

Mạng máy tính căn bản

Bài thực hành số 04

DNS, HTTP với Wireshark

Họ tên:

MSSV: Nhóm:

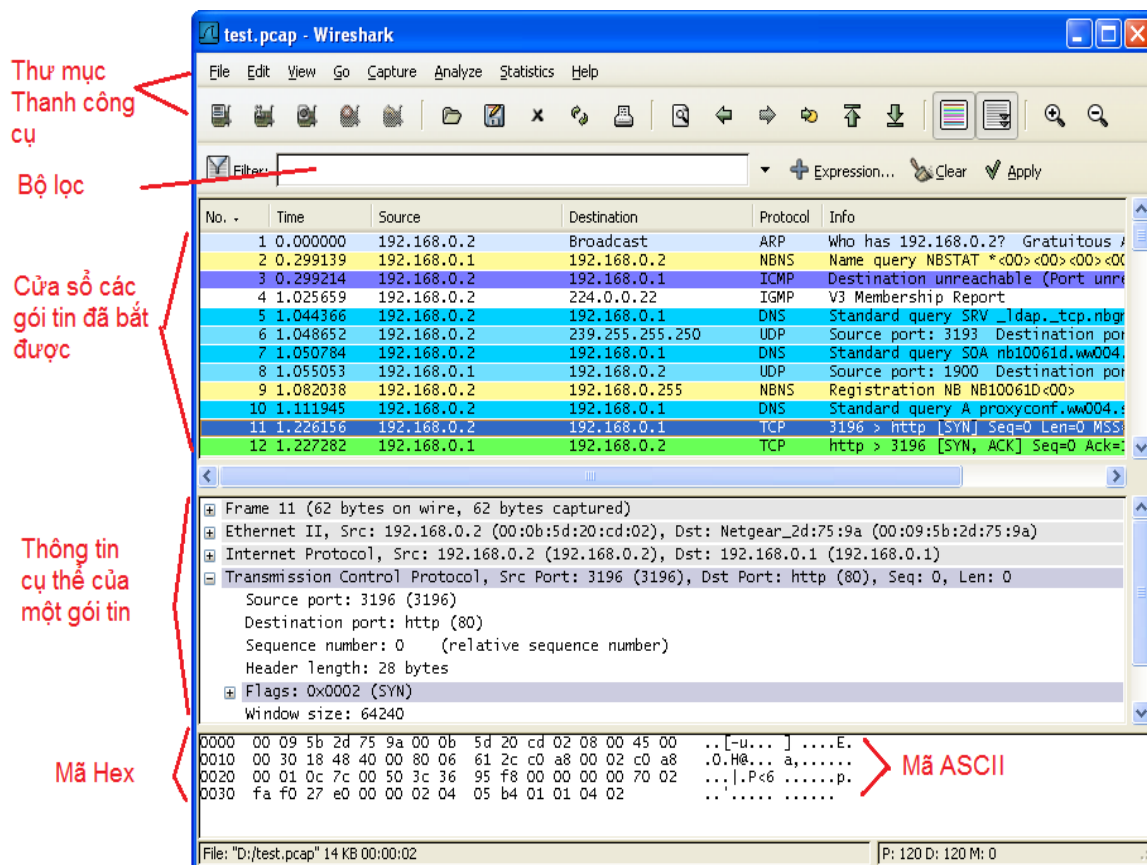
I. Mục tiêu

1. Tổng quan về Wireshark
2. Thực hành bắt gói tin thực tế
3. Phân tích gói tin HTTP và DNS

II. Nội dung

1. Tổng quan về Wireshark

Wireshark là một công cụ phân tích mạng, chức năng chính là để bắt các gói tin mạng và hiển thị dữ liệu gói tin càng chi tiết càng tốt.



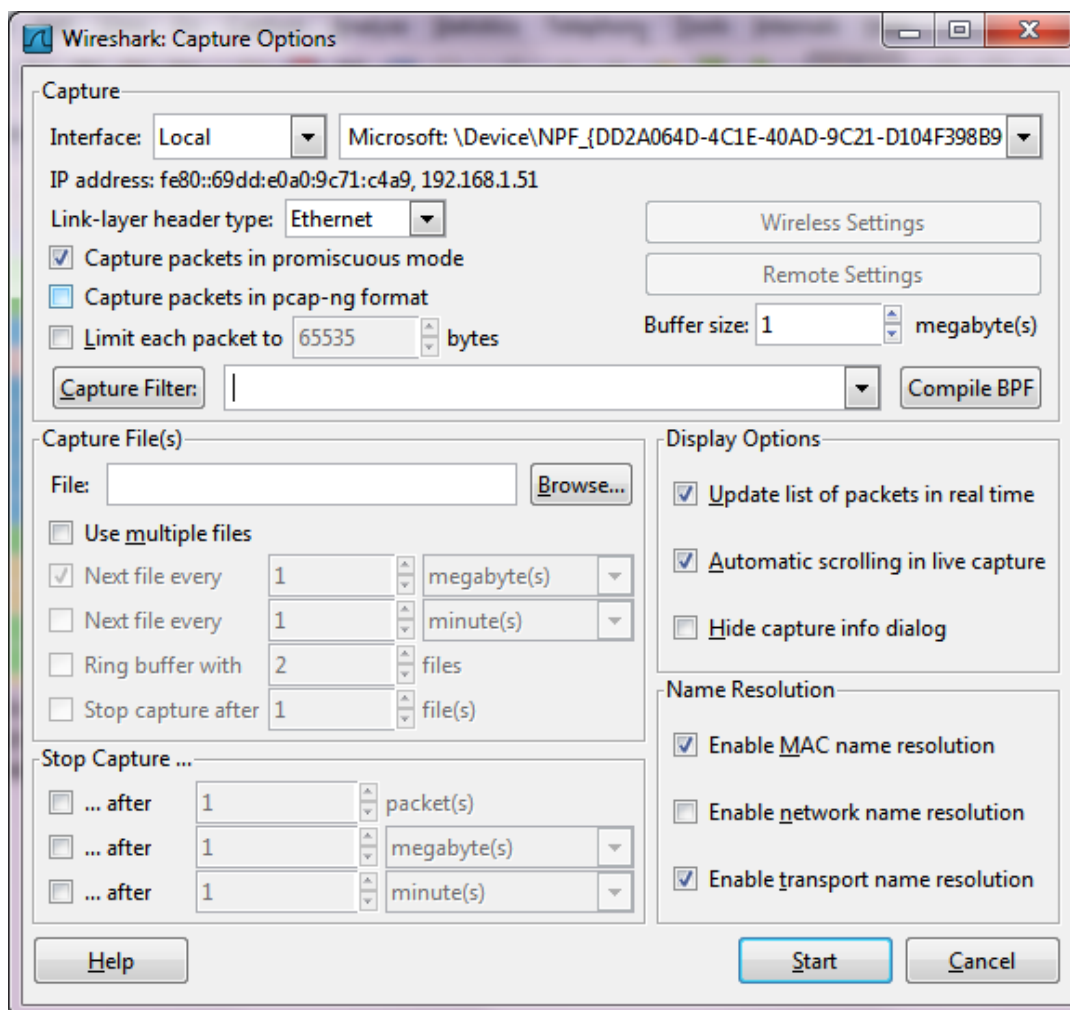
Hình 1. Giao diện của Wireshark.

- Các menu lệnh trình đơn bao gồm tất cả các tác vụ của chương trình. Chúng ta hiện tại sẽ sử dụng hai menu chính là File và Capture. Menu File cho phép bạn lưu dữ liệu gói tin bắt được hoặc mở một tập tin cùng loại, và thoát khỏi ứng dụng Wireshark. Các menu Capture cho phép bạn bắt đầu bắt các gói tin.
- Cửa sổ danh sách-gói tin hiển thị một bản tóm tắt một dòng cho mỗi gói tin bị bắt, bao gồm cả số gói tin được đánh số bởi Wireshark, thời gian mà gói tin bị bắt, địa chỉ nguồn và đích của gói, loại giao thức, và thông tin của giao thức cụ thể chứa trong gói tin. Danh sách-gói tin có thể được sắp xếp theo các thông số này bằng cách nhấn vào tên cột. Trường loại giao thức hiển thị giao thức ở tầng cao nhất mà gửi hoặc nhận gói tin này.
- Cửa sổ chi tiết mào đầu cung cấp các thông tin chi tiết về các gói tin được lựa chọn trong cửa sổ danh sách gói. (Để lựa chọn một gói dữ liệu trong cửa sổ danh sách gói, đặt con trỏ trên một dòng tóm tắt của gói tin trong cửa sổ danh sách gói và nhấn nút chuột trái.). Những chi tiết này bao gồm thông tin về các khung Ethernet (giả sử gói đã được gửi / nhận qua một giao diện Ethernet) và IP datagram có chứa gói tin này. Số lượng chi tiết hiển thị của Ethernet và lớp IP có thể được mở rộng hoặc giảm thiểu bằng cách nhấn vào các ô trừ cộng bên trái của khung Ethernet hoặc dòng gói tin IP trong cửa sổ chi tiết gói. Nếu gói dữ liệu đã được sử dụng giao thức TCP hoặc UDP, chi tiết TCP hoặc UDP cũng sẽ được hiển thị bằng cách mở rộng. Cuối cùng, thông tin chi tiết về giao thức tầng cao nhất gửi hoặc nhận gói tin này cũng được cung cấp.
- Cửa sổ nội dung gói tin hiển thị toàn bộ nội dung của khung bắt được ở cả hai định dạng ASCII và hệ thập lục phân.

3. Thực hành bắt gói tin thực tế

3.1 Bắt đầu bắt gói

- Khởi động trình duyệt web ưa thích của bạn.
- Khởi động phần mềm Wireshark.
 - Để bắt đầu bắt gói dữ liệu, chọn Capture menu sổ xuống và chọn Options. Cửa sổ "Wireshark: Capture Options" sẽ được hiển thị, như trong hình 2.

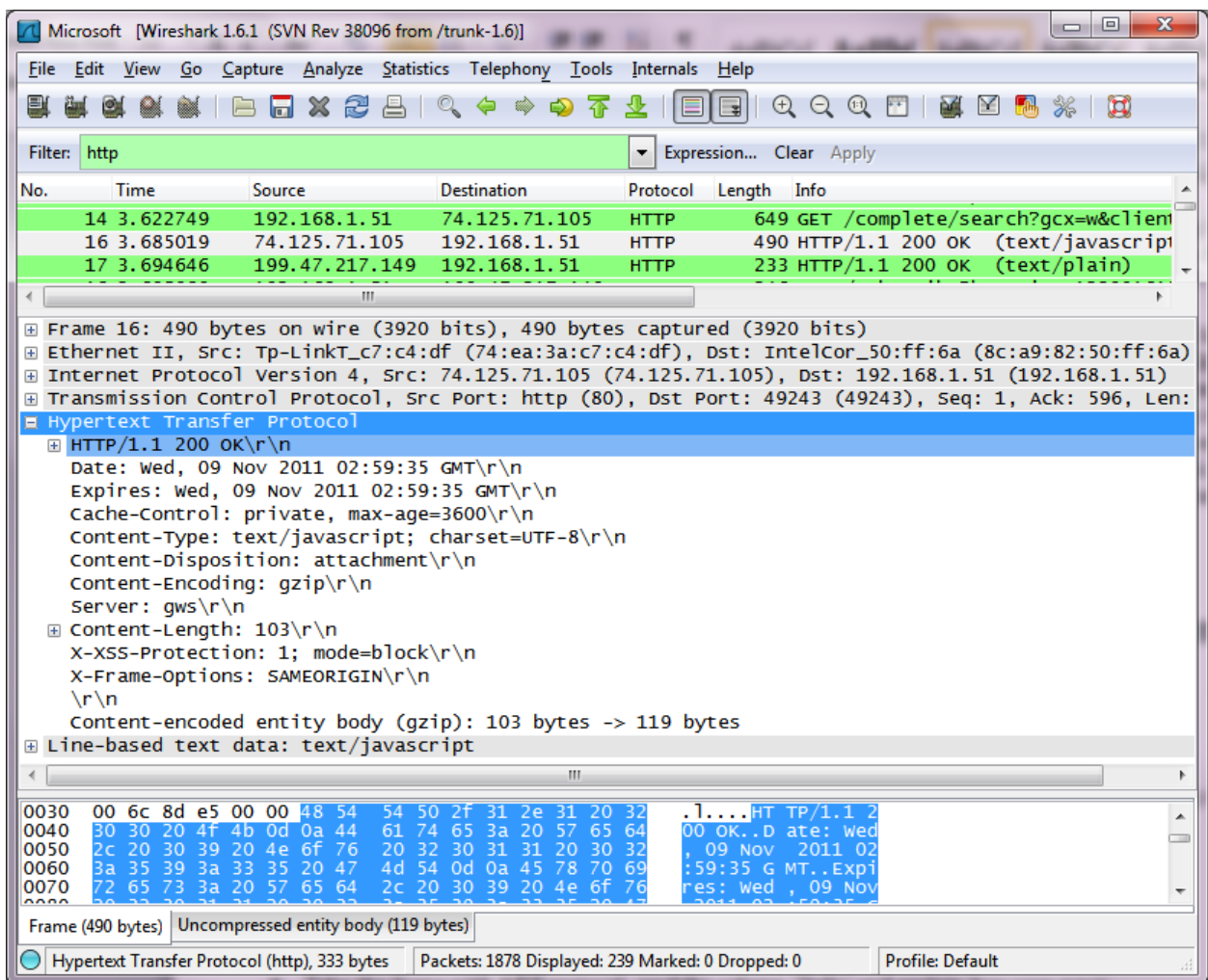


Hình 2. Lựa chọn giao diện mạng.

- Bạn có thể sử dụng hầu hết các giá trị mặc định trong cửa sổ này, nhưng bỏ chọn "Hide thoại nắm bắt thông tin" theo xếp. Các giao diện mạng (tức là, các kết nối vật lý) mà máy tính của bạn sử dụng để kết nối vào mạng sẽ được hiển thị trong giao diện trình đơn thả xuống ở phía trên cùng của cửa sổ Capture Options. Trong trường hợp máy tính của bạn có nhiều hơn một giao diện mạng hoạt động (ví dụ, nếu bạn có cả kết nối không dây và một kết nối Ethernet), bạn sẽ cần phải chọn một giao diện đang được sử dụng để gửi và nhận các gói tin. Sau khi chọn giao diện mạng (hoặc sử dụng giao diện mặc định được lựa chọn bởi Wireshark), nhấn Start. Quá trình bắt gói bây giờ sẽ bắt đầu - tất cả các gói tin được gửi / nhận từ máy tính của bạn đang được bắt bởi Wireshark!
- Trong khi Wireshark đang chạy, nhập URL: <http://cse.hcmut.edu.vn> và chờ trang đó hiển thị đầy đủ trong trình duyệt của bạn. Để hiển thị trang này, trình duyệt của bạn sẽ liên lạc với máy chủ HTTP và trao đổi với máy chủ để tải trang này. Các khung Ethernet có chứa các thông điệp HTTP sẽ được bắt bởi Wireshark.
- Sau khi trình duyệt của bạn đã hiển thị trang chủ của Khoa KH & KT Máy Tính, ngừng quá trình bắt gói tin Wireshark bằng cách chọn Stop ở cửa sổ thông tin bắt gói. Điều này sẽ làm cho cửa sổ Wireshark capture biến mất và cửa sổ chính của Wireshark sẽ hiển thị tất cả các gói tin bắt được. Cửa sổ chính của Wireshark nên bây giờ trông tương tự như hình 1. Bây giờ

bạn có các gói dữ liệu thực tế chứa tất cả các thông điệp giao thức được trao đổi giữa máy tính của bạn và các thực thể mạng khác! HTTP trao đổi thông điệp với máy chủ cse.hcmut.edu.vn sẽ xuất hiện một nơi nào đó trong danh sách các gói đã được bắt. Nhưng sẽ có nhiều loại khác của các gói tin cũng hiển thị (ví dụ như, các loại giao thức khác nhau được hiển thị trong cột Protocol trong hình 1). Mặc dù hành động duy nhất bạn là tải về một trang web, có rõ ràng nhiều giao thức khác chạy trên máy tính của bạn mà người sử dụng không nhìn thấy.

- Gõ "http" (không có dấu ngoặc kép, và trong trường hợp thấp hơn - tất cả các tên giao thức trong trường hợp thấp hơn trong Wireshark) vào bộ lọc ở phía trên cùng của cửa sổ chính của Wireshark. Sau đó chọn Apply (ở bên phải của nơi mà bạn đã nhập vào "http"). Điều này sẽ dẫn tới chỉ có tin nhắn HTTP được hiển thị trong cửa sổ danh sách-gói tin.
- Chọn thông điệp http đầu tiên được hiển thị trong cửa sổ danh sách gói tin. Thông điệp này phải là "GET HTTP" đã được gửi từ máy tính của bạn đến máy chủ HTTP. Khi bạn chọn thông điệp "HTTP GET" thì khung Ethernet, IP datagram, đoạn TCP, và thông tin tiêu đề thông điệp HTTP sẽ được hiển thị trong cửa sổ Packet-Header. Mở rộng hiển thị thông tin về giao thức HTTP. Wireshark bây giờ sẽ hiển thị gần như trong hình 4.



Hình 4. Thông điệp HTTP trong WireShark.

4. HTTP trong WireShark

Câu hỏi:

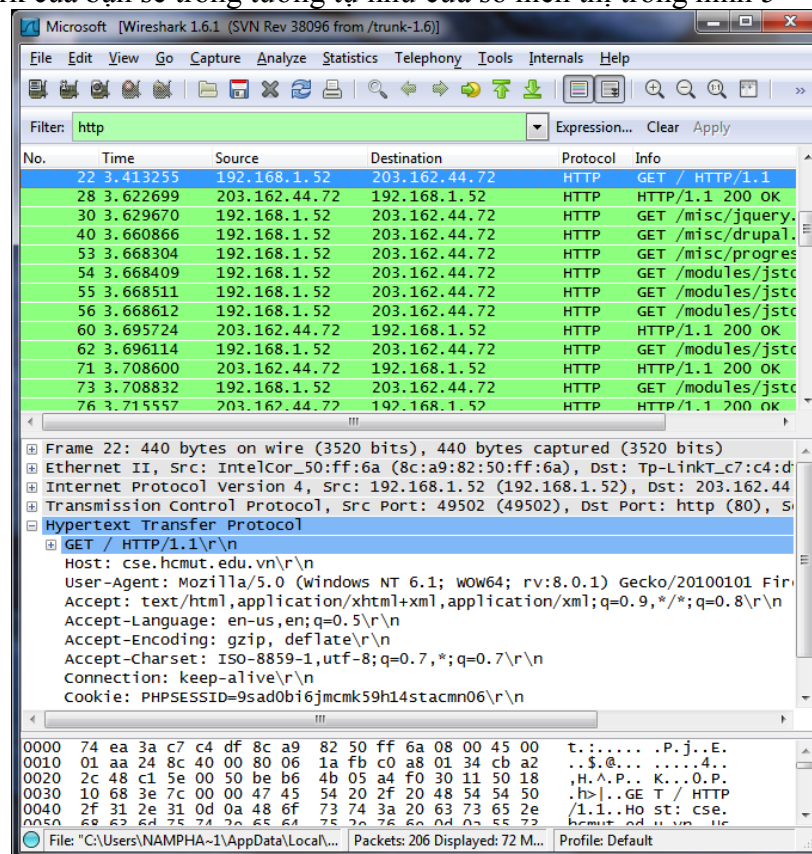
1. HTTP là gì?

4.1 Tương tác bắt gói tin HTTP GET

Hãy bắt đầu tìm hiểu HTTP bằng cách tải về một tập tin HTML đơn giản - một tập tin rất ngắn, và không chứa các đối tượng nhúng. Làm như sau:

1. Khởi động trình duyệt web của bạn.
2. Khởi động Wireshark, như mô tả trong lab trước (nhưng chưa bắt đầu bắt các gói tin). Nhập "http" (không gồm dấu nháy kép) trong cửa sổ bộ lọc-hiển thị, do đó chỉ những thông điệp HTTP sẽ được hiển thị trong cửa sổ danh sách gói. (Chúng ta chỉ quan tâm đến giao thức HTTP ở đây, và không muốn nhìn thấy tất cả các gói tin).
3. Bắt đầu bắt gói tin bằng Wireshark.
4. Nhập địa chỉ sau đây vào trình duyệt của bạn <http://cse.hcmut.edu.vn>
5. Ngừng bắt gói tin Wireshark.

Cửa sổ Wireshark của bạn sẽ trông tương tự như cửa sổ hiển thị trong hình 5



Hình 5: Hiển thị của Wireshark sau khi truy cập <http://cse.hcmut.edu.vn>

Tìm hiểu gói tin HTTP và trả lời các câu hỏi sau:

1. Phiên bản HTTP được sử dụng trong HTTP?
2. Địa chỉ IP, cổng được sử dụng trong giao tiếp của một gói tin HTTP hiện tại trong a máy tính của bạn là gì?
3. Địa chỉ IP, cổng được sử dụng trong giao tiếp của gói tin HTTP của máy chủ <http://cse.hcmut.edu.vn>?
4. Các mã trạng thái trả về từ máy chủ cho trình duyệt của bạn là gì?
5. Có bao nhiêu byte nội dung sẽ được trả lại cho trình duyệt của bạn?

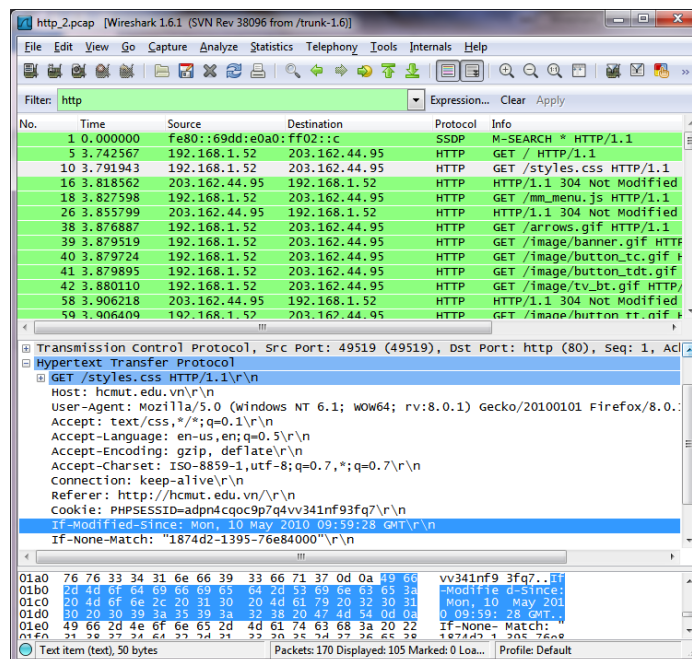
4.2 Tương tác bắt gói tin HTTP GET có điều kiện

Các trình duyệt hầu hết các web thực hiện bộ nhớ đệm đối tượng và do đó thực hiện một điều kiện GET khi lấy một đối tượng HTTP. Do đó trước khi thực hiện các bước dưới đây phải xóa thông tin trong cache của trình duyệt (xóa thông tin cache trong trình duyệt của bạn trong trường hợp này).

Bây giờ làm như sau:

1. Khởi động trình duyệt web của bạn, và chắc chắn rằng bộ nhớ cache của trình duyệt của bạn được xóa bỏ, như thảo luận ở trên.
2. Khởi động Wireshark
3. Nhập URL sau vào trình duyệt của bạn <http://cse.hcmut.edu.vn>
4. Nhanh chóng nhập địa chỉ URL vào trình duyệt của bạn một lần nữa (hoặc chỉ đơn giản là chọn nút làm mới trên trình duyệt của bạn)

Ngừng bắt gói tin Wireshark, và nhập vào "http" trong khung bộ lọc, theo đó, chỉ những thông điệp HTTP sẽ được hiển thị trong cửa sổ danh sách gói tin. Lúc đó cửa sổ Wireshark của bạn sẽ trông tương tự như cửa sổ hiển thị trong hình 6.



Hình 6: cửa sổ Wireshark khi truy cập vào <http://cse.hcmut.edu.vn> lần thứ 6



Tìm hiểu gói tin HTTP và trả lời các câu hỏi sau:

- Ở lần truy cập thứ nhất:
 1. Kiểm tra các nội dung của truy vấn HTTP GET đầu tiên từ trình duyệt của bạn tới máy chủ. Chỉ ra nội dung trong trường dữ liệu “MODIFIED-SINCE” (nếu có) trong dòng HTTP GET?
 2. Xác định nội dung phản hồi của máy chủ tương ứng với yêu cầu ở câu 1.
- Ở lần truy cập thứ 2:
 3. Xác định nội dung của các truy vấn HTTP GET thứ hai từ trình duyệt của bạn tới máy chủ. Chỉ ra nội dung trong trường dữ liệu “MODIFIED-SINCE” (nếu có) trong dòng HTTP GET?
 4. Các mã trạng thái HTTP và cụm từ trả về từ máy chủ để phản hồi cho HTTP GET thứ hai này là gì? Máy chủ có trả lại một cách toàn vẹn nội dung của tập tin? Giải thích.

5. DNS

Câu hỏi:

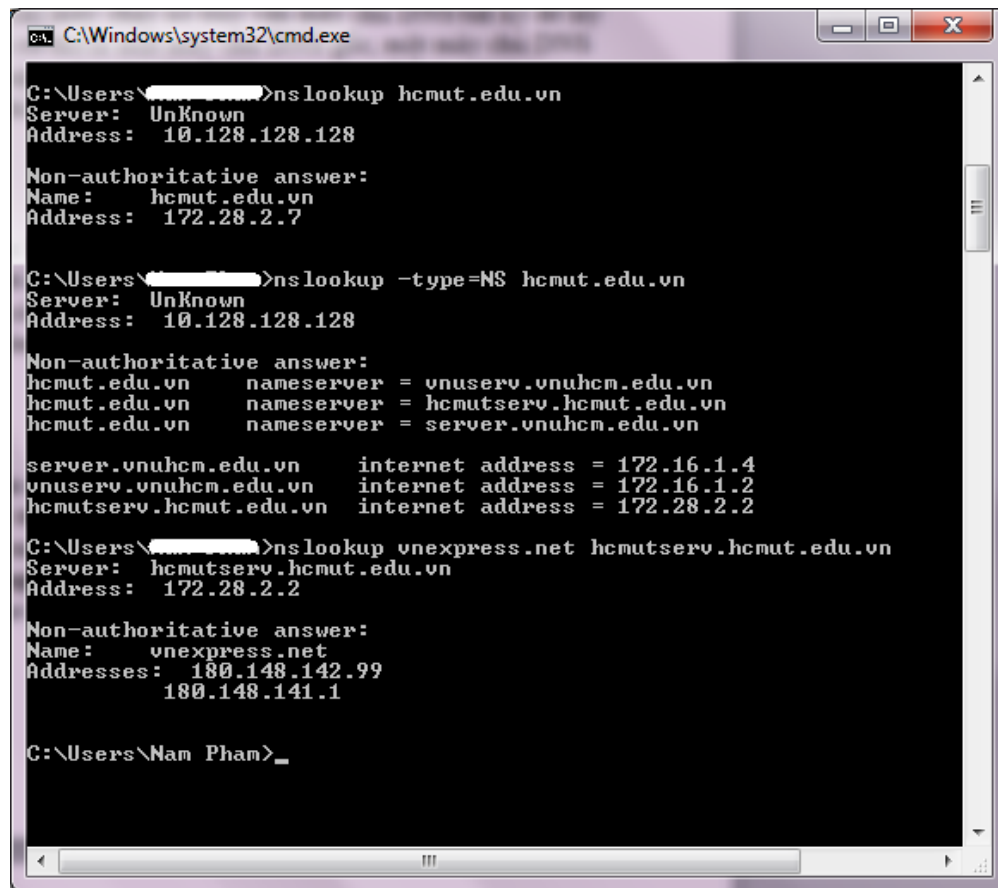
DNS là gì? Vai trò của DNS

5.1. Sử dụng lệnh nslookup để xem thông tin về DNS

Lệnh nslookup được học ở bài thực hành các lệnh cơ bản trong mạng

Câu hỏi:

Chức năng của lệnh nslookup?



```
C:\Windows\system32\cmd.exe

C:\Users\Nam Phan>nslookup hcmut.edu.vn
Server: UnKnown
Address: 10.128.128.128

Non-authoritative answer:
Name: hcmut.edu.vn
Address: 172.28.2.7

C:\Users\Nam Phan>nslookup -type=NS hcmut.edu.vn
Server: UnKnown
Address: 10.128.128.128

Non-authoritative answer:
hcmut.edu.vn nameserver = vnuser.vnuhcm.edu.vn
hcmut.edu.vn nameserver = hcmutserv.hcmut.edu.vn
hcmut.edu.vn nameserver = server.vnuhcm.edu.vn

server.vnuhcm.edu.vn internet address = 172.16.1.4
vnuser.vnuhcm.edu.vn internet address = 172.16.1.2
hcmutserv.hcmut.edu.vn internet address = 172.28.2.2

C:\Users\Nam Phan>nslookup vnexpress.net hcmutserv.hcmut.edu.vn
Server: hcmutserv.hcmut.edu.vn
Address: 172.28.2.2

Non-authoritative answer:
Name: vnexpress.net
Addresses: 180.148.142.99
          180.148.141.1

C:\Users\Nam Phan>
```

Hình 7. Kết quả chạy các lệnh nslookup

Ở hình 7 lệnh thứ nhất: **nslookup hcmut.edu.vn**

Kết quả của ba lệnh **nslookup** độc lập (Hiện thị trong Windows Command Prompt). Trong ví dụ này, máy của người dùng sử dụng máy chủ DNS mặc định là **10.128.128.128**. Khi chạy **nslookup**, nếu không có máy chủ DNS được chỉ định cụ thể, thì nslookup sẽ gửi truy vấn đến máy chủ DNS mặc định, trong trường hợp này là **10.128.128.128**. nslookup hcmut.edu.vn

Ở hình 7 lệnh thứ hai: **nslookup -type=NS hcmut.edu.vn**

Chúng ta đã cung cấp tùy chọn "-type=NS" và tên miền " hcmut.edu.vn". Điều này khiến **nslookup** gửi một truy vấn cho một thẻ ghi loại NS đến máy chủ DNS địa phương mặc định. Nói cách khác, truy vấn đang nói, "xin vui lòng gửi cho tôi tên máy chủ DNS có thẩm quyền của hcmut.edu.vn". (Khi tùy chọn loại không được sử dụng, nslookup sử dụng mặc định, thẻ ghi loại A). Câu trả lời, hiển thị trong hình trên, đầu tiên chỉ ra máy chủ DNS cung cấp câu trả lời (máy chủ DNS địa phương mặc định) cùng với ba máy chủ tên miền (NS) của hcmut.edu.vn. Mỗi máy chủ này là một máy chủ DNS có thẩm quyền cho các máy chủ trong khuôn viên HCMUT. Tuy nhiên, **nslookup** cũng chỉ ra rằng câu trả lời là "Không có thẩm quyền" (non-authorative), có nghĩa là câu trả lời này đến từ bộ nhớ cache của một số máy chủ trung gian thay vì từ một máy chủ DNS HCMUT có thẩm quyền.

Ở hình 7 lệnh thứ ba: **nslookup vnexpress.net hcmutserv.hcmut.edu.vn**



Chúng ta chỉ ra rằng chúng ta muốn truy vấn được gửi đến máy chủ DNS **hcmutserv.hcmut.edu.vn** thay vì máy chủ DNS mặc định (**10.128.128.128**). Vì vậy, các tương tác truy vấn phản hồi diễn ra trực tiếp giữa máy chủ của chúng ta và **hcmutserv.hcmut.edu.vn**. Trong ví dụ này, máy chủ DNS **vnuserv.vnuhcm.edu.vn** cung cấp địa chỉ IP của máy chủ **vnexpress.net**, là một máy chủ web tin tức.

Câu hỏi:

1. Chạy lệnh nslookup này để có được địa chỉ IP của một máy chủ ở Việt Nam.
2. Chạy lệnh nslookup để xác định máy chủ DNS có thẩm quyền cho một trường đại học ở Châu Âu.
3. Chạy lệnh nslookup sử dụng một trong các máy chủ DNS có được trong Câu hỏi 2 để tìm máy chủ mail cho Gmail Mail (www.gmail.com).

5.2 DNS với Wireshark

Bắt các gói tin DNS được tạo ra bởi hoạt động lướt Web bình thường. Xóa DNS trong máy tính sử dụng lên trong window và xóa cache trình duyệt.

- Xem DNS: ipconfig /displaydns
- Xóa DNS: ipconfig /flushdns
- Xóa bộ nhớ cache trong trình duyệt

Mở Wireshark và nhập "ip.addr == IP_address" vào bộ lọc, Bộ lọc này loại bỏ tất cả các gói không xuất phát từ hoặc là không gửi tới máy của bạn.

- Bắt đầu bắt gói tin trong Wireshark.
- Mở trình duyệt của bạn, hãy truy cập trang web: <http://aao.hcmut.edu.vn>
- Ngừng bắt gói.

Nếu bạn không thể chạy Wireshark trên một kết nối mạng trực tiếp, bạn có thể tải về một gói các tập tin đã bị bắt khi thực hiện các bước ở trên.

Câu hỏi:

1. Xác định các truy vấn DNS và các thông điệp trả lời. Chúng được gửi qua UDP hay TCP?
2. Cổng đích của các truy vấn DNS là gì? Cổng nguồn của thông điệp phản hồi DNS là gì?
3. Truy vấn DNS gửi tới địa chỉ IP nào? Sử dụng ipconfig để xác định địa chỉ IP của máy chủ DNS địa phương của bạn. Có phải hai địa chỉ IP này giống nhau?
4. Thông điệp truy vấn DNS. Loại (Type) của DNS truy vấn là gì?
5. Xem xét thông điệp trả lời DNS. Có bao nhiêu "câu trả lời" được cung cấp? Mỗi câu trả lời chứa thông tin gì?