1

Lab

**BÁO CÁO BÀI THỰC HÀNH SỐ 1**

**[Làm quen với Wireshark]**

**Môn học: NHẬP MÔN MẠNG MÁY TÍNH**

|  |  |
| --- | --- |
| **Sinh viên thực hiện** | Nguyễn Hải Thiện (23521481) |
| **Thời gian thực hiện** | 17/09/2024 – 24/09/2024 |
| **Số câu đã hoàn thành** | 14/14 |

**TRẢ LỜI CÁC CÂU HỎI**

**Gợi ý:** *Trả lời câu hỏi đúng, đầy đủ, cần giải thích lý do tại sao có được đáp án, có các hình ảnh, bằng chứng để chứng minh tính đúng đắn.*

*Câu 1. Tổng thời gian bắt gói tin đối với website đã thử nghiệm và tổng số gói tin bắt*

*được là bao nhiêu?*

***Trả lời:*** *Tổng thời gian bắt gói tin đối với website thử nghiệm là 9.422814  giây. Tổng số gói tin bắt được là 116.*

***Minh chứng:***

* **Thời gian bắt gói tin**: xem ở cột Time ở dòng packet số 116 (packet cuối cùng)



* **Số lượng gói tin tổng cộng** được hiển thị ở **góc dưới bên trái** của cửa sổ Wireshark, trong thanh trạng thái.



*Câu 2. Trong các gói tin bắt được, có tổng cộng bao nhiêu gói tin HTTP?*

***Trả lời:*** *4*

***Minh chứng:***

Trong thanh **Display Filter** của Wireshark, nhập: http. Ở **góc dưới bên phải** của Wireshark sẽ xuất hiện số lượng gói tin đã lọc được, hiển thị dưới dạng **Displayed**

*Câu 3. Liệt kê ít nhất* ***5 giao thức khác nhau*** *xuất hiện trong cột giao thức (Protocol) khi không áp dụng bộ lọc “http” khi truy cập website. Tìm hiểu trên Internet và mô tả*

*ngắn gọn chức năng chính của các giao thức đó.*

***Trả lời:*** *ARP, TCP, DNS, UDP, HTTP, SSDP, TLSv1.2*

***Minh chứng:***

Để xem các giao thức khác nhau, ta sẽ kiểm tra các giao thức trong cột **Protocol**

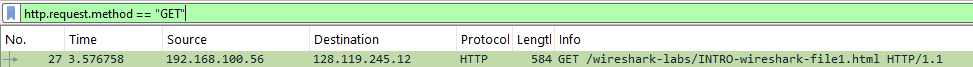
A close up of a text

Description automatically generated with medium confidence



*Câu 4. Xác định gói tin HTTP GET đầu tiên gửi đến website đã thử nghiệm. Cho biết gói tin này cơ bản dùng để làm gì?*

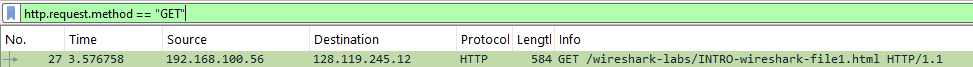
***Trả lời:*** *Gói tin HTTP GET đầu tiên*

**

*Gói tin HTTP GET này được sử dụng để yêu cầu máy chủ cung cấp tài nguyên cụ thể (một tệp HTML) để hiển thị hoặc xử lý thêm ở phía người dùng.*

***Minh chứng:***

Để xem gói tin HTTP GET đầu tiên, chúng ta sử dụng bộ lọc **http.request.method == "GET"** để lọc ra các gói tin sử dụng phương thức HTTP GET.



*Câu 5. Xác định gói tin phản hồi của gói tin HTTP GET ở câu 4, thông tin nào xác định*

*điều đó?*

***Trả lời:***

**

**

*Thông tin xác định được điều này là do địa chỉ IP Source và địa chỉ IP Destination của gói tin này ngược với gói tin HTTP GET ở câu 4.*

***Minh chứng:***

* Tìm gói tin phản hồi bằng cách sử dụng bộ lọc **http.response** trong **Wireshark** để lọc ra các gói tin phản hồi HTTP.

A screenshot of a computer

Description automatically generated

* Và địa chỉ IP Source và địa chỉ IP Destination của gói tin này ngược với gói tin HTTP GET ở câu 4 nên xác định được rằng đây chính là gói tin phản hồi của gói tin HTTP GET ở câu 4*.*

*A screenshot of a computer

Description automatically generated*

*Câu 6. Tính thời gian từ khi gói tin* ***HTTP GET*** *đầu tiên được gửi cho đến khi có gói tin*

*phản hồi* ***HTTP 200 OK*** *đối với website đã thử nghiệm. (mặc định, giá trị của cột*

*thời gian (Time) trong packet-listing window là khoảng thời gian tính bằng giây kể*

*từ khi chương trình Wireshark bắt đầu bắt gói tin)*

***Trả lời:*** *0.255703 giây.*

***Minh chứng:***

Tính thời gian phản hồi:

* Gói tin HTTP GET được gửi lúc 3.576758 giây.
* Gói tin phản hồi HTTP 304 Not Modified được nhận lúc 3.832461 giây.

=>Thời gian phản hồi = 3.576758 − 3.832461 = *0.255703*giây



*Câu 7. 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 hay không? Nếu có, hãy tìm và xác định vị trí của nội dung này trong các gói tin bắt được.*

***Trả lời:***Có. Vị trí nằm trong phần **"Line-based text data"** trong phần chi tiết của gói tin.

***Minh chứng:***

* Bước 1: tìm các gói tin **HTTP** có mã phản hồi **200 OK**.



* Bước 2: Xem nội dung HTML trong phần "Line-based text data".

A screenshot of a computer

Description automatically generated

*Câu 8. Hãy tìm hiểu về định dạng của địa chỉ IP và thử phỏng đoán địa chỉ IP của*

***gaia.cs.umass.edu*** *là gì? Địa chỉ IP của máy tính đang sử dụng là gì?*

***Trả lời:***

* *Địa chỉ IP (Internet Protocol) là một chuỗi số được sử dụng để định danh các thiết bị trên mạng. Có hai phiên bản địa chỉ IP chính:* ***IPv4*** *và* ***IPv6****.*
* *Địa chỉ IP của* ***gaia.cs.umass.edu:*** *128.119.245.12*
* *Địa chỉ IP của máy tính đang sử dụng: 192.168.100.56*

***Minh chứng:***

* Địa chỉ IP của **gaia.cs.umass.edu** trong cột **Destination**
* Địa chỉ IP của máy tính đang sử dụng thì xem trong cột Source



*Câu 9. Từ các nội dung trên, hãy mô tả cơ bản khi truy cập một website (ví dụ website*

*đã thử nghiệm ở trên) thì quá trình gửi và nhận gói tin đã hoạt động như thế nào?*

*Trình duyệt mà bạn đang sử dụng đóng vai trò gì?*

***Lưu ý:*** *Mô tả lại quá trình này một cách cơ bản dựa trên gói tin từ khi nhập đường*

*dẫn website đến khi website được hiển thị đầy đủ.*

***Trả lời:*** *Các bước:*

* *Bước 1: Nhập URL và bắt đầu kết nối. Khi nhập một URL là http://gaia.cs.umass.edu) vào trình duyệt, trình duyệt sẽ phân tích URL để xác định máy chủ đích (gaia.cs.umass.edu).*
* *Bước 2: Thiết lập kết nối TCP*
* *Bước 3: Gửi yêu cầu HTTP GET*
* *Bước 4: Máy chủ phản hồi với HTTP Response*
* *Bước 5: Trình duyệt hiển thị nội dung*
* *Bước 6: Kết thúc kết nối*

***Vai trò của trình duyệt:*** *Trình duyệt đóng vai trò là giao diện giữa người dùng và máy chủ web. Nó chịu trách nhiệm:*

* *Gửi yêu cầu* ***HTTP*** *tới máy chủ.*
* *Hiển thị nội dung trang web cho người dùng.*
* *Quản lý quá trình tải tài nguyên và hiển thị chúng đúng thứ tự.*
* *Xử lý các giao thức bảo mật nếu dùng HTTPS (mã hóa và giải mã thông tin)*

***Minh chứng:***

Để xem địa chỉ IP của máy tính trên Windows, mở **Control Panel** và chọn **View network status and tasks.** Chọn mạng tương ứng đang sử dụng để kết nối Internet, chọn **Details** trong cửa sổ trạng thái. Xem địa chỉ IP trong Ipv4 Address



**\*Dựa vào file *MSSV-Task2.pcapng*, sinh viên thực hiện trả lời các câu hỏi sau:**

*Câu 10.Khi sử dụng bộ lọc “http” như ở đối với website ở Task 1 thì kết quả thu được như thế nào, có các gói tin HTTP tương tự không?*

***Trả lời:*** *Kết quả thu được không có các gói tin HTTP tương tự ở Task 1*

***Minh chứng:***

Gõ HTTP vào phần “Apply a display filter thì không thấy xuất hiện gói tin HTTP nào

A screenshot of a computer

Description automatically generated

*Câu 11.Tìm cách xác định địa chỉ IP của website đã chọn là bao nhiêu? Địa chỉ IP của máy tính bạn lúc này là bao nhiêu?*

***Trả lời:***

* *Địa chỉ IP của courses.uit.edu.vn: 10.204.2.4.*
* *Địa chỉ IP của máy tính của tôi là: 192.168.20.4.*

***Minh chứng:***

* Dòng số **337**: Trong cột **"Info"**, có kết quả của truy vấn **DNS** cho **courses.uit.edu.vn.** Xem ở cột **Destination**, đó chính là địa chỉ website của trang **courses.uit.edu.vn** là **10.204.2.4**
* Cũng trong dòng đó, xem ở cột **Source** thì đó là địa chỉ IP của máy tính của tôi là **192.168.20.4**



*Câu 12.Sử dụng thành phần packet-display filter để hiển thị đầy đủ quá trình trao đổi gói tin giữa máy tính của bạn và website bằng cú pháp: ip.addr==<địa chỉ IP của máy*

*tính> && ip.addr==<địa chỉ IP của website> . Cho biết rằng bạn có thể thấy được*

*nội dung trả về của website không? Mô tả.*

***Trả lời:*** *Không thấy nội dung trả về*

***Minh chứng:***

Sau khi nhập **ip.addr==10.45.117.203 && ip.addr==192.168.20.4** trên phần “Apply a display filter” thì không thấy phần nội dung trả về vì đây là website sử dụng HTTPS

A screenshot of a computer

Description automatically generated

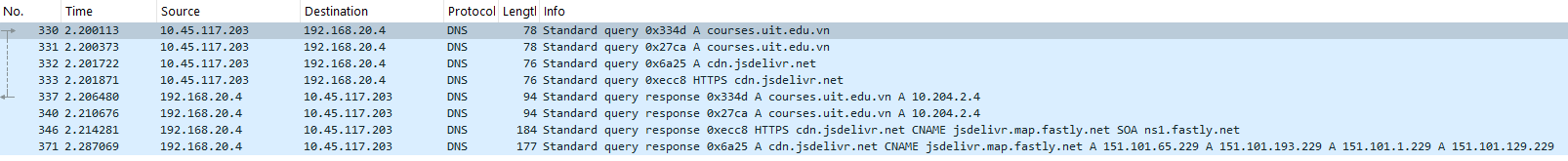
*Câu 13.Hãy chỉ ra* ***ít nhất 2 gói tin*** *mà bạn cho rằng là quan trọng khi truy cập website*

*này. Tìm hiểu và mô tả ngắn gọn các giao thức này. Giải thích.*

***Trả lời:*** *2 gói tin quan trọng là DNS query (dòng 330) và DNS response (dòng 337).*

* *Gói tin DNS Query (dòng 330): Máy gửi yêu cầu phân giải tên miền (ví dụ: courses.uit.edu.vn) đến máy chủ DNS. Nhằm giúp máy tính tìm địa chỉ IP của trang web.*
* *Gói tin DNS Response (dòng 337): Máy chủ DNS trả về địa chỉ IP tương ứng với tên miền. Nhằm giúp máy tính nhận được IP và có thể kết nối với máy chủ trang web.*

***Minh chứng:***



***Câu hỏi số 14: Theo bạn, địa chỉ IP dùng để làm gì và có cách nào khác để xem địa chỉ IP của máy tính và của một website khác hay không? Hãy thực hiện thực hiện để minh họa điều đó. Tìm được càng nhiều cách càng tốt***

***Trả lời:*** *Địa chỉ IP cung cấp nhận dạng cho một thiết bị mạng*

* *Các cách để xem địa chỉ IP trên máy tính:*
  + *Cách 1: vào Command Prompt => Gõ ipconfig => xem địa chỉ IP ở phần IPv4 Address*

***Minh chứng:***

*A screen shot of a computer

Description automatically generated*

* + *Cách 2: Vào Task Manager => Chọn Ethernet => xem địa chỉ IP ở phần IPv4 Address*

***Minh chứng:***

*A screenshot of a computer

Description automatically generated*

* *Cách xem địa chỉ IP của 1 website*
  + *Bước 1: vào Command Prompt*
  + *Bước 2: gõ* ***nslookup <tên miền>*** *hoặc* ***ping <tên miền>.*** *Đối với lệnh* ***nslookup*** *thì xem ở phần* ***Address*** *còn với lệnh* ***ping*** *thì xem ở phần* ***Reply from***

***Minh chứng:***

*A screenshot of a computer

Description automatically generated*