

Bài thực hành:

Quan sát lưu lượng bên trong gói tin pcapng

1. Mục đích:

- Giúp giúp sinh viên làm quen với file pcap và phân tích lưu lượng truy cập bằng Wireshark.

2. Yêu cầu đối với sinh viên:

- Có kiến thức cơ bản về hệ điều hành Linux, các thao tác với Wireshark.

3. Nội dung thực hành:

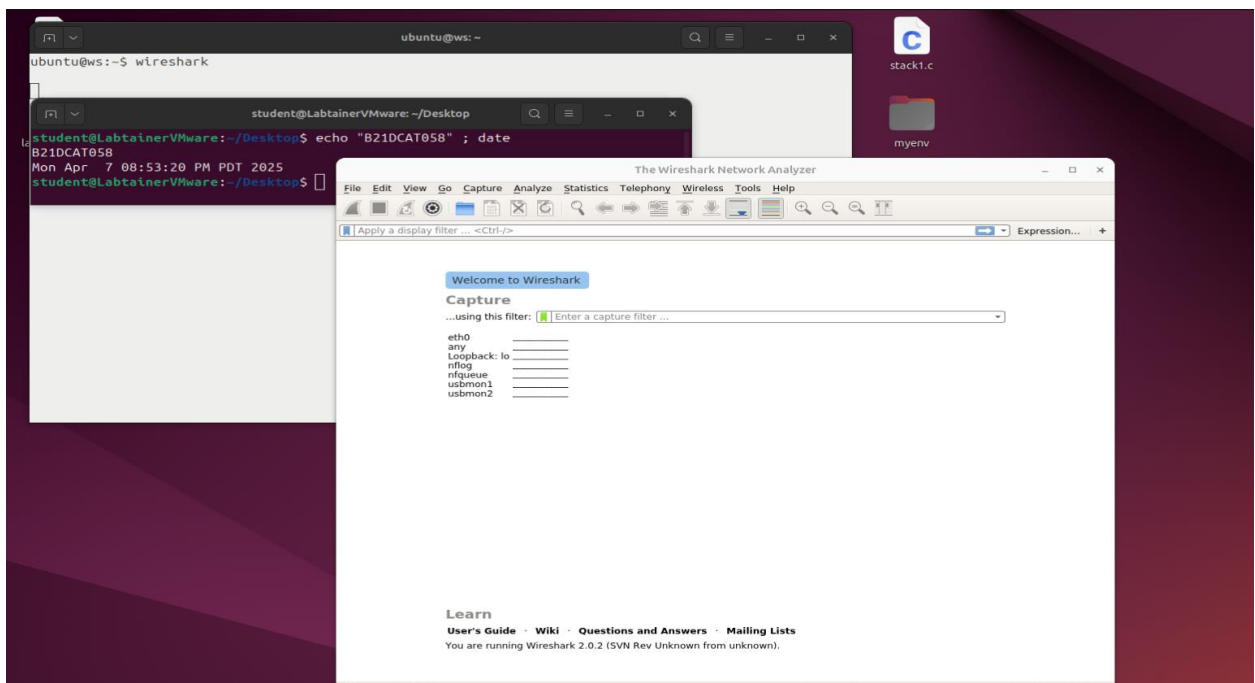
- Khởi động bài lab:
 - Vào terminal, gõ:

labtainer -r packet-introspection

(chú ý: sinh viên sử dụng mã sinh viên của mình để nhập thông tin người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm.)

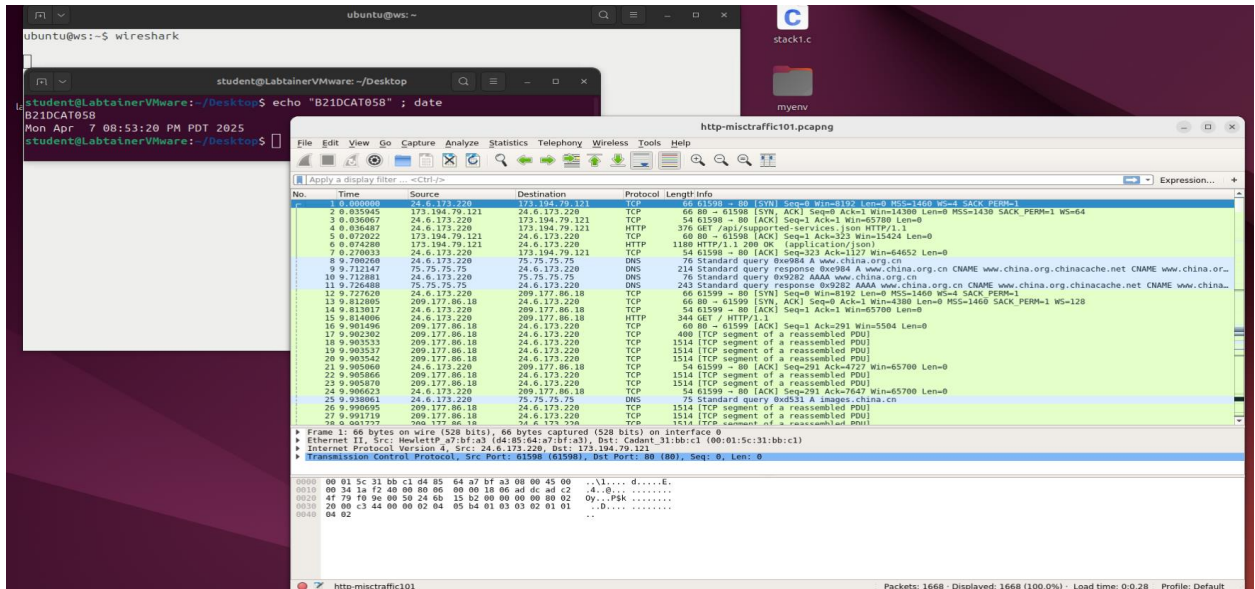
Sau khi khởi động xong có 1 terminal ảo sẽ xuất hiện, là nơi sinh viên sẽ sử dụng Wireshark để phân tích các gói tin..

- Trên terminal **ubuntu@ws:** sử dụng lệnh “wireshark” để khởi động Wireshark.

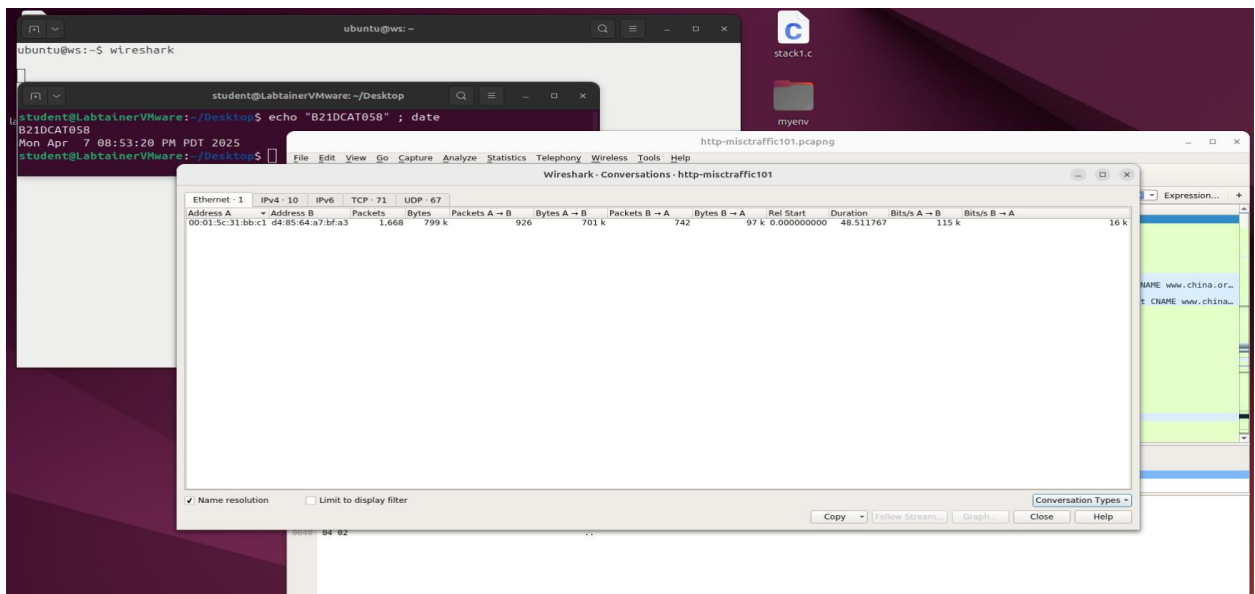


3.1. Tìm luồng hoạt động nhiều nhất

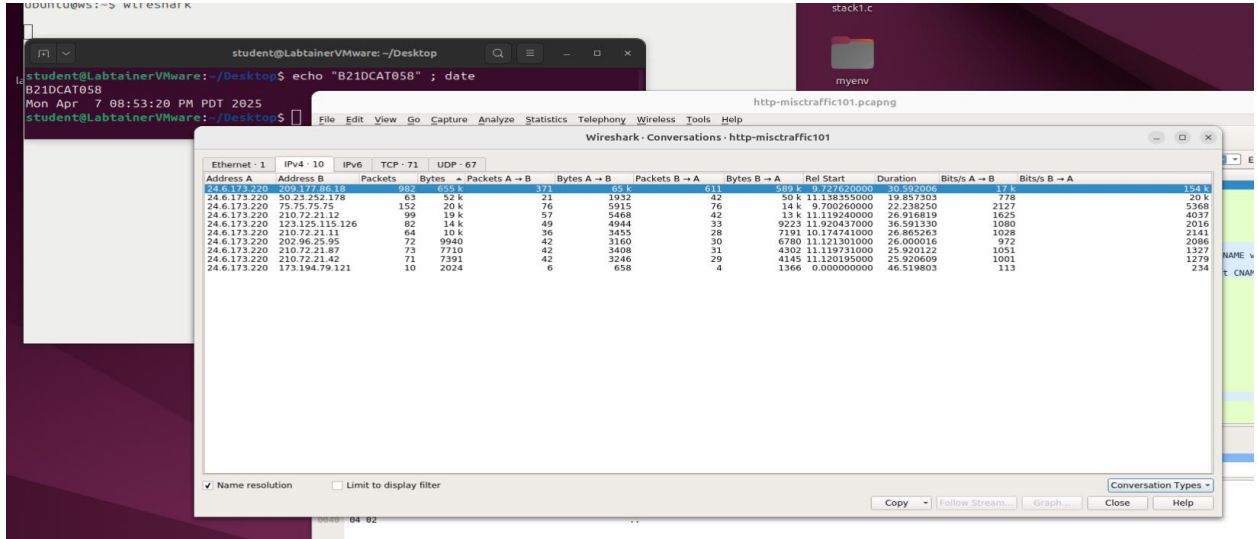
- Mở file pcaps/http-misctraffic101.pcapng trong Wireshark



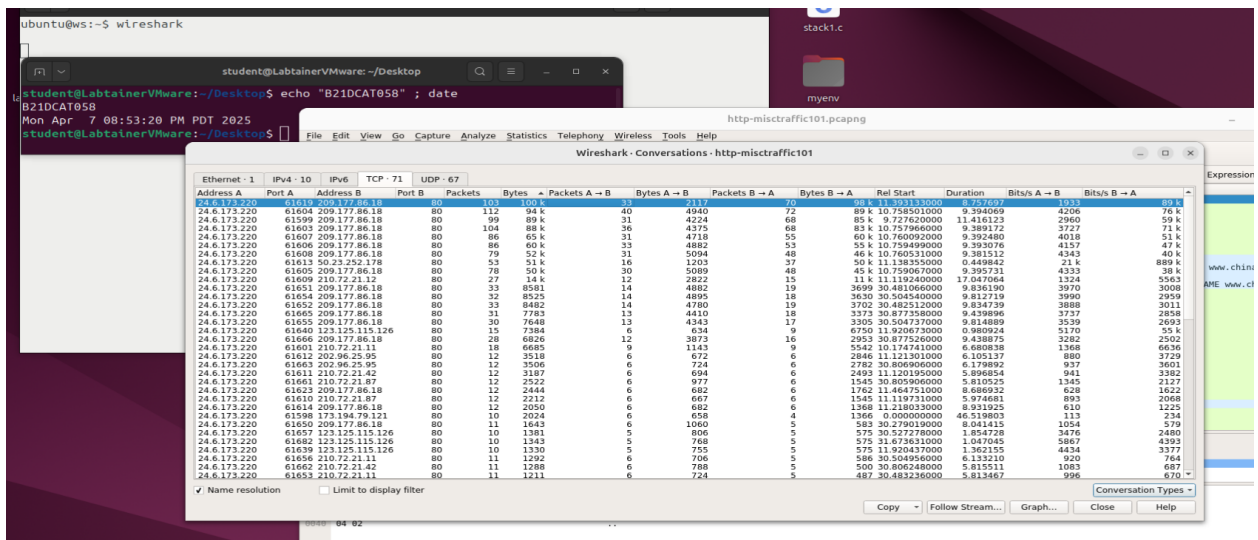
- Chọn Statistics — Conversations. Nhấp vào tab Ethernet. Lưu ý rằng chỉ có một cặp máy chủ giao tiếp trên mạng cục bộ. Tích chọn vào ô Name resolution. Địa chỉ MAC được liệt kê với Cadant là bộ định tuyến cục bộ, Flextron là máy khách mà từ đó lưu lượng truy cập được ghi lại.



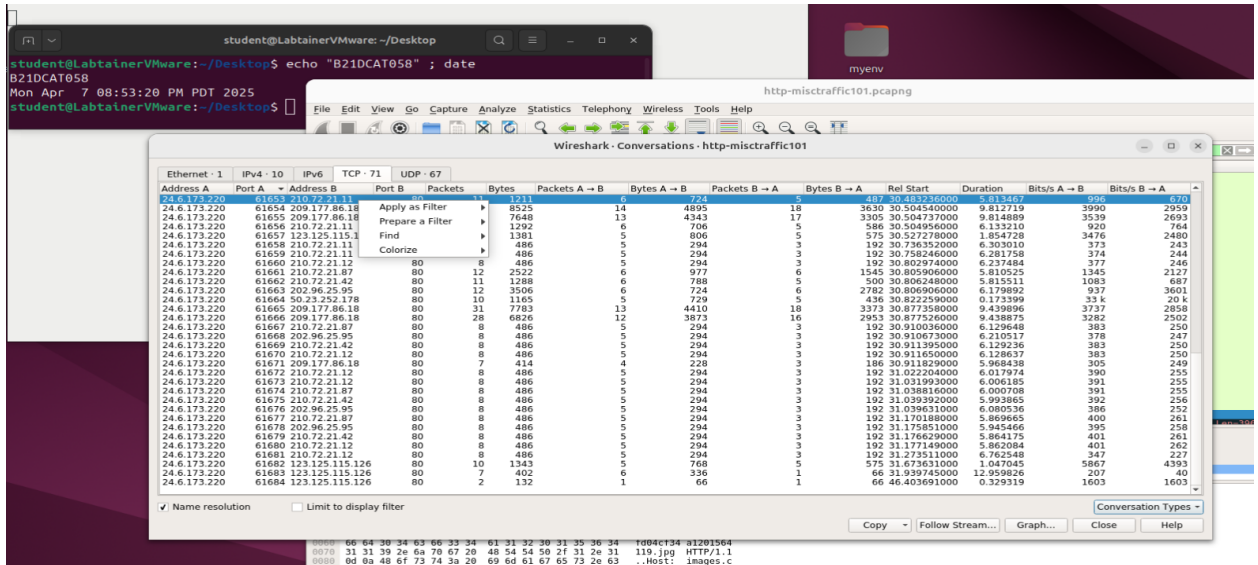
- Nhấp vào tab IPv4 để kiểm tra các cuộc hội thoại IPv4 trong tệp theo dõi này. **Dựa trên số byte, địa chỉ IP nào tham gia vào cuộc hội thoại IPv4 tích cực nhất?**
- ➔ Đoạn hội thoại đầu tiên được bôi đen ở hình dưới là tích cực nhất



- Nhấp vào tab TCP để xác định cuộc hội thoại TCP tích cực nhất. Sắp xếp theo byte bằng cách nhấp vào cột Byte.
- ➔ Đoạn hội thoại đầu tiên được bôi đen ở hình dưới là tích cực nhất



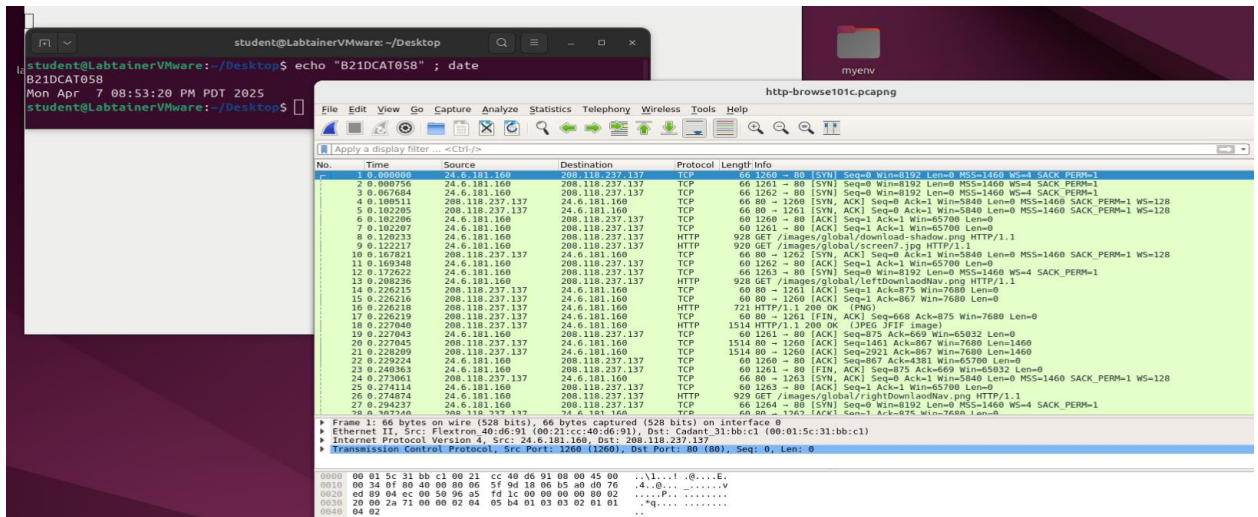
- Nhấp chuột phải vào cuộc hội thoại TCP tích cực nhất và chọn Apply as a Filter — Selected — A<-->B. Wireshark tự động tạo và áp dụng bộ lọc hiển thị cho cuộc hội thoại TCP này. **Có bao nhiêu gói phù hợp với bộ lọc này?**
- ➔ Có 73 gói phù hợp với bộ lọc



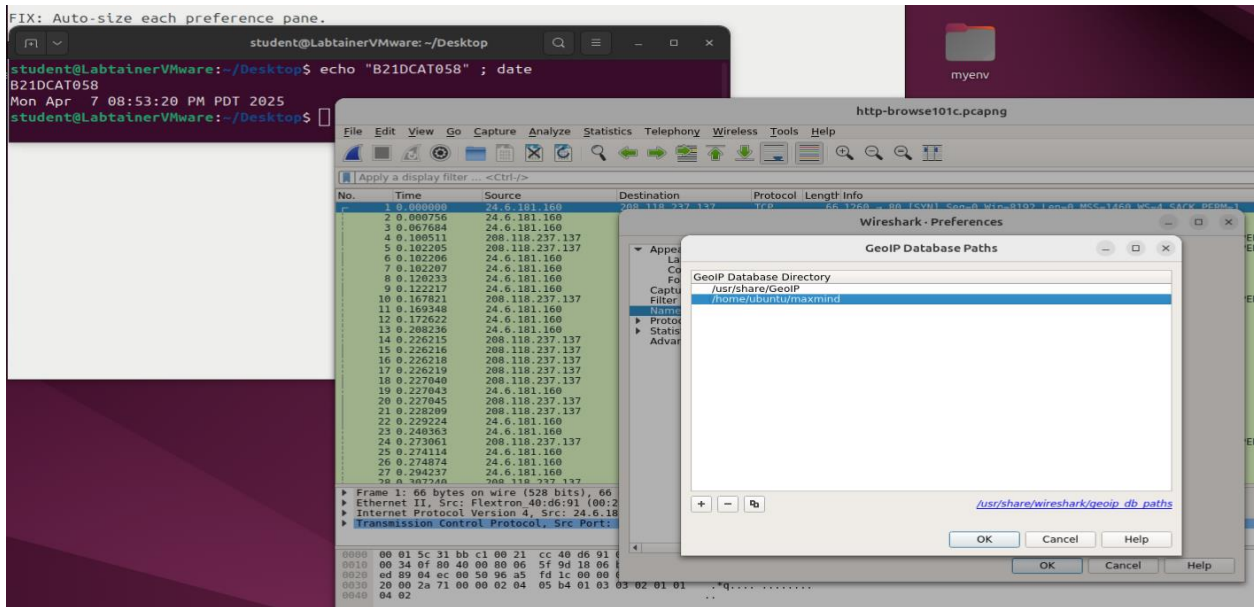
3.2. Định vị địa lý địa chỉ IP

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.

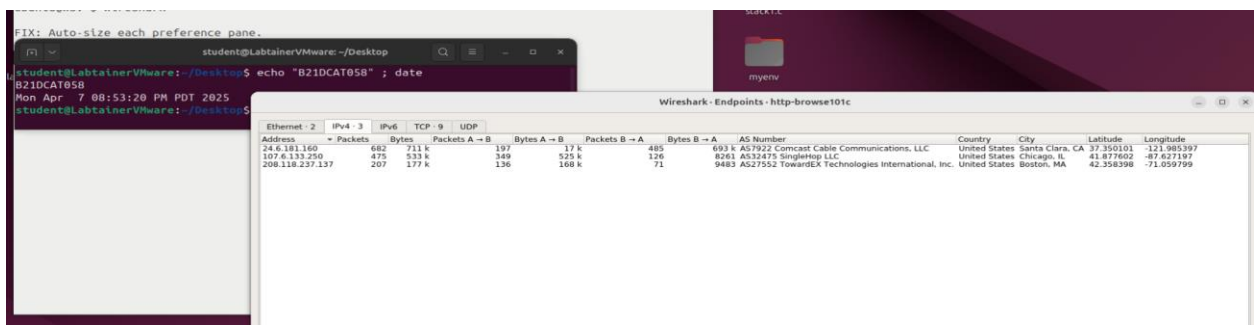
- Mở file pcaps/http-browse101c.pcapng trong Wireshark.



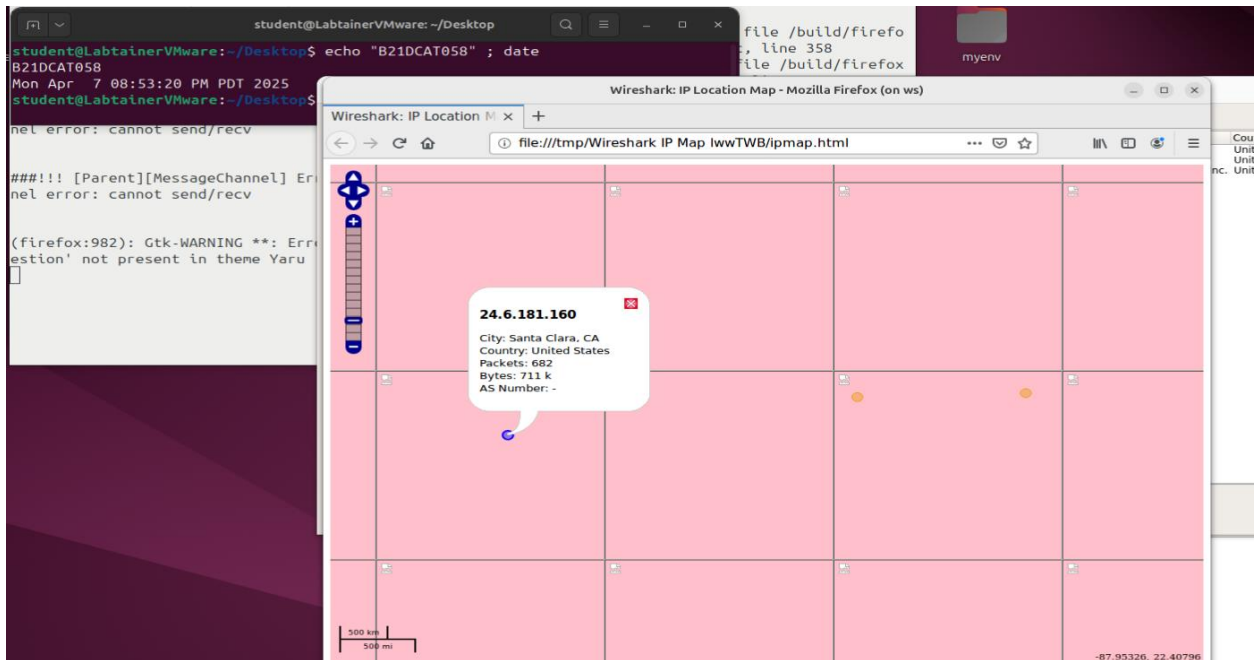
- Chọn Edit — Preferences — Name Resolution, nhấp vào Edit trong thư mục cơ sở dữ liệu GeoIP. Nhấp vào New và trở đến thư mục maxmind (có các tệp cơ sở dữ liệu được tải xuống từ <http://dev.maxmind.com/geoip/legacy/geolite/>). Tiếp tục nhấp vào OK cho đến khi bạn đóng cửa sổ đường dẫn cơ sở dữ liệu GeoIP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

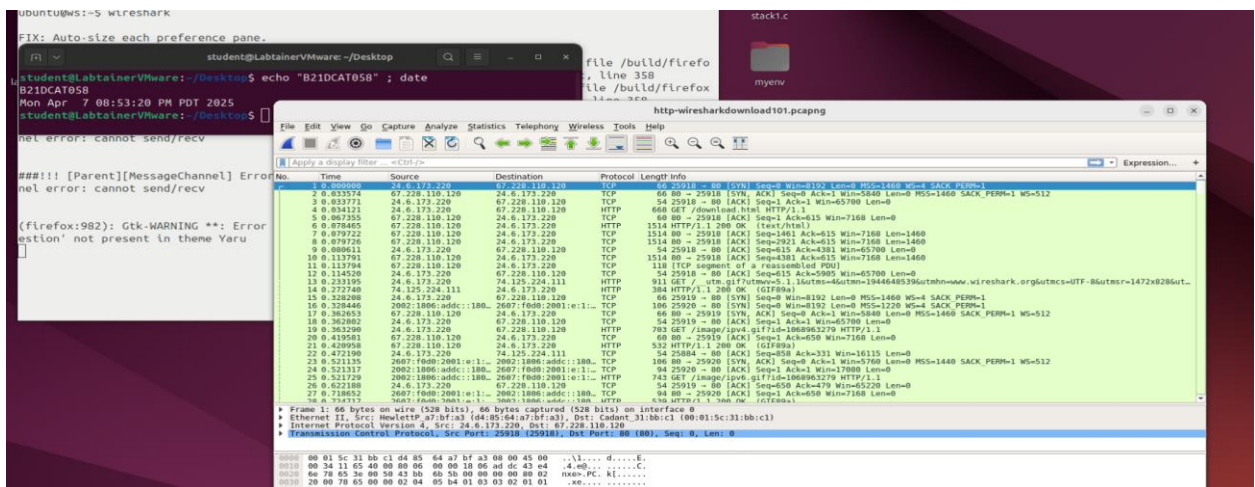


- Tổng lưu lượng truy cập đến/từ Santa Clara, CA là bao nhiêu?
- Tổng lưu lượng truy cập đến/từ Santa Clara, CA là: 711k bytes

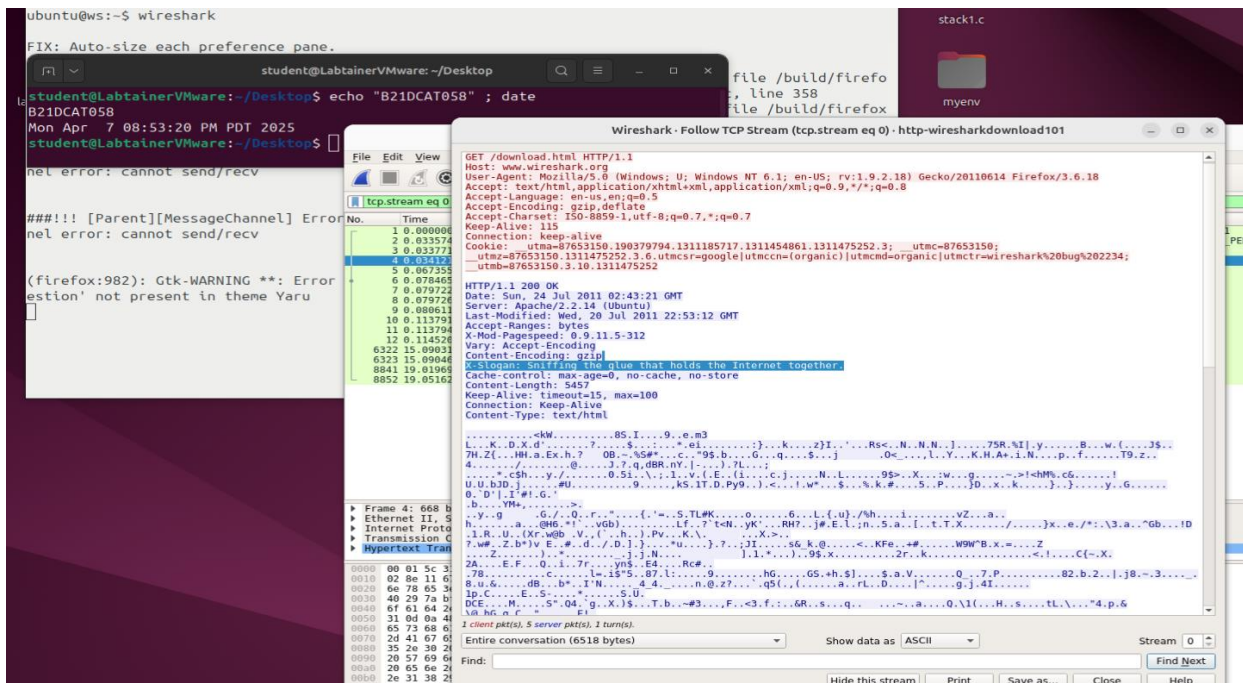
3.3. Tập hợp lại văn bản từ luồng TCP

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.



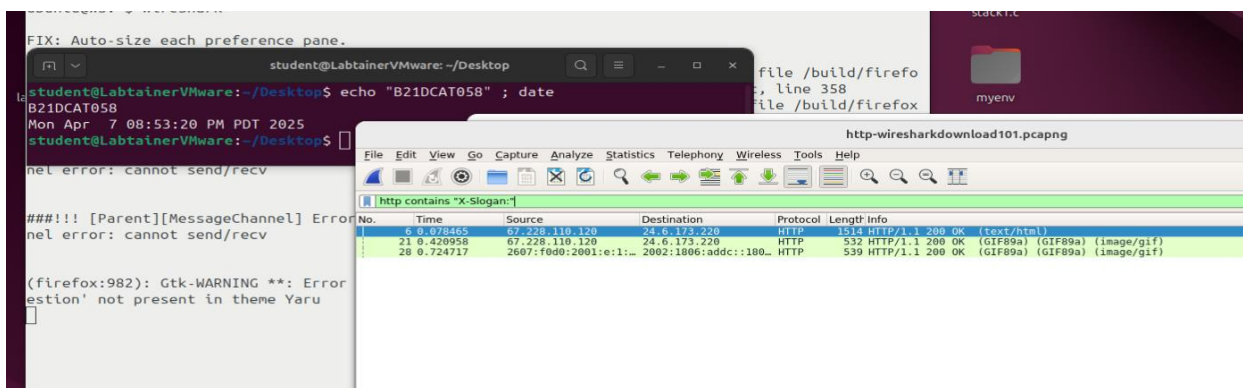
phải vào khung 4 và chọn Follow — TCP Stream. Lưu lượng truy cập đầu tiên được nhìn thấy trong tệp là từ máy khách, có màu đỏ. Lưu lượng truy cập thứ hai là từ máy chủ, có màu xanh lam.



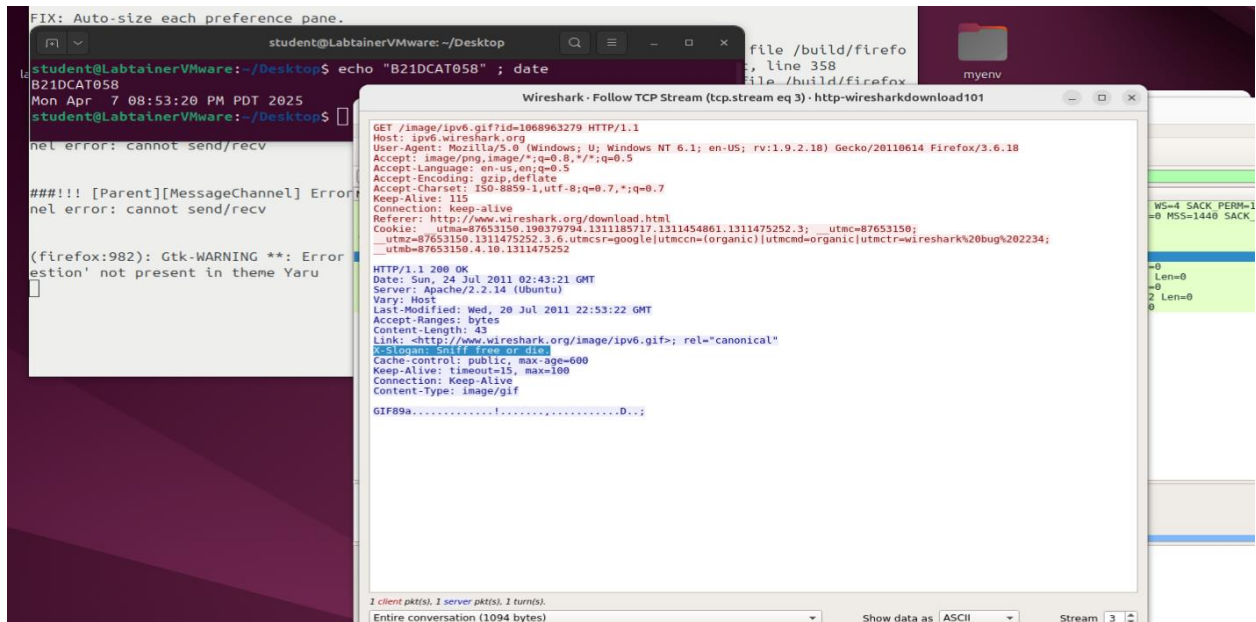
- Wireshark hiển thị cuộc hội thoại không có tiêu đề Ethernet, IP hoặc TCP. Cuộn qua luồng để tìm thông báo ẩn từ Gerald Combs, người tạo ra Wireshark. Nó nằm trong luồng máy chủ và bắt đầu bằng X-Slogan. **Thông điệp là gì?**

➔ **X-Slogan: Sniffing the glue that holds the Internet together**

- Đây không phải là tin nhắn duy nhất bị ẩn trong phiên duyệt web. Bây giờ bạn đã biết thông báo bắt đầu bằng X-Slogan, bạn có thể yêu cầu Wireshark hiển thị mọi khung bao gồm chuỗi ASCII này.
- Hãy dùng lệnh lọc frame có chứa “X-Slogan”.



- Nhấp chuột phải vào hai khung được hiển thị khác và chọn Follow — TCP Stream để kiểm tra các tiêu đề HTTP được trao đổi giữa các máy chủ.

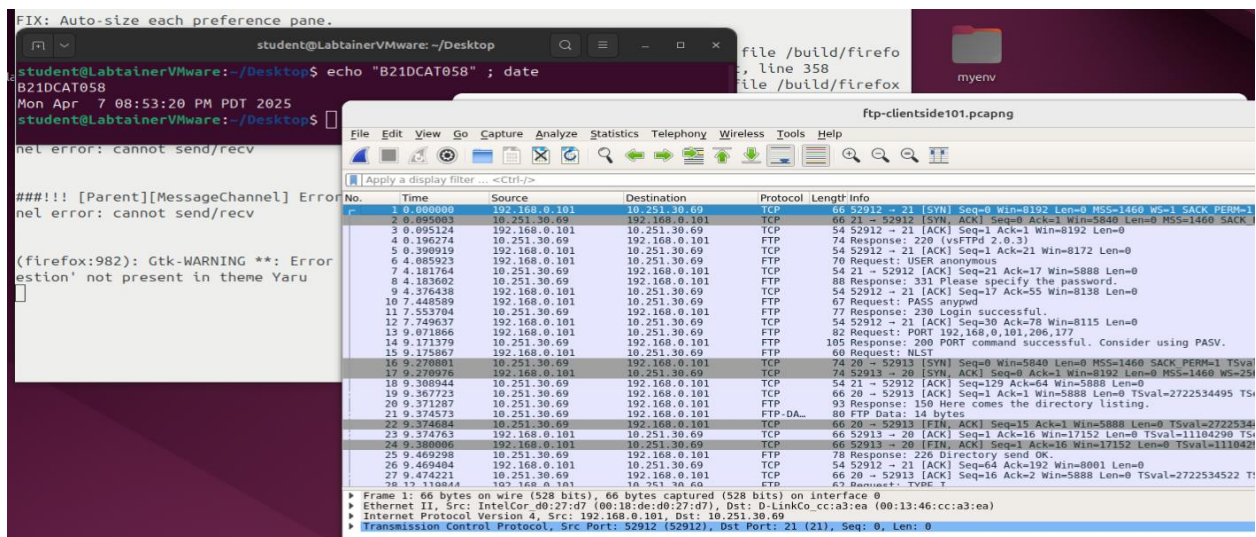


- thông điệp khác : X-Slogan: Sniff free or die.

3.4. Giải nén tệp nhị phân từ phiên FTP

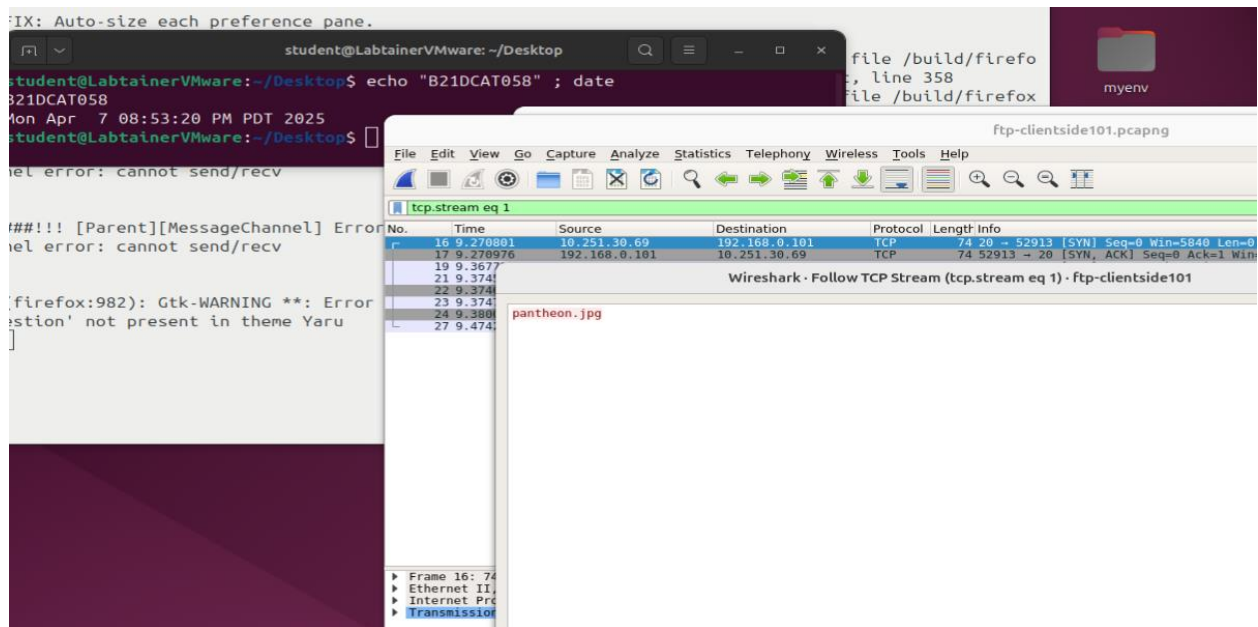
Trong phần trước, chúng ta đã trích xuất các tin nhắn văn bản ASCII từ các gói. Còn dữ liệu nhị phân thì sao? Wireshark cũng có các công cụ cho việc này.

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

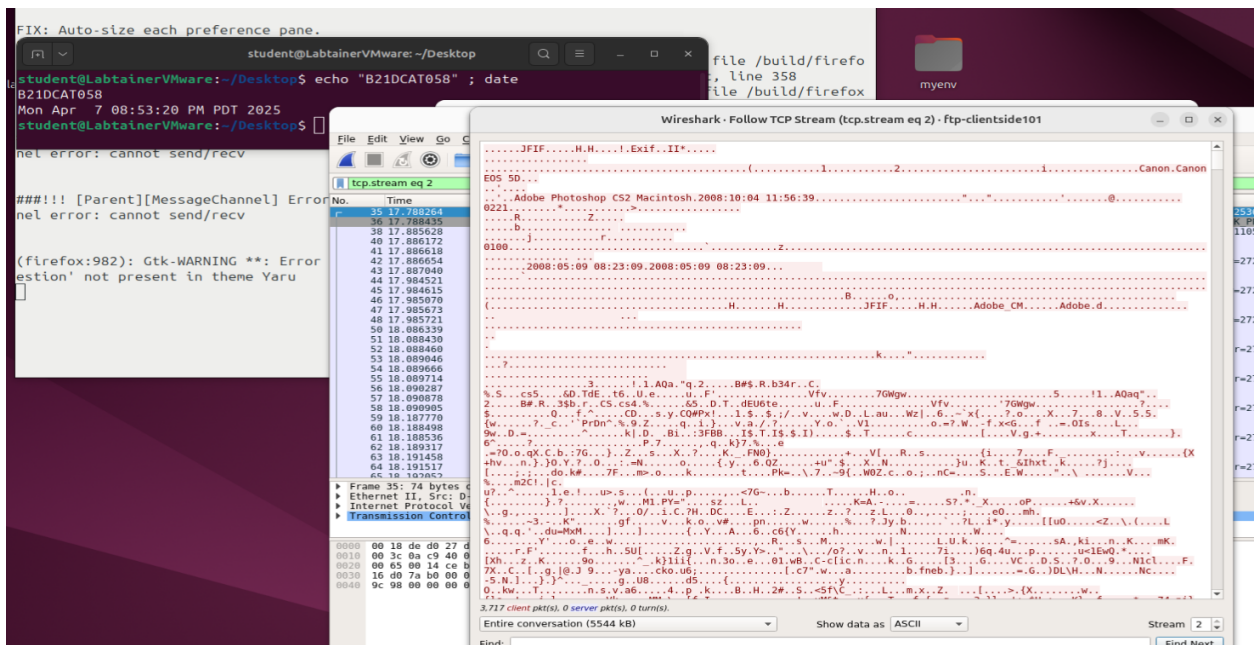


- Phần đầu của file pcap này bạn sẽ thấy nhiều lệnh FTP được sử dụng để đăng nhập, yêu cầu một thư mục, xác định số cổng để truyền dữ liệu và truy xuất tệp.

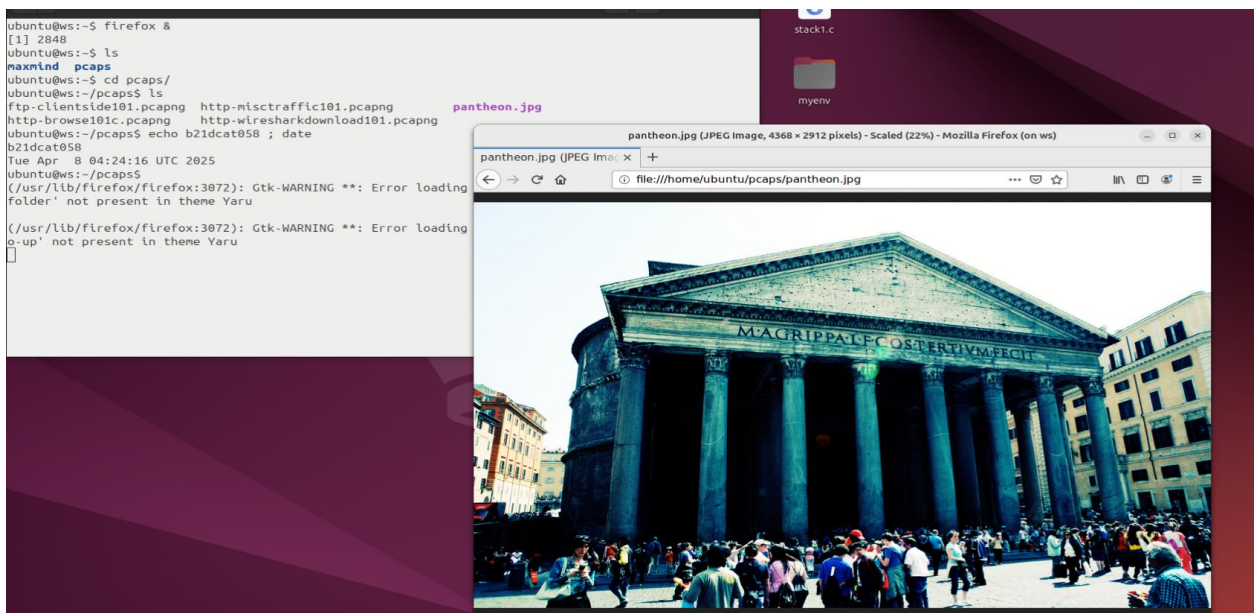
- Chúng ta chỉ quan tâm đến hai luồng dữ liệu: một luồng danh sách thư mục và một luồng truyền tệp. Trong cửa sổ Follow TCP Stream, nhấp vào nút Hide This Stream. Thao tác này sẽ đóng cửa sổ luồng TCP và áp dụng bộ lọc loại trừ.
- Các khung từ 16 đến 18 và các khung từ 35 đến 38 là các gói bắt tay TCP 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.



- **Tên của tệp đó là gì? : pantheon.jpg**
- 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.



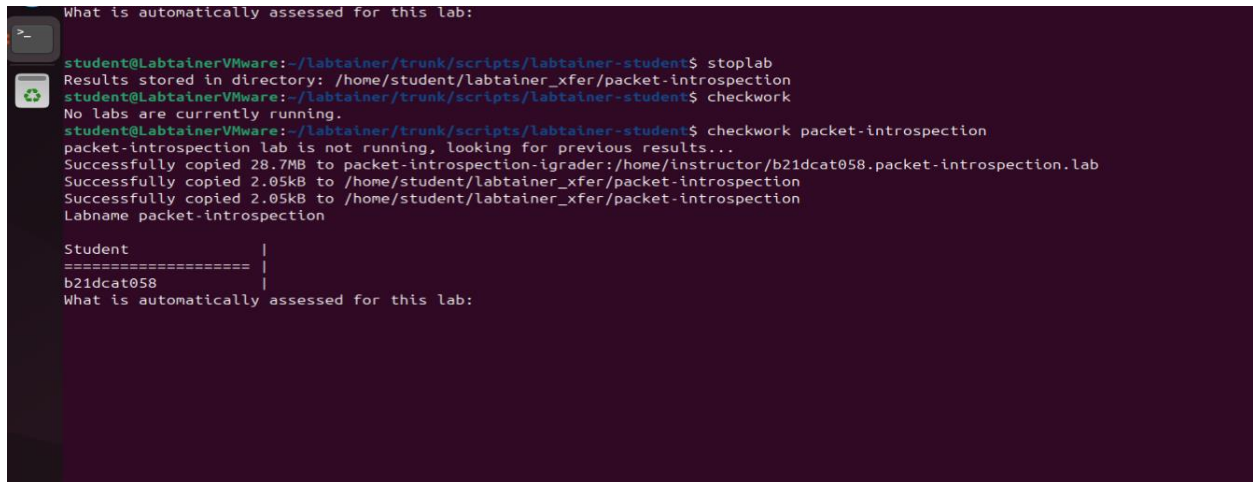
3.5. Kết thúc bài lab:

- Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:

stoplab packet-introspection

- Khi bài lab kết thúc, một tệp lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab. 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

A terminal window with a dark purple background. The prompt is 'student@LabtainerVMware:~/labtainer/trunk/scripts/labtainer-student\$'. The user enters 'stoplab', and the output shows results stored in a directory. Then the user enters 'checkwork', and the output shows no labs are running. Finally, the user enters 'checkwork packet-introspection', and the output shows the lab is not running and previous results are being looked for. It then shows successful copying of files to a directory. The terminal ends with a table header for 'Student' and a row for 'b21dcat058'.

```
What is automatically assessed for this lab:

student@LabtainerVMware:~/labtainer/trunk/scripts/labtainer-student$ stoplab
Results stored in directory: /home/student/labtainer_xfer/packet-introspection
student@LabtainerVMware:~/labtainer/trunk/scripts/labtainer-student$ checkwork
No labs are currently running.
student@LabtainerVMware:~/labtainer/trunk/scripts/labtainer-student$ checkwork packet-introspection
packet-introspection lab is not running, looking for previous results...
Successfully copied 28.7MB to packet-introspection-igrader:/home/instructor/b21dcat058.packet-introspection.lab
Successfully copied 2.05kB to /home/student/labtainer_xfer/packet-introspection
Successfully copied 2.05kB to /home/student/labtainer_xfer/packet-introspection
Labname packet-introspection

Student      |
=====      |
b21dcat058   |
What is automatically assessed for this lab:
```