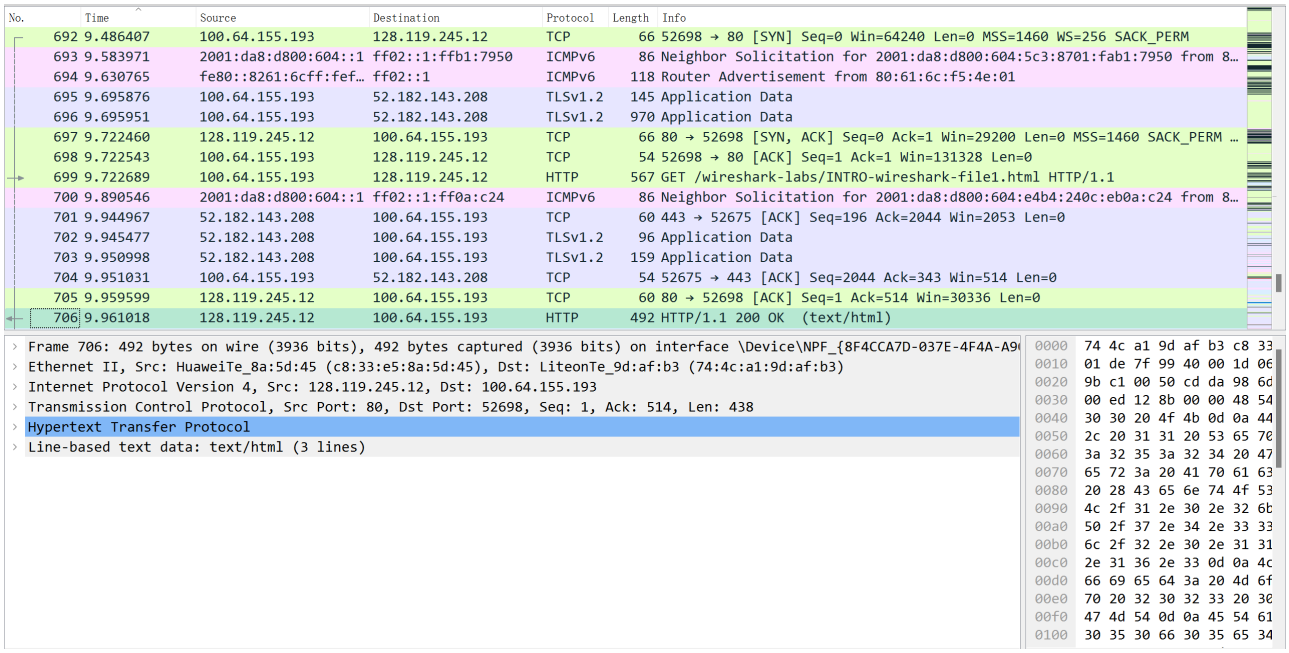
LAB1

牛庆源 PB21111733

- **STEP1：开启捕获**

  部分内容如下（可以看到有TCP，ICMPv6，TLSv1.2等不同的协议）



No.	Time	Source	Destination	Protocol	Length	Info
692	9.486407	100.64.155.193	128.119.245.12	TCP	66	52698 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
693	9.583971	2001:da8:d800:604::1	ff02::1:ffb1:7950	ICMPv6	86	Neighbor Solicitation for 2001:da8:d800:604:5c3:8701:fab1:7950 from 8…
694	9.630765	fe80::8261:6cff:fef…	ff02::1	ICMPv6	118	Router Advertisement from 80:61:6c:f5:4e:01
695	9.695876	100.64.155.193	52.182.143.208	TLSv1.2	145	Application Data
696	9.695951	100.64.155.193	52.182.143.208	TLSv1.2	970	Application Data
697	9.722460	128.119.245.12	100.64.155.193	TCP	66	80 → 52698 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM …
698	9.722543	100.64.155.193	128.119.245.12	TCP	54	52698 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
699	9.722689	100.64.155.193	128.119.245.12	HTTP	567	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
700	9.890546	2001:da8:d800:604::1	ff02::1:ff0a:c24	ICMPv6	86	Neighbor Solicitation for 2001:da8:d800:604:e4b4:240c:eb0a:c24 from 8…
701	9.944967	52.182.143.208	100.64.155.193	TCP	60	443 → 52675 [ACK] Seq=196 Ack=2044 Win=2053 Len=0
702	9.945477	52.182.143.208	100.64.155.193	TLSv1.2	96	Application Data
703	9.950998	52.182.143.208	100.64.155.193	TLSv1.2	159	Application Data
704	9.951031	100.64.155.193	52.182.143.208	TCP	54	52675 → 443 [ACK] Seq=2044 Ack=343 Win=514 Len=0
705	9.959599	128.119.245.12	100.64.155.193	TCP	60	80 → 52698 [ACK] Seq=1 Ack=514 Win=30336 Len=0
706	9.961018	128.119.245.12	100.64.155.193	HTTP	492	HTTP/1.1 200 OK (text/html)

```
Frame 706: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{8F4CCA7D-037E-4F4A-A9
Ethernet II, Src: HuaweiTe_8a:5d:45 (c8:33:e5:8a:5d:45), Dst: LiteonTe_9d:af:b3 (74:4c:a1:9d:af:b3)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 100.64.155.193
Transmission Control Protocol, Src Port: 80, Dst Port: 52698, Seq: 1, Ack: 514, Len: 438
Hypertext Transfer Protocol
Line-based text data: text/html (3 lines)
```

```
0000  74 4c a1 9d af b3 c8 33
0010  01 de 7f 99 40 00 1d 06
0020  9b c1 00 50 cd da 98 6d
0030  00 ed 12 8b 00 00 48 54
0040  30 30 20 4f 4b 0d 0a 44
0050  2c 20 31 31 20 53 65 70
0060  3a 32 35 3a 32 34 20 47
0070  65 72 3a 20 41 70 61 63
0080  20 28 43 65 6e 74 4f 53
0090  4c 2f 31 2e 30 2e 32 6b
00a0  50 2f 37 2e 34 2e 33 33
00b0  6c 2f 32 2e 30 2e 31 31
00c0  2e 31 36 2e 33 0d 0a 4c
00d0  66 69 65 64 3a 20 4d 6f
00e0  70 20 32 30 32 33 20 30
00f0  47 4d 54 0d 0a 45 54 61
0100  30 35 30 66 30 35 65 34
```

- **STEP2：打开网址并停止捕获，搜索http协议**

  按照info排序找到get和response（OK）如下

699	9.722689	100.64.155.193	128.119.245.12	HTTP	567	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
706	9.961018	128.119.245.12	100.64.155.193	HTTP	492	HTTP/1.1 200 OK (text/html)

  通过观察time可以计算出响应时间为`9.961018 - 9.722689 = 0.238329`秒

- **STEP3：判断本机ip和目标ip**

  通过观察Source和Destination可以判断出gaia.cs.umass.edu地址为128.119.245.12，本机地址为100.64.155.193

- **STEP4：将STEP2中的两个http消息打印**

如下：（为部分截图，具体内容在同名pdf内）

```
No.     Time           Source                Destination           Protocol Length Info
    706 9.961018       128.119.245.12        100.64.155.193        HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 706: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{8F4CCA7D-037E-4F4A-
A903-982EA39577AF}, id 0
    Section number: 1
    Interface id: 0 (\Device\NPF_{8F4CCA7D-037E-4F4A-A903-982EA39577AF})
        Interface name: \Device\NPF_{8F4CCA7D-037E-4F4A-A903-982EA39577AF}
        Interface description: WLAN
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 11, 2023 17:25:22.709497000 中国标准时间
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1694424322.709497000 seconds
    [Time delta from previous captured frame: 0.001419000 seconds]
    [Time delta from previous displayed frame: 0.238329000 seconds]
    [Time since reference or first frame: 9.961018000 seconds]
    Frame Number: 706
    Frame Length: 492 bytes (3936 bits)
    Capture Length: 492 bytes (3936 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: HuaweiTe_8a:5d:45 (c8:33:e5:8a:5d:45), Dst: LiteonTe_9d:af:b3 (74:4c:a1:9d:af:b3)
    Destination: LiteonTe_9d:af:b3 (74:4c:a1:9d:af:b3)
        Address: LiteonTe_9d:af:b3 (74:4c:a1:9d:af:b3)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: HuaweiTe_8a:5d:45 (c8:33:e5:8a:5d:45)
        Address: HuaweiTe_8a:5d:45 (c8:33:e5:8a:5d:45)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 100.64.155.193
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 478
```

```
No.     Time           Source                Destination           Protocol Length Info
    699 9.722689       100.64.155.193        128.119.245.12        HTTP     567    GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 699: 567 bytes on wire (4536 bits), 567 bytes captured (4536 bits) on interface \Device\NPF_{8F4CCA7D-037E-4F4A-
A903-982EA39577AF}, id 0
    Section number: 1
    Interface id: 0 (\Device\NPF_{8F4CCA7D-037E-4F4A-A903-982EA39577AF})
        Interface name: \Device\NPF_{8F4CCA7D-037E-4F4A-A903-982EA39577AF}
        Interface description: WLAN
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 11, 2023 17:25:22.471168000 中国标准时间
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1694424322.471168000 seconds
    [Time delta from previous captured frame: 0.000146000 seconds]
    [Time delta from previous displayed frame: 1.380241000 seconds]
    [Time since reference or first frame: 9.722689000 seconds]
    Frame Number: 699
    Frame Length: 567 bytes (4536 bits)
    Capture Length: 567 bytes (4536 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: LiteonTe_9d:af:b3 (74:4c:a1:9d:af:b3), Dst: HuaweiTe_8a:5d:45 (c8:33:e5:8a:5d:45)
    Destination: HuaweiTe_8a:5d:45 (c8:33:e5:8a:5d:45)
        Address: HuaweiTe_8a:5d:45 (c8:33:e5:8a:5d:45)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: LiteonTe_9d:af:b3 (74:4c:a1:9d:af:b3)
        Address: LiteonTe_9d:af:b3 (74:4c:a1:9d:af:b3)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 100.64.155.193, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 553
```