计算机网络

吴欣怡　PB21051111

2023 年 9 月 14 日

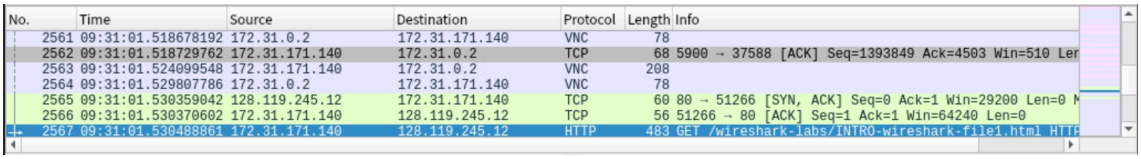
实验目的

入门 wireshark，熟悉 wireshark 软件界面、功能，学习基本的分组捕获与分析方法，尝试阅读网络信息

实验结果

问题 1：列举 3 个捕获的分组中出现的网络协议

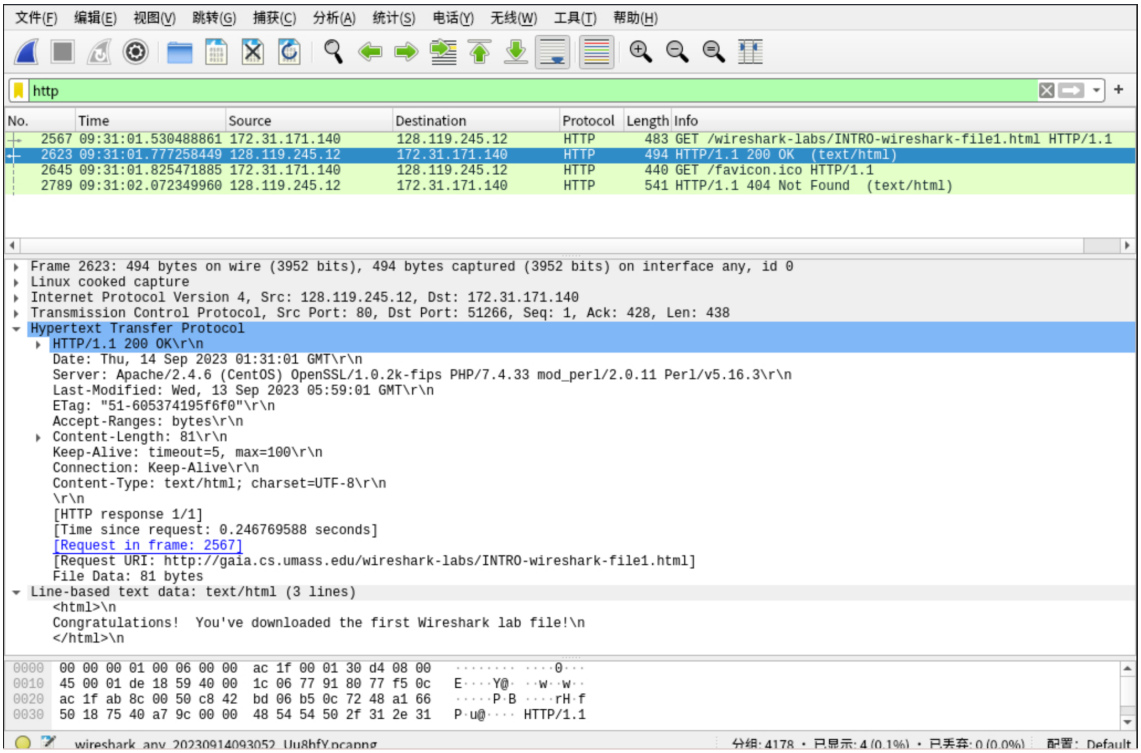
- VNC,TCP,HTTP



No.	Time	Source	Destination	Protocol	Length	Info
2561	09:31:01.518678192	172.31.0.2	172.31.171.140	VNC	78	
2562	09:31:01.518729762	172.31.171.140	172.31.0.2	TCP	68	5900 → 37588 [ACK] Seq=1393849 Ack=4503 Win=510 Len
2563	09:31:01.524099548	172.31.171.140	172.31.0.2	VNC	208	
2564	09:31:01.529807786	172.31.0.2	172.31.171.140	VNC	78	
2565	09:31:01.530359042	128.119.245.12	172.31.171.140	TCP	60	80 → 51266 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 M
2566	09:31:01.530370602	172.31.171.140	128.119.245.12	TCP	56	51266 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
2567	09:31:01.530488861	172.31.171.140	128.119.245.12	HTTP	483	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP

问题 2：获取网络请求发出到获得响应的间隔时间

- 根据截图中的 Time Since Request 可知，时间为 0.246769588s



问题 3：获取本机与目标站点的网络地址

由上图可知

- 目标站点：gaia.cs.umass.edu：128.119.245.12
- 本机：172.31.171.140

问题 4：打印输出结果

- 如下图：

/tmp/wireshark_any_20230914093052_Uu8hfY.pcapng 4178 总分组数,4 已显示

```
No.     Time              Source                Destination           Protocol Length Info
   2567 09:31:01.530488861 172.31.171.140        128.119.245.12        HTTP     483    GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 2567: 483 bytes on wire (3864 bits), 483 bytes captured (3864 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 172.31.171.140, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 51266, Dst Port: 80, Seq: 1, Ack: 1, Len: 427
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 2623]
No.     Time              Source                Destination           Protocol Length Info
   2623 09:31:01.777258449 128.119.245.12        172.31.171.140        HTTP     494    HTTP/1.1 200 OK  (text/html)
Frame 2623: 494 bytes on wire (3952 bits), 494 bytes captured (3952 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.31.171.140
Transmission Control Protocol, Src Port: 80, Dst Port: 51266, Seq: 1, Ack: 428, Len: 438
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Thu, 14 Sep 2023 01:31:01 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: Wed, 13 Sep 2023 05:59:01 GMT\r\n
    ETag: "51-605374195f6f0"\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 1/1]
    [Time since request: 0.246769588 seconds]
    [Request in frame: 2567]
    [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)
    <html>\n
    Congratulations!  You've downloaded the first Wireshark lab file!\n
    </html>\n
```

实验总结

通过对于 wireshark 软件的尝试和摸索，掌握了其基本功能及部分使用方法，包括捕获分组、查看分组头部细节、打印输出捕获结果等。进一步地，通过一个简单 HTTP 协议的例子，观察了分组细节，回顾了已学习的相关知识。