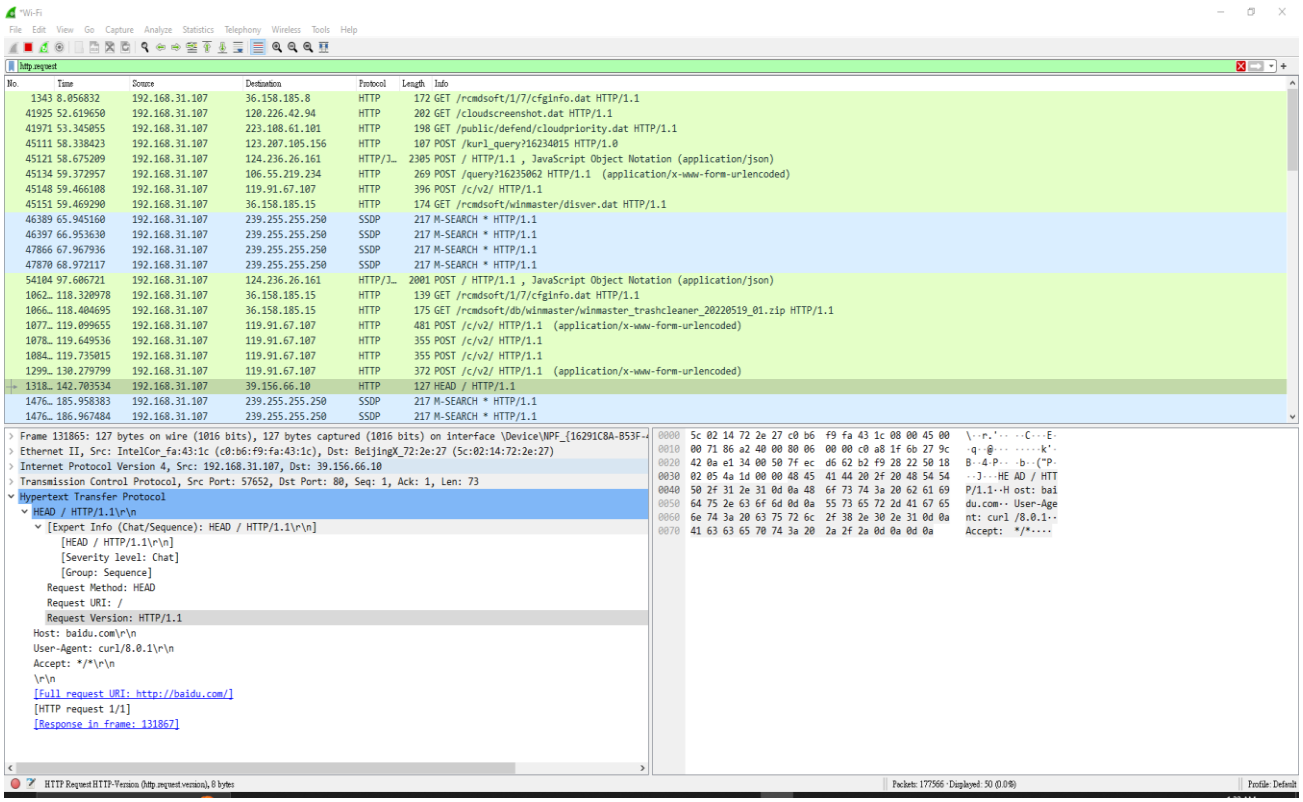
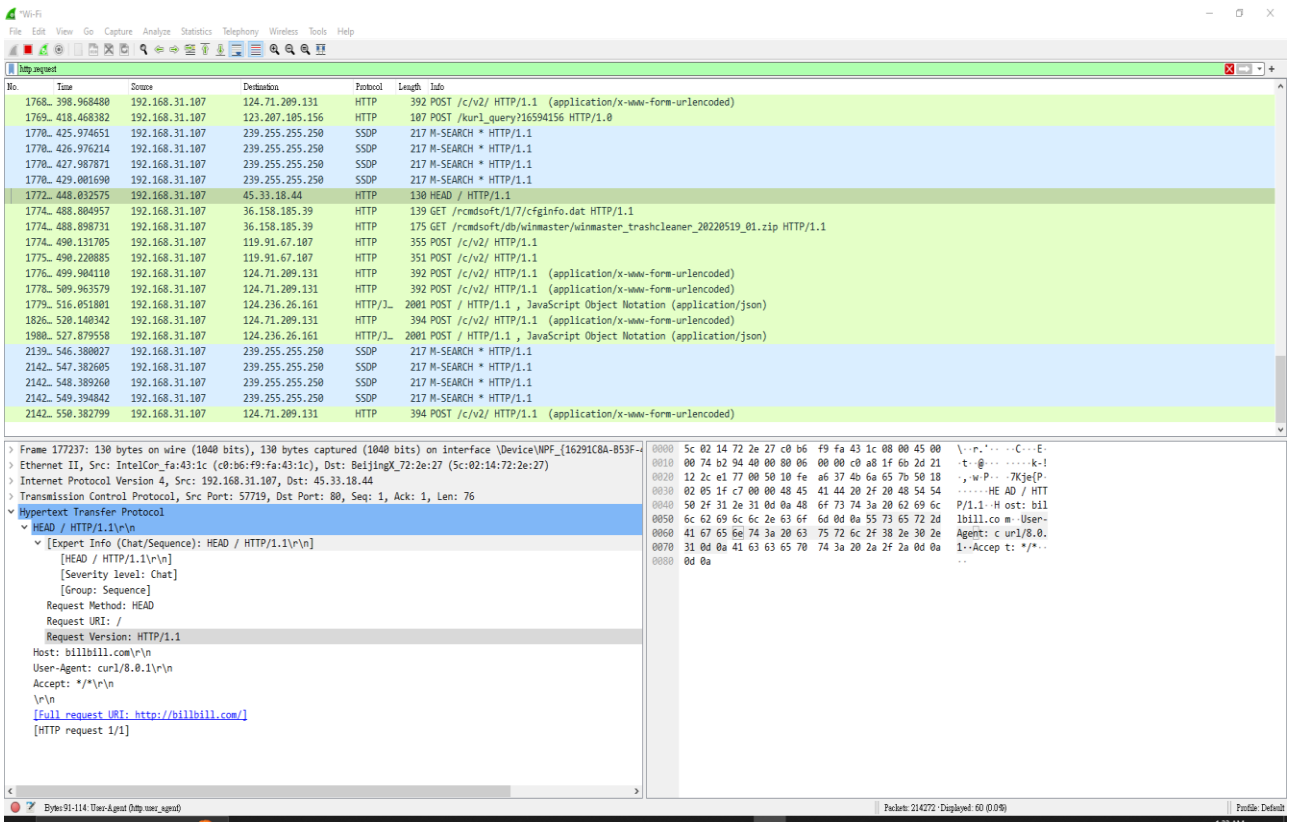
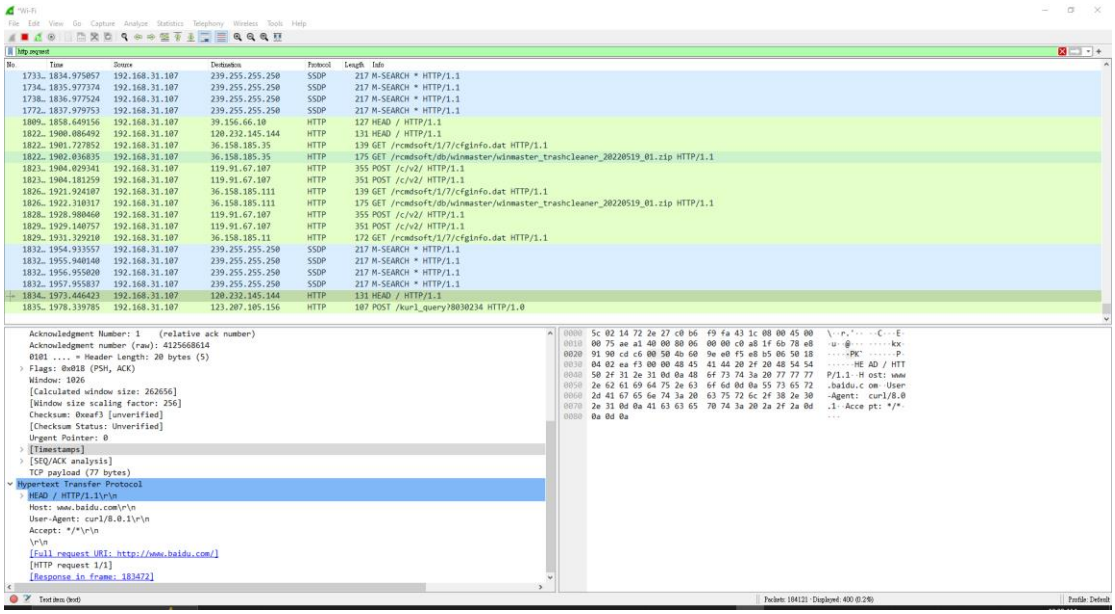
Wireshark 抓包作业

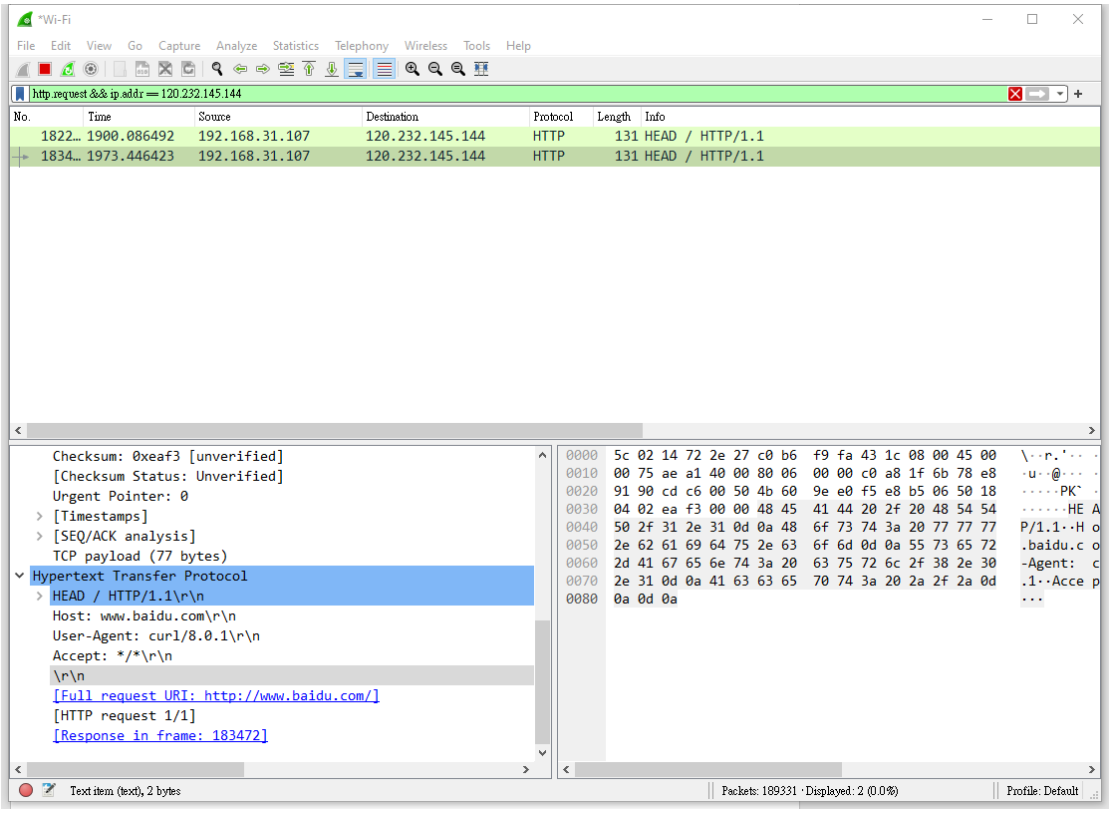


通过 cmd 指令获得 billbill.com 和 baidu.com 网址的 IPv4 网址，然后通过抓包工具抓包显示 HTTP 连接的版本和形式

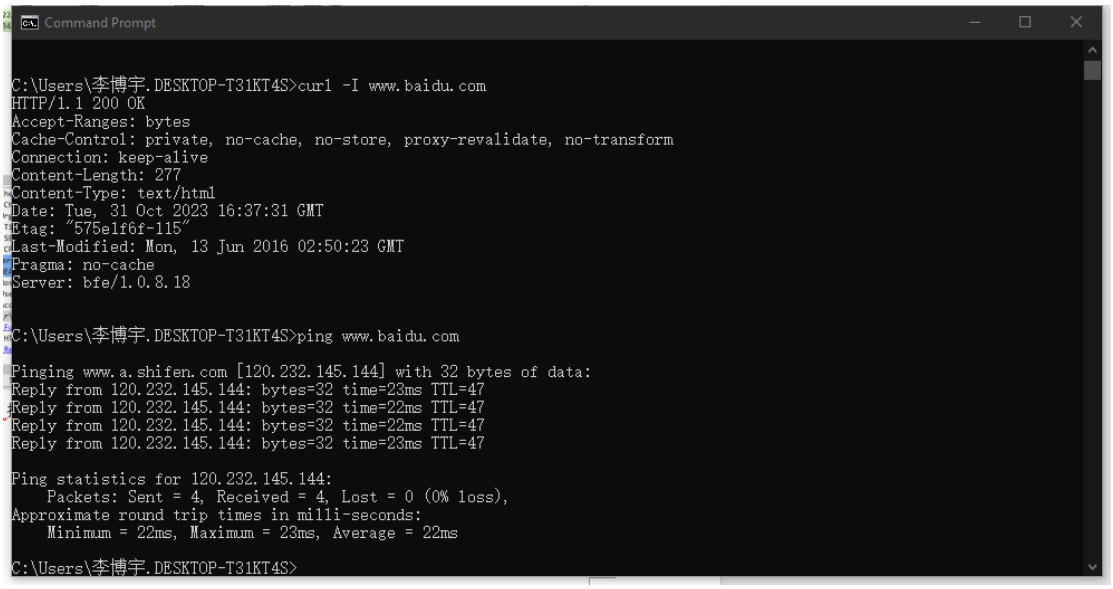




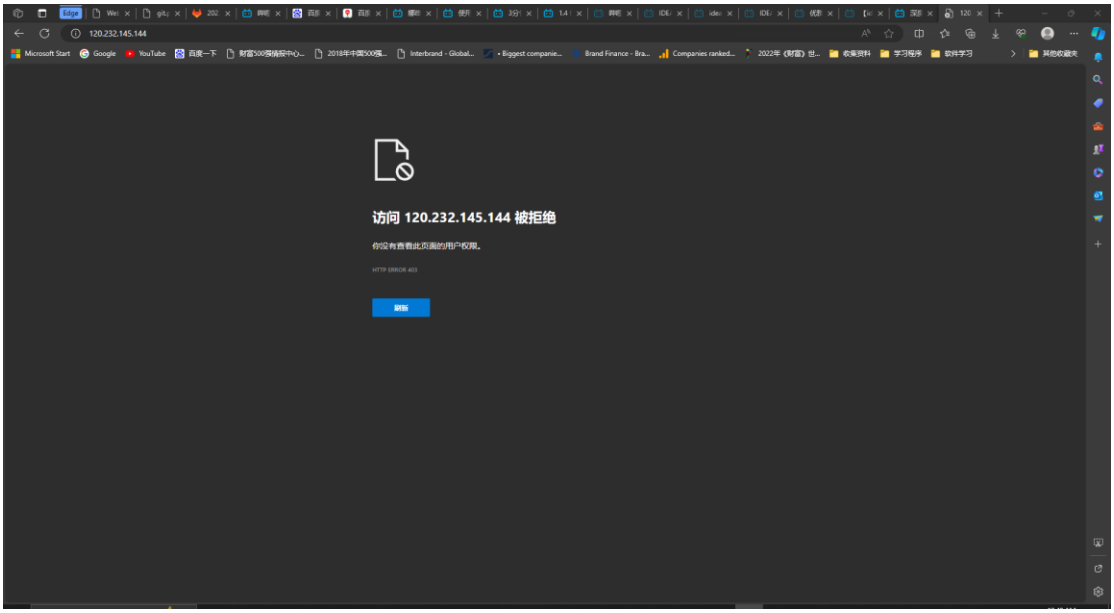
通过 cmd 指令获得 www.baidu.com 网址的 IPv4 网址，然后通过抓包工具抓包显示 HTTP 连接的版本和形式，然后使用 http.request 的命令过滤掉其他类型的请求使用 IP.addr 命令获得特定网址的 HTTP 请求。



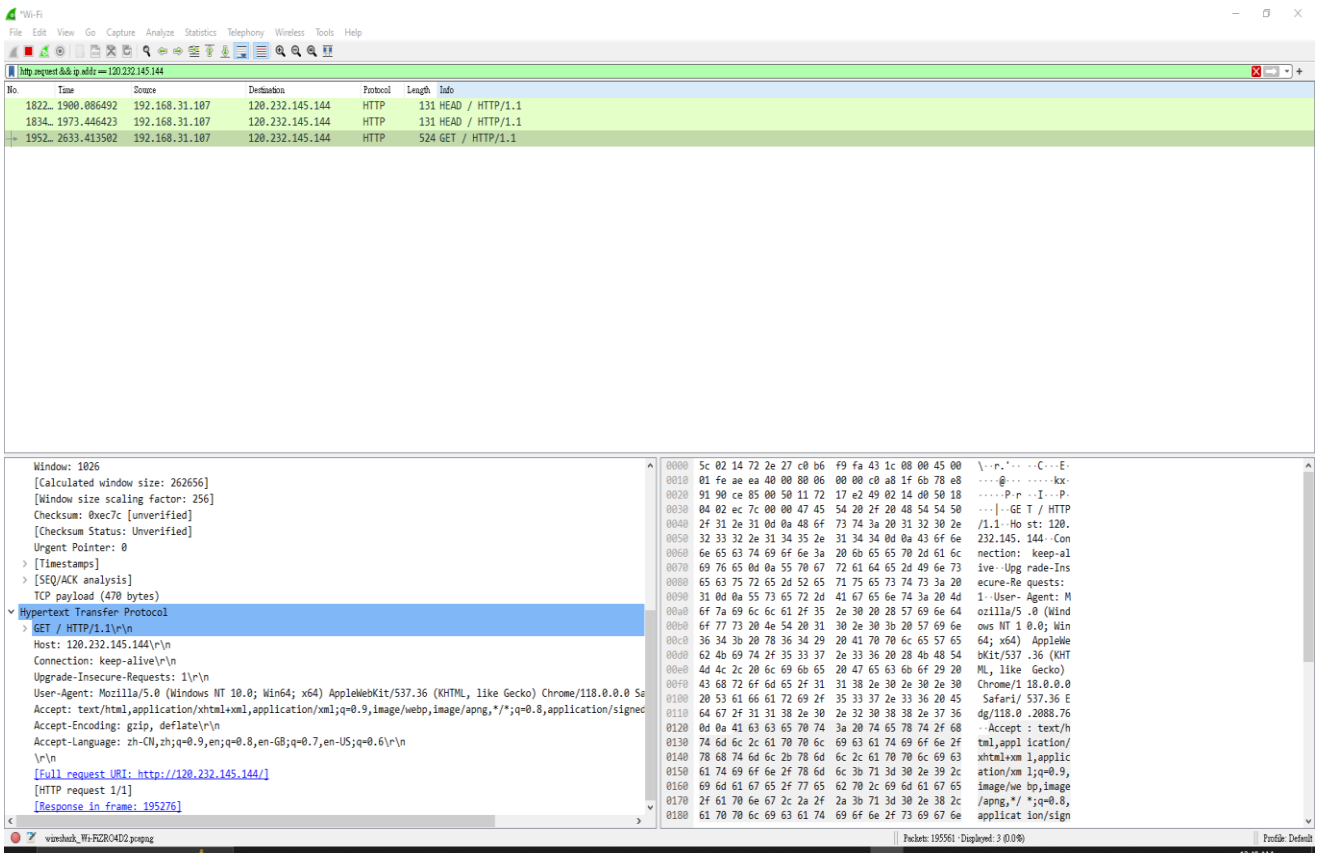
Cmd 指令操作截图



当 www.baidu.com 访问拒绝的时候



对应爬取到的 HTTP 链接以及对应的 HTTP 请求报文样式如下


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request && ip.addr == 120.232.145.144
No. Time Source Destination Protocol Length Info
1822... 1900.086492 192.168.31.107 120.232.145.144 HTTP 131 HEAD / HTTP/1.1
1834... 1973.446423 192.168.31.107 120.232.145.144 HTTP 131 HEAD / HTTP/1.1
1952... 2633.413502 192.168.31.107 120.232.145.144 HTTP 524 GET / HTTP/1.1
Window: 1026
[Calculated window size: 262656]
[Window size scaling factor: 256]
Checksum: 0xec7c [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
TCP payload (470 bytes)
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Host: 120.232.145.144\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/118.0.0.0 Sa
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
\r\n
[Full request URI: http://120.232.145.144/]
[HTTP request 1/1]
[Response in frame: 195276]
0000 5c 02 14 72 2e 27 c0 b6 f9 fa 43 1c 08 00 45 00
0010 01 fe ae ea 40 00 80 06 00 00 c0 a8 1f 6b 78 e8
0020 91 90 ce 85 00 50 11 72 17 e2 49 02 14 d0 50 18
0030 04 02 ec 7c 00 00 47 45 54 20 2f 20 48 54 54 50
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 31 32 30 2e
0050 32 33 32 2e 31 34 35 2e 31 34 34 0d 0a 43 6f 6e
0060 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c
0070 69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73
0080 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20
0090 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d
00a0 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64
00b0 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e
00c0 36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57 65
00d0 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 54
00e0 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20
00f0 43 68 72 6f 6d 65 2f 31 31 38 2e 30 2e 30 2e 30
0100 20 53 61 66 61 72 69 2f 35 33 37 2e 33 36 20 45
0110 64 67 2f 31 31 38 2e 30 2e 32 30 38 38 2e 37 36
0120 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68
0130 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f
0140 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63
0150 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c
0160 69 6d 61 67 65 2f 77 65 62 70 2c 69 6d 61 67 65
0170 2f 61 70 6e 67 2c 2a 2f 2a 3b 71 3d 30 2e 38 2c
0180 61 70 70 6c 69 63 61 74 69 6f 6e 2f 73 69 67 6e
wireshark_Wi-FiZRO4D2.pcapng
Packets: 195561 · Displayed: 3 (0.0%)
Profile: Default