

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



BÁO CÁO BÀI TẬP TRÊN LỚP
MÔN KỸ THUẬT THEO DÕI VÀ
GIÁM SÁT AN TOÀN MẠNG

Giảng viên: Ninh Thị Thu Trang

Nhóm lớp: 01

Sinh viên: Hoàng Trung Kiên

Mã sinh viên: B20DCAT098

Hà Nội – 2024

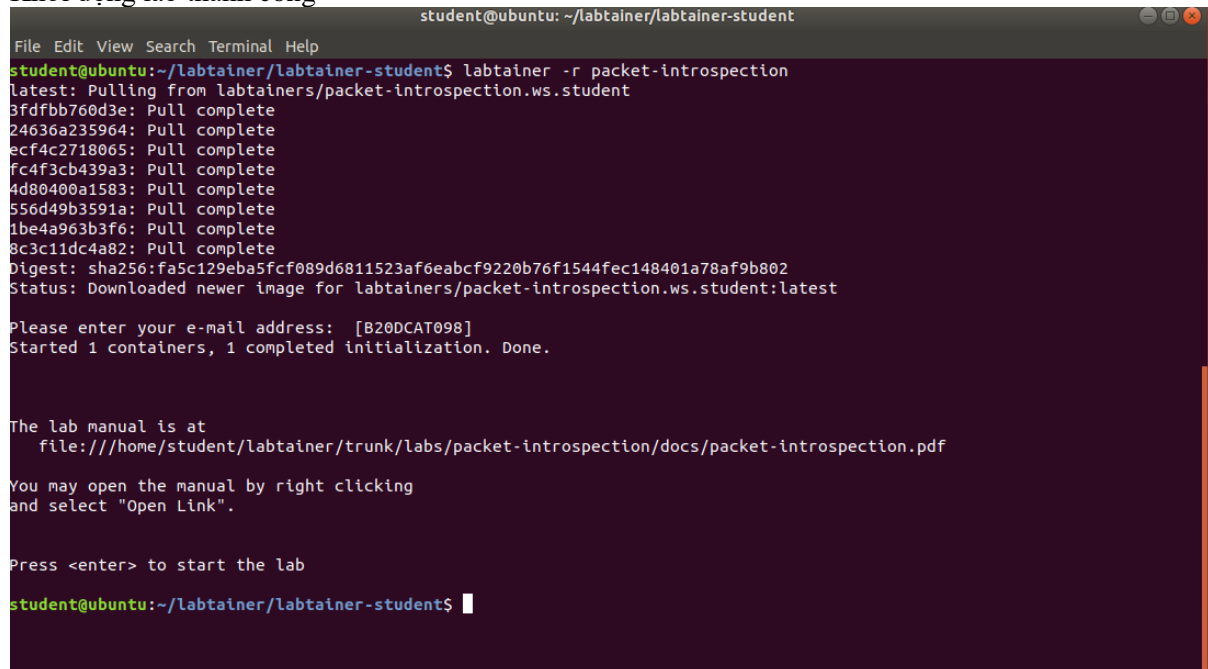
1.1. Bắt đầu bài lab

- Khởi động bài lab:
- Vào terminal, gõ: `labtainer -r packet-introspection`

1.2. Tìm luồng hoạt động nhiều nhất

- Mở file `pcaps/http-misctrffic101.pcapng` trong Wireshark
- Chọn Statistics — Conversations. Nhấp vào tab Ethernet. Lưu ý rằng chỉ có một cặp máy chủ giao tiếp trên mạng cục bộ. Tích chọn vào ô Name resolution. Địa chỉ MAC được liệt kê với Cadant là bộ định tuyến cục bộ, Flextron là máy khách mà từ đó lưu lượng truy cập được ghi lại

Khởi động lab thành công



```
student@ubuntu: ~/labtainer/labtainer-student
File Edit View Search Terminal Help
student@ubuntu:~/labtainer/labtainer-student$ labtainer -r packet-introspection
latest: Pulling from labtainers/packet-introspection.ws.student
3fdfbb760d3e: Pull complete
24636a235964: Pull complete
ecf4c2718065: Pull complete
fc4f3cb439a3: Pull complete
4d80400a1583: Pull complete
556d49b3591a: Pull complete
1be4a963b3f6: Pull complete
8c3c11dc4a82: Pull complete
Digest: sha256:fa5c129eba5fcf089d6811523af6eabcf9220b76f1544fec148401a78af9b802
Status: Downloaded newer image for labtainers/packet-introspection.ws.student:latest

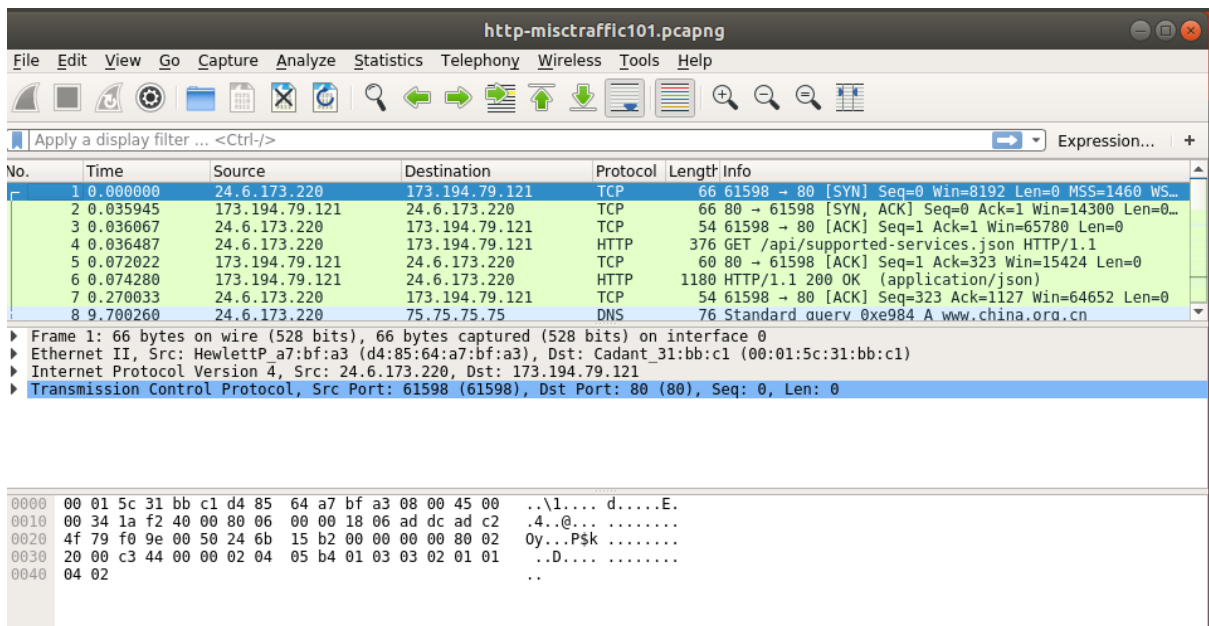
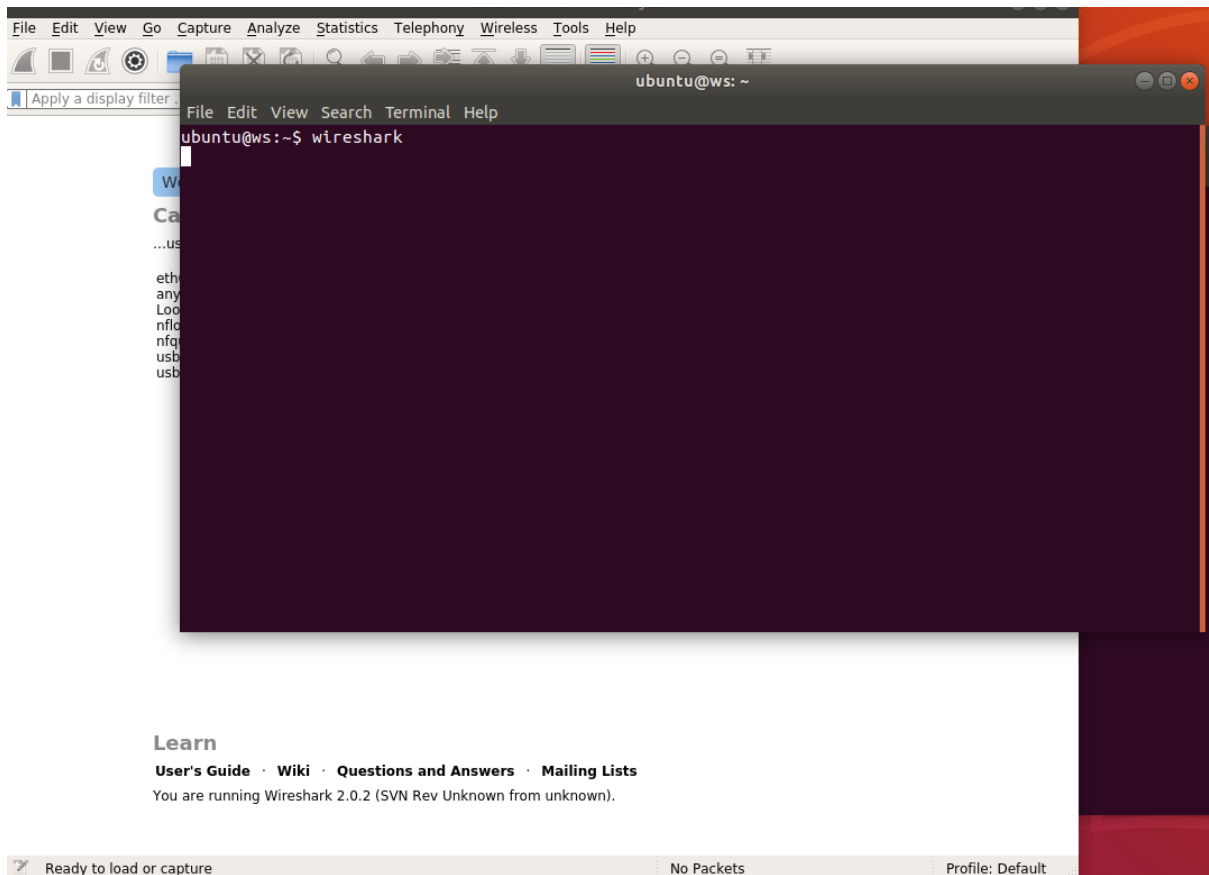
Please enter your e-mail address: [B20DCAT098]
Started 1 containers, 1 completed initialization. Done.

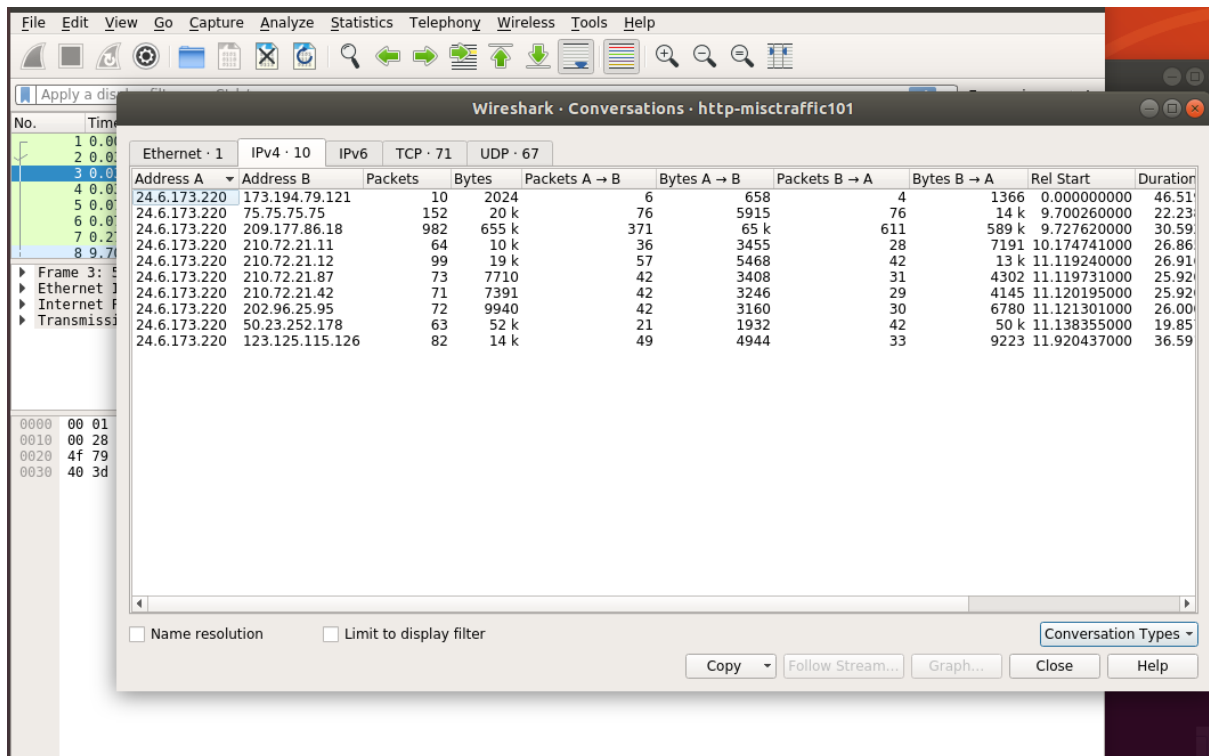
The lab manual is at
  file:///home/student/labtainer/trunk/labs/packet-introspection/docs/packet-introspection.pdf

You may open the manual by right clicking
and select "Open Link".

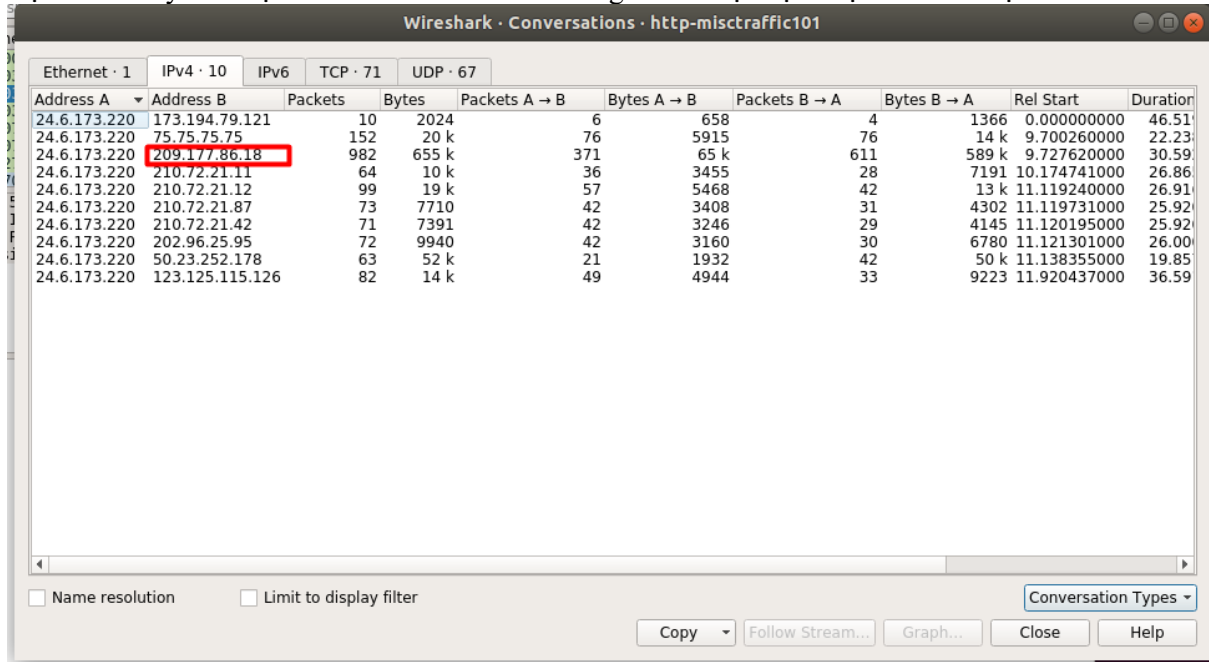
Press <enter> to start the lab

student@ubuntu:~/labtainer/labtainer-student$
```





Dựa trên số byte thì địa chỉ IP 209.177.86.18 tham gia vào cuộc hội thoại IPv4 tích cực nhất



- Nhấp vào tab TCP để xác định cuộc hội thoại TCP tích cực nhất. Sắp xếp theo byte bằng cách nhấp vào cột Byte.

Wireshark · Conversations · http-misctraffic101

Ethernet · 1		IPv4 · 10		IPv6		TCP · 71		UDP · 67	
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
24.6.173.220	61619	209.177.86.18	80	103	100 k	33	2117	70	98 k
24.6.173.220	61604	209.177.86.18	80	112	94 k	40	4940	72	89 k
24.6.173.220	61599	209.177.86.18	80	99	89 k	31	4224	68	85 k
24.6.173.220	61603	209.177.86.18	80	104	88 k	36	4375	68	83 k
24.6.173.220	61607	209.177.86.18	80	86	65 k	31	4718	55	60 k
24.6.173.220	61606	209.177.86.18	80	86	60 k	33	4882	53	55 k
24.6.173.220	61608	209.177.86.18	80	79	52 k	31	5094	48	46 k
24.6.173.220	61613	50.23.252.178	80	53	51 k	16	1203	37	50 k
24.6.173.220	61605	209.177.86.18	80	78	50 k	30	5089	48	45 k
24.6.173.220	61609	210.72.21.12	80	27	14 k	12	2822	15	11 k
24.6.173.220	61651	209.177.86.18	80	33	8581	14	4882	19	3699
24.6.173.220	61654	209.177.86.18	80	32	8525	14	4895	18	3630
24.6.173.220	61652	209.177.86.18	80	33	8482	14	4780	19	3702
24.6.173.220	61665	209.177.86.18	80	31	7783	13	4410	18	3373
24.6.173.220	61655	209.177.86.18	80	30	7648	13	4343	17	3305
24.6.173.220	61640	123.125.115.126	80	15	7384	6	634	9	6750
24.6.173.220	61666	209.177.86.18	80	28	6826	12	3873	16	2953
24.6.173.220	61601	210.72.21.11	80	18	6685	9	1143	9	5542
24.6.173.220	61612	202.96.25.95	80	12	3518	6	672	6	2846
24.6.173.220	61663	202.96.25.95	80	12	3506	6	724	6	2782
24.6.173.220	61611	210.72.21.42	80	12	3187	6	694	6	2493
24.6.173.220	61661	210.72.21.87	80	12	2522	6	977	6	1545
24.6.173.220	61623	209.177.86.18	80	12	2444	6	682	6	1762
24.6.173.220	61610	210.72.21.87	80	12	2212	6	667	6	1545
24.6.173.220	61614	209.177.86.18	80	12	2050	6	682	6	1368

☐ Name resolution ☐ Limit to display filter

Conversation Types

Copy Follow Stream... Graph... Close Help

- Nhấp chuột phải vào cuộc hội thoại TCP tích cực nhất và chọn Apply as a Filter — Selected — A<->B. Wireshark tự động tạo và áp dụng bộ lọc hiển thị cho cuộc hội thoại TCP này.

Wireshark · Conversations · http-misctraffic101

Ethernet · 1		IPv4 · 10		IPv6		TCP · 71		UDP · 67	
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
24.6.173.220	61619	209.177.86.18	80	103	100 k	33	2117	70	98 k
24.6.173.220	61604	209.177.86.18	80	112	94 k	40	4940	72	89 k
24.6.173.220	61599	209.177.86.18	80	99	89 k	31	4224	68	85 k
24.6.173.220	61603	209.177.86.18	80	104	88 k	36	4375	68	83 k
24.6.173.220	61607	209.177.86.18	80	86	65 k	31	4718	55	60 k
24.6.173.220	61606	209.177.86.18	80	86	60 k	33	4882	53	55 k
24.6.173.220	61608	209.177.86.18	80	79	52 k	31	5094	48	46 k
24.6.173.220	61613	50.23.252.178	80	53	51 k	16	1203	37	50 k
24.6.173.220	61605	209.177.86.18	80	78	50 k	30	5089	48	45 k
24.6.173.220	61609	210.72.21.12	80	27	14 k	12	2822	15	11 k
24.6.173.220	61651	209.177.86.18	80	33	8581	14	4882	19	3699
24.6.173.220	61654	209.177.86.18	80	32	8525	14	4895	18	3630
24.6.173.220	61652	209.177.86.18	80	33	8482	14	4780	19	3702
24.6.173.220	61665	209.177.86.18	80	31	7783	13	4410	18	3373
24.6.173.220	61655	209.177.86.18	80	30	7648	13	4343	17	3305
24.6.173.220	61640	123.125.115.126	80	15	7384	6	634	9	6750
24.6.173.220	61666	209.177.86.18	80	28	6826	12	3873	16	2953
24.6.173.220	61601	210.72.21.11	80	18	6685	9	1143	9	5542
24.6.173.220	61612	202.96.25.95	80	12	3518	6	672	6	2846
24.6.173.220	61663	202.96.25.95	80	12	3506	6	724	6	2782
24.6.173.220	61611	210.72.21.42	80	12	3187	6	694	6	2493
24.6.173.220	61661	210.72.21.87	80	12	2522	6	977	6	1545
24.6.173.220	61623	209.177.86.18	80	12	2444	6	682	6	1762
24.6.173.220	61610	210.72.21.87	80	12	2212	6	667	6	1545
24.6.173.220	61614	209.177.86.18	80	12	2050	6	682	6	1368

☐ Name resolution ☐ Limit to display filter

Conversation Types

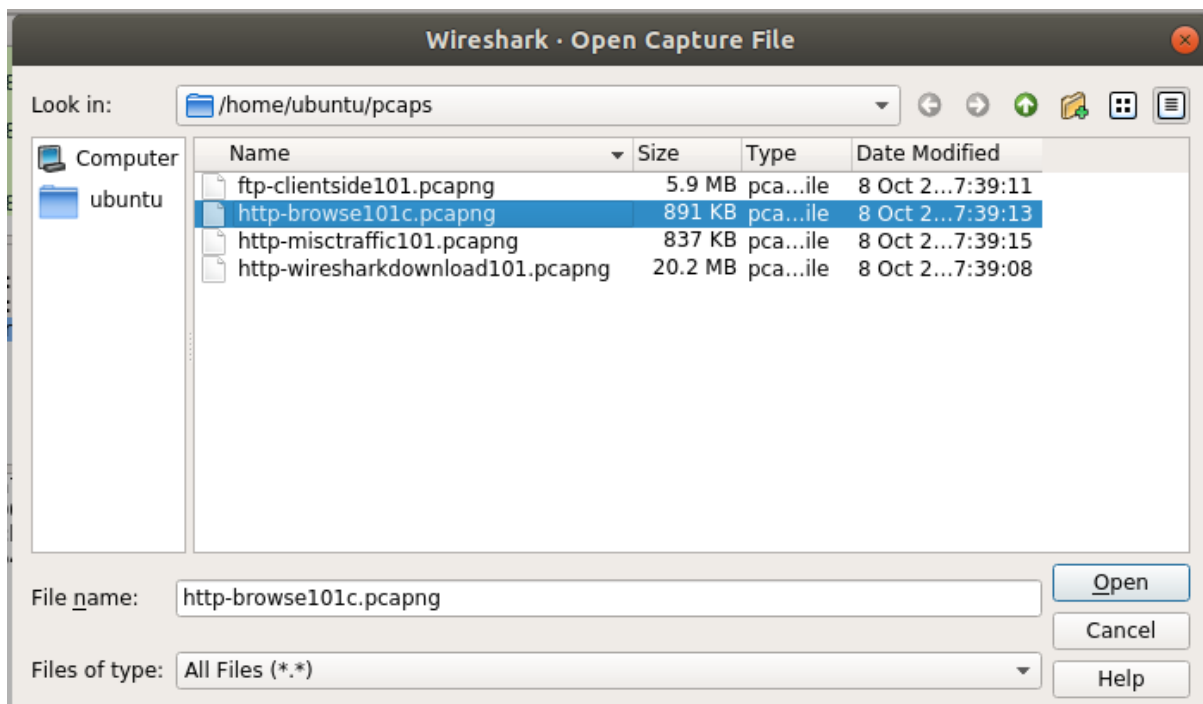
Copy Follow Stream... Graph... Close Help

Có 103 gói phù hợp

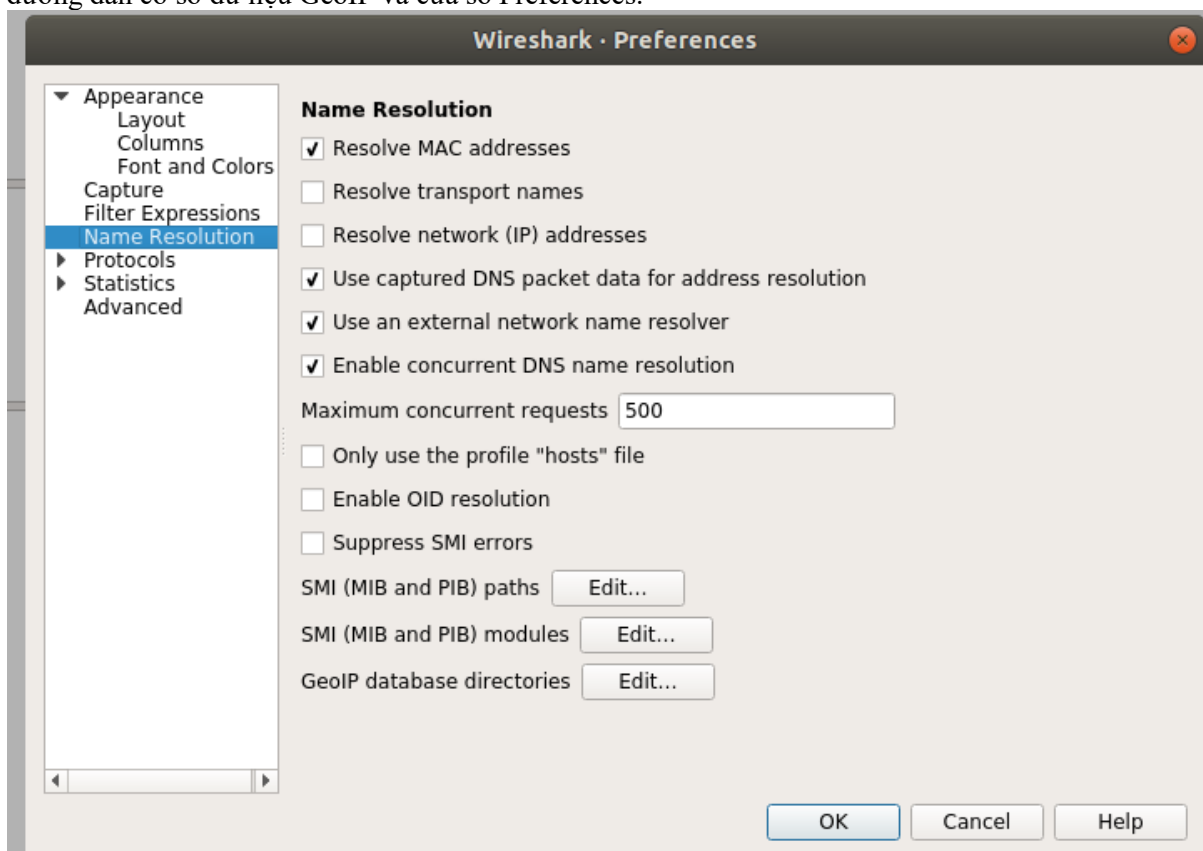
1.3. Định vị địa lý địa chỉ IP

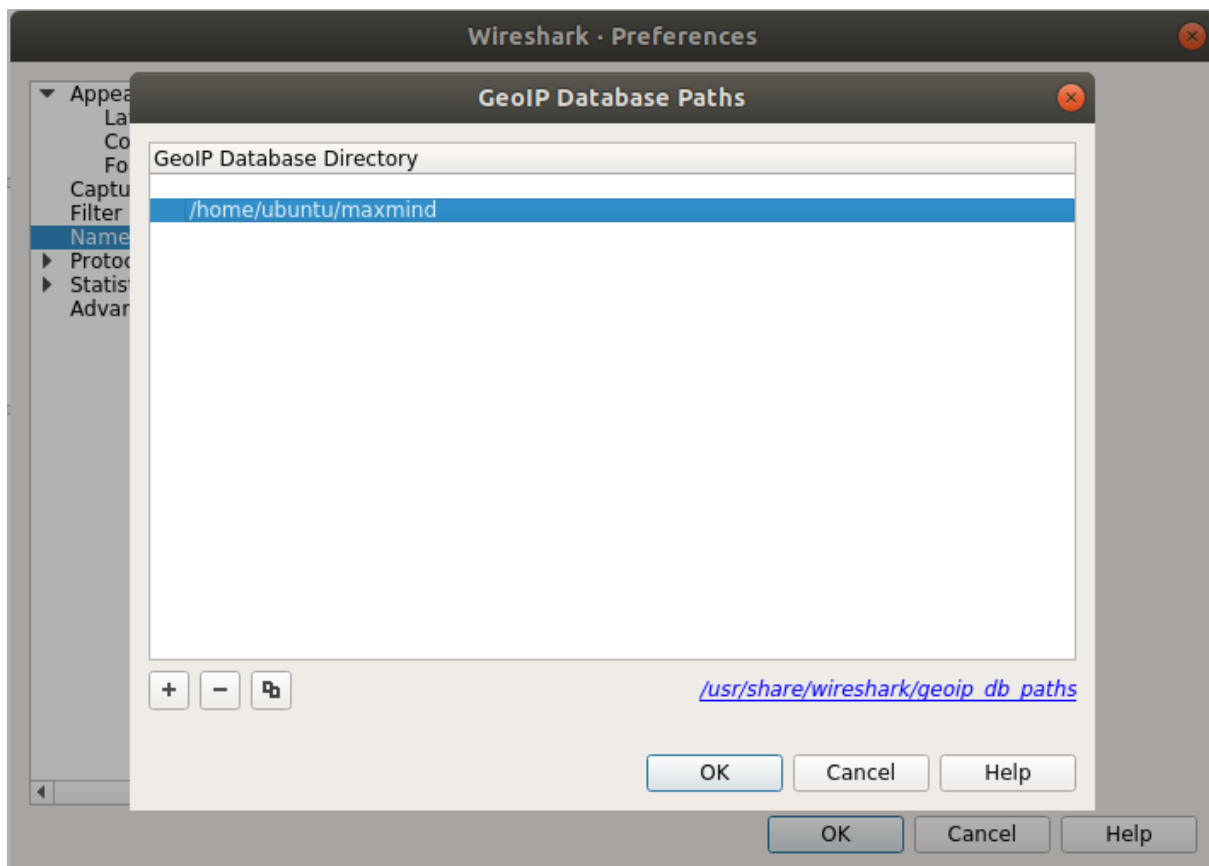
Tương quan giao diện mạng/địa chỉ IP với các vị trí địa lý thực tế là một thông tin hữu ích cho các cuộc điều tra. Wireshark cung cấp một khả năng cơ bản cho vấn đề này, sử dụng các phiên bản miễn phí của cơ sở dữ liệu MaxMind2. Tuy nhiên, phải luôn nhớ rằng không có cơ sở dữ liệu định vị địa lý IP nào là không có lỗi.

- Mở file pcaps/http-browse101c.pcapng trong Wireshark.

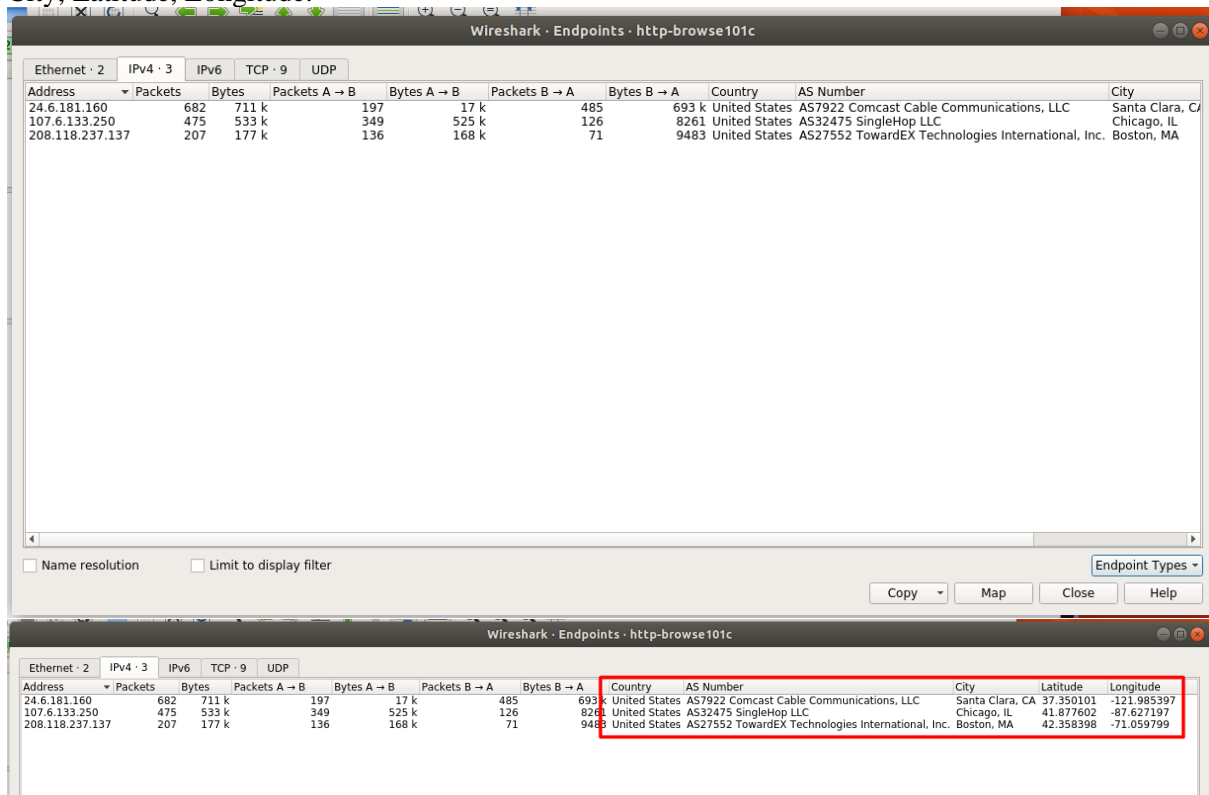


- Chọn Edit — Preferences — Name Resolution, nhấp vào Edit trong thư mục cơ sở dữ liệu GeoIP. Nhấp vào New và trở đến thư mục maxmind (có các tệp cơ sở dữ liệu được tải xuống từ <http://dev.maxmind.com/geoip/legacy/geolite/>). Tiếp tục nhấp vào OK cho đến khi bạn đóng cửa sổ đường dẫn cơ sở dữ liệu GeoIP và cửa sổ Preferences.

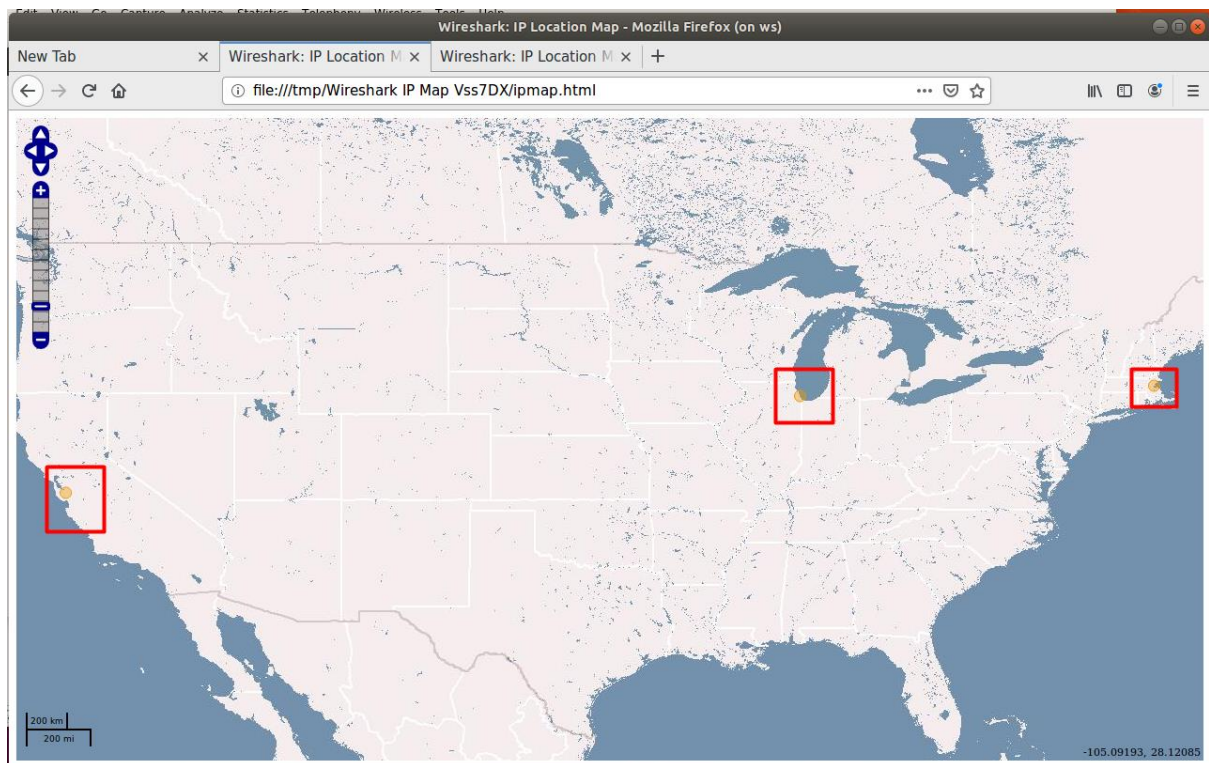




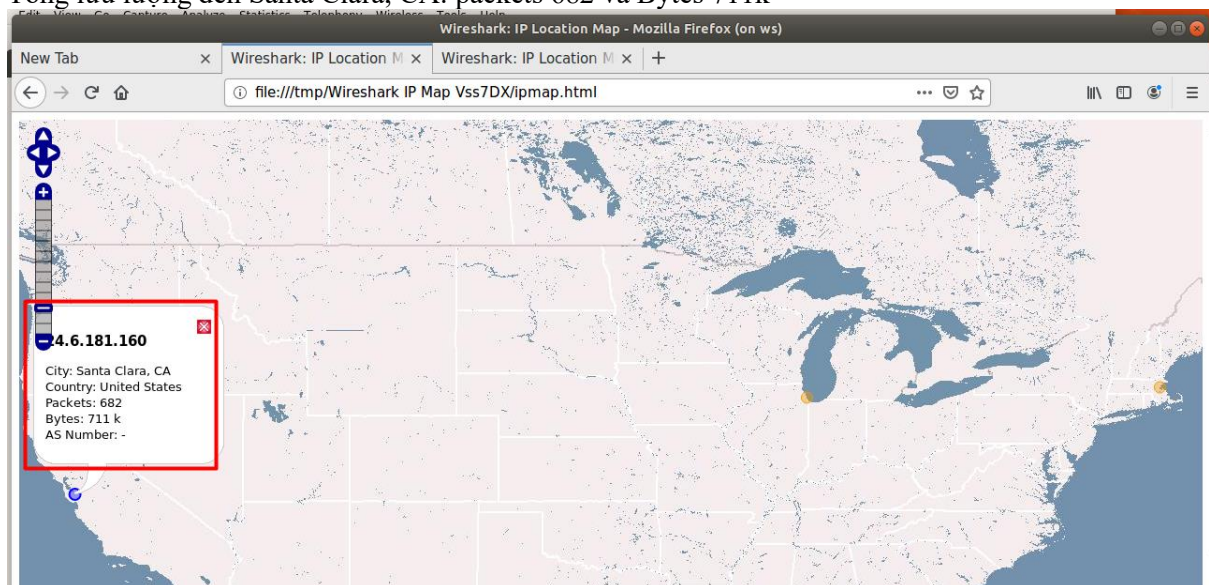
- Chọn Statistics — Endpoints và nhấn vào tab IPv4. Bạn có thể xem thông tin trong các cột Country, City, Latitude, Longitude.



- Nhấn vào nút Map, Wireshark sẽ khởi chạy chế độ xem bản đồ trong trình duyệt của bạn với các địa chỉ IP đã biết được vẽ dưới dạng các điểm trên bản đồ. Nhấp vào điểm bất kỳ để tìm thêm thông tin về địa chỉ IP



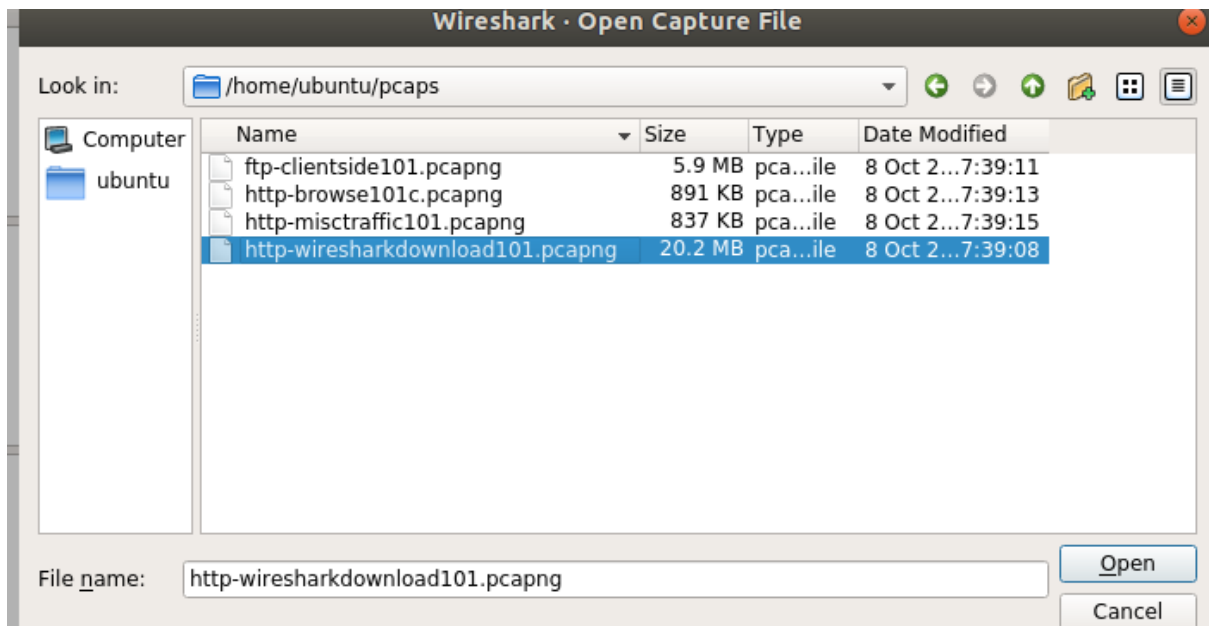
Tổng lưu lượng đến Santa Clara, CA: packets 682 và Bytes 711k



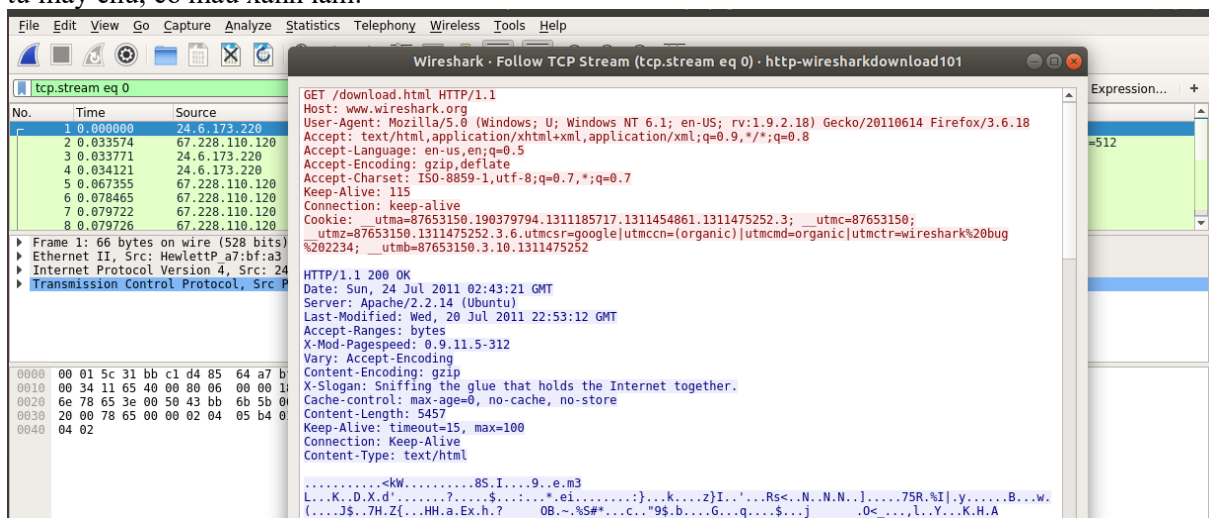
1.4. Tập hợp lại văn bản từ luồng TCP

Là một giao thức định hướng luồng byte, TCP phân đoạn dữ liệu dựa trên MSS của nó, không dựa trên ngữ nghĩa của ngôn ngữ tiếng Anh hoặc thậm chí định dạng dữ liệu ứng dụng. Do đó, có thể hữu ích nếu tập hợp lại dữ liệu này trước khi kiểm tra thủ công.

- Mở file pcaps/http-wiresharkdownload101.pcapng trong Wireshark.



- Ba gói đầu tiên là bắt tay TCP cho kết nối máy chủ web. Khung 4 chứa các máy khách GET yêu cầu cho trang download.html. Nhấp chuột phải vào khung 4 và chọn Follow — TCP Stream. Lưu lượng truy cập đầu tiên được nhìn thấy trong tệp là từ máy khách, có màu đỏ. Lưu lượng truy cập thứ hai là từ máy chủ, có màu xanh lam.



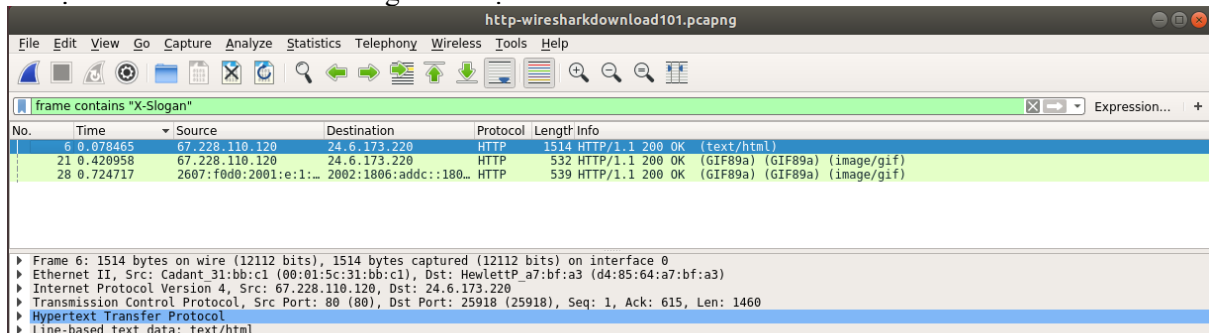
- Wireshark hiển thị cuộc hội thoại không có tiêu đề Ethernet, IP hoặc TCP. Cuộn qua luồng để tìm thông báo ản từ Gerald Combs, người tạo ra Wireshark. Nó nằm trong luồng máy chủ và bắt đầu bằng X-Slogan. Thông điệp là gì?

```
Wireshark · Follow TCP Stream (tcp.stream eq 0) · http-wiresharkdownload101

GET /download.html HTTP/1.1
Host: www.wireshark.org
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.18) Gecko/20110614 Firefox/3.6.18
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Cookie: __utma=87653150.190379794.1311185717.1311454861.1311475252.3; __utmc=87653150;
__utmz=87653150.1311475252.3.6.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=wireshark%20bug%202234; __utmb=87653150.3.10.1311475252

HTTP/1.1 200 OK
Date: Sun, 24 Jul 2011 02:43:21 GMT
Server: Apache/2.2.14 (Ubuntu)
Last-Modified: Wed, 20 Jul 2011 22:53:12 GMT
Accept-Ranges: bytes
X-Mod-Pagespeed: 0.9.11.5-312
Vary: Accept-Encoding
Content-Encoding: gzip
X-Slogan: Sniffing the glue that holds the Internet together.
Cache-Control: max-age=0, no-cache, no-store
Content-Length: 5457
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
```

Thông điệp là : X-Slogan: Sniffing the glue that holds the Internet together
Gõ lệnh “frame contains “X-Slogan” để lọc frame



```
Wireshark · Follow TCP Stream (tcp.stream eq 3) · http-wiresharkdownload101

GET /image/ipv6.gif?id=1068963279 HTTP/1.1
Host: ipv6.wireshark.org
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.18) Gecko/20110614 Firefox/3.6.18
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Referer: http://www.wireshark.org/download.html
Cookie: __utma=87653150.190379794.1311185717.1311454861.1311475252.3; __utmc=87653150;
__utmz=87653150.1311475252.3.6.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=wireshark%20bug%202234;
__utmb=87653150.4.10.1311475252

HTTP/1.1 200 OK
Date: Sun, 24 Jul 2011 02:43:21 GMT
Server: Apache/2.2.14 (Ubuntu)
Vary: Host
Last-Modified: Wed, 20 Jul 2011 22:53:22 GMT
Accept-Ranges: bytes
Content-Length: 43
Link: <http://www.wireshark.org/image/ipv6.gif>; rel="canonical"
X-Slogan: Sniff free or die.
Cache-Control: public, max-age=600
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: image/gif

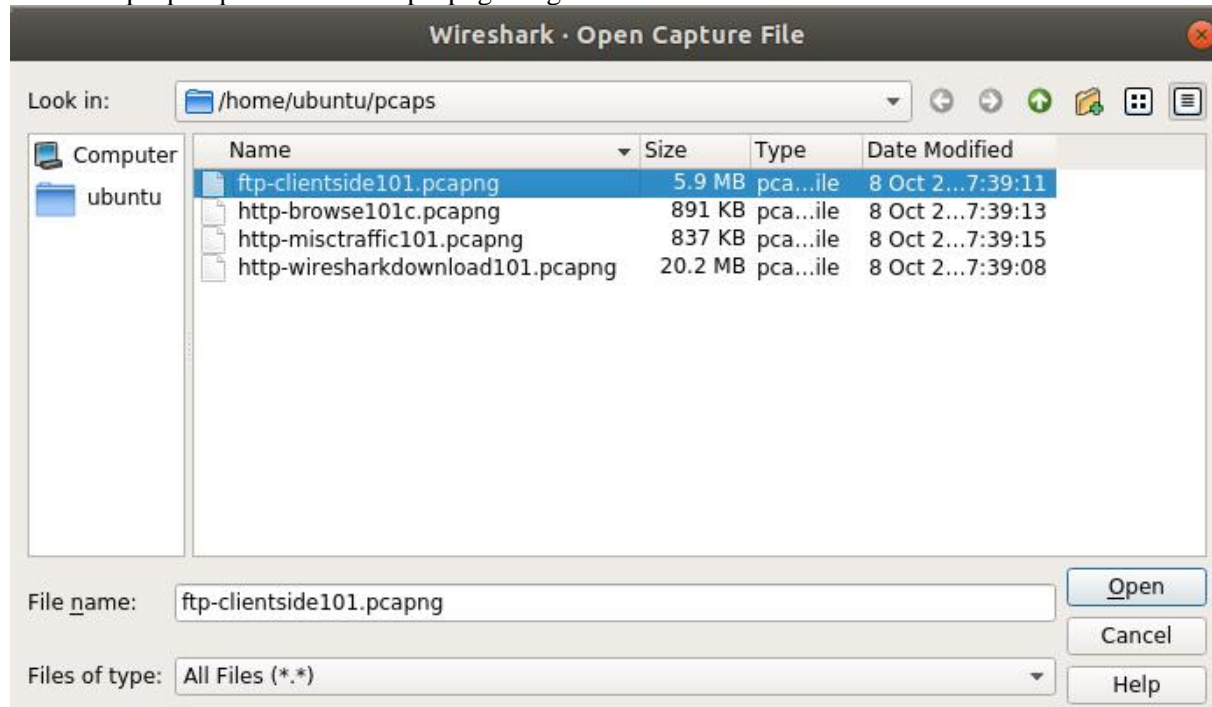
GIF89a.....!.....D..;
```

Ta tìm được một thông điệp khác là : X-Slogan: Sniff free or die.

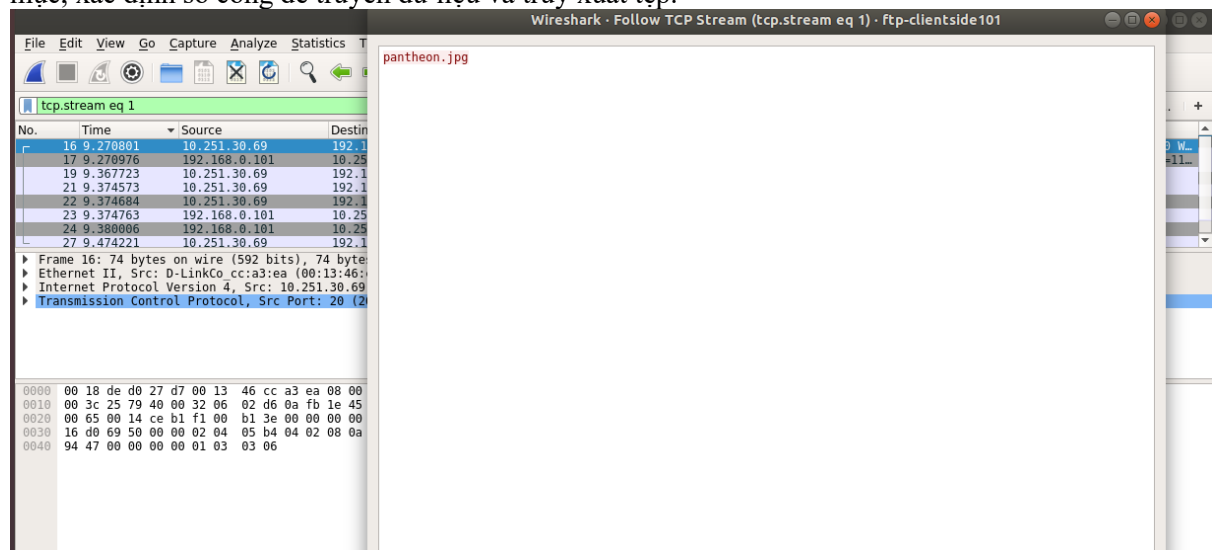
1.5. Giải nén tệp nhị phân từ phiên FTP

Trong phần trước, chúng ta đã trích xuất các tin nhắn văn bản ASCII từ các gói. Còn dữ liệu nhị phân thì sao? Wireshark cũng có các công cụ cho việc này.

- Mở file pcaps/ftp-clientside101.pcapng trong Wireshark.

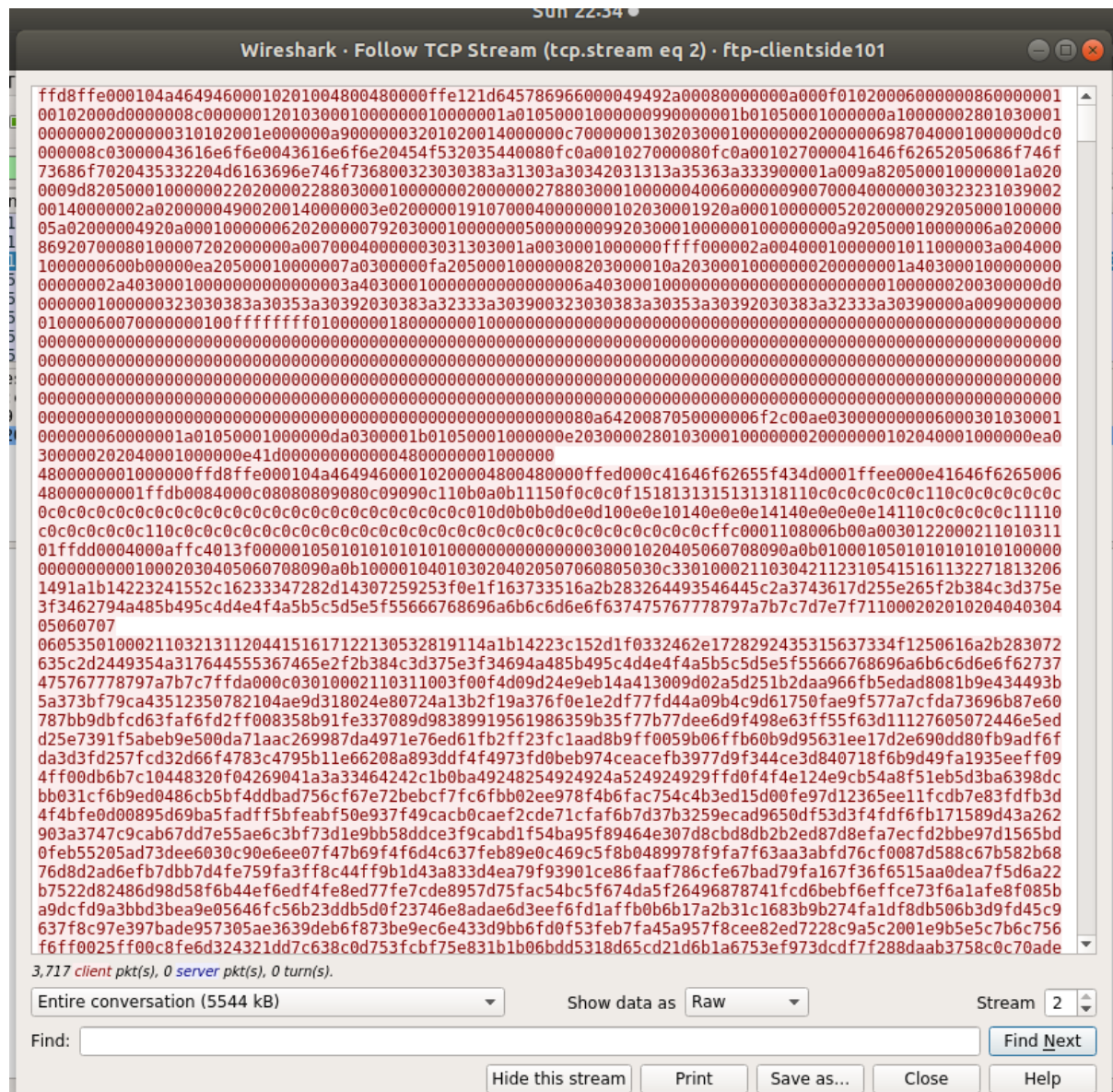


- Phần đầu của file pcap này bạn sẽ thấy nhiều lệnh FTP được sử dụng để đăng nhập, yêu cầu một thư mục, xác định số cổng để truyền dữ liệu và truy xuất tệp.

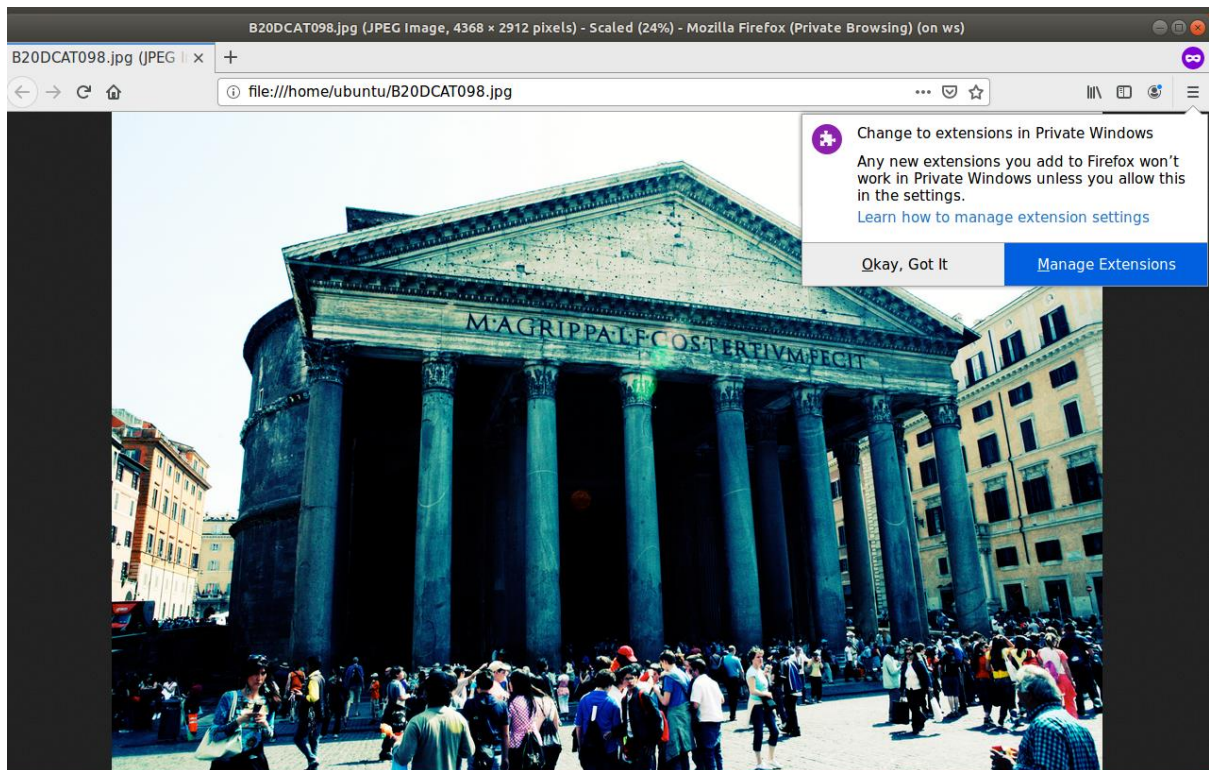


- Chúng ta chỉ quan tâm đến hai luồng dữ liệu: một luồng danh sách thư mục và một luồng truyền tệp. Trong cửa sổ Follow TCP Stream, nhấp vào nút Hide This Stream. Thao tác này sẽ đóng cửa sổ luồng TCP và áp dụng bộ lọc loại trừ.
- Các khung từ 16 đến 18 và các khung từ 35 đến 38 là các gói bắt tay TCP để thiết lập hai kênh dữ liệu cần thiết. Nhấp chuột phải vào khung 16 và chọn Follow — TCP Stream. Danh sách luồng này cho biết chỉ có một tệp trong thư mục.
- Nhấn nút Hide This Stream để đóng cửa sổ luồng TCP và thêm vào cửa sổ hiện có vào bộ lọc loại trừ.
- Lưu lượng còn lại duy nhất được hiển thị là lưu lượng truyền tệp. Nhấp chuột phải vào bất kỳ khung nào và chọn Follow — TCP Stream. Bạn có thể xem mã định danh tệp cho biết đây là tệp .jpg (JFIF) và siêu dữ liệu có trong tệp đồ họa.

- Để tập hợp lại hình ảnh đồ họa được truyền trong kết nối FTP này, hãy thay đổi phần Show data as thành Raw và chọn Save as bằng tên tệp mà bạn tìm được bên trên và ghi nhớ đường dẫn lưu file đó
- Quay lại terminal ubuntu@ws nhấn Ctr+C để đóng wireshark. Dùng trình duyệt để mở file mà bạn vừa lưu, chụp ảnh và dán vào báo cáo để nộp bài.



```
ubuntu@ws:~$ xdg-open B20DCAT098.jpg
Unescaped left brace in regex is deprecated, passed through in regex; marked by <-- HERE in m/%{ <--
HERE (.*)}/ at /usr/bin/run-mailcap line 528.
```

1.6. Kết thúc bài lab:

- o Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab: `stoptlab packet-introspection`
- o Khi bài lab kết thúc, một tệp lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới `stoptlab`. Sinh viên cần nộp file `.lab` để chấm điểm.
- Khởi động lại bài lab: Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng câu lệnh: `labtainer -r packet-introspection`