Báo cáo thực hành

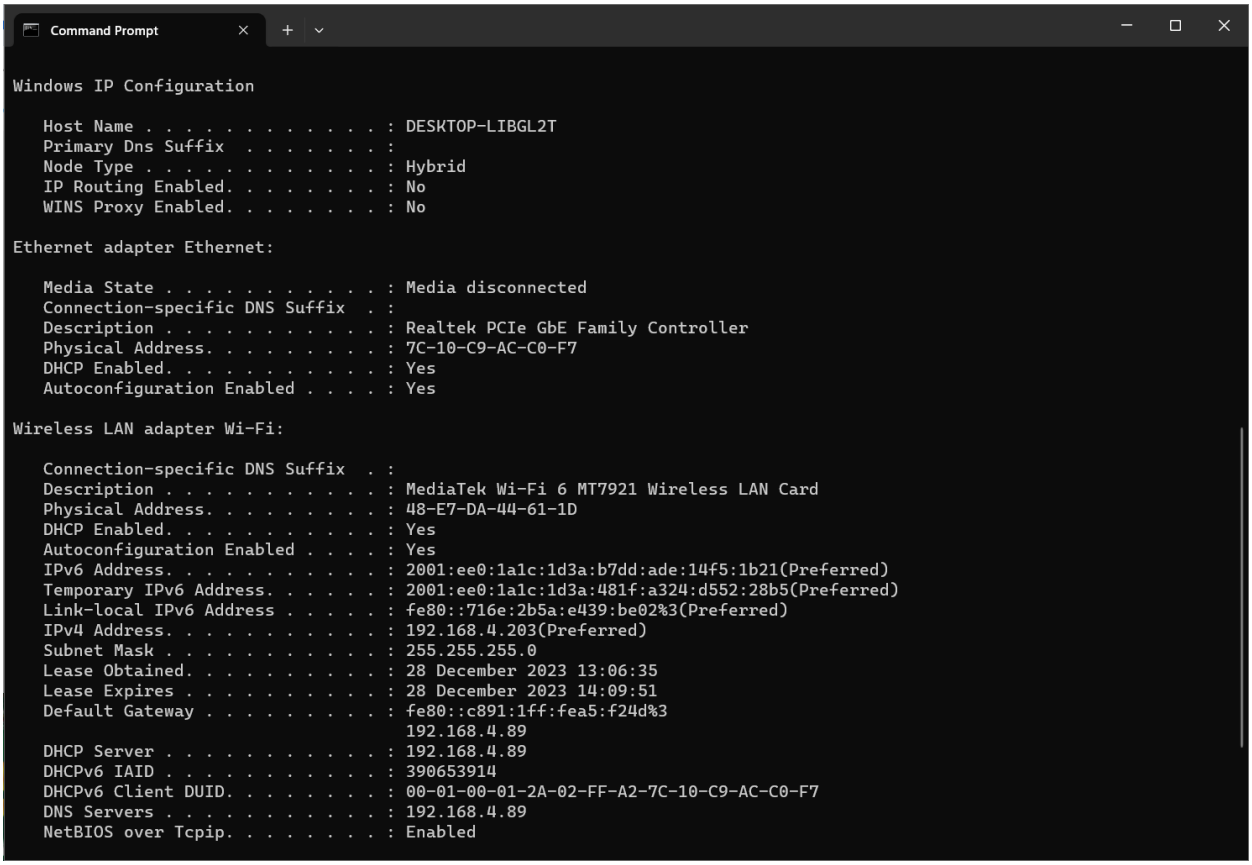
BÀI THỰC HÀNH SỐ 5:

PHÂN TÍCH HOẠT ĐỘNG CỦA GIAO THỨC DNS VÀ HTTP

Thành Viên:

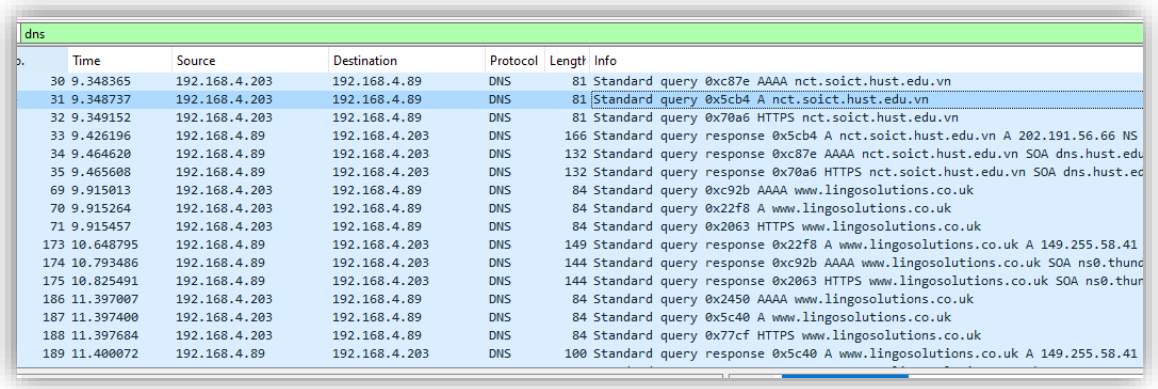
- Phan Trung Đức 20215038
- Nguyễn Gia Tùng Dương 20215023
- Dương Văn Giới 20215041
- Lê Đức Mạnh 20215086

1. **Địa chỉ Ipv4 và DNS servers của máy**



2. **Thu thập file lưu lượng**

3. Quan sát quá trình truyền dữ liệu trong DNS



dns

No.	Time	Source	Destination	Protocol	Length	Info
30	9.348365	192.168.4.203	192.168.4.89	DNS	81	Standard query 0xc87e AAAA nct.soict.hust.edu.vn
31	9.348737	192.168.4.203	192.168.4.89	DNS	81	Standard query 0x5cb4 A nct.soict.hust.edu.vn
32	9.349152	192.168.4.203	192.168.4.89	DNS	81	Standard query 0x70a6 HTTPS nct.soict.hust.edu.vn
33	9.426196	192.168.4.89	192.168.4.203	DNS	166	Standard query response 0x5cb4 A nct.soict.hust.edu.vn A 202.191.56.66 NS
34	9.464620	192.168.4.89	192.168.4.203	DNS	132	Standard query response 0xc87e AAAA nct.soict.hust.edu.vn SOA dns.hust.edu
35	9.465608	192.168.4.89	192.168.4.203	DNS	132	Standard query response 0x70a6 HTTPS nct.soict.hust.edu.vn SOA dns.hust.ed
69	9.915013	192.168.4.203	192.168.4.89	DNS	84	Standard query 0xc92b AAAA www.lingosolutions.co.uk
70	9.915264	192.168.4.203	192.168.4.89	DNS	84	Standard query 0x22f8 A www.lingosolutions.co.uk
71	9.915457	192.168.4.203	192.168.4.89	DNS	84	Standard query 0x2063 HTTPS www.lingosolutions.co.uk
173	10.648795	192.168.4.89	192.168.4.203	DNS	149	Standard query response 0x22f8 A www.lingosolutions.co.uk A 149.255.58.41
174	10.793486	192.168.4.89	192.168.4.203	DNS	144	Standard query response 0xc92b AAAA www.lingosolutions.co.uk SOA ns0.thunc
175	10.825491	192.168.4.89	192.168.4.203	DNS	144	Standard query response 0x2063 HTTPS www.lingosolutions.co.uk SOA ns0.thur
186	11.397007	192.168.4.203	192.168.4.89	DNS	84	Standard query 0x2450 AAAA www.lingosolutions.co.uk
187	11.397400	192.168.4.203	192.168.4.89	DNS	84	Standard query 0x5c40 A www.lingosolutions.co.uk
188	11.397684	192.168.4.203	192.168.4.89	DNS	84	Standard query 0x77cf HTTPS www.lingosolutions.co.uk
189	11.400072	192.168.4.89	192.168.4.203	DNS	100	Standard query response 0x5c40 A www.lingosolutions.co.uk A 149.255.58.41

Câu hỏi 1(*1 điểm*): Hãy xác định các thông tin sau trên thông điệp

- *STT gói tin(No.): 31*
- *Giao thức tầng giao vận được sử dụng để gửi thông điệp đi: UDP*
- *Địa chỉ IP nguồn: 192.168.4.203*
- *Số hiệu cổng ứng dụng nguồn: 56433*
- *Địa chỉ IP đích: 192.168.4.89*
- *Số hiệu cổng đích 53 Đây là số hiệu cổng ứng dụng của dịch vụ DNS*
- *Kiểu thông tin truy vấn(Type): A*

Qua việc xác định các thông số mạng trên máy trạm của sinh viên ở mục 3.1, cho biết thông điệp này được gửi tới DNS servers

- **Bước 3**: Tìm thông điệp DNS Response trả lời cho thông điệp yêu cầu ở bước 2 để quan sát và trả lời câu hỏi 2

Câu hỏi 2(*1 điểm*): Hãy xác định các thông tin sau trên thông điệp

- *STT gói tin(No.): 33*
- *Giao thức tầng giao vận được sử dụng để gửi thông điệp đi: UDP*
- *Địa chỉ IP nguồn: 192.168.4.89*
- *Số hiệu cổng ứng dụng nguồn: 53*
- *Địa chỉ IP đích: 192.168.4.203*
- *Số hiệu cổng đích: 56433*
- *Kiểu thông tin truy vấn(Type): A*
- *Tên miền được truy vấn: nct.soict.hust.edu.vn*

- *Địa chỉ IP của tên miền được truy vấn: 202.191.56.66*

Tại sao xác định được đây là thông điệp trả lời cho thông điệp yêu cầu ở bước 2?

Tại vì trên phần info có ghi thông tin đây là respone của query 0x5cb4 , địa chỉ nguồn và đích, số hiệu cổng nguồn và đích đảo ngược so với gói tin 31.

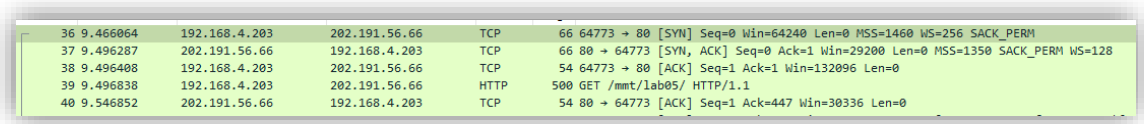
- **Bước 4:** Quan sát tất cả các thông điệp DNS và trả lời câu hỏi 3?

Câu hỏi 3(*1 điểm*): Tại sao ngoài tên miền nct.soict.hust.edu.vn được truy vấn do người dùng truy cập vào trang Web http://nct.soict.hust.edu.vn/mmt/lab05/, còn có truy vấn tới tên miền khác. Các tên miền khác được truy vấn và địa chỉ IP của các tên miền đó là gì?

-dns.hust.edu.vn : IP:202.191.57.194

-dns1.hust.edu.vn :IP:202.191.56.194

7.2.4. Quan sát quá trình truyền dữ liệu của HTTP



36	9.466064	192.168.4.203	202.191.56.66	TCP	66	64773 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
37	9.496287	202.191.56.66	192.168.4.203	TCP	66	80 → 64773 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1350 SACK_PERM WS=128
38	9.496408	192.168.4.203	202.191.56.66	TCP	54	64773 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0
39	9.496838	192.168.4.203	202.191.56.66	HTTP	500	GET /mmt/lab05/ HTTP/1.1
40	9.546852	202.191.56.66	192.168.4.203	TCP	54	80 → 64773 [ACK] Seq=1 Ack=447 Win=30336 Len=0

Câu hỏi 4(*1 điểm*): Trước khi thông điệp HTTP đầu tiên được gửi đi tới máy chủ nct.soict.hust.edu.vn, máy trạm và máy chủ đã thực hiện quá trình gì? Số thứ tự (No) của các gói tin trong quá trình đó mà sinh viên quan sát được là gì? Số hiệu cổng ứng dụng của các bên đã sử dụng là bao nhiêu? Số hiệu cổng ứng dụng trên máy chủ là cổng ứng dụng của dịch vụ nào?

Trước khi thông điệp HTTP đầu tiên được gửi đi tới máy chủ nct.soict.hust.edu.vn, máy trạm và máy chủ đã thực hiện quá trình thiết lập kết nối .

Số thứ tự : 36 37 38

Số hiệu cổng ứng dụng của các bên đã sử dụng: 80 64773

Số hiệu cổng ứng dụng trên máy chủ là cổng ứng dụng của dịch vụ HTTP

- **Bước 2:** Điền giá trị **http** vào mục Filter của Wireshark. Sinh viên sẽ quan sát thấy các gói tin HTTP mà máy trạm đã trao đổi trên mạng.
- **Bước 3:** Quan sát các thông điệp HTTP trao đổi giữa máy trạm và máy chủ Web nct.soict.hust.edu.vn và trả lời câu hỏi 5

Câu hỏi 5(2 *điểm*): Có bao nhiêu thông điệp HTTP Request được gửi đi? Liệt kê các thông tin sau về các thông điệp HTTP giữa máy trạm và máy chủ Web nct.soict.hust.edu.vn

HTTP Request			HTTP Response		
No.	Phương thức yêu cầu	Đối tượng yêu cầu	No.	Mã trả lời	Ý nghĩa mã trả lời
39	GET	/mmt/lab05/	53	200 OK	Request được tiếp nhận và xử lý thành công
57	GET	/mmt/lab05/en.jpg	60	200 OK	Request được tiếp nhận và xử lý thành công
64	GET	/mmt/lab05/vi.jpg	67	200 OK	Request được tiếp nhận và xử lý thành công
72	GET	/mmt/lab05/http_request.png	168	200 OK	Request được tiếp nhận và xử lý thành công
73	GET	/web1.jpg	75	404 Not found	Không tìm thấy tài nguyên
80	GET	/web2.jpg	95	404 Not found	Không tìm thấy tài nguyên

Trong các thông điệp HTTP Request, có những thông điệp nào được gửi đi liên tiếp mà không đợi thông điệp trả lời từ máy chủ không? Nếu có, tại sao trình duyệt Web trên máy trạm thực hiện như vậy?

Tất cả đều sử dụng phương thức HTTP 1.1
Dòng 39: Máy trạm gửi yêu cầu GET để lấy trang web "/mmt/lab05/".
Dòng 57: Ngay sau đó, máy trạm gửi yêu cầu GET để lấy hình ảnh "/mmt/lab05/en.jpg".
Dòng 64: Tiếp theo, máy trạm gửi yêu cầu GET để lấy hình ảnh "/mmt/lab05/vi.jpg".
Dòng 72: Máy trạm gửi yêu cầu GET để lấy hình ảnh "/mmt/lab05/http_request.png".
Dòng 73: Ngay sau đó, máy trạm gửi yêu cầu GET để lấy hình ảnh "/web1.jpg".
Dòng 80: Máy trạm gửi yêu cầu GET để lấy hình ảnh "/web2.jpg".
Tổng cộng, các yêu cầu này được gửi một cách liên tục mà không đợi phản hồi từ máy chủ cho mỗi yêu cầu riêng lẻ. Điều này giúp tối ưu hóa sử dụng băng thông và giảm độ trễ trên mạng.

- **Bước 4**: Chọn thông điệp HTTP Request đầu tiên được máy trạm gửi cho máy chủ Web nct.hust.edu.vn và trả lời câu hỏi 6.

Câu hỏi 6(*1 điểm*): Hãy cho biết các thông tin sau về thông điệp yêu cầu:

- *Giao thức tầng giao vận được sử dụng để truyền thông điệp :TCP*
- *Số hiệu cổng ứng dụng đích :80*
- *Phiên bản của giao thức HTTP mà máy trạm sử dụng :HTTP 1.1*
- *Giá trị của trường Connection trong tiêu đề HTTP : keep-alive\r\n*

- **Bước 5:** Tìm thông điệp HTTP Response mà máy chủ Web trả lời cho thông điệp yêu cầu ở bước 5 và trả lời câu hỏi 7

Câu hỏi 7(*1 điểm*): Hãy cho biết các thông tin sau về thông điệp trả lời:

- *Phiên bản của giao thức HTTP mà máy chủ sử dụng :HTTP 1.1*
- *Giá trị của trường Connection trong tiêu đề HTTP : Keep-Alive\r\n*
- *Phần thân chứa dữ liệu :Text Dữ liệu này có kích thước là :22017 bytes - Thông điệp này đóng gói trong 9 gói tin TCP*

Sau khi thông điệp này được gửi đi, kết nối TCP vẫn duy trì

Câu hỏi 8(*1 điểm*): Ngoài quá trình trao đổi dữ liệu với máy chủ Web nct.soict.hust.edu.vn, máy trạm còn gửi thông điệp HTTP Request tới máy chủ Web có tên miền và địa chỉ IP là gì? Tại sao máy trạm phát đi thông điệp này? *(Gợi ý: Xem lại nội dung trong phần thân của thông điệp HTTP Response trong bước 5)*

Xem phần tiêu đề của thông điệp HTTP Request trên và cho biết giá trị trường **Referer** là gì?

Tên miền : www.lingosolutions.co.uk IP:149.255.58.41

Máy phát thông điệp này bởi vì trong phần dữ liệu của web có nguồn của ảnh

\t\t\t
<img src="http://www.lingosolutions.co.uk/wp-content/uploads/2016/05/HTTP-wallpaper.jpg" width = "320">\r\n

Referer: http://nct.soict.hust.edu.vn

Câu hỏi 9(*1 điểm*): Đoạn sau đây mô tả ngắn gọn quá trình xử lý truy cập vào một trang Web trên trình duyệt Web. Hãy điền vào chỗ trống cụm từ còn thiếu

Khi nhận được yêu cầu truy cập vào một trang Web nào đó qua địa chỉ URL, nếu chưa biết địa chỉ IP của máy chủ Web. Trình duyệt gửi thông điệp……DNS……tới ……máy chủ DNS…… Trong thông điệp……DNS…….. trả lời nhận được, trình duyệt xác định được địa chỉ IP của máy chủ Web. Sau đó, trình duyệt gửi yêu cầu để thiết lập……kết nối TCP…… với máy chủ Web. Trên……kết nối TCP……..đã được thiết lập, trình duyệt gửi đi thông điệp ……HTTP GET……..để yêu cầu nội dung của trang Web. Máy chủ Web tìm kiếm nội dung được yêu cầu và trả lại thông điệp……HTTP…… cùng với mã trả lời……200 OK….. nếu tìm thấy, hoặc mã……40 Not Found….. nếu không tìm thấy. Nếu hai bên sử dụng giao thức HTTP có phiên bản…persistent…….. thì liên kết sẽ được duy trì cho tới khi trình duyệt đã tải xong nội dung trang Web từ máy chủ.