cc 11 40 00 80 06 43 34 ac 19 a3 7a 67 4a .j..@...C4...zgJ

0020 32 6a 3a 91 00 50 63 ca 96 b4 ad c4 73 c9 80 18 2j:...Pc...s...s...

0030 04 00 cc 16 00 00 01 01 08 0a 39 32 8b 28 57 5992.(WY

0040 42 11 47 45 54 20 2f 61 70 70 73 2f 75 70 64 61 B-GET /a pps/upda

0050 74 65 35 2f 64 69 63 74 75 70 64 61 74 65 2e 78 te5/dict update.x

0060 6d 6c 3f 76 65 72 3d 31 37 32 30 26 5f 3d 31 36 ml?ver=1 720&_=-16

0070 37 37 34 38 30 38 38 39 31 37 31 26 63 6c 69 65 77480889 171&lie

0080 6e 74 3d 64 65 73 6b 64 69 63 74 26 69 64 3d 35 nt=deskd ict&id=5

0090 64 33 33 30 65 35 61 37 35 39 36 38 31 36 65 31 d330e5a7 596816e1

00a0 26 76 65 6e 64 6f 72 3d 77 65 62 64 69 63 74 5f &vendor= webdict_

00b0 64 65 66 61 75 6c 74 26 69 6e 3d 33 32 38 38 2d default& in=3288-

00c0 32 30 32 31 2d 31 31 2d 31 33 30 33 30 33 33 35 2021-11- 13030335

00d0 2d 31 36 33 36 37 34 33 38 31 35 33 38 30 26 61 -1636743 815380&a

00e0 70 70 56 65 72 3d 39 2e 31 2e 36 2e 30 26 61 70 ppver=9. 1.6.0&ap

00f0 70 5a 65 6e 67 71 69 61 6e 67 3d 30 26 61 62 54 pzengqia ng-0&abT

0100 65 73 74 3d 33 26 6d 6f 64 65 6c 3d 4c 45 4e 4f est=3&ao del=LEH0

0110 56 4f 26 73 63 72 65 65 6e 3d 31 39 32 30 2a 31 v0&scree n=1920*1

0120 30 38 30 26 4f 73 56 65 72 73 69 6f 6e 3d 31 30 08080sve rsion=10

0130 2e 30 2e 31 39 30 34 34 20 48 54 54 50 2f 31 2e .o.19044 HTTP/1.

0140 31 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 1- Accept: */*..

0150 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a Accept-E ncoding:

0160 20 67 74 69 70 0d 0a 55 73 65 72 2d 41 67 65 6e gzip: U ser-Agen

0170 74 3a 20 59 6f 75 64 61 6f 20 44 65 73 6b 74 6f t: Youda o Desкто

0180 70 20 44 69 63 74 20 28 57 69 6e 64 6f 77 73 20 p Dict (Windows

0190 4e 54 20 31 30 2e 30 29 0d 0a 48 6f 73 74 3a 20 NT 10.0) ..Host:

先是在顶部的分组显示过滤器窗口中选择 HTTP，然后找到里面的 GET 消息，即可查看相关信息。

问题一：

答：HTTP，DNS，UDP

问题二：

答：需要的时间可以由 2023-02-27 14:54:49.202978 相减得到 2023-02-27 14:54:49.276113

问题三：

答：wwwnet.cs.umass.edu 的地址为 103.74.50.106, 我的计算机 IP 地址为: 172.25.163.122

结论分析与体会：

通过对 Wireshark 的简单使用，初步学会了如何使用 Wireshark 进行抓包，并查看相应的信息，对 Wireshark 中一些信息所表示的意思也有所明确，对网络有了进一步的认知。