LAB 8. Phân tích gói tin WireShark

I. Yêu cầu:

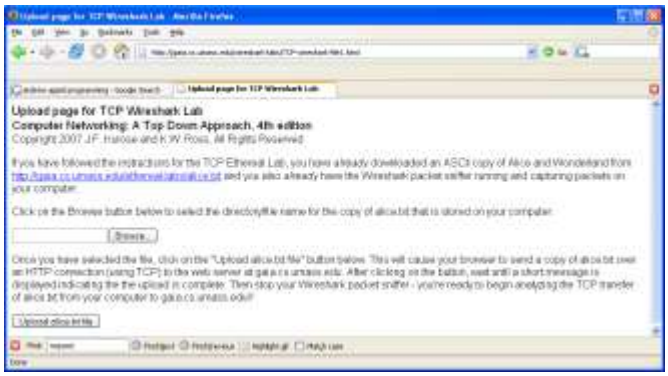
- Nắm được các kiểu định dạng gói tin: TCP, UDP, telnet, internet frame, ipv6
- Nắm được kỹ thuật bắt và phân tích các gói tin trên bằng WireShark.

Chuẩn bị

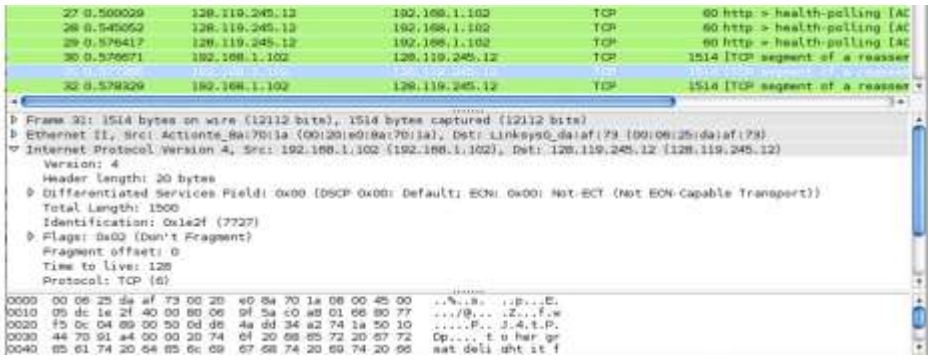
- Bài LAB sử dụng 1 máy Windows 7
- Bảo đảm đường truyền internet đã thông.
- Đổi password của Administrator máy Windows 7 là abc@123
- Cài đặt sẵn phần mềm Wireshark

IV. Triển khai

1. **Phân tích gói tin TCP**
   a. Sử dụng trình duyệt, download tập tin http://gaia.cs.umass.edu/wireshark-labs/alice.txt
   b. Truy xuất trang http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html

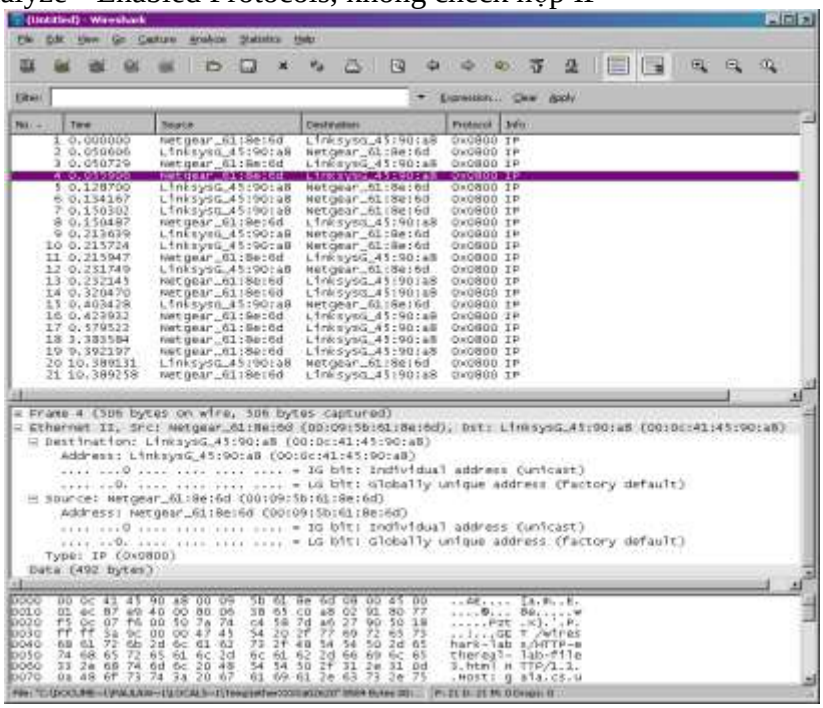


   c. Nhấp nút Browse, chọn file vừa download alice.txt.
   d. Khởi động Wireshark và chọn Capture > Start để bắt đầu bắt gói.
   e. Trở lại trình duyệt, nhấp nút "Upload alice.txt file" để upload file tới server gaia.cs.umass.edu. Một thông báo chúc mừng sẽ được hiển thị trên cửa sổ trình duyệt khi file upload thành công.
   f. Dừng việc bắt gói Wireshark và tiến hành phân tích các gói tin TCP.



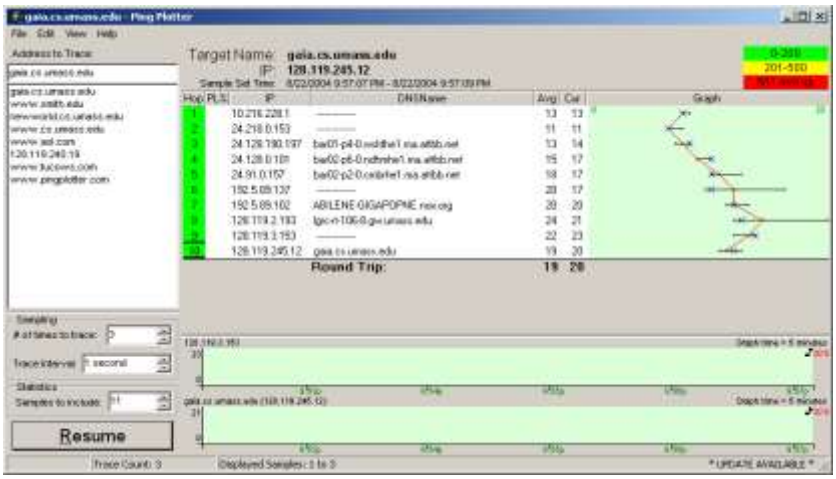
2. **Phân tích gói tin Internet Frame**

- Xóa trống cache trình duyệt (*Tools->Internet Options->Delete Files).*
- Khởi động Wireshark packet sniffer
- Truy xuất trang http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html
- Dừng bắt gói Wireshark. Tìm các gói tin HTTP GET được gửi từ máy bạn tới gaia.cs.umass.edu, và các gói tin HTTP response gửi từ gaia.cs.umass.edu tới máy của bạn.
- Chọn Analyze->Enabled Protocols, không check hộp IP



3. **Phân tích gói tin IP**

- Khởi động Wireshark và bắt đầu bắt gói tin.
- Khởi động *pingplotter* và nhập tên www.huflit.edu.vn trong mục "Address to Trace Window." Nhập số 3 vào field "# of times to Trace".
- Chọn lệnh *Edit->Advanced Options->Packet Options* và nhập vào giá trị 56 trong field *Packet Size* và nhấn OK. Nhấn nút Trace.

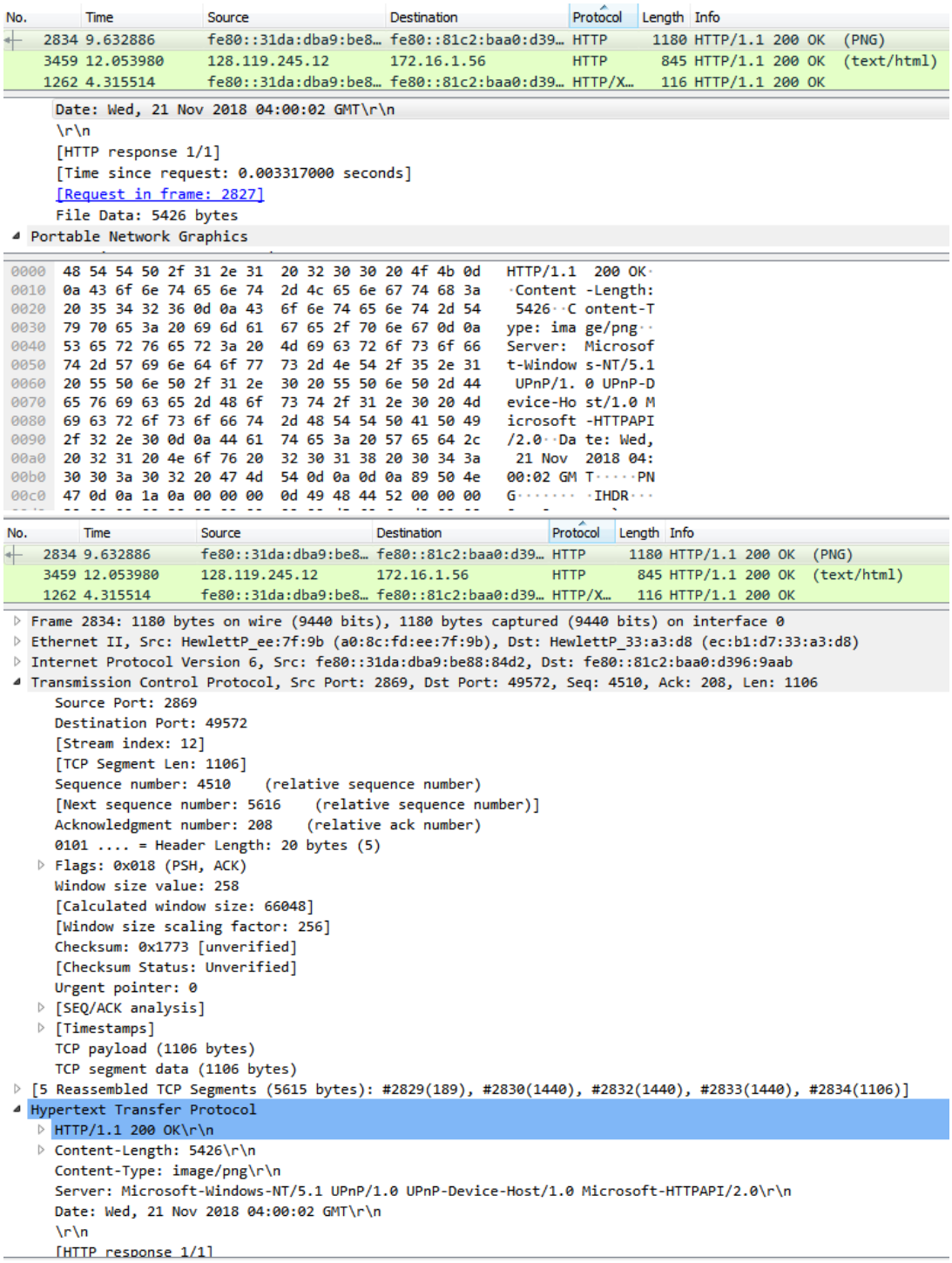


- Kế tiếp, gửi 1 bộ datagrams với chiều dài 2000, bằng cách chọn *Edit->Advanced Options->Packet Options, nhập giá trị* 2000 trong field *Packet Size*. Xong nhấn OK, rồi nhấn nút Resume.
- Cuối cùng, gửi 1 bộ datagrams với chiều dài 3500, bằng cách chọn *Edit->Advanced Options->Packet Options, nhập giá trị* 2000 trong field *Packet Size*. Xong nhấn OK, rồi nhấn nút Resume.
- Dừng việc bắt gói tin Wireshark.
- Phân tích gói tin ICMP Echo Request đầu tiên đã bắt được.

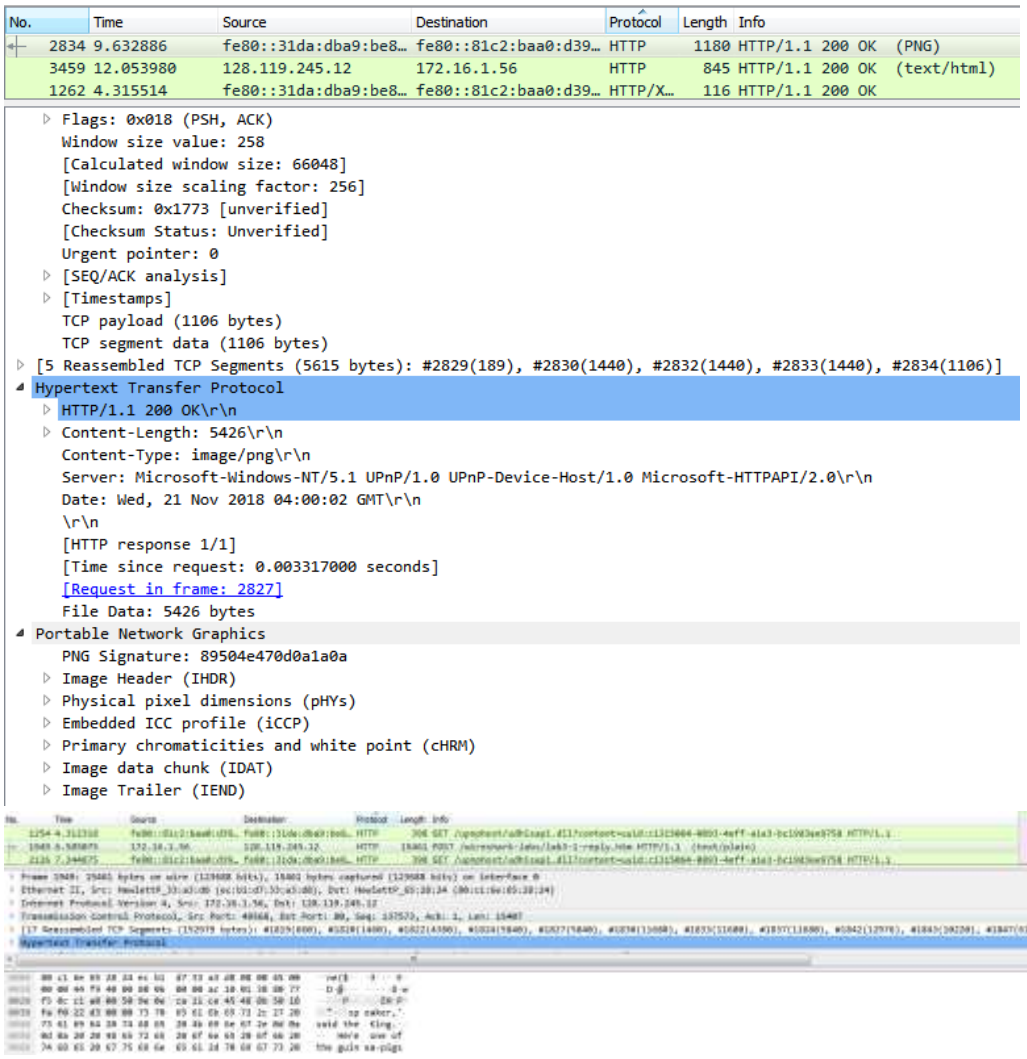
4. **Phân tích gói tin UDP**:
   - Bắt đầu bắt các gói tin trong Wireshark và thực hiện lệnh nslookup www.huflit.edu.vn.
   - Dừng việc bắt gói tin. Tiến hành lọc các gói tin UDP đã gửi và nhận được trên host của bạn. Chọn một gói tin UDP và phân tích chi tiết.

V. Ví dụ:

a. Phân tích gói tin HTTP

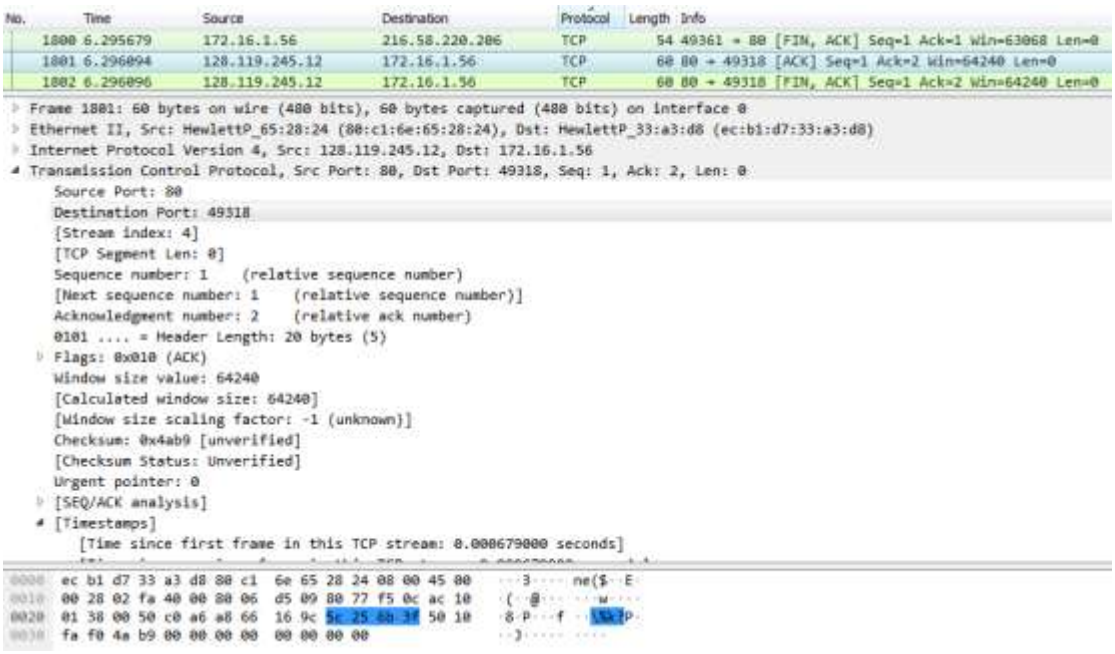


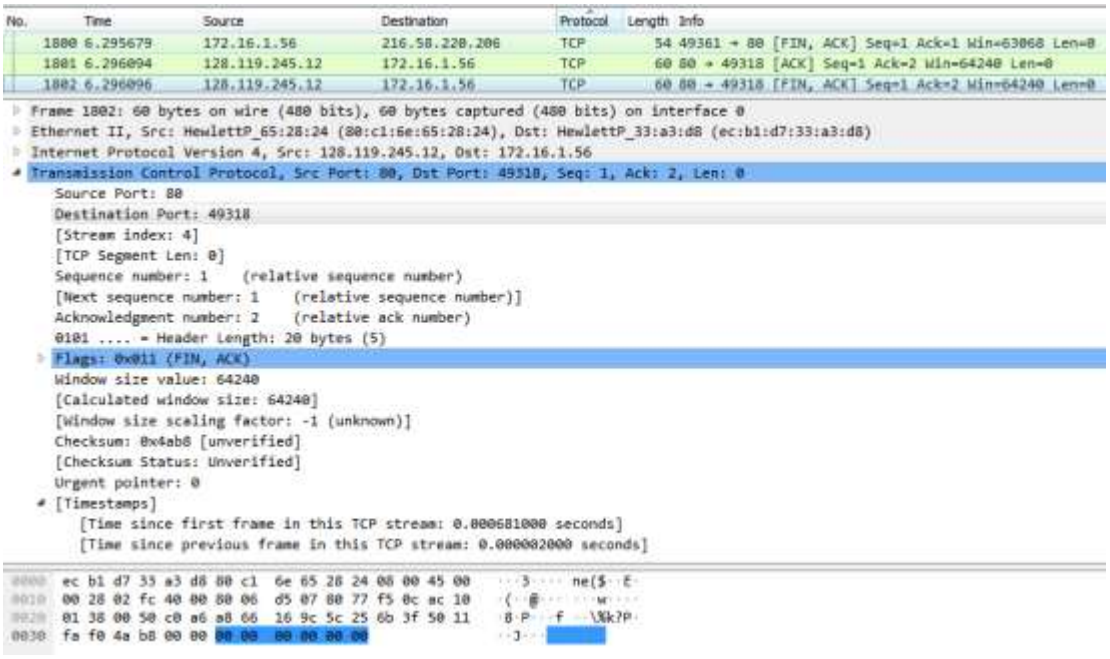
```
No.   Time        Source                Destination           Protocol Length Info
 2834 9.632886    fe80::31da:dba9:be8…  fe80::81c2:baa0:d39…  HTTP      1180 HTTP/1.1 200 OK  (PNG)
 3459 12.053980   128.119.245.12        172.16.1.56           HTTP       845 HTTP/1.1 200 OK  (text/html)
 1262 4.315514    fe80::31da:dba9:be8…  fe80::81c2:baa0:d39…  HTTP/X…    116 HTTP/1.1 200 OK

    Date: Wed, 21 Nov 2018 04:00:02 GMT\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.003317000 seconds]
    [Request in frame: 2827]
    File Data: 5426 bytes
  Portable Network Graphics

0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK·
0010  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67 74 68 3a   ·Content -Length:
0020  20 35 34 32 36 0d 0a 43  6f 6e 74 65 6e 74 2d 54    5426··C ontent-T
0030  79 70 65 3a 20 69 6d 61  67 65 2f 70 6e 67 0d 0a   ype: ima ge/png··
0040  53 65 72 76 65 72 3a 20  4d 69 63 72 6f 73 6f 66   Server:  Microsof
0050  74 2d 57 69 6e 64 6f 77  73 2d 4e 54 2f 35 2e 31   t-Window s-NT/5.1
0060  20 55 50 6e 50 2f 31 2e  30 20 55 50 6e 50 2d 44    UPnP/1. 0 UPnP-D
0070  65 76 69 63 65 2d 48 6f  73 74 2f 31 2e 30 20 4d   evice-Ho st/1.0 M
0080  69 63 72 6f 73 6f 66 74  2d 48 54 54 50 41 50 49   icrosoft -HTTPAPI
0090  2f 32 2e 30 0d 0a 44 61  74 65 3a 20 57 65 64 2c   /2.0··Da te: Wed,
00a0  20 32 31 20 4e 6f 76 20  32 30 31 38 20 30 34 3a    21 Nov  2018 04:
00b0  30 30 3a 30 32 20 47 4d  54 0d 0a 0d 0a 89 50 4e   00:02 GM T·····PN
00c0  47 0d 0a 1a 0a 00 00 00  0d 49 48 44 52 00 00 00   G······ ·IHDR···

No.   Time        Source                Destination           Protocol Length Info
 2834 9.632886    fe80::31da:dba9:be8…  fe80::81c2:baa0:d39…  HTTP      1180 HTTP/1.1 200 OK  (PNG)
 3459 12.053980   128.119.245.12        172.16.1.56           HTTP       845 HTTP/1.1 200 OK  (text/html)
 1262 4.315514    fe80::31da:dba9:be8…  fe80::81c2:baa0:d39…  HTTP/X…    116 HTTP/1.1 200 OK

  Frame 2834: 1180 bytes on wire (9440 bits), 1180 bytes captured (9440 bits) on interface 0
  Ethernet II, Src: HewlettP_ee:7f:9b (a0:8c:fd:ee:7f:9b), Dst: HewlettP_33:a3:d8 (ec:b1:d7:33:a3:d8)
  Internet Protocol Version 6, Src: fe80::31da:dba9:be88:84d2, Dst: fe80::81c2:baa0:d396:9aab
  Transmission Control Protocol, Src Port: 2869, Dst Port: 49572, Seq: 4510, Ack: 208, Len: 1106
    Source Port: 2869
    Destination Port: 49572
    [Stream index: 12]
    [TCP Segment Len: 1106]
    Sequence number: 4510    (relative sequence number)
    [Next sequence number: 5616    (relative sequence number)]
    Acknowledgment number: 208    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window size value: 258
    [Calculated window size: 66048]
    [Window size scaling factor: 256]
    Checksum: 0x1773 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
    [Timestamps]
    TCP payload (1106 bytes)
    TCP segment data (1106 bytes)
  [5 Reassembled TCP Segments (5615 bytes): #2829(189), #2830(1440), #2832(1440), #2833(1440), #2834(1106)]
  Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Content-Length: 5426\r\n
    Content-Type: image/png\r\n
    Server: Microsoft-Windows-NT/5.1 UPnP/1.0 UPnP-Device-Host/1.0 Microsoft-HTTPAPI/2.0\r\n
    Date: Wed, 21 Nov 2018 04:00:02 GMT\r\n
    \r\n
    [HTTP response 1/1]
```

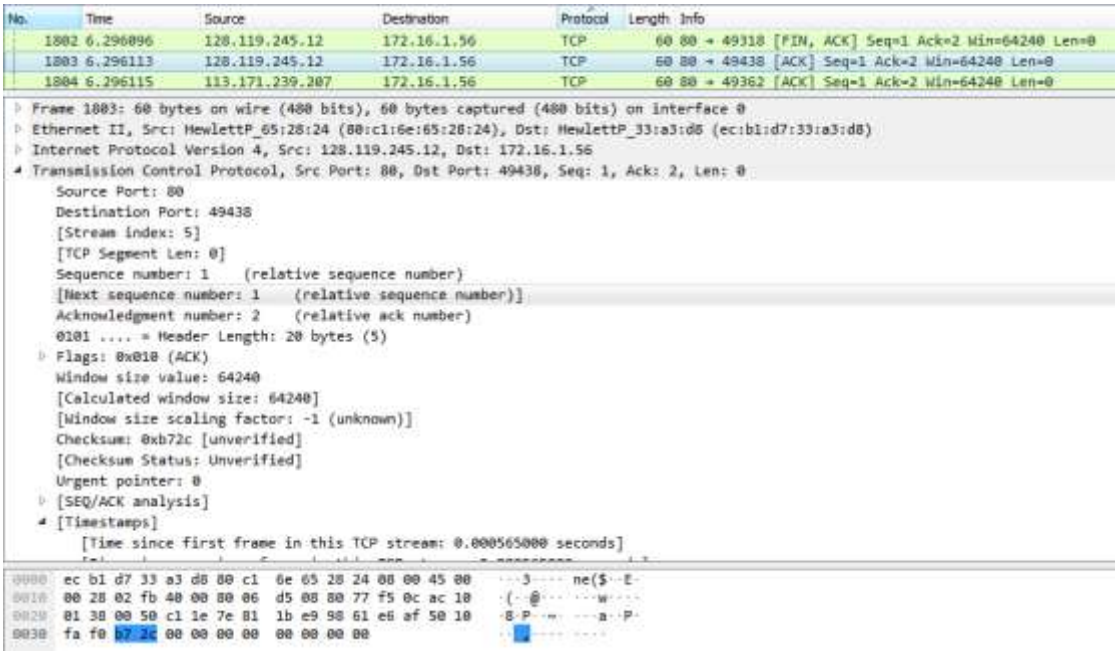


Phân tích gói tin TCP

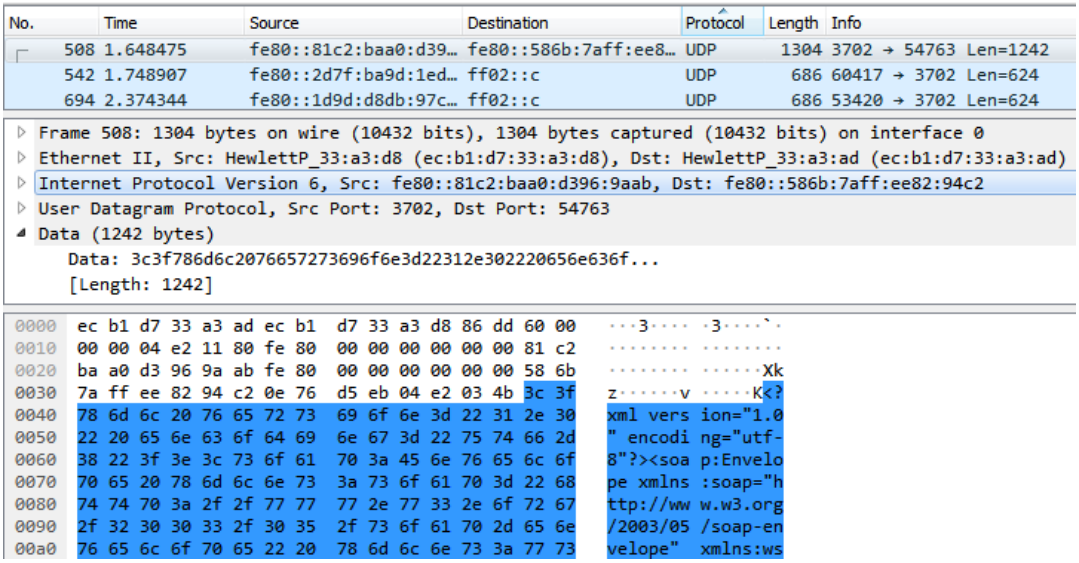
1797	6.295415	172.16.1.56	128.119.245.12	TCP	54 49318 → 80 [FIN, ACK] Seq=1 Ack=1 Win=64240 Len=0
1798	6.295548	172.16.1.56	128.119.245.12	TCP	54 49438 → 80 [FIN, ACK] Seq=1 Ack=1 Win=64240 Len=0
1799	6.295615	172.16.1.56	113.171.239.207	TCP	54 49362 → 80 [FIN, ACK] Seq=1 Ack=1 Win=64240 Len=0
1800	6.295679	172.16.1.56	216.58.220.206	TCP	54 49361 → 80 [FIN, ACK] Seq=1 Ack=1 Win=63068 Len=0
1801	6.296094	128.119.245.12	172.16.1.56	TCP	60 80 → 49318 [ACK] Seq=1 Ack=2 Win=64240 Len=0
1802	6.296096	128.119.245.12	172.16.1.56	TCP	60 80 → 49318 [FIN, ACK] Seq=1 Ack=2 Win=64240 Len=0
1803	6.296113	128.119.245.12	172.16.1.56	TCP	60 80 → 49438 [ACK] Seq=1 Ack=2 Win=64240 Len=0
1804	6.296115	113.171.239.207	172.16.1.56	TCP	60 80 → 49362 [ACK] Seq=1 Ack=2 Win=64240 Len=0
1805	6.296116	128.119.245.12	172.16.1.56	TCP	60 80 → 49438 [FIN, ACK] Seq=1 Ack=2 Win=64240 Len=0
1806	6.296116	113.171.239.207	172.16.1.56	TCP	60 80 → 49362 [FIN, ACK] Seq=1 Ack=2 Win=64240 Len=0
1807	6.296128	216.58.220.206	172.16.1.56	TCP	60 80 → 49361 [ACK] Seq=1 Ack=2 Win=64240 Len=0
1808	6.296152	172.16.1.56	128.119.245.12	TCP	54 49318 → 80 [ACK] Seq=2 Ack=2 Win=64240 Len=0
1809	6.296180	172.16.1.56	128.119.245.12	TCP	54 49438 → 80 [ACK] Seq=2 Ack=2 Win=64240 Len=0
1810	6.296215	172.16.1.56	113.171.239.207	TCP	54 49362 → 80 [ACK] Seq=2 Ack=2 Win=64240 Len=0
1811	6.296367	172.16.1.56	128.119.245.12	TCP	66 49568 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
1812	6.296881	216.58.220.206	172.16.1.56	TCP	60 80 → 49361 [FIN, ACK] Seq=1 Ack=2 Win=64240 Len=0
1813	6.296882	128.119.245.12	172.16.1.56	TCP	62 80 → 49568 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM=1
1814	6.296930	172.16.1.56	216.58.220.206	TCP	54 49361 → 80 [ACK] Seq=2 Ack=2 Win=63068 Len=0
1815	6.296967	172.16.1.56	128.119.245.12	TCP	66 49569 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
1816	6.297041	172.16.1.56	128.119.245.12	TCP	54 49568 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1817	6.297680	128.119.245.12	172.16.1.56	TCP	62 80 → 49569 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM=1


No. Time Source Destination Protocol Length Info
1800 6.295679 172.16.1.56 216.58.220.206 TCP 54 49361 → 80 [FIN, ACK] Seq=1 Ack=1 Win=63068 Len=0
1801 6.296094 128.119.245.12 172.16.1.56 TCP 60 80 → 49318 [ACK] Seq=1 Ack=2 Win=64240 Len=0
1802 6.296096 128.119.245.12 172.16.1.56 TCP 60 80 → 49318 [FIN, ACK] Seq=1 Ack=2 Win=64240 Len=0
Frame 1801: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: HewlettP_65:28:24 (80:c1:6e:65:28:24), Dst: HewlettP_33:a3:d8 (ec:b1:d7:33:a3:d8)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.16.1.56
Transmission Control Protocol, Src Port: 80, Dst Port: 49318, Seq: 1, Ack: 2, Len: 0
Source Port: 80
Destination Port: 49318
[Stream index: 4]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 2 (relative ack number)
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window size value: 64240
[Calculated window size: 64240]
[Window size scaling factor: -1 (unknown)]
Checksum: 0x4ab9 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
[Timestamps]
[Time since first frame in this TCP stream: 0.000679000 seconds]
ec b1 d7 33 a3 d8 80 c1 6e 65 28 24 08 00 45 00
00 28 02 fa 40 00 80 06 d5 09 80 77 f5 0c ac 10
01 38 00 50 c0 a6 a8 66 16 9c 5c 25 6b 3f 50 10
fa f0 4a b9 00 00 00 00 00 00 00 00


No. Time Source Destination Protocol Length Info
1800 6.295679 172.16.1.56 216.58.220.206 TCP 54 49361 → 80 [FIN, ACK] Seq=1 Ack=1 Win=63068 Len=0
1801 6.296094 128.119.245.12 172.16.1.56 TCP 60 80 → 49318 [ACK] Seq=1 Ack=2 Win=64240 Len=0
1802 6.296096 128.119.245.12 172.16.1.56 TCP 60 80 → 49318 [FIN, ACK] Seq=1 Ack=2 Win=64240 Len=0
Frame 1802: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: HewlettP_65:28:24 (80:c1:6e:65:28:24), Dst: HewlettP_33:a3:d8 (ec:b1:d7:33:a3:d8)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.16.1.56
Transmission Control Protocol, Src Port: 80, Dst Port: 49318, Seq: 1, Ack: 2, Len: 0
Source Port: 80
Destination Port: 49318
[Stream index: 4]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 2 (relative ack number)
0101 .... = Header Length: 20 bytes (5)
Flags: 0x011 (FIN, ACK)
Window size value: 64240
[Calculated window size: 64240]
[Window size scaling factor: -1 (unknown)]
Checksum: 0x4ab8 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[Timestamps]
[Time since first frame in this TCP stream: 0.000681000 seconds]
[Time since previous frame in this TCP stream: 0.000002000 seconds]
ec b1 d7 33 a3 d8 80 c1 6e 65 28 24 08 00 45 00
00 28 02 fc 40 00 80 06 d5 07 80 77 f5 0c ac 10
01 38 00 50 c0 a6 a8 66 16 9c 5c 25 6b 3f 50 11
fa f0 4a b8 00 00 00 00 00 00 00 00



b. Phân tích gói tin UDP



No.	Time	Source	Destination	Protocol	Length	Info
508	1.648475	fe80::81c2:baa0:d39…	fe80::586b:7aff:ee8…	UDP	1304	3702 → 54763 Len=1242
542	1.748907	fe80::2d7f:ba9d:1ed…	ff02::c	UDP	686	60417 → 3702 Len=624
694	2.374344	fe80::1d9d:d8db:97c…	ff02::c	UDP	686	53420 → 3702 Len=624
698	2.413399	172.16.0.159	239.255.255.250	UDP	666	53004 → 3702 Len=624
699	2.414150	fe80::5de2:5fbe:5d9…	ff02::c	UDP	686	53005 → 3702 Len=624
721	2.505764	fe80::1d9d:d8db:97c…	ff02::c	UDP	686	53420 → 3702 Len=624
743	2.580303	fe80::5de2:5fbe:5d9…	ff02::c	UDP	686	53005 → 3702 Len=624
769	2.657437	172.16.0.159	239.255.255.250	UDP	666	53004 → 3702 Len=624
861	3.034562	172.16.0.217	239.255.255.250	UDP	666	59954 → 3702 Len=624
862	3.035305	fe80::616a:3acf:2ce…	ff02::c	UDP	686	59955 → 3702 Len=624
869	3.091683	fe80::616a:3acf:2ce…	ff02::c	UDP	686	59955 → 3702 Len=624
893	3.167676	172.16.0.217	239.255.255.250	UDP	666	59954 → 3702 Len=624
940	3.356492	172.16.1.56	172.16.0.217	UDP	1269	3702 → 59954 Len=1227
978	3.542443	172.16.1.56	172.16.0.217	UDP	1269	3702 → 59954 Len=1227
1395	4.620522	172.16.1.56	172.16.0.159	UDP	1269	3702 → 53004 Len=1227
1465	4.835381	172.16.1.56	172.16.0.159	UDP	1269	3702 → 53004 Len=1227
1472	4.847494	fe80::5c27:29a5:686…	ff02::c	UDP	686	58917 → 3702 Len=624
1495	4.967379	fe80::5c27:29a5:686…	ff02::c	UDP	686	58917 → 3702 Len=624
1937	6.546281	fe80::a884:843b:661…	ff02::c	UDP	686	58204 → 3702 Len=624
1987	6.714654	fe80::a884:843b:661…	ff02::c	UDP	686	58204 → 3702 Len=624
2824	9.629403	fe80::d511:9732:3c3…	ff02::c	UDP	686	54646 → 3702 Len=624
3024	10.446194	fe80::e0df:223e:8f7…	ff02::c	UDP	686	63084 → 3702 Len=624