PHỤC LỤC 2

**HƯỚNG DẪN PHÂN TÍCH KHUNG TIN ETHERNET**

# Mục tiêu:

Cung cấp cho sinh viên các kỹ năng cơ bản sử dụng phần mềm Wireshark để phân tích khung tin Ethernet, bao gồm:

* Xác định cách thức truyền của khung tin trong mạng.
* Xác định giá trị các trường trong khung tin.
* Lọc và phân tích lưu lượng mạng theo yêu cầu.

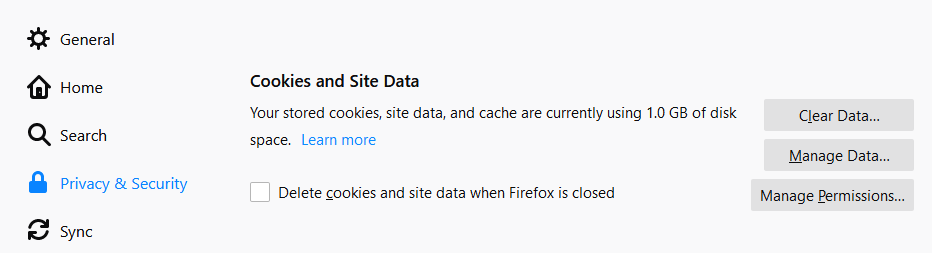
**Môi trường:** Hệ điều hành Windows 10.

# Nội dung

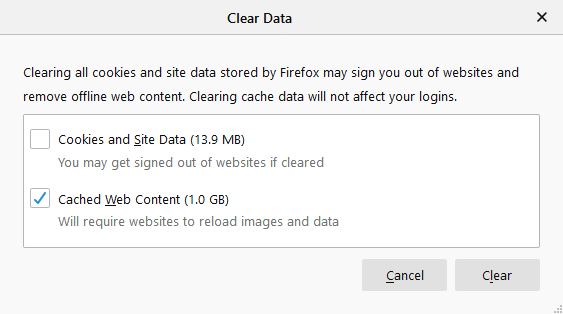
***Lưu ý: Trước khi thực hiện các nội dung thực hành sau đây, nên tắt các ứng dụng mạng đang sử dụng.***

## 1. Sử dụng Wireshark để bắt gói tin

* ***Bước 1***: Mở trình duyệt Firefox và xóa bộ đệm của ứng dụng như sau:
* Nhấn chuột vào biểu tượng  ở góc trên bên phải.
* Chọn *Options.*
* Trong mục *Privacy & Security*, tìm mục *Cookies and Site Data* nhấn nút *Clear Data.*



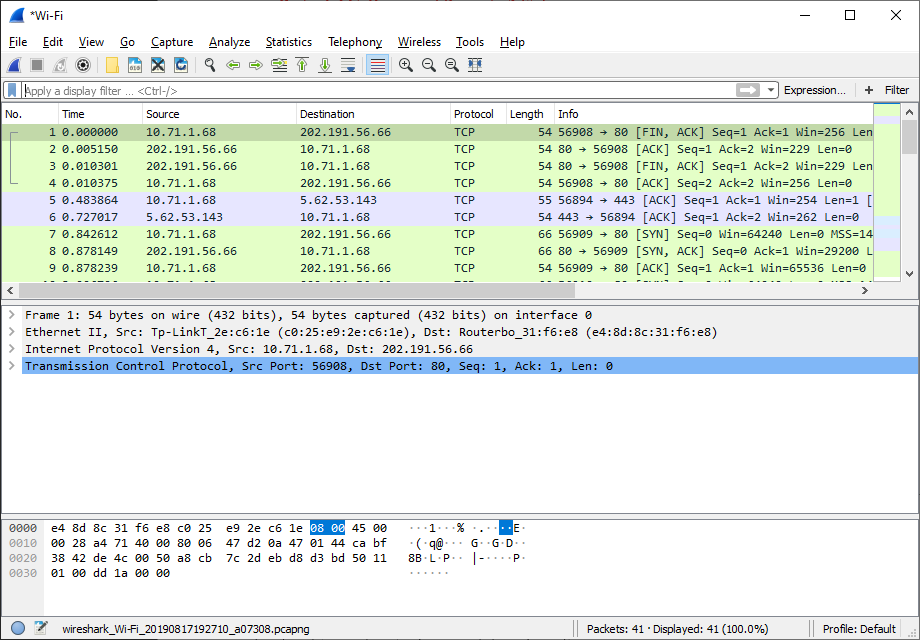
* Chọn mục *Cached Web Content* và nhấn nút *Clear.*



* ***Bước 2***:Mở Windows Explorer vào đường dẫn cài đặt, khởi động Wireshark (ví dụ đường dẫn mặc định là:
* ***Bước 3***: Bắt đầu bắt gói tin trên cổng mạng với Wireshark.
* ***Bước 4***:Mở Command Prompt với quyền quản trị Administrator (Nhấn Windows + X, chọn Command Prompt (Admin) gõ lệnh sau:



* **Bước 5:** Trên trình duyệt Firefox, truy cập vào trang http://nct.soict.hust.edu.vn. Sau khi trang Web được tải về. Dừng bắt gói tin trên Wirshark. Kết quả bắt gói tin trên Wireshark tương tự như sau:



***Lưu ý:***

*- Nếu trên máy học viên không bắt được các gói tin có Protocol là ARP thì nên thực hiện lại từ bước 1.*

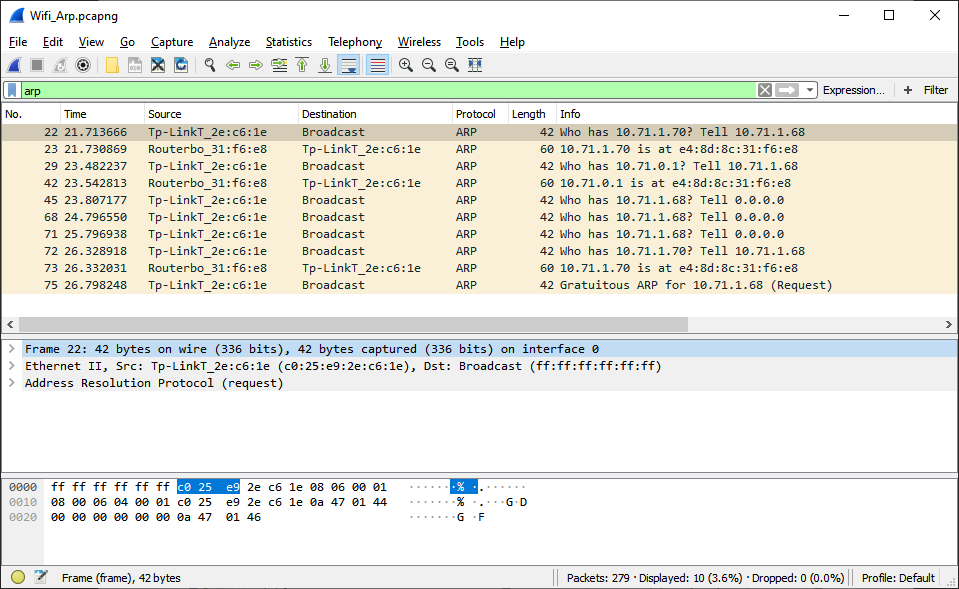
*- Các gói tin bắt được trên máy các bạn có thể sẽ có thông số khác. Điều này là hoàn toàn bình thường và không có ảnh hưởng tới quá trình thực hành.*

## 2. Phân tích lưu lượng

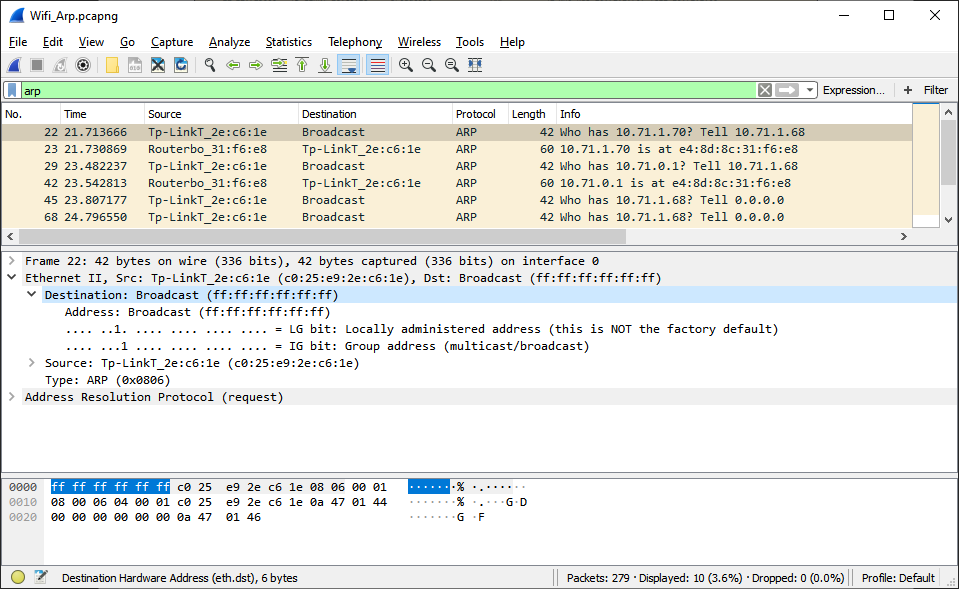
*Lưu ý: Các giá trị phân tích dưới đây chỉ mang tính chất minh họa. Với lưu lượng bắt trên máy sinh viên, kết quả có thể sẽ khác. Các bạn có thể download file lưu lượng mẫu tại địa chỉ sau cho nội dung minh họa dưới đây:*

<https://drive.google.com/file/d/1Lk2PJ6m-7nmc4hJfeDoaf-V7akShVchz>

* **Bước 1**: Chọn một gói tin có **Protocol** là **ARP** và **Destination** là **Broadcast** (Filter từ khóa arp).

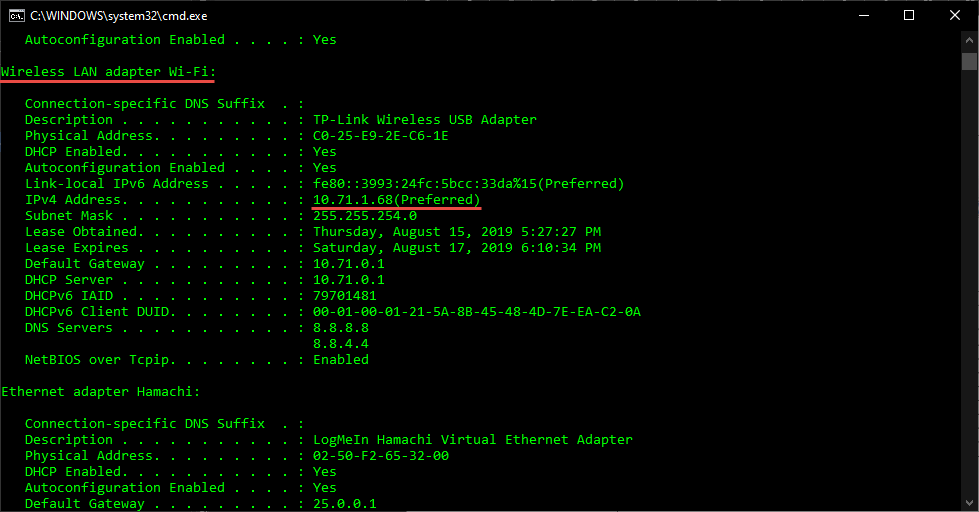


* **Bước 2**: Mở rộng phần tiêu đề Ethernet II như sau:



Chúng ta sẽ thấy trường Destination có giá trị là ff:ff:ff:ff:ff:ff. Đây chính là địa chỉ MAC quảng bá. Như vậy, gói tin này đã được gửi đi theo phương thức quảng bá.

* ***Bước 3***: Trên cửa sổ Command Prompt, thực hiện lệnh **ipconfig /all**, chúng ta nhận được danh sách các cạc mạng đang có trên máy tính. Kết quả tương tự như sau:

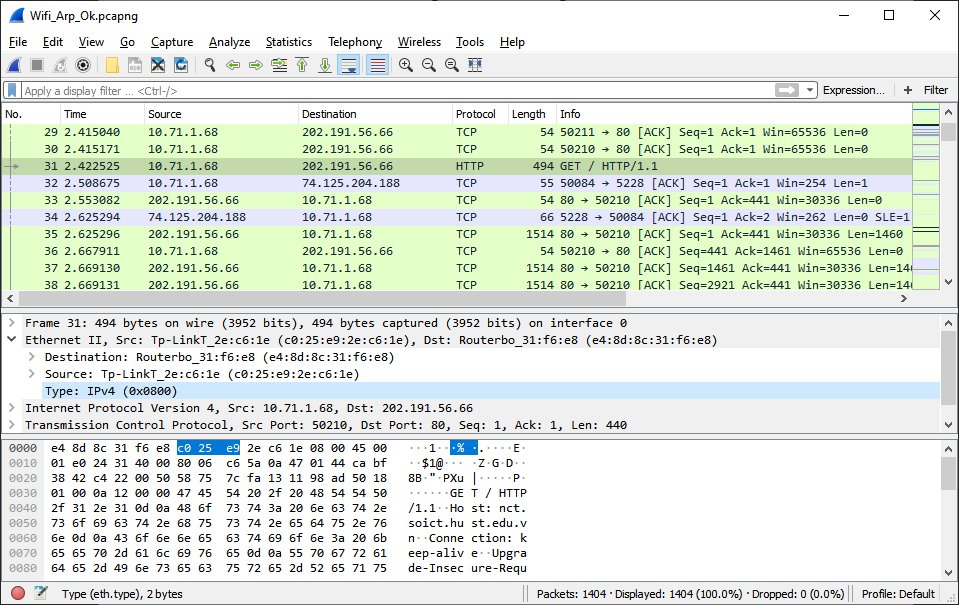


Trong kết quả minh họa trên, ta thấy cạc mạng Wireless LAN adapter Wi-Fi là TP-Link Wireless Wireless USB Adapter có địa chỉ MAC là C0-25-E9-2E-C6-1E. Đối chiếu với trường Source trong tiêu đề Ethernet của gói tin trên, ta có thể thấy đây chính là giá trị của trường đó. Như vậy gói tin quảng bá mà chúng ta vừa phân tích được gửi đi trên chính máy tính này.

* ***Bước 4***: Trên Wireshark chọn gói tin có các thông số như sau:
* Destination: 202.191.56.66
* Protocol: HTTP
* Info: GET / HTTP/1.1

Đây chính là gói tin được gửi đi từ máy của bạn tới máy chủ có tên miền nct.soict.hust.edu.vn.

* ***Bước 5***: Trên cửa sổ Wireshark mở rộng phần tiêu đề Ethernet II.



Rất dễ để nhận thấy, địa chỉ MAC nguồn của gói tin này là địa chỉ máy tính của bạn. Tuy nhiên, địa chỉ MAC đích không phải là địa chỉ của máy chủ nct.soict.hust.edu.vn. Chúng ta sẽ đề cập đến điều này trong những bài học sau.

Trường Type ghi nhận giá trị 0x0800 chính là số hiệu của giao thức IP theo chuẩn Ethernet. Như vậy có thể thấy, khung tin Ethernet này mang theo trong phần Payload của nó một gói tin IPv4.

Chúng ta có thể để ý thêm phần nội dung của gói tin có xâu “GET / HTTP/1.1” và “nct.soict.hust.edu.vn”. Đây chính là dữ liệu của dịch vụ Web. Trong các bài học sau, chúng sẽ phân tích rõ hơn.

* ***Bước 6***: Chọn gói tin mà máy chủ nct.soict.hust.edu.vn gửi lại cho máy tính của chúng ta và thực hiện các bước phân tích tương tự trên. Các bạn có thể tự luyện tập để xác định các thông số trên tiêu đề Ethernet II của gói tin.

# Kết luận

Với nội dung mà các bạn vừa thực hiện, các bạn đã làm quen được với cách sử dụng công cụ Wireshark để phân tích lưu lượng Ethernet.

Chúc mừng các bạn đã hoàn thành:

* Nhận biết được lưu lượng gửi đi theo phương thức broadcast.
* Xác định được giá trị của các trường trong tiêu đề Ethernet của gói tin.