Đặng Vân Khánh – 24520777

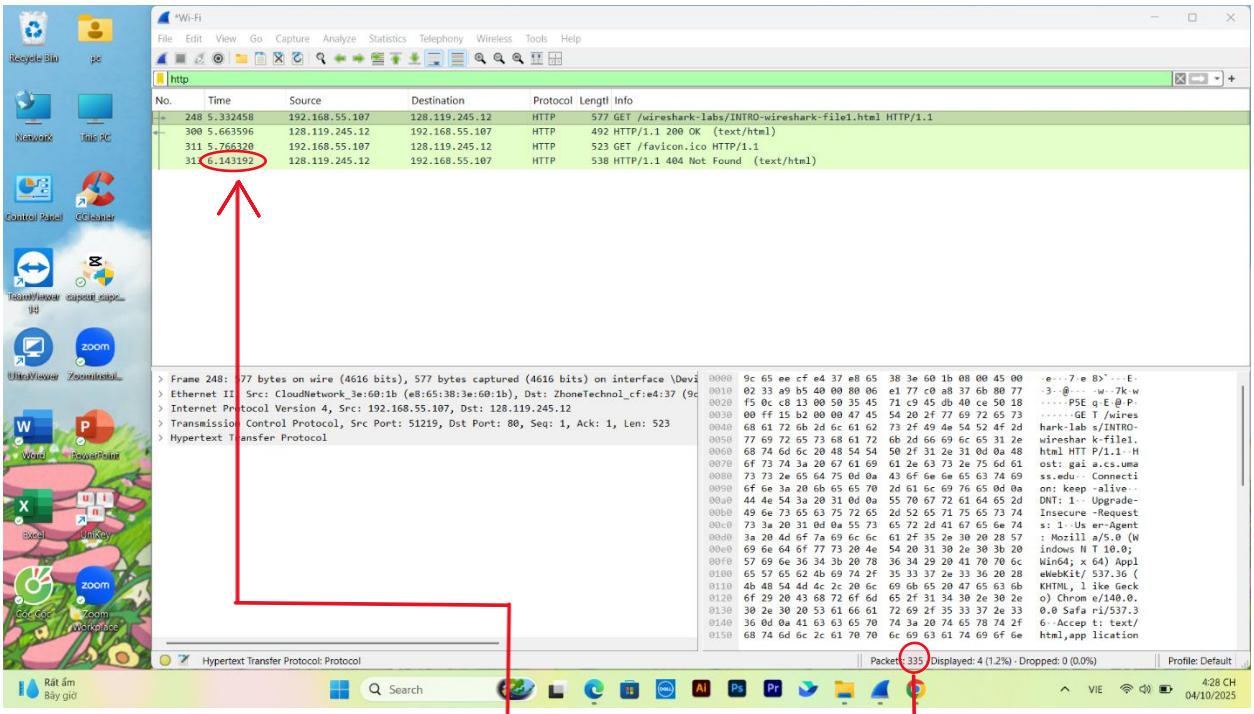
LAB 1

Làm quen với Wireshark

B. THỰC HÀNH

Task 2: Làm quen với Wireshark và thử nghiệm bắt gói tin trong mạng

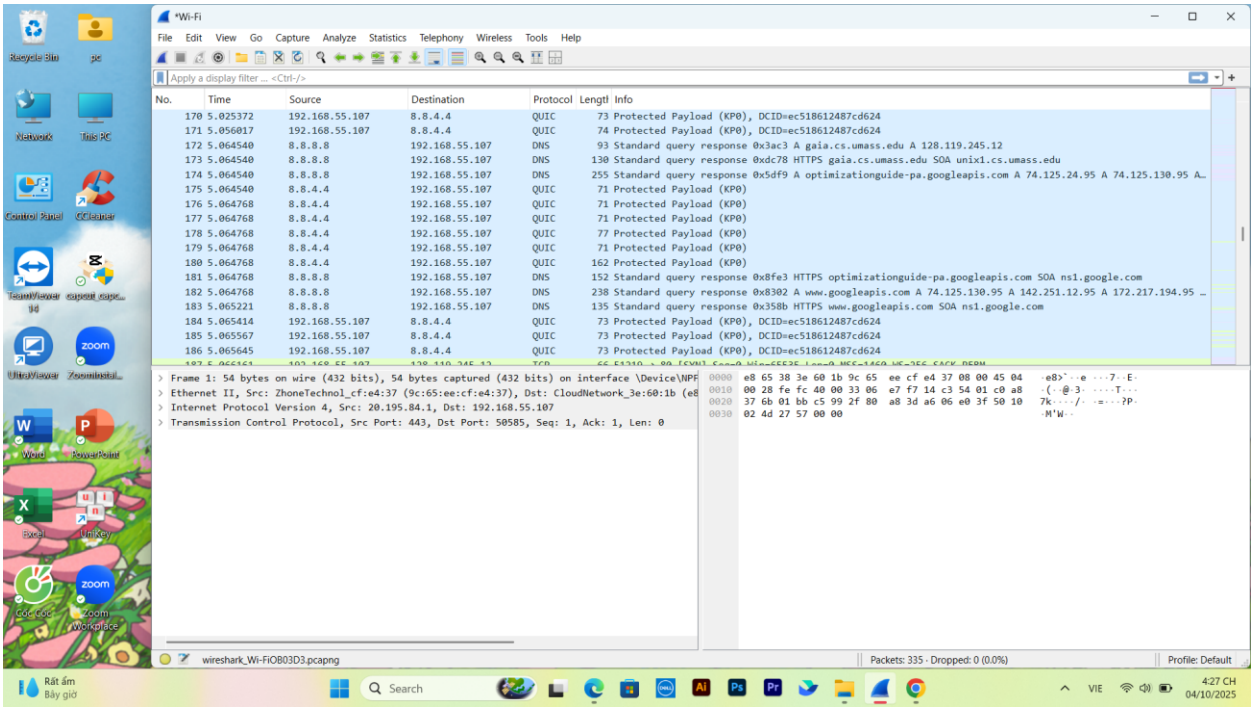
1. Tổng thời gian bắt gói tin trong web http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html



Hình 1

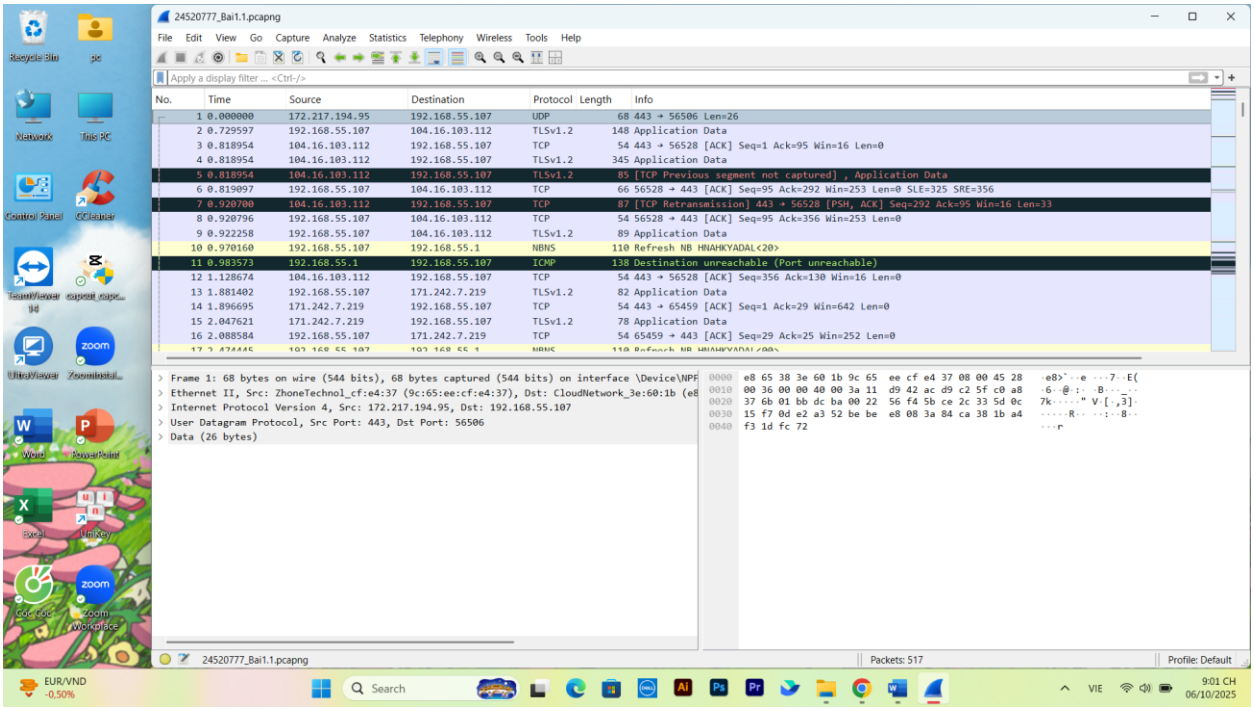
- Tổng thời gian bắt gói tin: 6.143192
- Tổng số gói tin bắt được khoanh vùng màu đỏ 335 gói

2. 5 Giao thức khác nhau xuất hiện trong cột giao thức khi không dùng bộ lọc http khi truy cập http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html



Hình 2

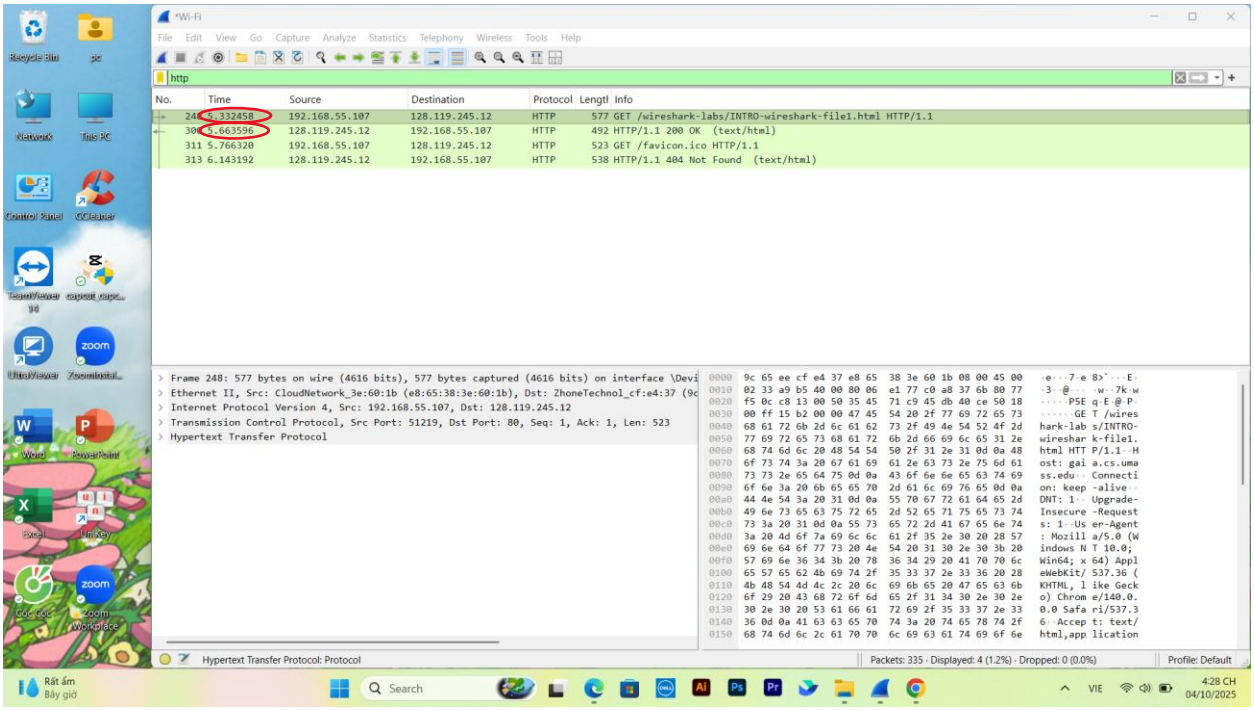
- **TCP**: Truyền dữ liệu đáng tin cậy giữa 2 máy tính, đảm bảo dữ liệu đến đúng thứ tự, không bị mất mát, có cơ chế kiểm tra lỗi và gửi lại nếu gói tin bị mất.
- **UDP**: Truyền dữ liệu nhanh, không cần đảm bảo về độ tin cậy hay thứ tự gói tin. Không kiểm tra lỗi, không gửi lại, nhưng rất nhanh và tiết kiệm băng thông.
- **TLSv1.2:** Là giao thức bảo mật lớp truyền tải dùng để mã hóa dữ liệu khi truyền trên mạng, xác thực máy chủ thông qua chứng chỉ số, đảm bảo tính toàn vẹn của dữ liệu tránh bị thay đổi hoặc giả mạo.
- **DNS**: Là hệ thống phân giải tên miền, chuyển từ tên miền chữ cái sang thành địa chỉ IP để máy tính hiểu và kết nối được.
- **QUIC:** Là một giao thức truyền tải do Google phát triển, giúp kết nối nhanh hơn, giảm độ trễ khi mất gói, bảo mật mặc định với TLS 1.3.



Hình 2.1

- **UDP:** Truyền dữ liệu nhanh, không cần đảm bảo về độ tin cậy hay thứ tự gói tin. Không kiểm tra lỗi, không gửi lại, nhưng rất nhanh và tiết kiệm băng thông.
- **TCP:** Truyền dữ liệu đáng tin cậy giữa 2 máy tính, đảm bảo dữ liệu đến đúng thứ tự, không bị mất mát, có cơ chế kiểm tra lỗi và gửi lại nếu gói tin bị mất.
- **TLSv1.2:** Là giao thức bảo mật lớp truyền tải dùng để mã hóa dữ liệu khi truyền trên mạng, xác thực máy chủ thông qua chứng chỉ số, đảm bảo tính toàn vẹn của dữ liệu tránh bị thay đổi hoặc giả mạo.
- **NBNS:** Là giao thức thuộc bộ NetBIOS, hoạt động ở tầng ứng dụng, thường dùng trong các mạng Windows cũ, chức năng chính là ánh xạ tên NetBIOS của 1 máy sang địa chỉ IP tương ứng để các máy trong mạng có thể liên lạc được.
- **ICMP:** Là một giao thức tầng mạng, đi kèm với IP, không truyền dữ liệu người dùng mà dùng để báo lỗi mạng, gửi thông báo về tình trạng đường truyền.

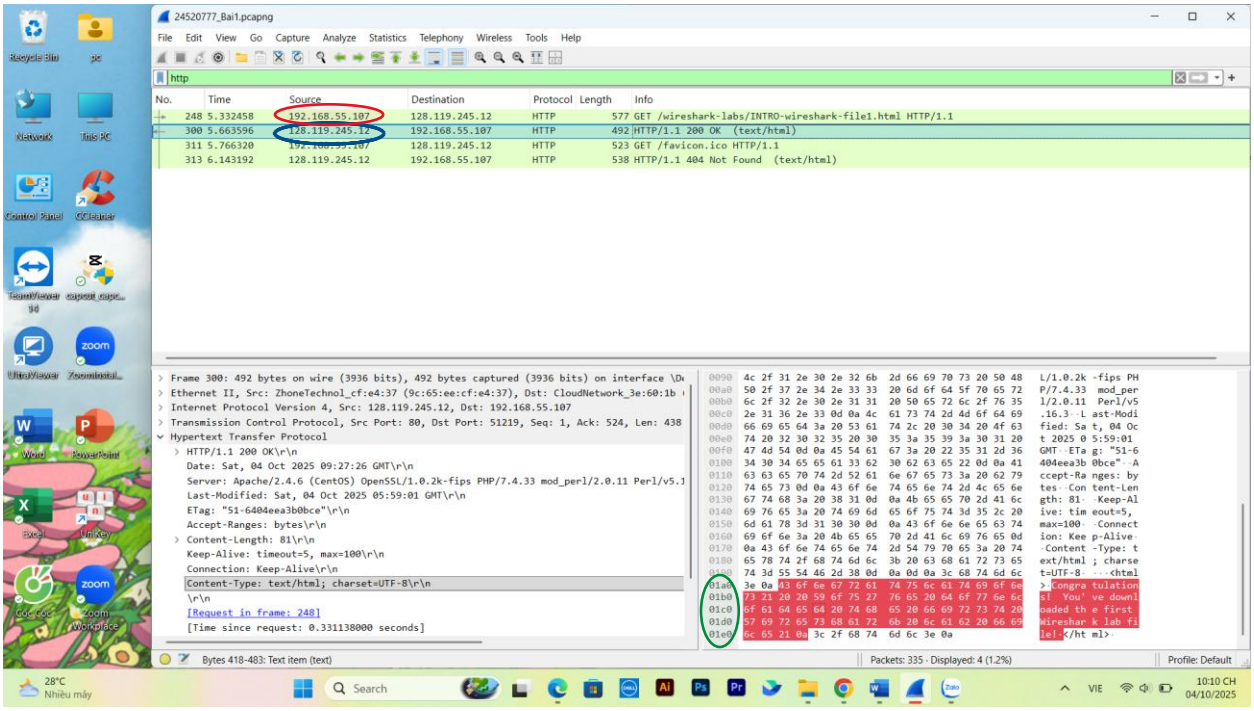
3. Từ khi gói tin HTTP GET đầu tiên được gửi cho đến khi HTTP 200 OK đầu tiên được nhận đối với mỗi website đã thử nghiệm



Hình 3

- Thời gian từ khi gói tin HTTP GET đầu tiên được gửi đến khi HTTP 200 OK đầu tiên được nhận với website http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html : 0.331138
- Giải thích:
    - Thời gian bắt gói tin HTTP GET đầu tiên là: 5.332458
    - Thời gian nhận gói HTTP 200 OK là: 5.663596
    - Thời gian: 5.663596 – 5.332458 = 0.331138

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
    - Có. Nằm ở khoản vị trí 01a0 đến 01e0 được khoanh tròn viền xanh lá ở hình 4.

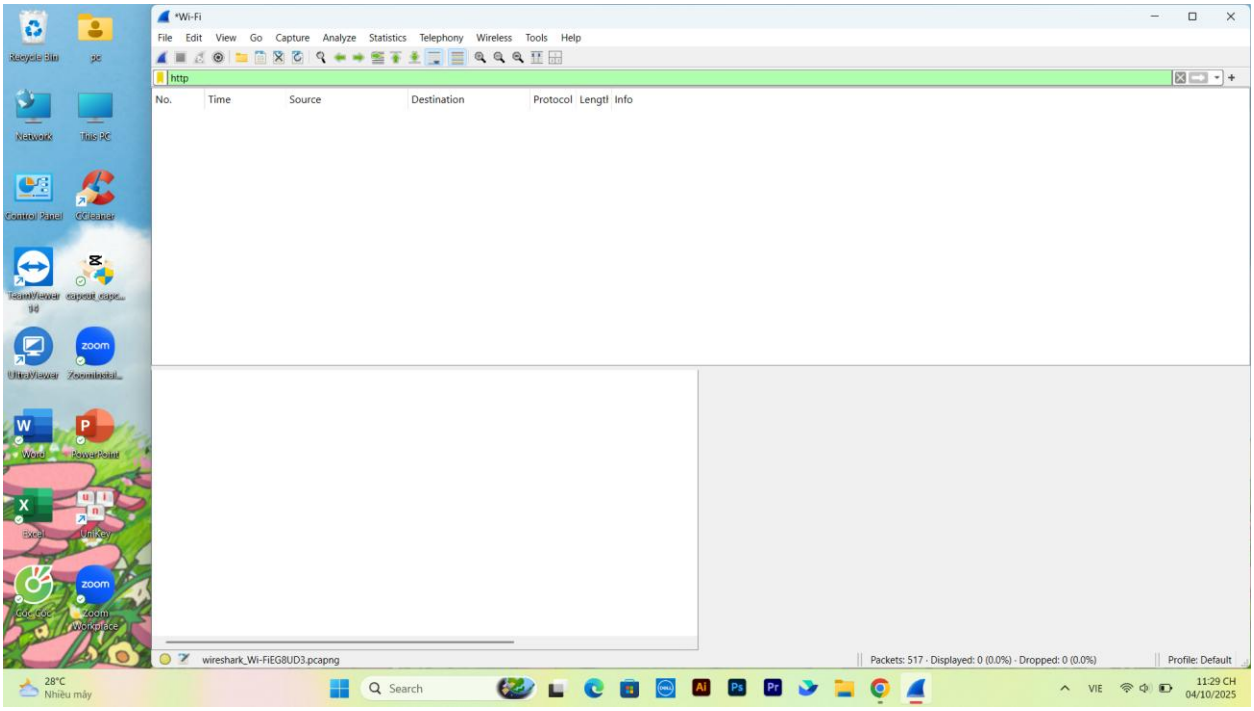


Hình 4

5. Địa chỉ IP của gaia.cs.umass.edu đã chọn ở bước 10 là:
   - 128.119.245.12 được khoanh vùng màu xanh dương ở hình 4

   Địa chỉ IP của máy tính đang sử dụng là:
   - 192.168.55.107 được khoanh vùng màu đỏ ở hình 4

   Địa chỉ IP của website https://student.uit.edu.vn/ đã chọn là không bắt được do là https.



Hình 5

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 bắt đầu kết nối, thì sẽ gọi đến tên miền gaia.cs.umass.edu để biên dịch URL trước khi trang web trở thành địa chỉ IP.
   - Theo sau đó, trình duyệt sẽ sử dụng địa chỉ IP yêu cầu http gọi đến máy chủ lưu trữ trang web đó.
   - Nếu máy chủ chấp nhận, máy chủ sẽ gửi lại thông báo 200 OK và truy xuất mã HTML của trang web được yêu cầu
   - Trình duyệt sau khi nhận được mã HTML sẽ hiển thị ra cửa sổ của trình duyệt trang web hoàn chỉnh mà mình muốn truy cập.