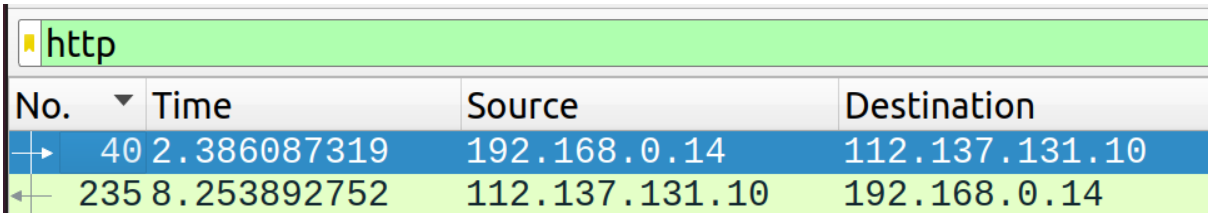
Bài thực hành Lab 1 - IT005.M11.KHTN.1

Huỳnh Hoàng Vũ - MSSV: 20520864

1. Tổng thời gian bắt gói tin trong từng trang web đã thử nghiệm và tổng số gói tin bắt được là bao nhiêu?

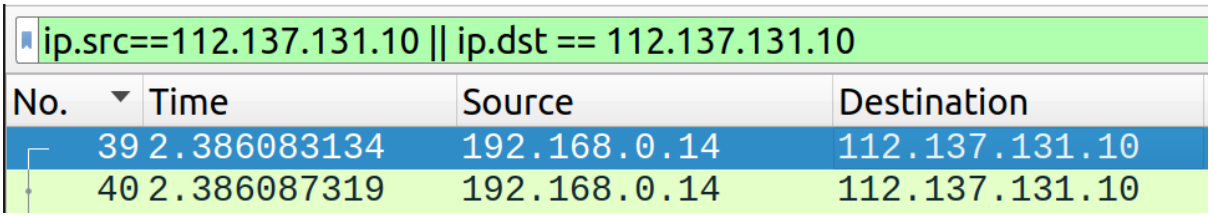
a. http://doit.uet.vnu.edu.vn/

Gõ http vào packet-display filter, quan sát địa chỉ đích của gói tin đầu tiền. Đó chính là IP của trang web.

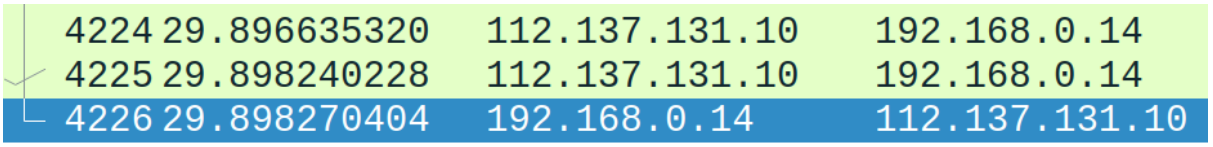


Gõ ip.src==112.137.131.10 || ip.dst == 112.137.131.10 vào packet-display filter.

Quan sát thời điểm bắt gói tin đầu tiên và gói tin cuối cùng.



Thời điểm bắt gói tin đầu tiên = 2.386083134 s

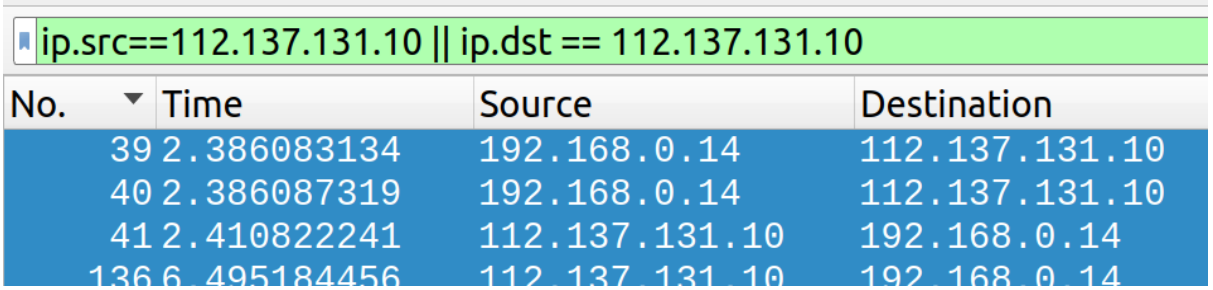


Thời điểm bắt gói tin cuối cùng = 29.898270404 s
Vậy tổng thời gian bắt gói tin trong trang web

= 29.898270404 - 2.386083134 = 27.51218727 s.

Vẫn filter với ip.src==112.137.131.10 || ip.dst == 112.137.131.10.

Chọn một gói tin bất kỳ, sau đó chọn tất cả gói tin với tổ hợp phím Ctrl + A.

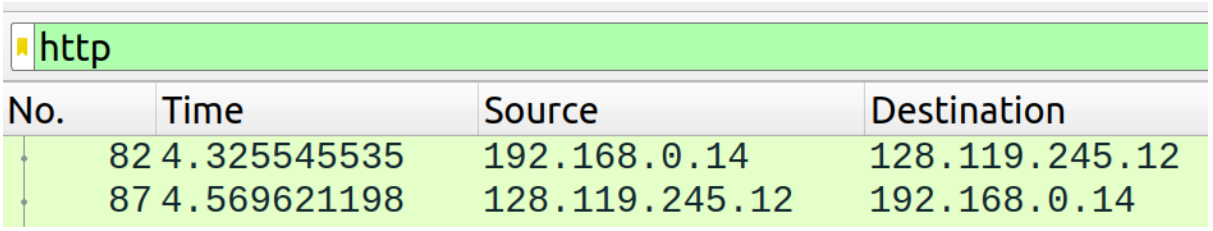


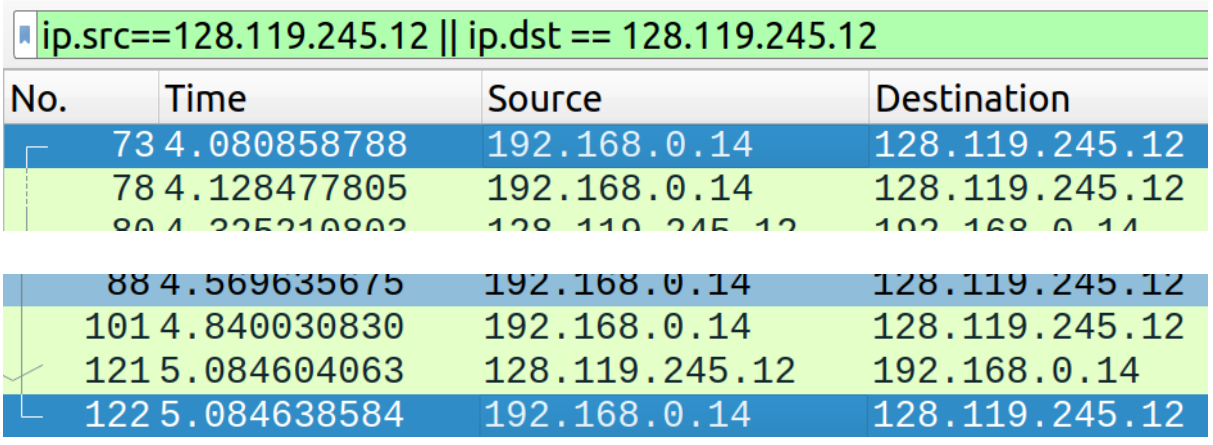
Quan sát Selected (Số gói tin được chọn) ở góc phải dưới phần mềm.

Vậy ta biết được tổng số gói tin bắt được = 3097 gói.

b. http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

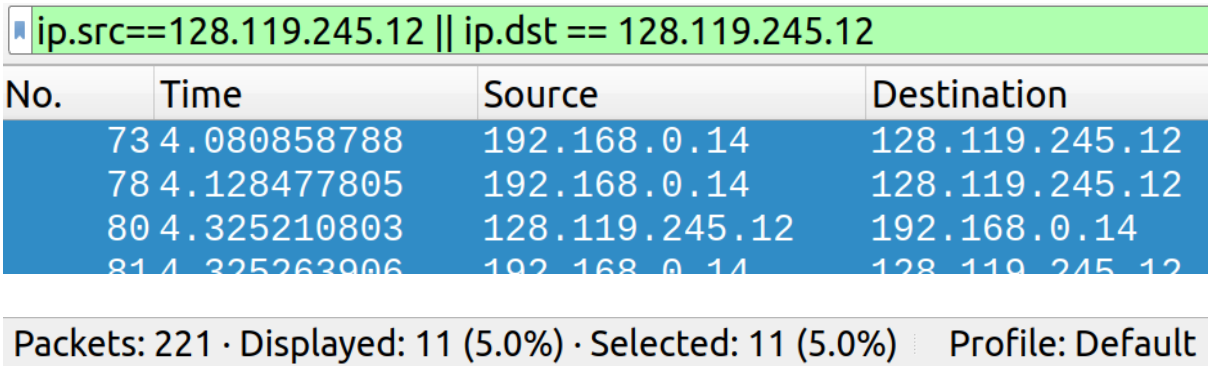
Thực hiện tương tự, ta được.





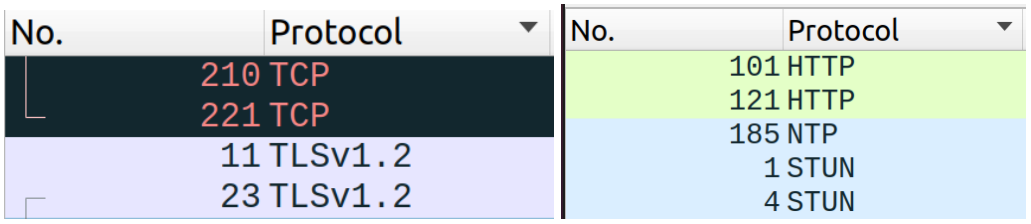
Tổng thời gian bắt gói tin trong trang web

= 5.084638584 - 4.080858788 = 1.003779796 s.



Tổng số gói tin bắt được = 11 gói.

2. Liệt kê ít nhất 5 giao thức khác nhau xuất hiện trong cột giao thức (Protocol) khi không áp dụng bộ lọc "http" khi truy cập 2 website. Tìm hiểu trên Internet và mô tả ngắn gọn chức năng chính của các giao thức đó.



(Ở file 20520864_Bai1.pcapng)

- Giao thức HTTP:

HTTP là nền tảng của truyền thông dữ liệu cho World Wide Web , nơi siêu văn bản tài liệu bao gồm các siêu liên kết đến các tài nguyên khác mà người dùng có thể dễ dàng truy cập.

- Giao thức TCP:

TCP cung cấp vận chuyển đáng tin cậy, có thứ tự và được kiểm tra lỗi của dòng các byte thông tin giữa các ứng dụng chạy trên các host giao tiếp qua mạng IP.

- Giao thức NTP:

NTP giúp đồng bộ đồng hồ của các hệ thống máy tính thông qua mạng dữ liệu chuyển mạch gói với độ trễ biến đổi.

- Giao thức STUN:

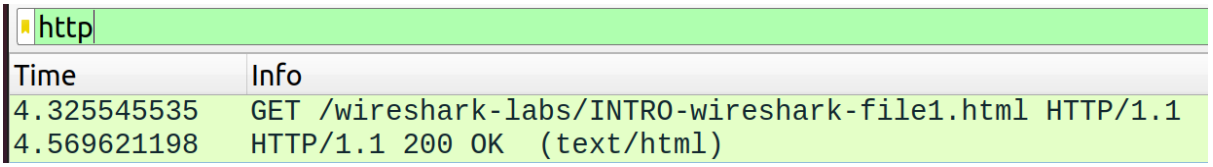
STUN là tập hợp các phương pháp được tiêu chuẩn hóa, cũng là một giao thức mạng dùng để truyền qua các cổng phiên dịch địa chỉ mạng (NAT)

trong các ứng dụng thoại, video, nhắn tin thời gian thực và các giao tiếp tương tác thời gian thực khác.

- Giao thức TLS1.2:

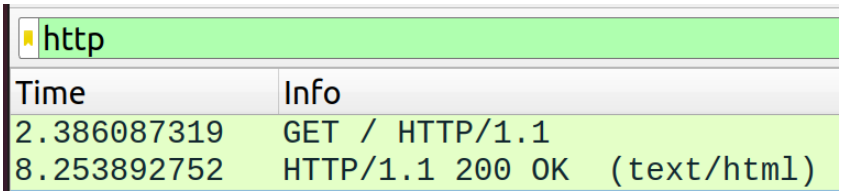
TLS là một giao thức mật mã được thiết kế để cung cấp bảo mật thông tin liên lạc qua mạng máy tính ở lớp Transport.

3. Mất bao lâu từ khi gói tin HTTP GET đầu tiên được gửi cho đến khi HTTP 200 OK đầu tiên được nhận đối với mỗi website đã thử nghiệm. (mặc định, giá trị của cột thời gian (Time) trong packet-listing window là khoảng thời gian tính bằng giây kể từ khi chương trình Wireshark bắt đầu bắt gói tin).



Trang http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

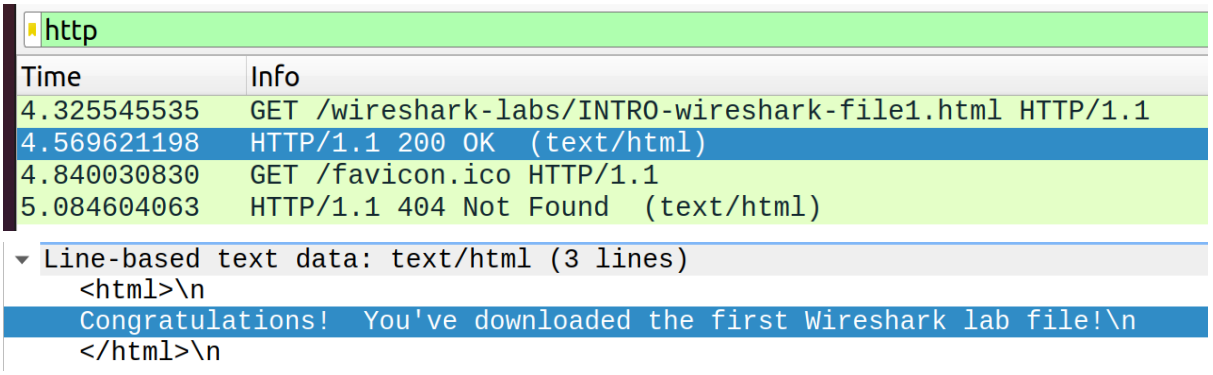
t = 4.569621198 – 4.325545535 = 0.244075663 s



Trang http://doit.uet.vnu.edu.vn/

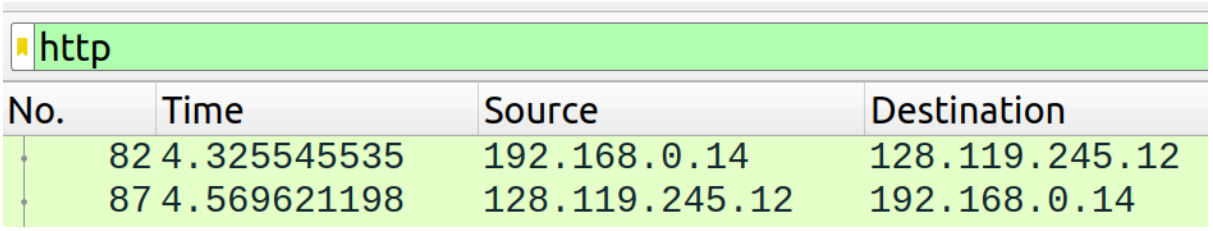
t = 8.253892752 – 2.386087319 = 5.867805433 s

4. Nội dung hiển thị trên trang web gaia.cs.umass.edu "Congratulations! You've downloaded the first Wireshark lab file!" có nằm trong các gói tin HTTP bắt được hay không? Nếu có, hãy tìm và xác định vị trí của nội dung này trong các gói tin bắt được.



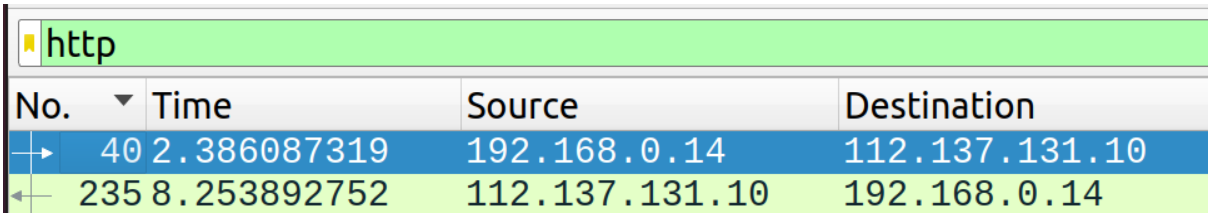
5. Địa chỉ IP của gaia.cs.umass.edu và website đã chọn ở bước 10 là gì? Địa chỉ IP của máy tính đang sử dụng là gì?

Gõ http vào packet-display filter. Quan sát địa chỉ đích của gói tin đầu tiền, đó chính là IP của trang web. Còn địa chỉ nguồn của gói tin đầu tiên là IP của máy tính.



Trang http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

Địa chỉ IP: 128.119.245.12



Trang http://doit.uet.vnu.edu.vn/

Địa chỉ IP: 112.137.131.10

Địa chỉ IP của máy ở cả 2 lần bắt gói tin: 192.168.0.14

6. Qua ví dụ bắt gói tin trên và kết quả bắt gói tin từ Wireshark, hãy mô tả ngắn gọn diễn biến xảy ra khi bắt đầu truy cập vào một đường dẫn đến một trang web cho đến lúc xem được các nội dung trên trang web đó.

- Khi truy cập một trang web, máy tính sẽ gửi một yêu cầu nội dung của trang web đến trang web.

- Sau đó trang web sẽ gửi nội dung về máy tình nếu người truy cập có đủ quyền và nội dung được tìm thấy tại máy chủ.

- Máy tính tiếp tục yêu cầu các nội dung cần thiết như icon trang web, ảnh trong trang web...

- Và tương tự như bước trên cho đến khi tất cả nội dung cần thiết đều đã yêu cầu.