**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**CƠ SỞ TẠI THÀNH PHỐ HỒ CHÍ MINH**



**BÀI TẬP 1:**

***Report về Lab liên quan đến Security Onion***

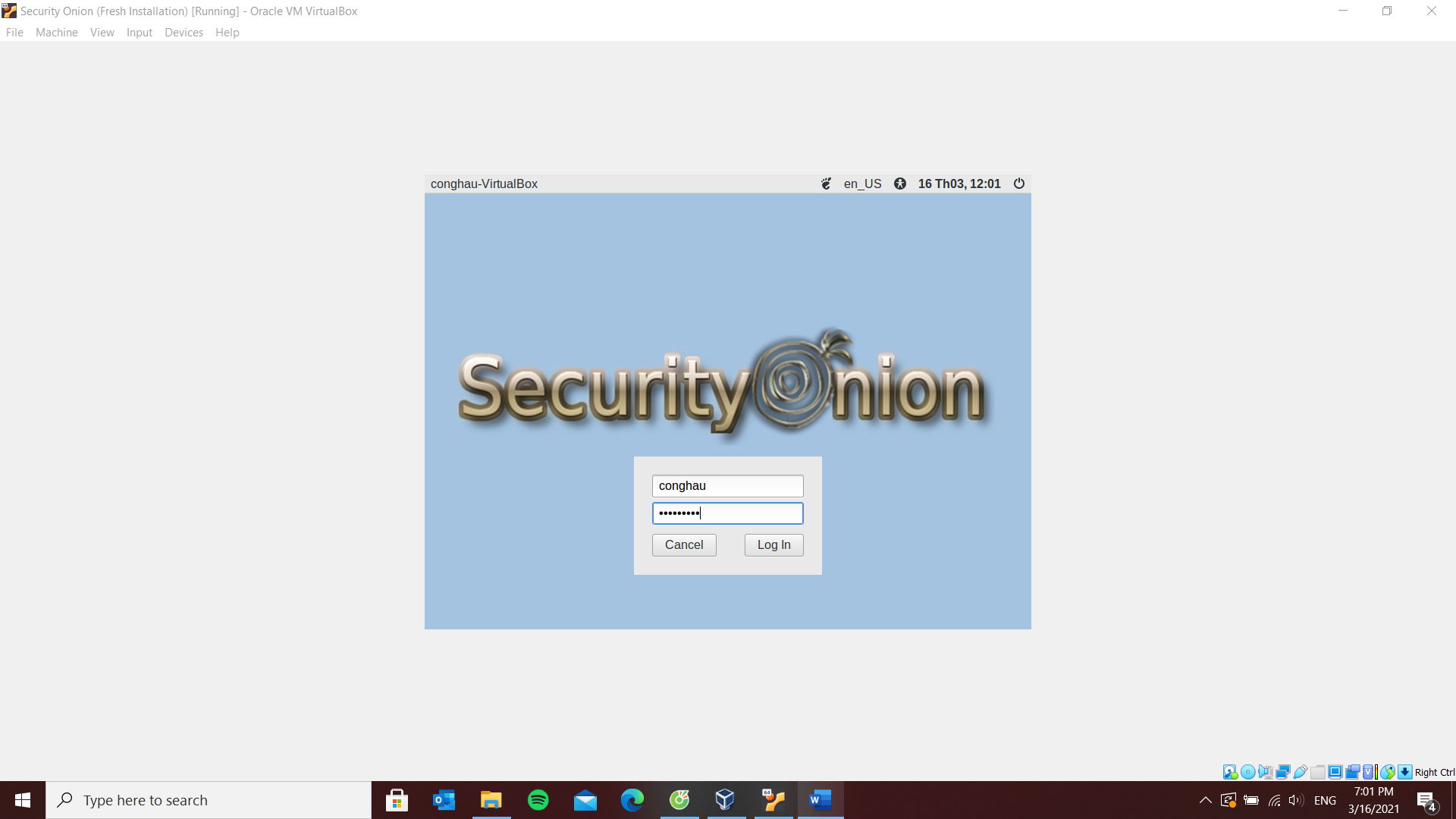
**Môn :** Kỹ Thuật Theo Dõi, Giám Sát An Toàn Mạng

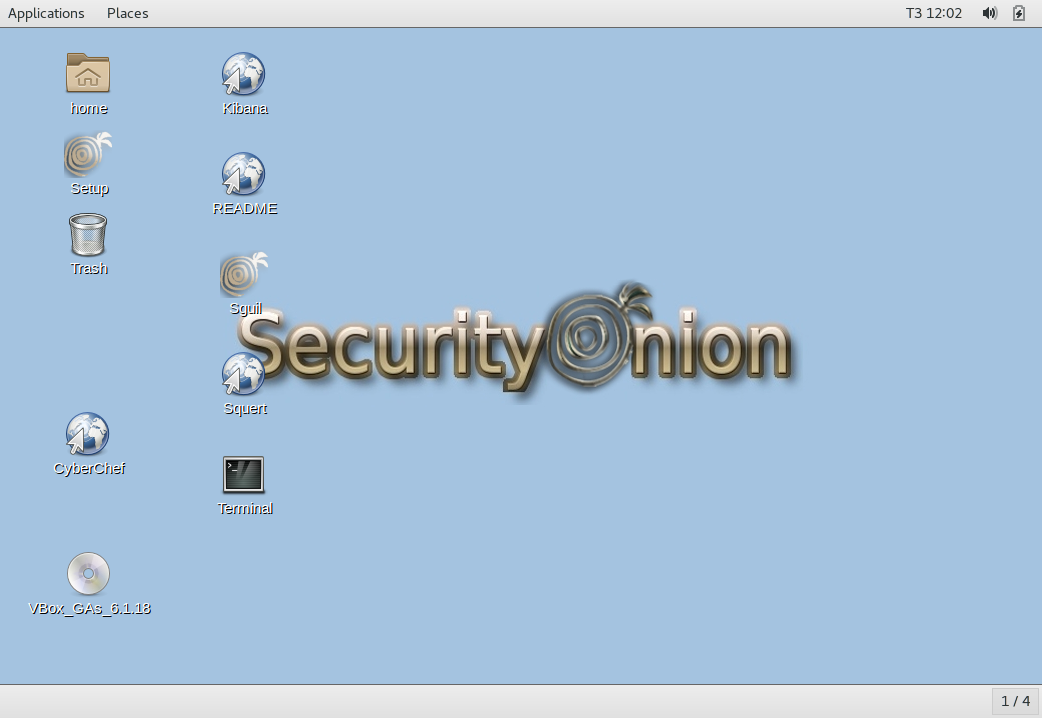
Tên: Chế Công Hậu

MSSV: N17DCAT023

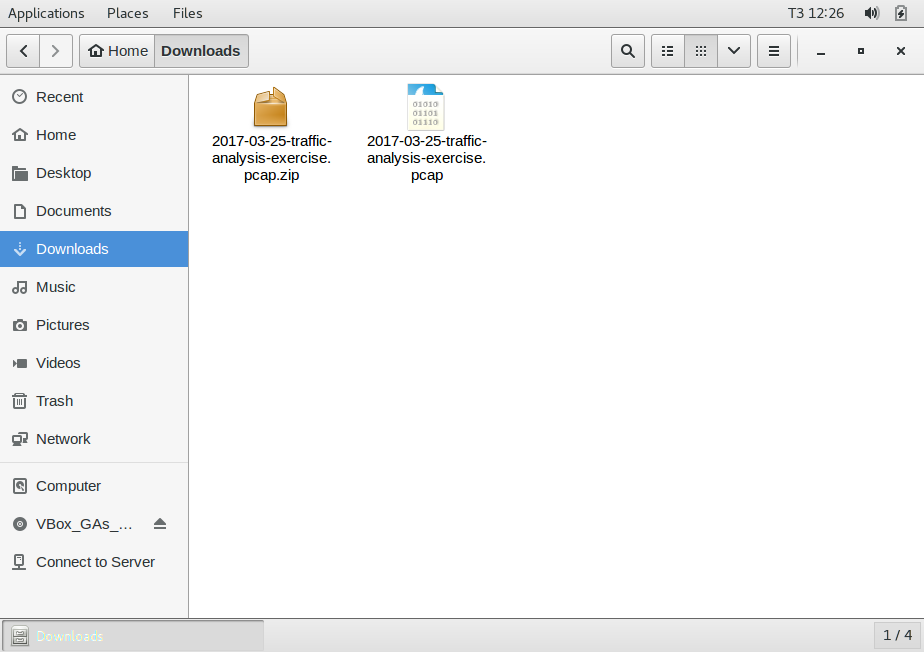
*Ngày 17 tháng 3 năm 2021*

Đã hoàn thành cài đặt Security Onion theo hướng dẫn của Lab 1.

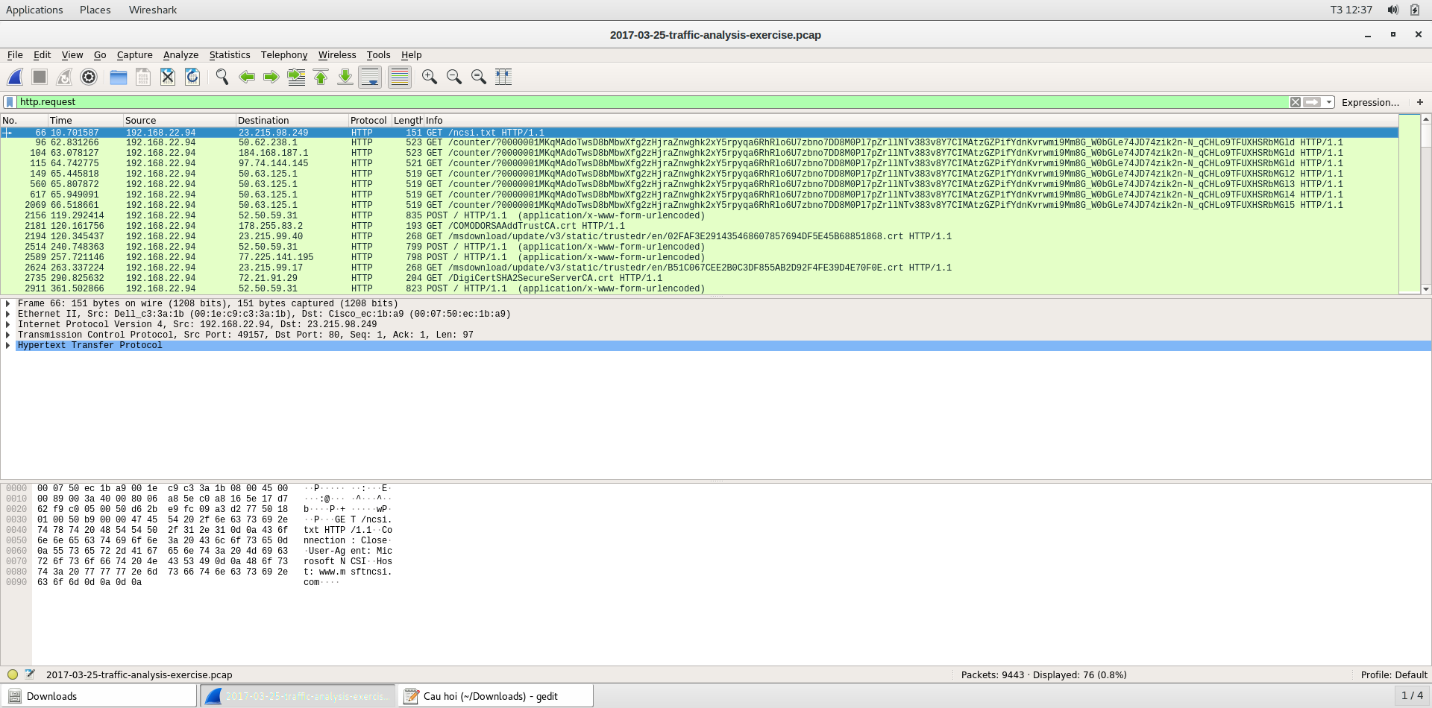




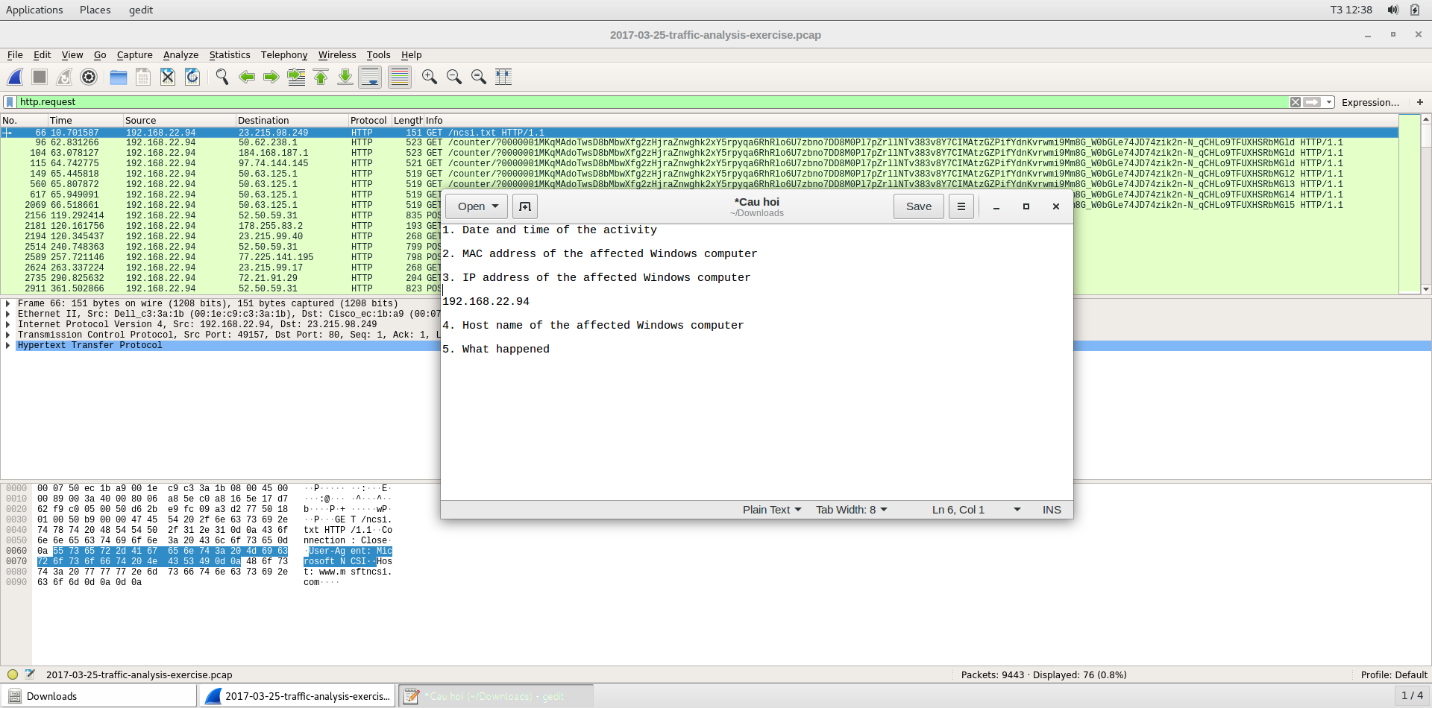
Download file cần phân tích theo hướng dẫn của Lab 2

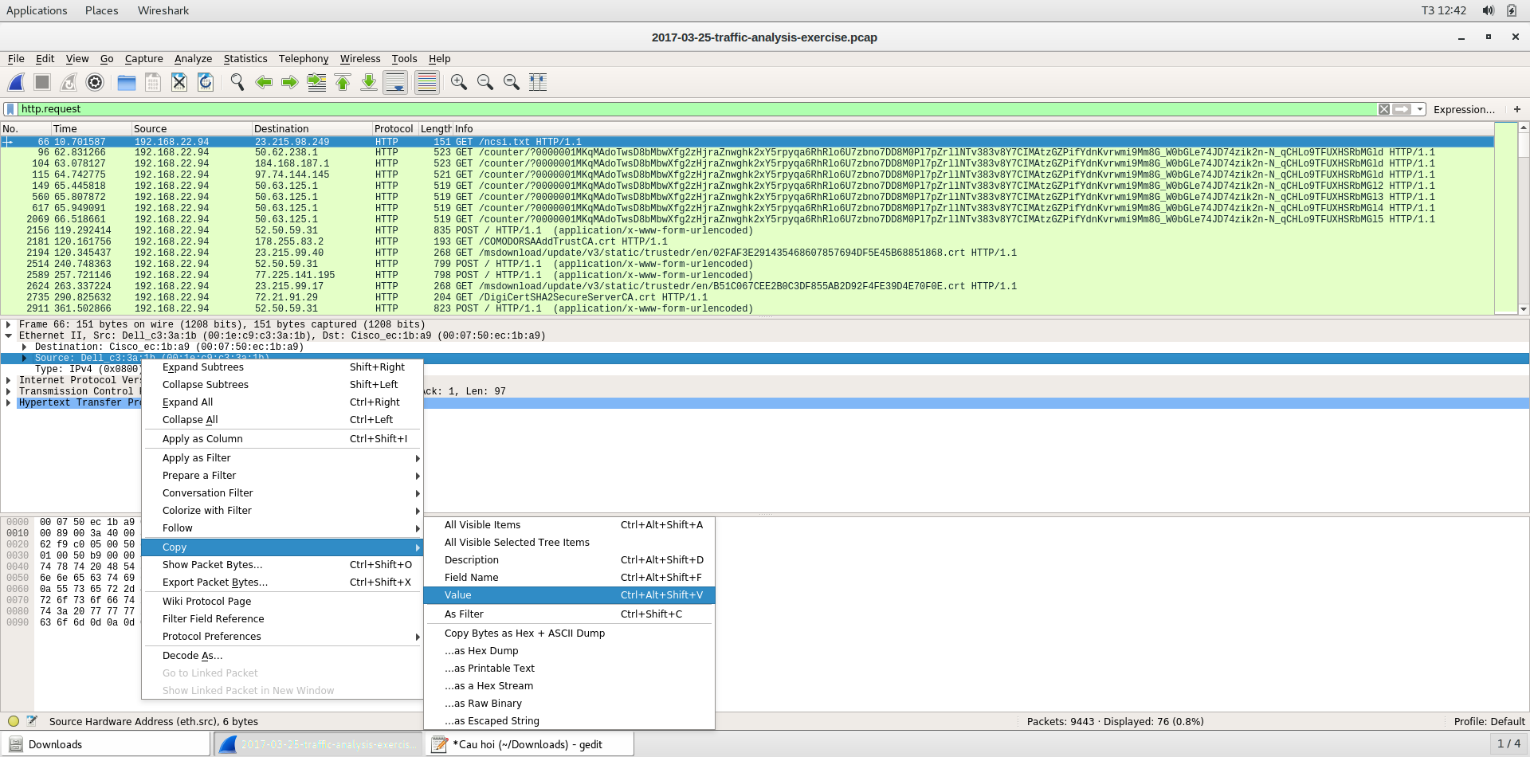


Dùng Wireshark để phân tích. Gõ http.request vào thanh Filter



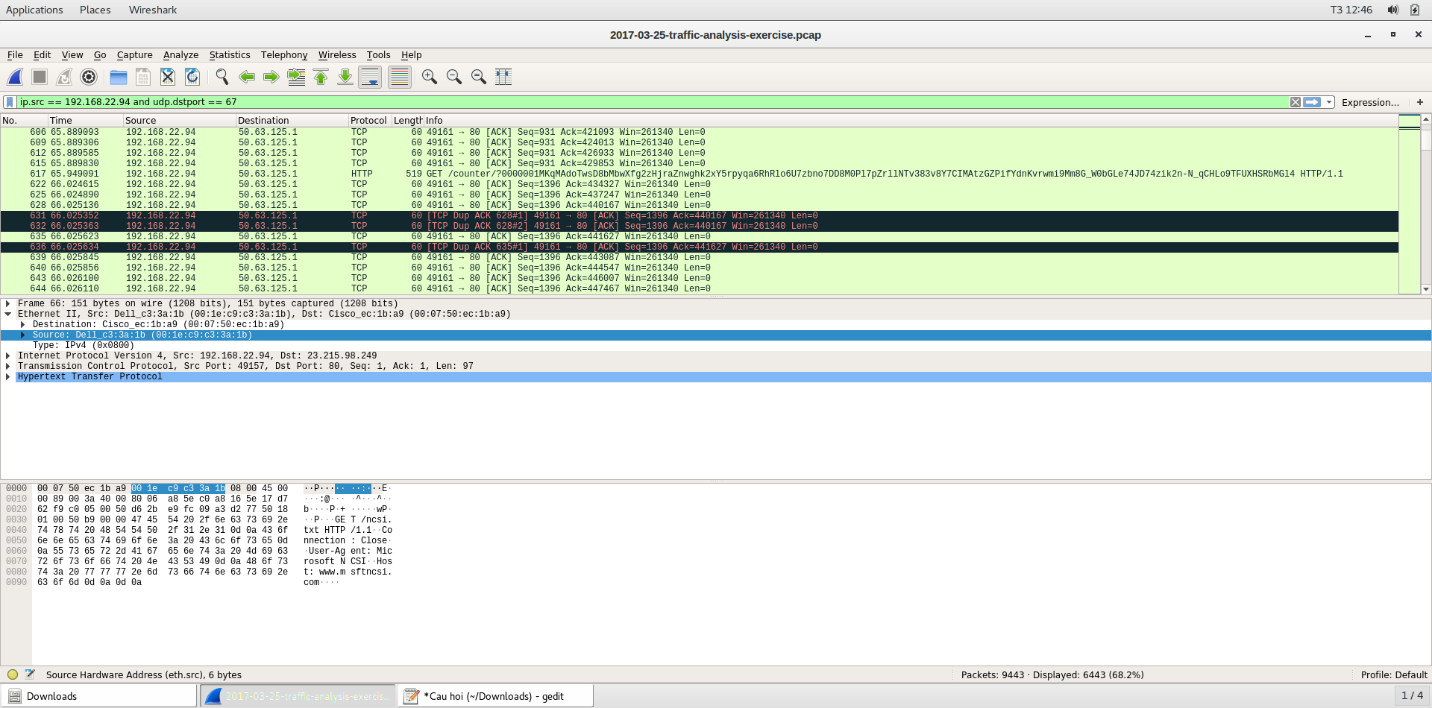
Phân tích và sẽ có câu trả lời cho câu 3 và câu 4.

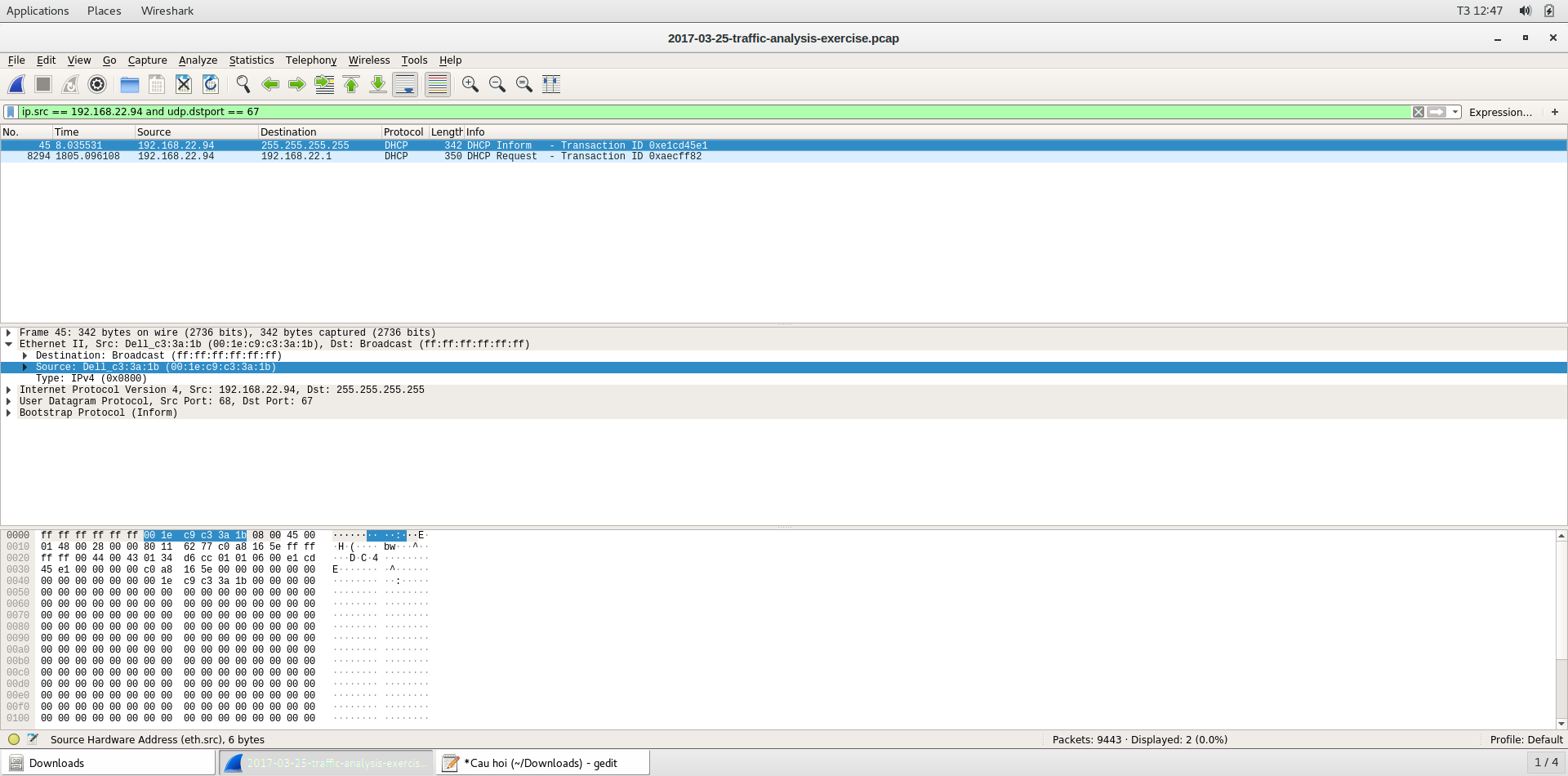




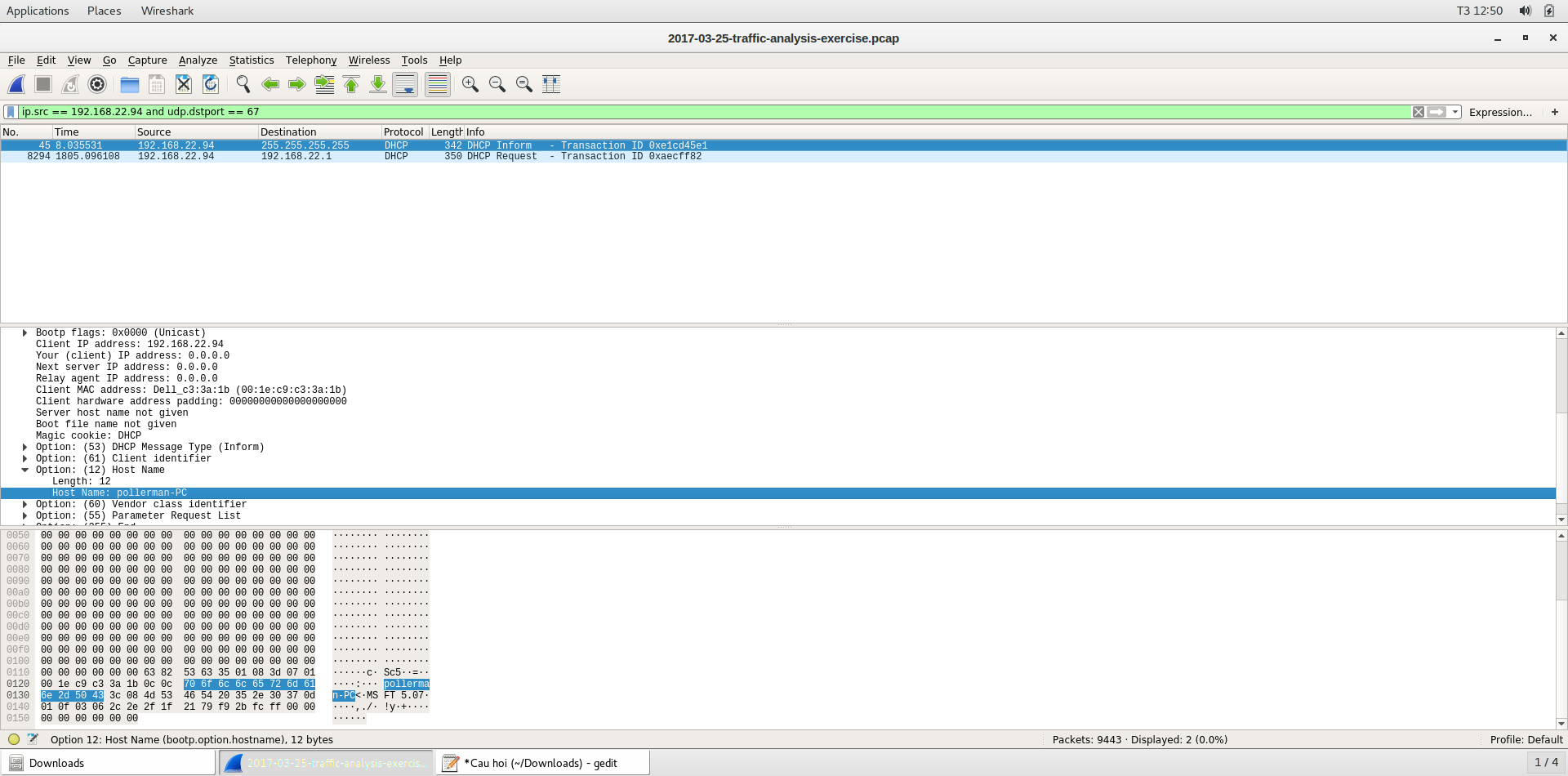


Gõ ip.src == ip nạn nhân (192.168.22.94) and upd.dstport == 67 (67 là port mặc định của phương thức DHCP).

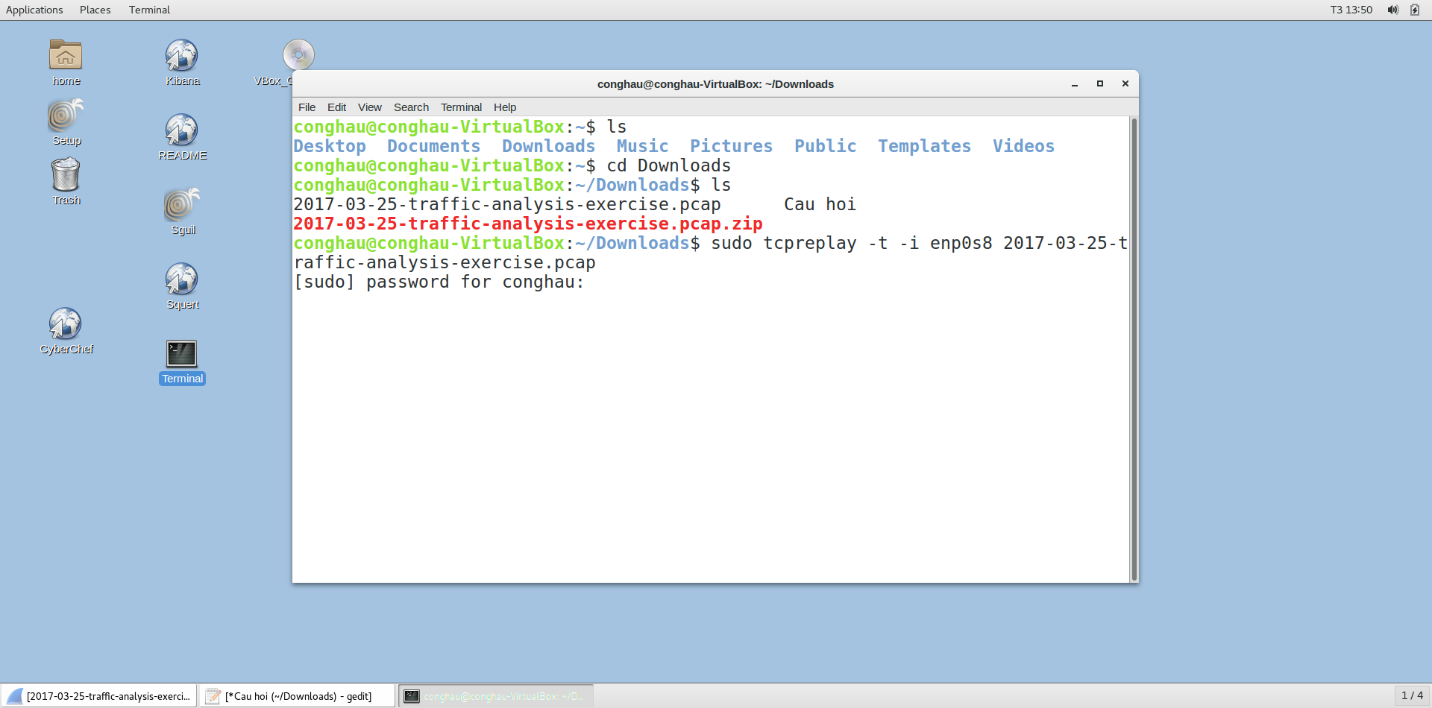


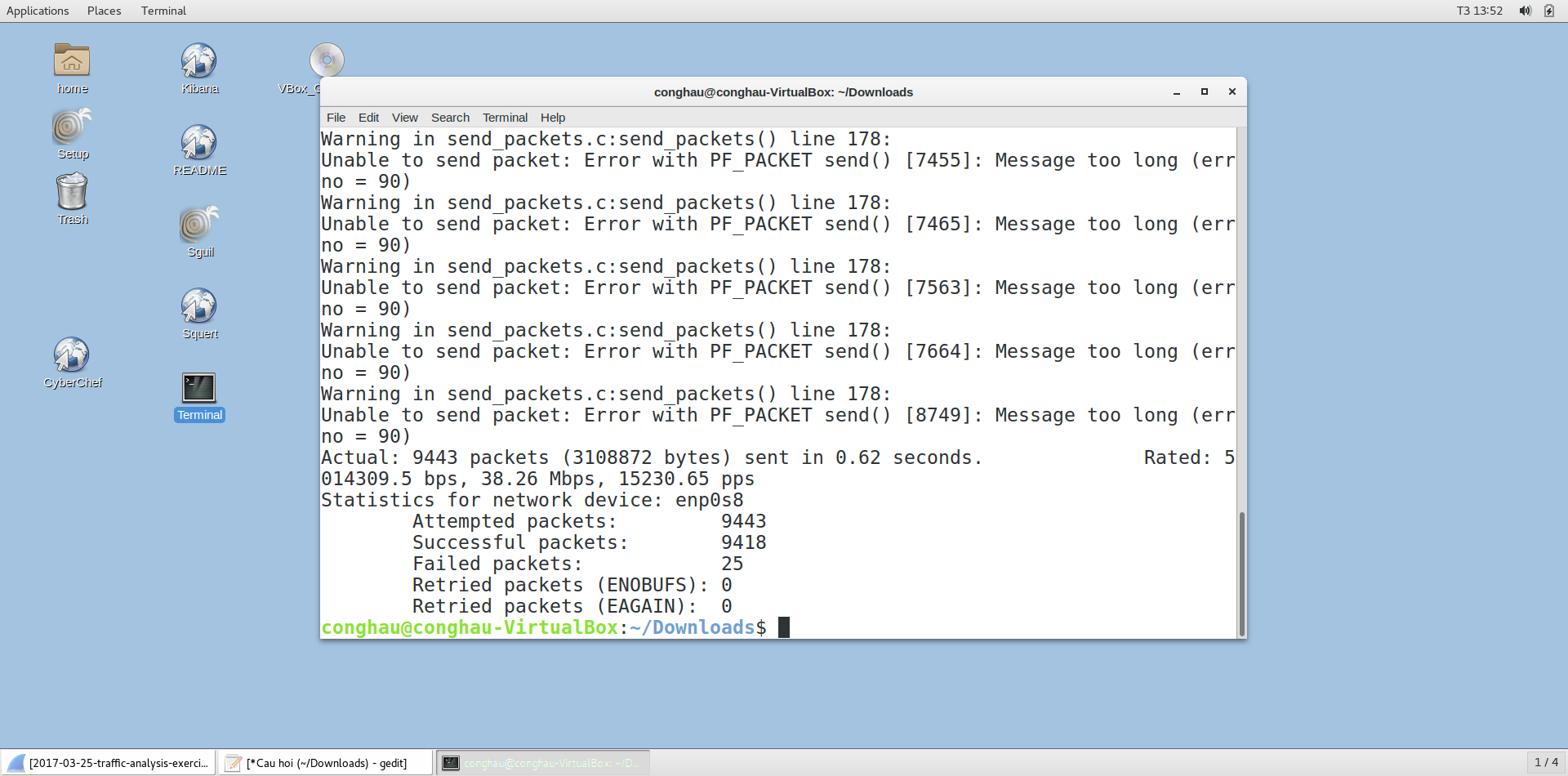


Tìm được Host name cho câu hỏi số 4 (pollerman-PC).

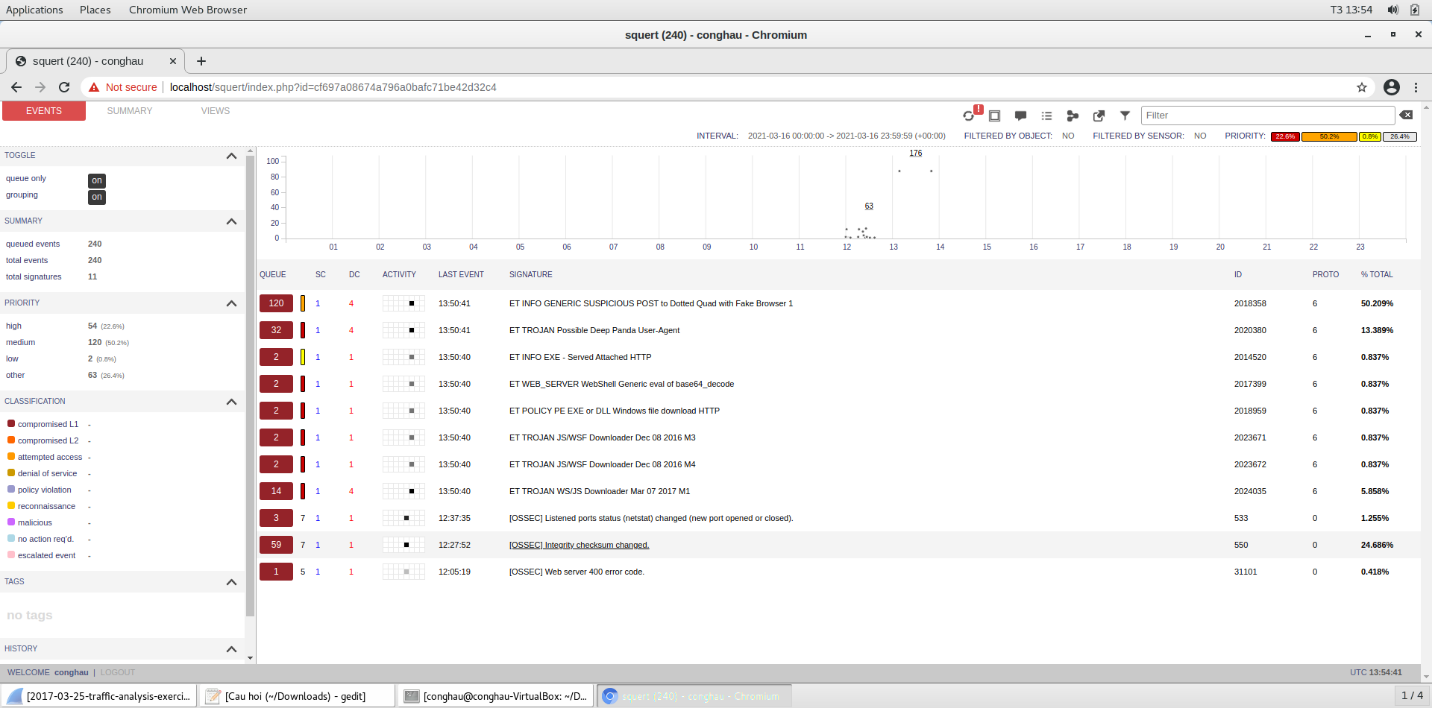


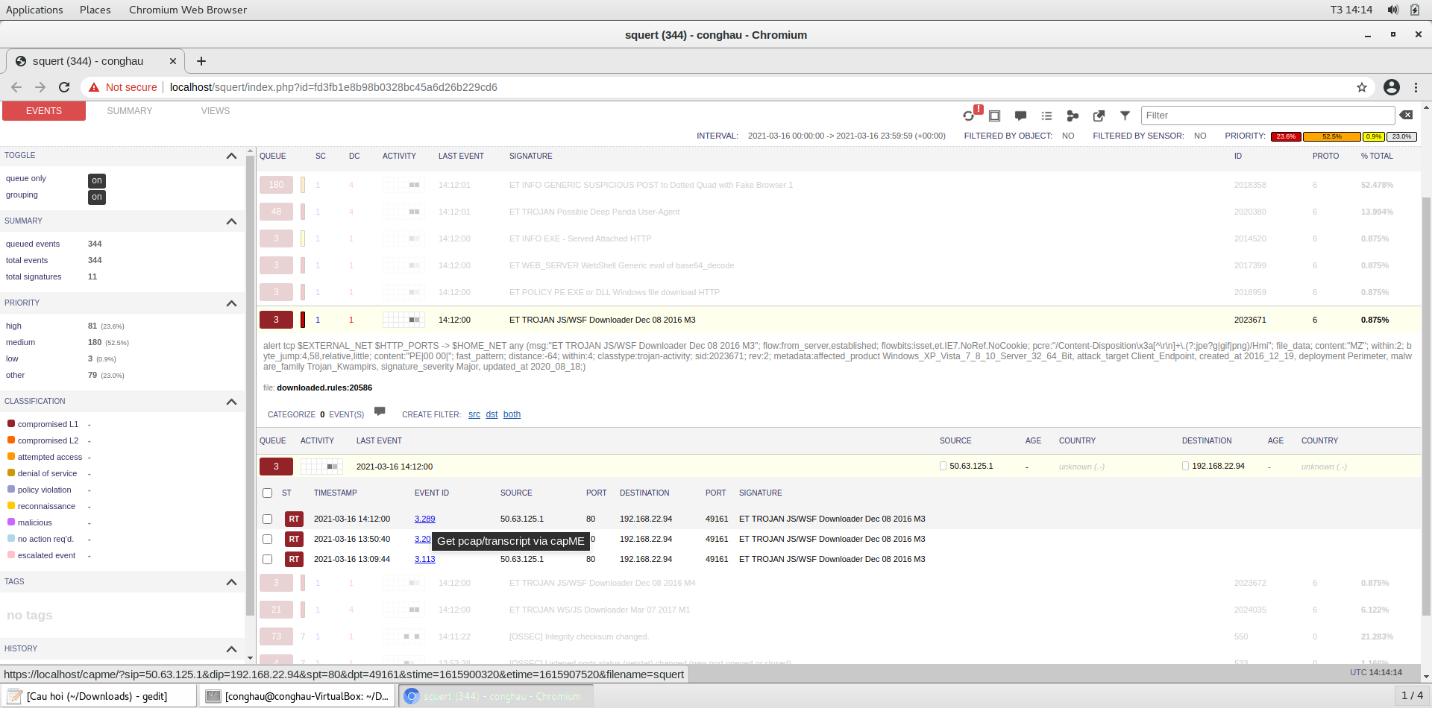
Nhập lệnh tcpreplay với enp0s8 là Sniffing Interface.



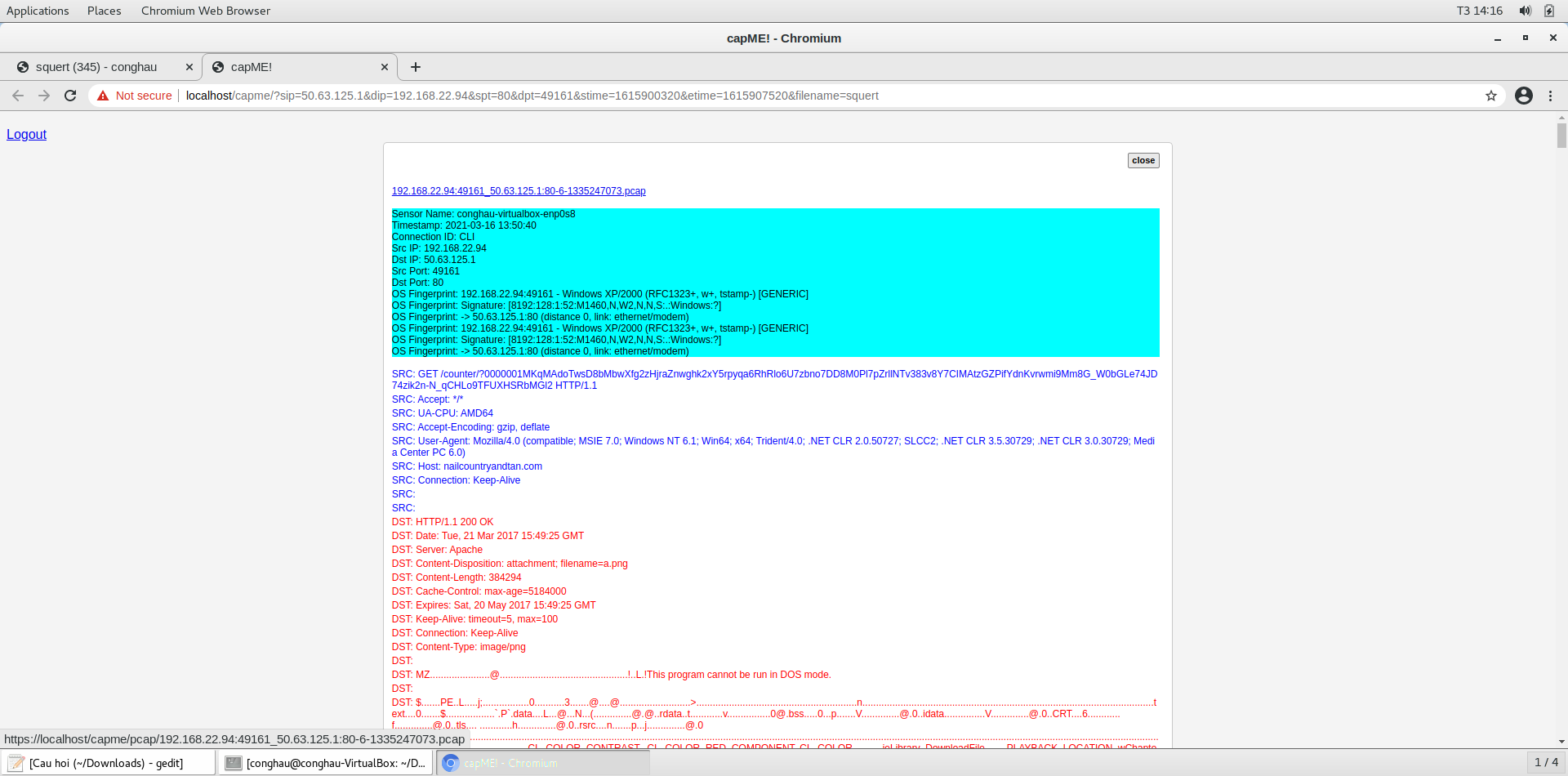


Vào **squert** sẽ thấy các lỗi như hình dưới.



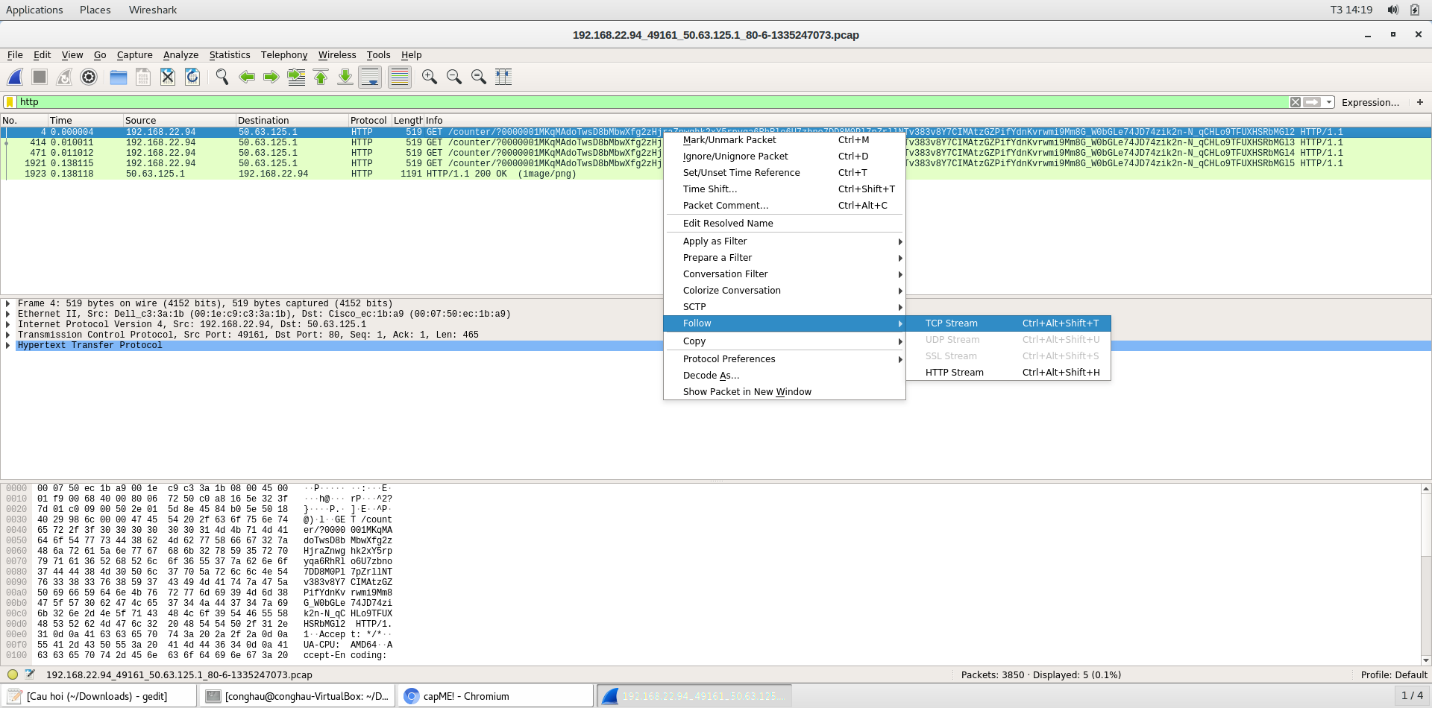


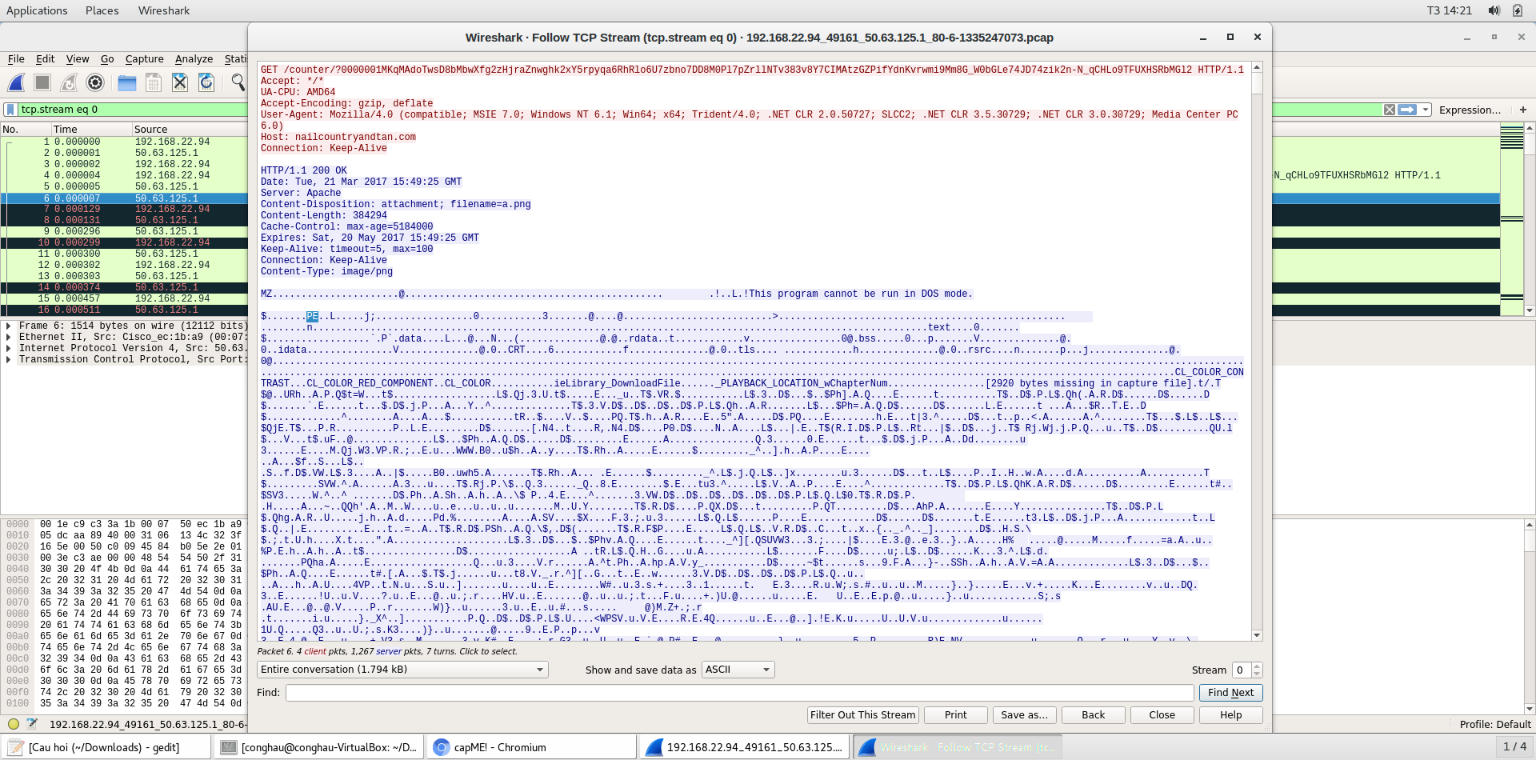
Download file pcap trên cùng của capME! về để phân tích bằng Wireshark.



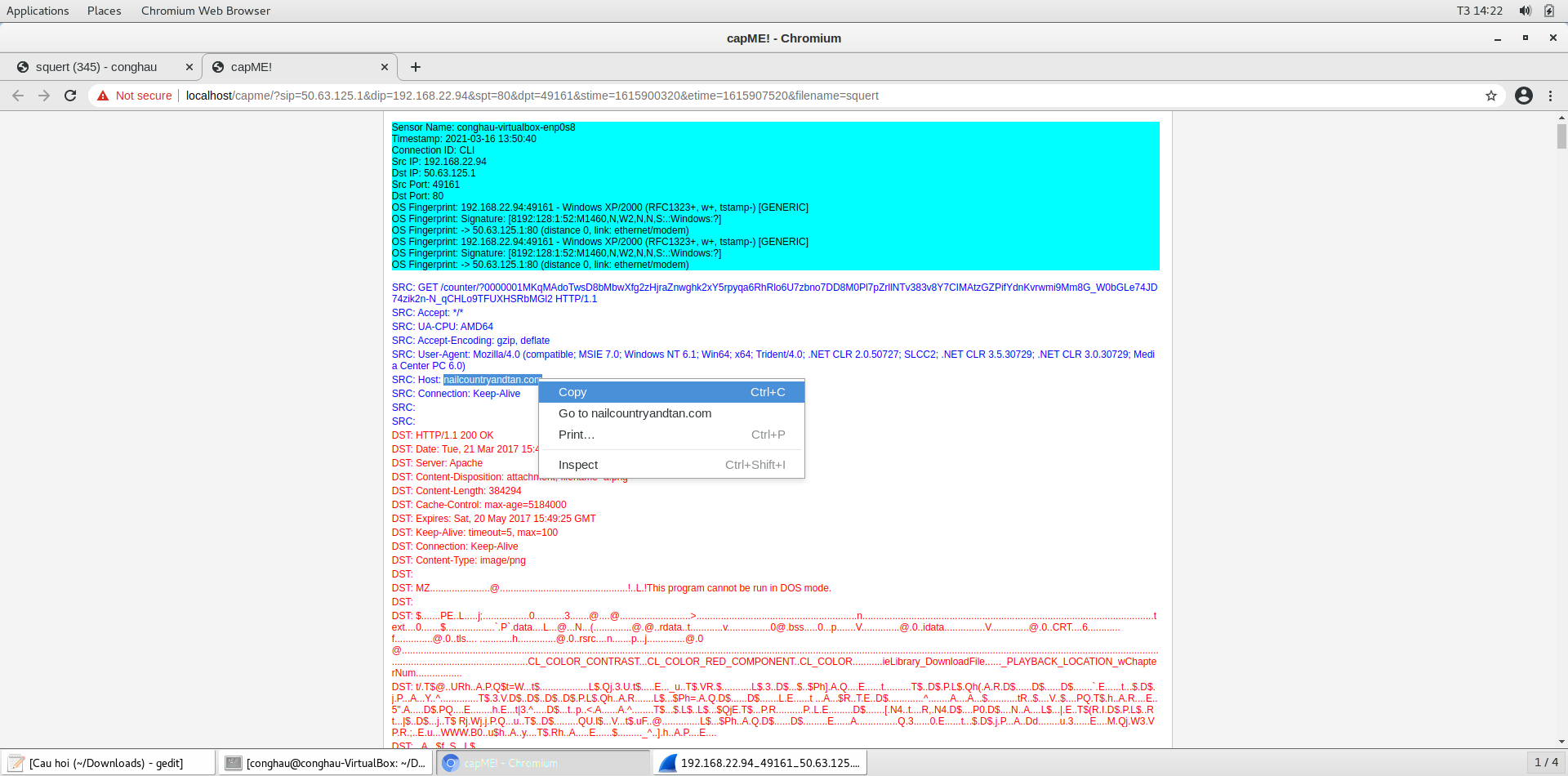


Nhập http vào Filter và Follow TCP Stream của nó để kiểm tra xem có giống với khi kiểm tra trong squer và capME!.

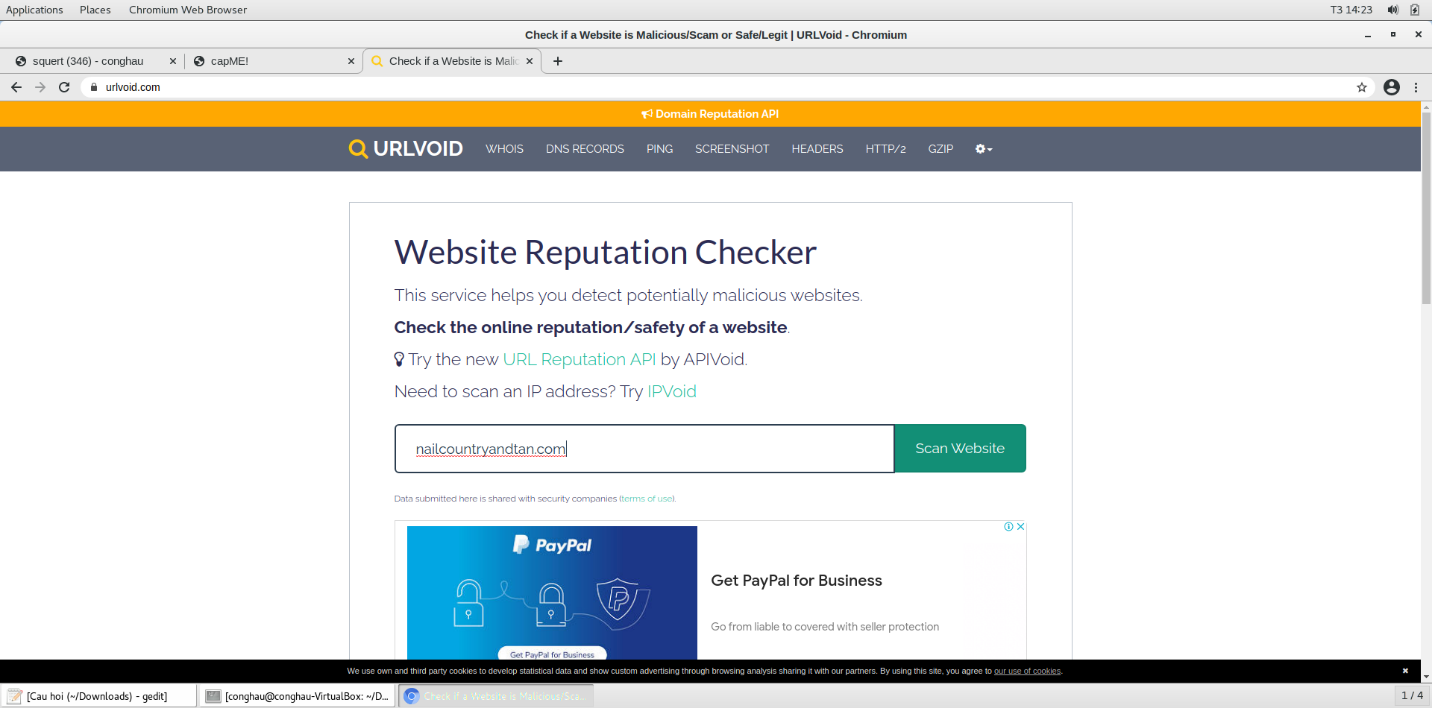




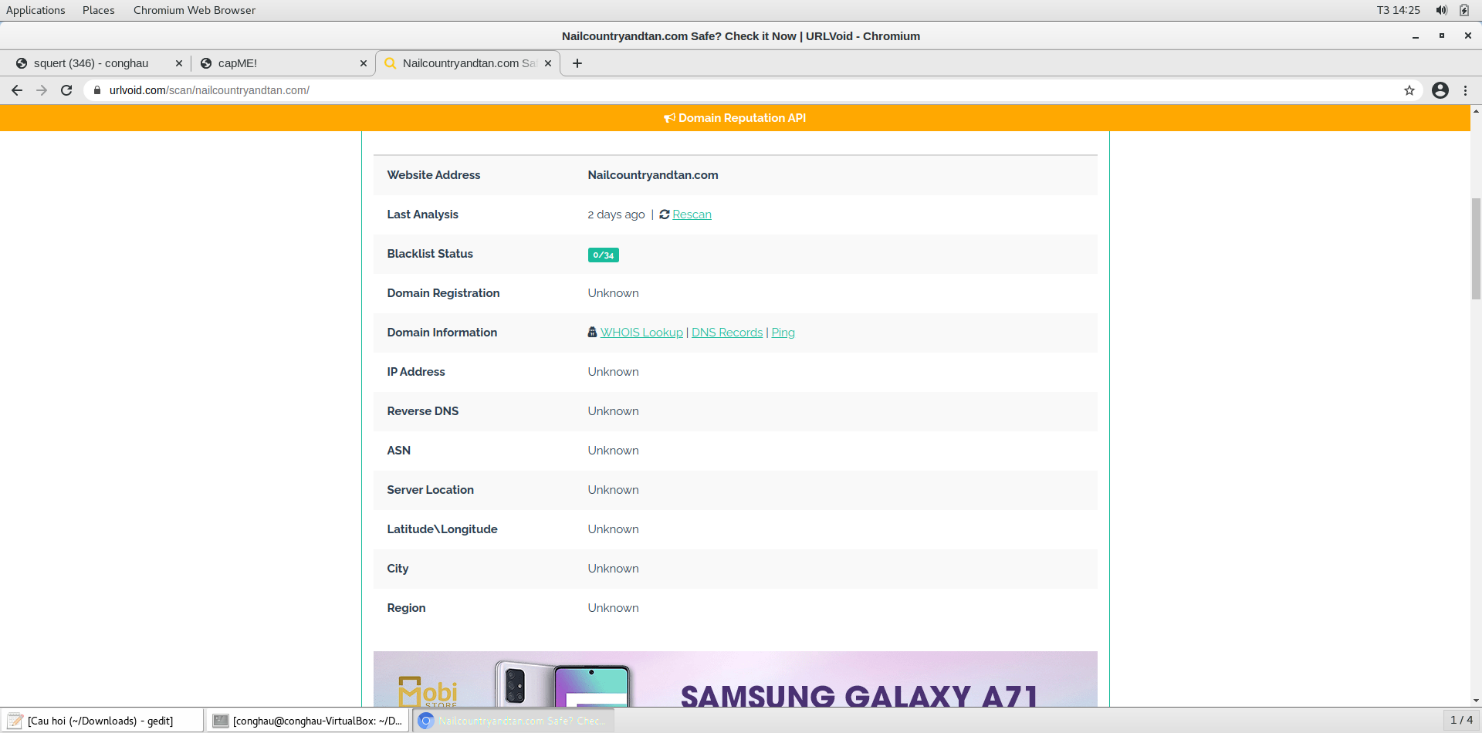
Copy trang web ở SRC Host của capME! để kiểm tra tính độc hại, khả nghi của trang web này.



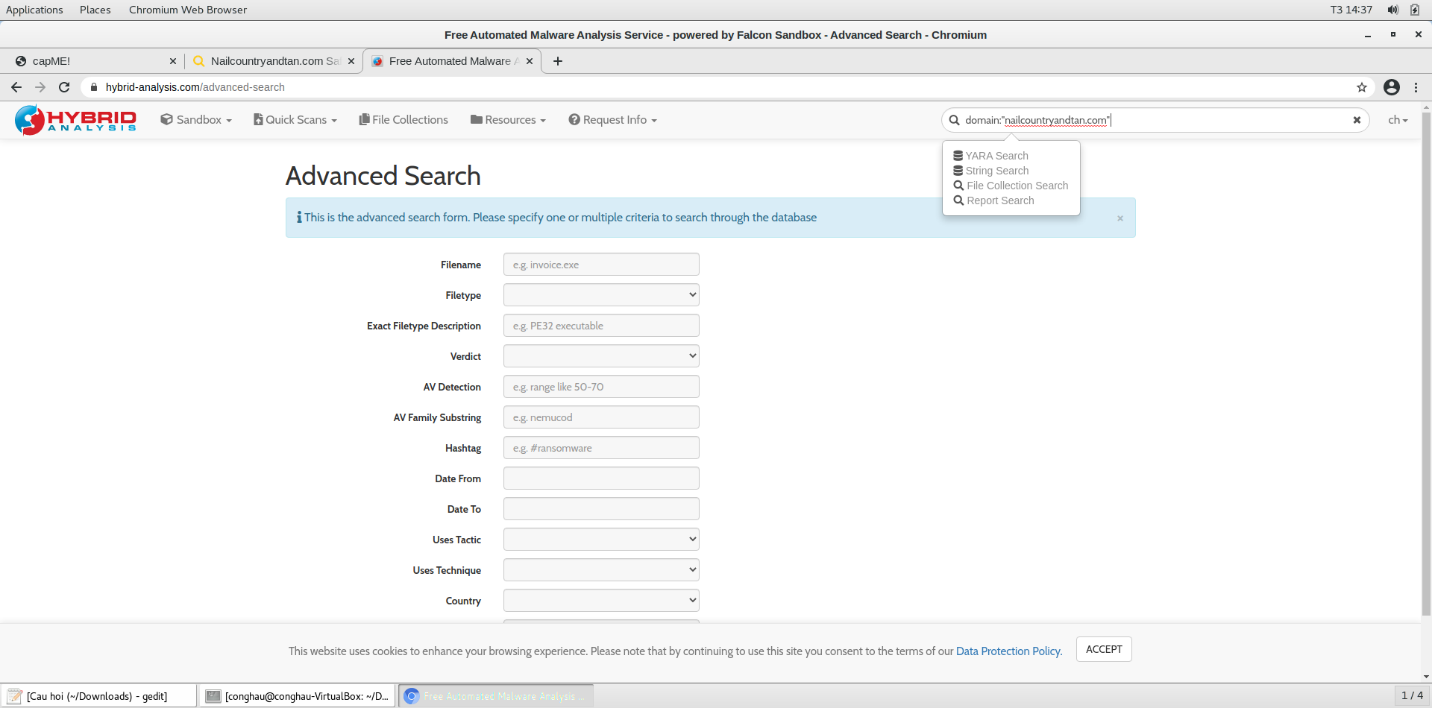
Sử dụng urlvoid.com để Scan trang web nghi ngờ.



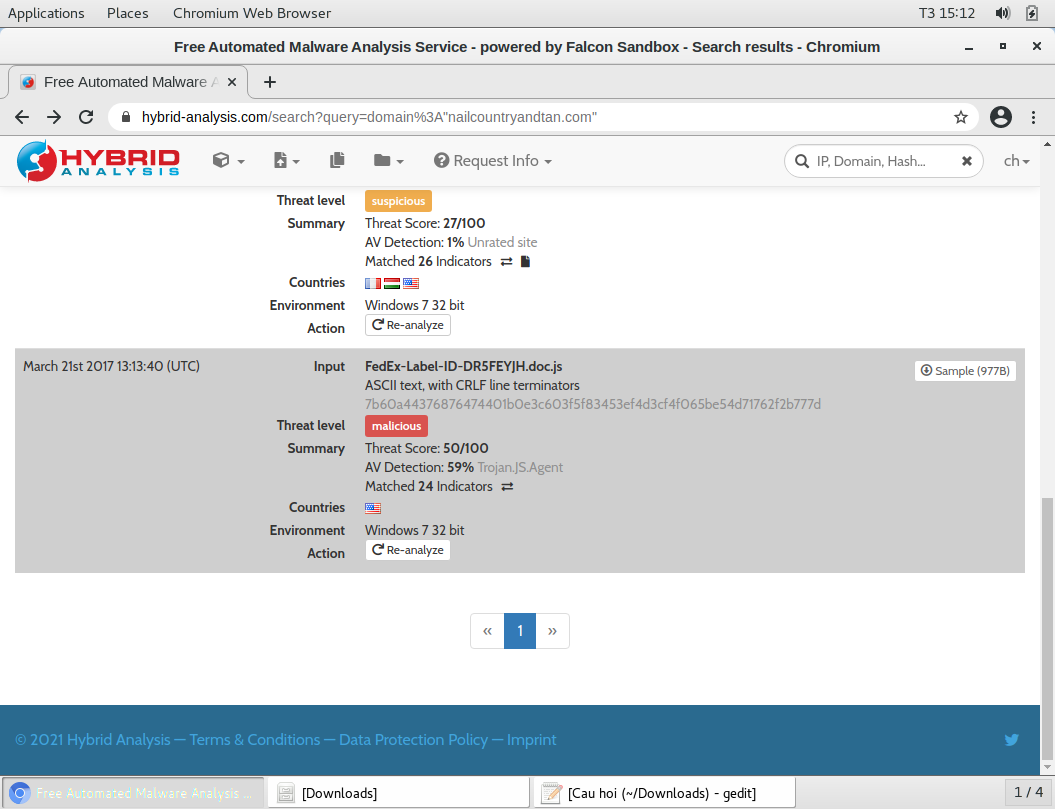
Không thấy tính khả nghi hay độc hại của trang web nghi ngờ. Cần scan sâu hơn trang web nghi ngờ để kiểm tra lại.



Sử dụng phần advanced search của trang web :“hybrid-analysis.com” để scan lại kỹ hơn trang web nghi ngờ. Nhập domain: “trang web nghi ngờ” vào phần advanced search. Lưu ý: cần phải đăng ký tài khoản để sử dụng được advanced search.



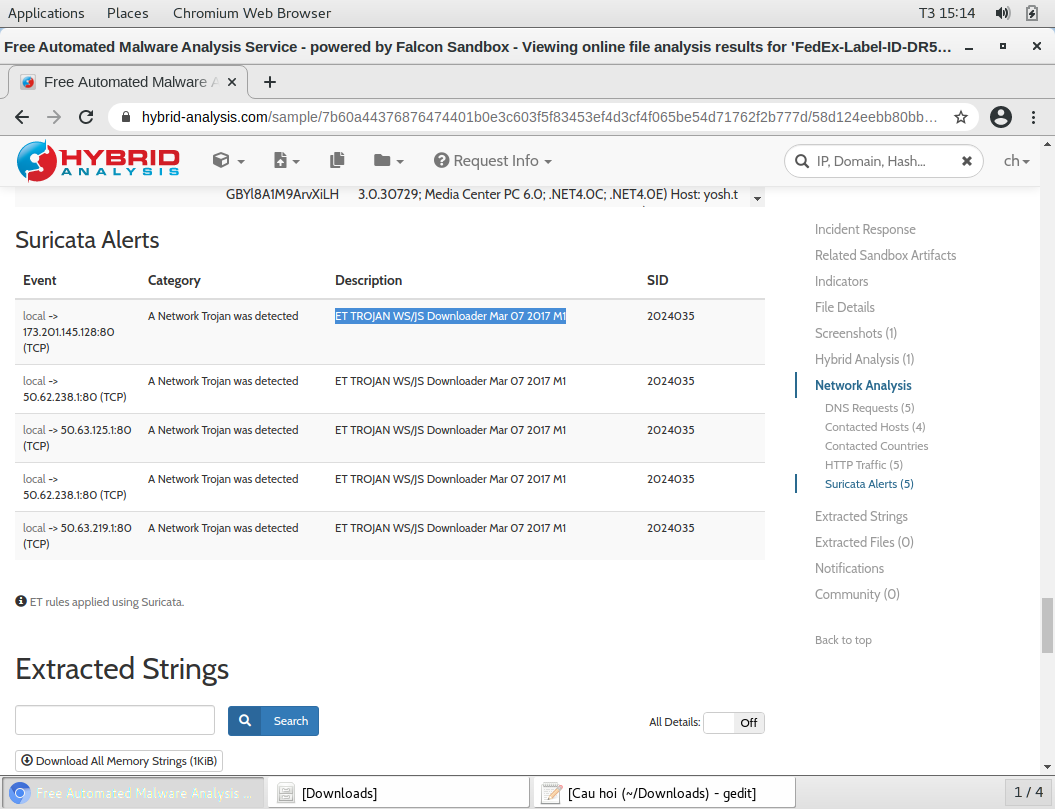
Chọn ngày gần nhất với lúc máy nạn nhân bị nhiễm độc. Ở đây gần nhất là ngày 21/3/2017



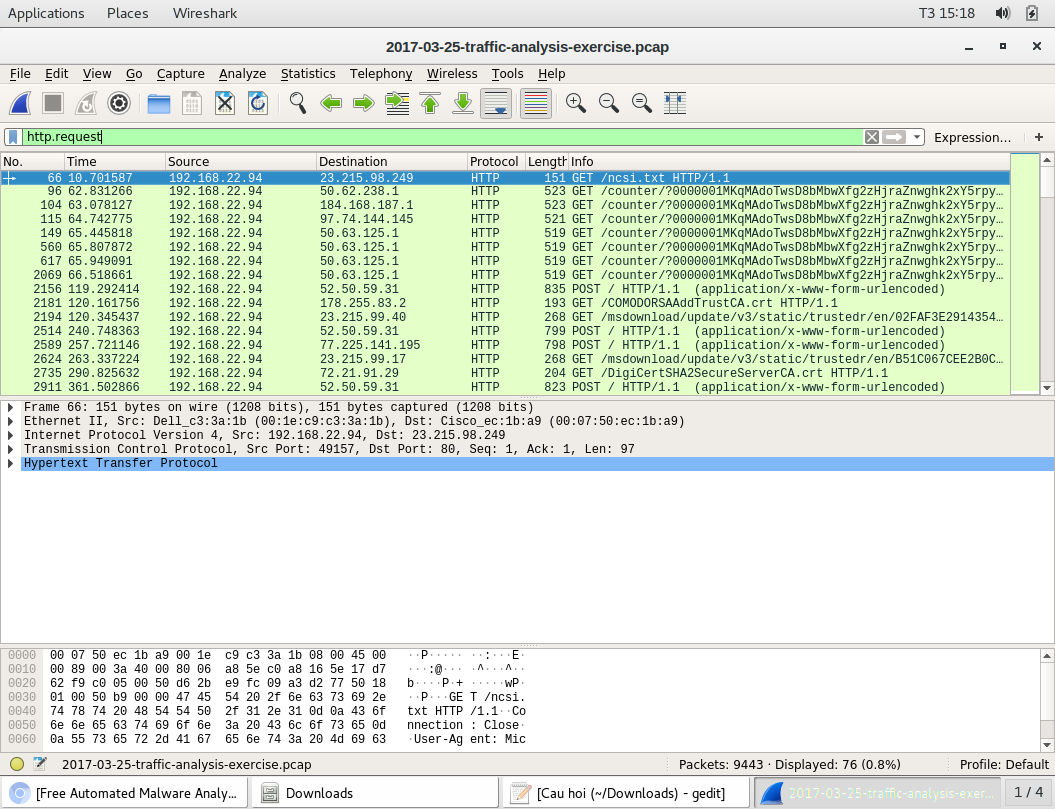
Sẽ thấy được IP của trang web nghi ngờ.



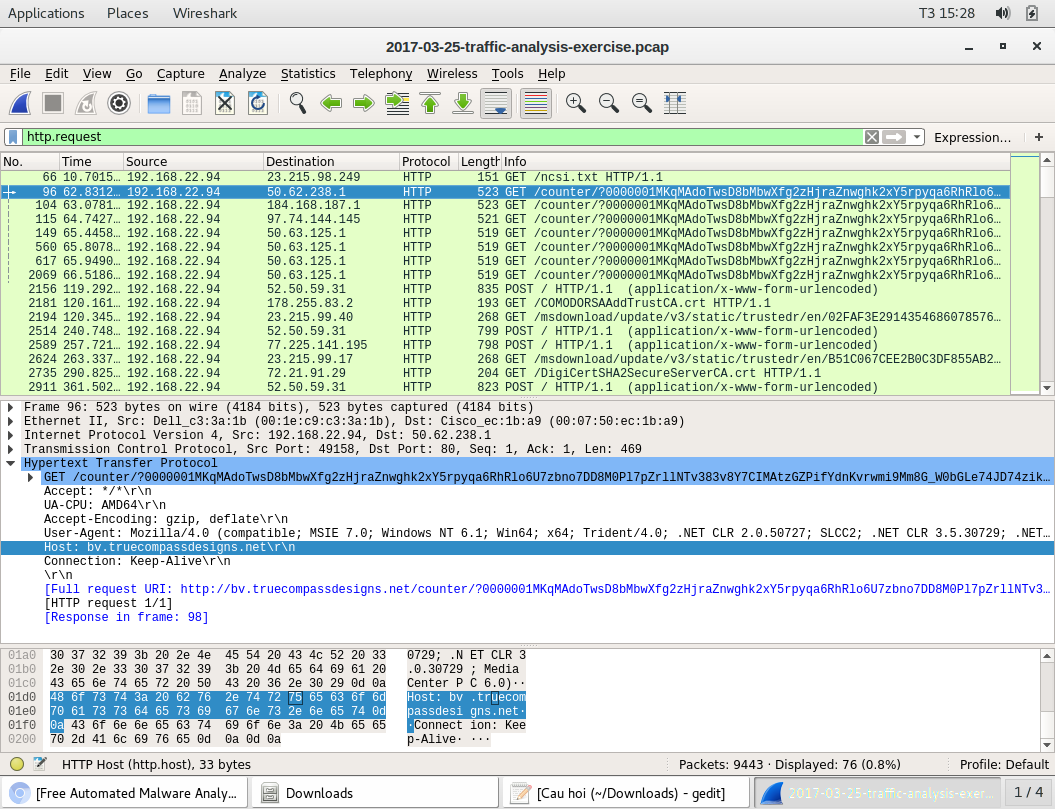
Sẽ thấy được mã độc giống với mã độc máy của nạn nhân bị nhiễm.

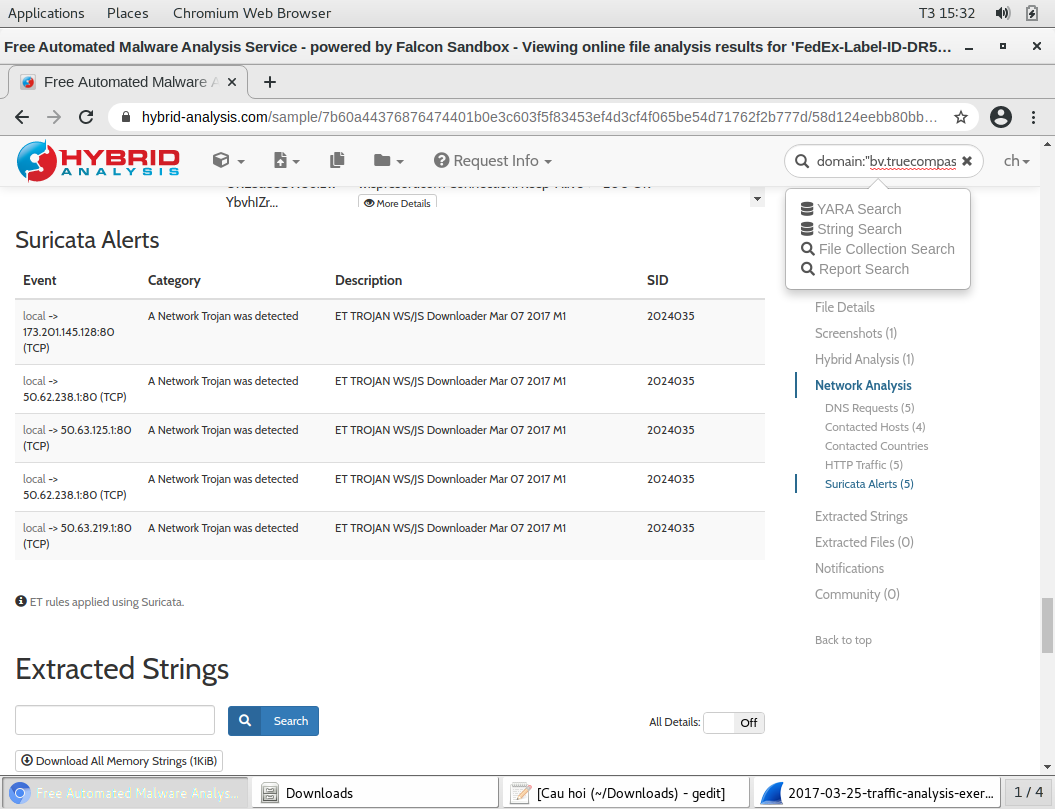


Mở lại file pcap lúc đầu và nhập http.request vào Filter.

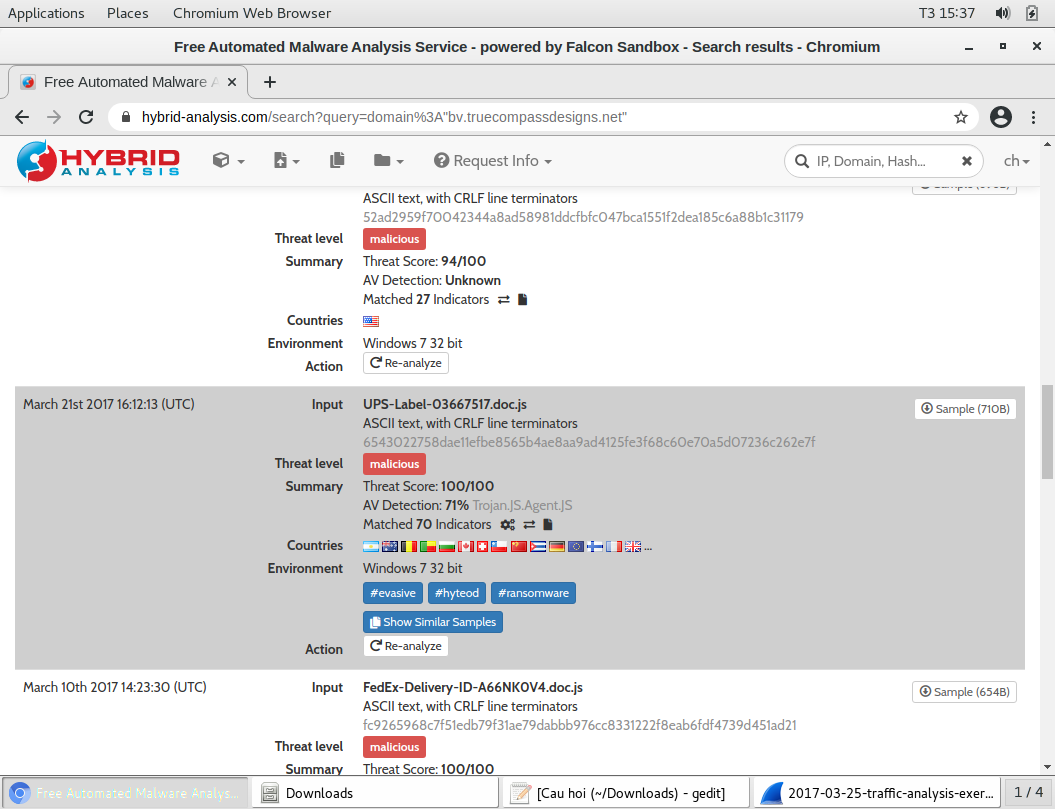


Tìm được host là 1 trang web như trong hình và sẽ kiểm tra thử tính độc hại, nghi ngờ của trang web này.

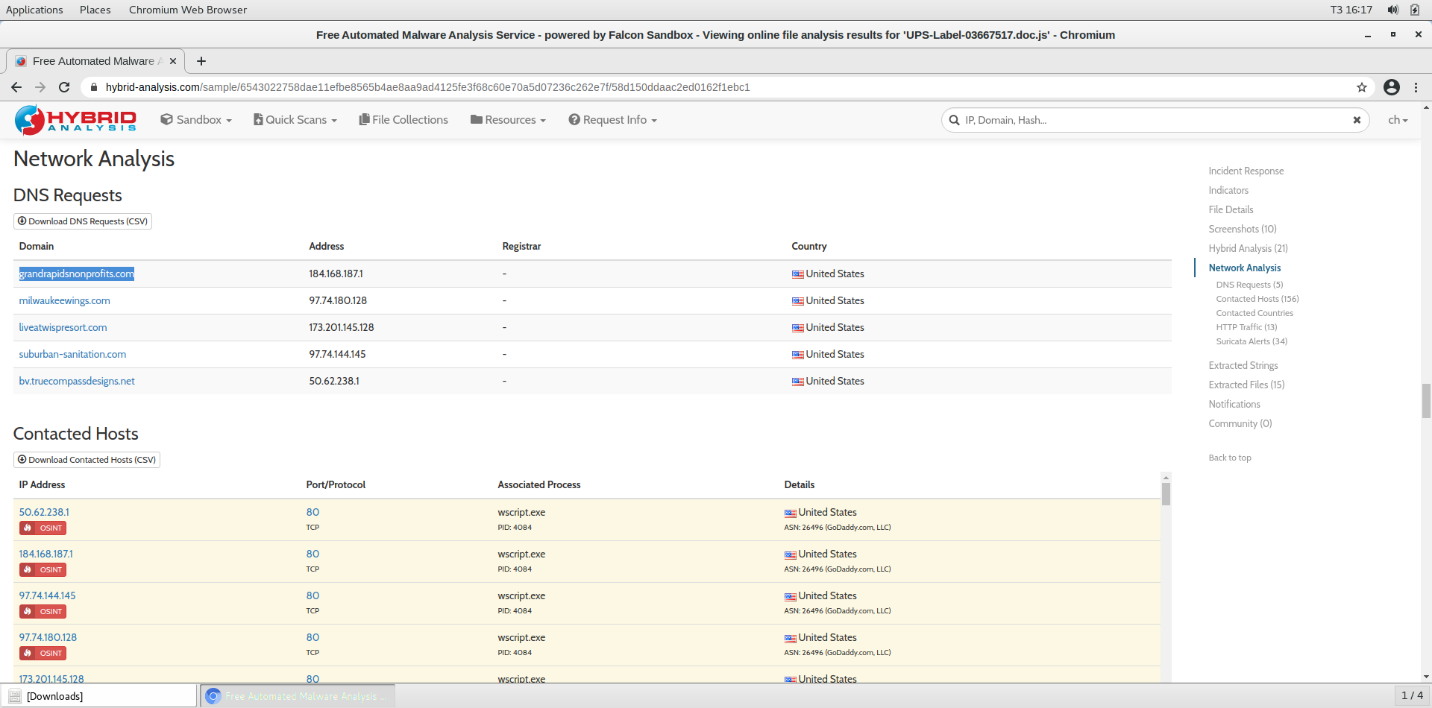




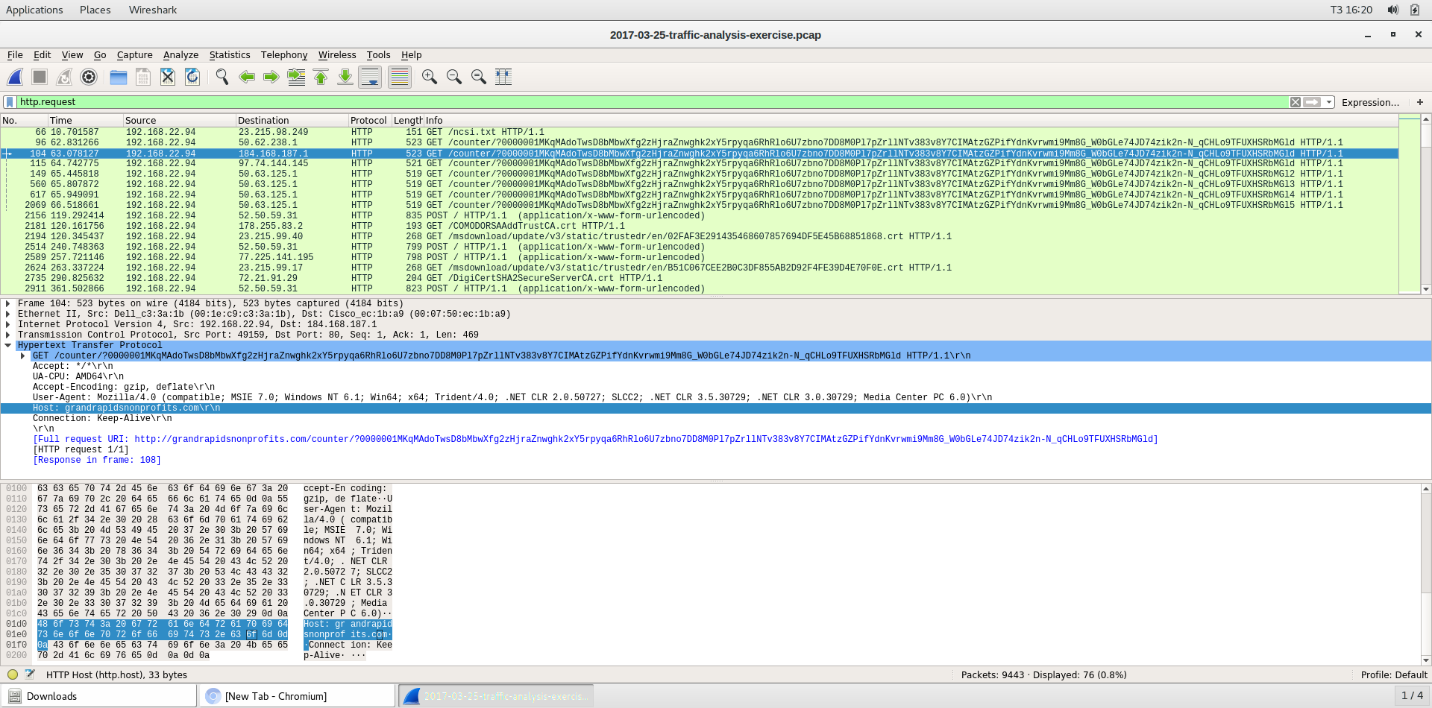
Chọn ngày gần nhất máy nạn nhân bị nhiễm.



Ta sẽ thấy được các domain như trong hình và sẽ kiểm tra thử 1 domain xem có tìm thấy được domain đó không trong file đang phân tích ở Wireshark.



Tìm thấy được domain đó.



Trả lời các câu hỏi còn lại để report.

