

BÁO CÁO THỰC HÀNH

Môn học: Nhập môn mạng máy tính

Buổi báo cáo: Lab 1

Tên chủ đề: Làm quen với Wireshark

GVHD: Phan Trung Phát

Ngày thực hiện: 5/10/2022

Ngày nộp báo cáo: 5/10/2022

1. THÔNG TIN CHUNG:

Lớp: IT005.N11.KHTN.1

ST T	Họ và tên	MSSV	Email
1	Lương Toàn Bách	21521845	21521845@gm.uit.edu.vn

2. ĐÁNH GIÁ KHÁC:

Nội dung	Kết quả
Tổng thời gian thực hiện bài thực hành trung bình	1.5 tiếng
Link Video thực hiện (nếu có)	Không có
Ý kiến (nếu có) + Khó khăn + Đề xuất ...	Không có
Điểm tự đánh giá	10.0

Phần bên dưới của báo cáo này là báo cáo chi tiết của nhóm thực hiện.

BÁO CÁO CHI TIẾT

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

Câu 1: Tổng thời gian bắt gói tin trong từng trang web đã thử nghiệm và tổng số gói tin bắt được là bao nhiêu?

- Trang web: <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>

496	3.037598637	10.45.234.170	128.119.245.12	HTTP	517 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
620	3.701840676	128.119.245.12	10.45.234.170	HTTP	504 HTTP/1.1 200 OK (text/html)

- Tổng thời gian bắt gói tin: 0.664242039
- Tổng số gói tin bắt được: 124

- Trang web: <https://courses.uit.edu.vn/login/index.php>

44	3.274090240	10.0.140.125	118.69.123.142	TCP	74 59690 -> 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=700825746 TSecr=0 WS=128
45	3.288195152	118.69.123.142	10.0.140.125	TCP	74 443 -> 59690 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1440 SACK_PERM=1 TSval=2715331609 TSecr=700825746 WS=128

- Tổng thời gian bắt gói tin: 0.014104912
- Tổng số gói tin bắt được: 1

Câu 2: 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 2 website. Tìm hiểu trên Internet và mô tả ngắn gọn chức năng chính của các giao thức đó:

- **QUIC** là một mô hình tuyệt vời để tạo ra một chồng các giao thức độc lập mà mỗi giao thức có thể phát triển và cải tiến theo tốc độ riêng của chúng, nhưng nó tạo ra sự thiếu hiệu quả. Trong ví dụ mà chúng ta đã thảo luận trước đây, TCP phải hoàn thành quá trình bắt tay ba bước trước khi TLS có thể bắt đầu thiết lập các tham số mã hóa. Không hiệu quả như vậy.
- **TCP** hoạt động với giao thức Internet (IP) để chỉ định cách dữ liệu được trao đổi trực tuyến. IP chịu trách nhiệm gửi từng gói đến đích của nó, trong khi TCP đảm bảo rằng

các byte được truyền theo thứ tự mà chúng được gửi mà không có lỗi hoặc thiếu sót nào. Hai giao thức kết hợp với nhau được gọi là TCP/IP.

- **TLSv1.2** chức năng chính của giao thức TLS là cung cấp sự riêng tư bảo đảm sự nguyên vẹn cho dữ liệu giữa hai ứng dụng trong môi trường mạng. Không chỉ có vậy, giao thức TLS còn có thể sử dụng để đóng gói, mã hóa dữ liệu, phân mảnh, hỗ trợ các máy chủ nhận ra nhau để từ đó tiến hành thỏa thuận mã hóa.
- **SSDP** là tiêu chuẩn cho các dịch vụ quảng cáo trên mạng TCP/IP và phát hiện ra chúng. Giao thức Universal Plug and Play (UPnP) sử dụng SSDP để thông báo và tìm thiết bị theo thứ tự, chẳng hạn như để truyền video từ nguồn đến hệ thống phát lại.
- **HTTP** là giao thức để thông qua đó, máy chủ và máy khách giao tiếp với nhau. Http hoạt động dựa trên mô hình Client (máy khách) – Server (máy chủ). Các máy tính của người dùng sẽ đóng vai trò làm máy khách (Client). Sau một thao tác nào đó của người dùng, các máy khách sẽ gửi yêu cầu đến máy chủ (Server) và chờ đợi câu trả lời từ những máy chủ này.

Câu 3: Mất bao lâu từ khi gói HTTP GET đầu tiên được gửi cho đến khi HTTP 200 OK đầu tiên được nhận đối với mỗi 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):

496	3.037598637	10.45.234.170	128.119.245.12	HTTP	517	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
620	3.701840676	128.119.245.12	10.45.234.170	HTTP	504	HTTP/1.1 200 OK (text/html)

- Mất 0.664242039 để gói tin HTTP GET đầu tiên được gửi cho đến khi HTTP 200 OK đầu tiên được nhận.

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

620	3.701840676	128.119.245.12	10.45.234.170	HTTP	504 HTTP/1.1 200 OK (text/html)
Wireshark - Packet 620 - Test1.pcapng					
Frame 620: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface wlp2s0, id 0 Ethernet II, Src: JuniperN_8c:35:b0 (44:f4:77:8c:35:b0), Dst: IntelCor_e7:65:0d (74:70:fd:e7:65:0d) Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.45.234.170 Transmission Control Protocol, Src Port: 80, Dst Port: 32926, Seq: 1, Ack: 452, Len: 438 Hypertext Transfer Protocol					
Line-based text data: text/html (3 lines) <html>\n Congratulations! You've downloaded the first Wireshark lab file!\n </html>\n					

- Nội dung hiển thị trên trang web có nằm trong các gói tin HTTP.
- Nằm trong gói tin HTTP 200 OK.

Câu 5: Địa chỉ IP của gaia.cs.umass.edu và website đã chọn ở bước 10 là gì? Địa chỉ IP của máy tính đang sử dụng là gì?

496	3.037598637	10.45.234.170	128.119.245.12	HTTP	517 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
620	3.701840676	128.119.245.12	10.45.234.170	HTTP	504 HTTP/1.1 200 OK (text/html)

- IP của **gaia.cs.umass.edu** là: 128.119.245.12
- Địa chỉ IP của máy tính đang sử dụng là: 10.45.234.170

69	5.910074	172.20.11.222	118.69.123.142	TCP	66 63255 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
70	5.914156	204.79.197.200	172.20.11.222	TCP	56 443 → 63219 [ACK] Seq=1127 Ack=4644 Win=16384 Len=0
71	5.918855	172.20.11.222	8.8.8.8	UDP	247 51143 → 443 Len=205
72	5.925904	8.8.8.8	172.20.11.222	UDP	67 443 → 51143 Len=25
73	5.926314	172.20.11.222	8.8.8.8	DNS	94 Standard query 0xb170 A nav-edge.smartscreen.microsoft.com
74	5.933226	204.79.197.200	172.20.11.222	TCP	56 443 → 63219 [ACK] Seq=1127 Ack=6084 Win=16385 Len=0
75	5.933226	204.79.197.200	172.20.11.222	TCP	56 443 → 63219 [ACK] Seq=1127 Ack=7524 Win=16385 Len=0
76	5.933483	204.79.197.200	172.20.11.222	TCP	56 443 → 63219 [ACK] Seq=1127 Ack=8964 Win=16385 Len=0
77	5.933971	204.79.197.200	172.20.11.222	TCP	56 443 → 63219 [ACK] Seq=1127 Ack=9199 Win=16384 Len=0
78	5.936038	118.69.123.142	172.20.11.222	TCP	66 80 → 63255 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM=1 WS=128

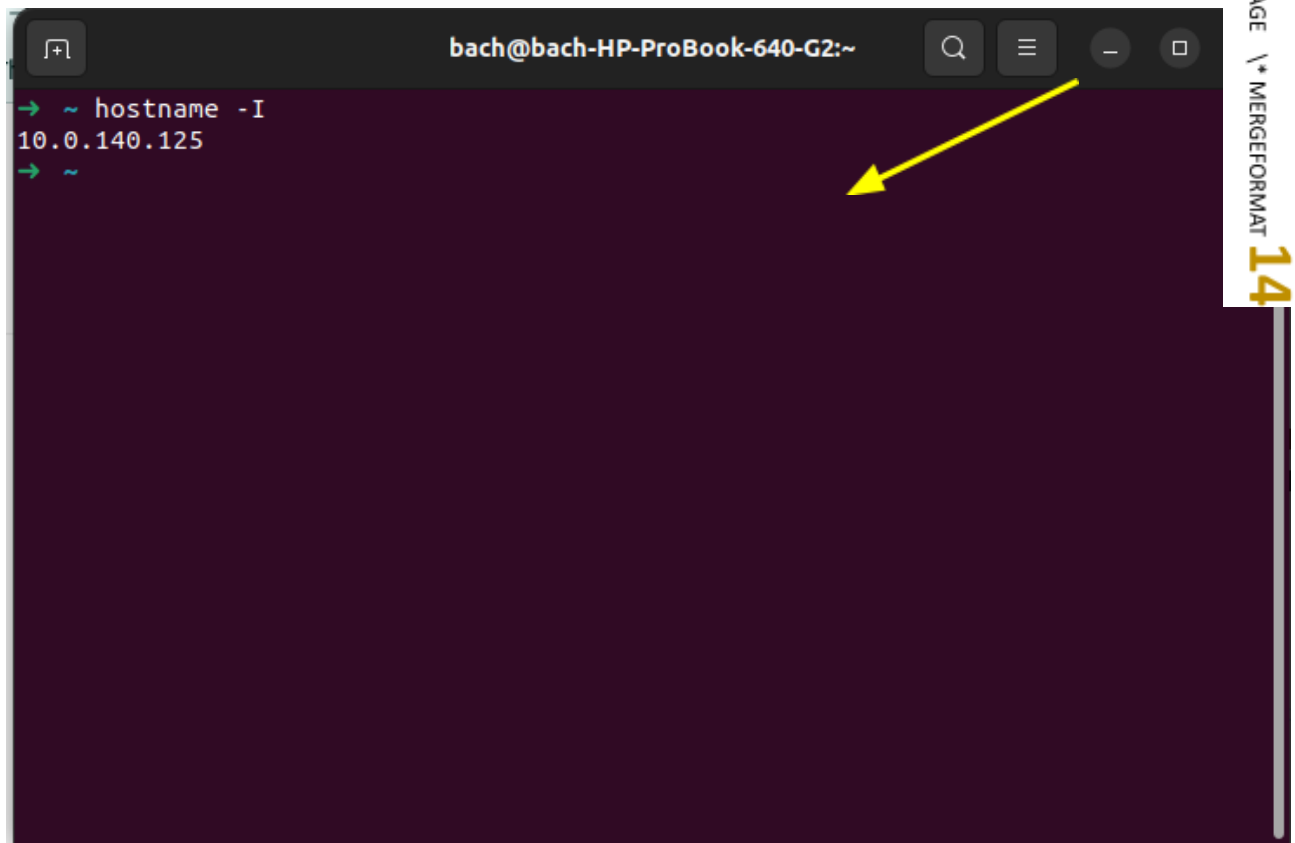
- IP của **course.uit.edu.vn** là: 118.69.123.142
- Địa chỉ IP của máy tính đang sử dụng là: 172.20.11.222

Câu 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:

- Đầu tiên, để một kết nối giữa sever và client được thiết lập, client cần gửi một gói dữ liệu SYN Request (Synchronize Sequence Number) đến Web sever. Tiếp theo, Web sever nhận gói SYN Request từ client và respond một bản xác nhận - gói ACK (Acknowledgement Sequence Number) về cho Client. Sau khi nhận SYN/ACK từ web sever, Client responds với một gói ACK và HTTP Request. Sau đó webserver trả về những hình ảnh và text về cho client.

Mở rộng: Theo bạn địa chỉ IP dùng để làm gì và có cách nào khác để xem địa chỉ IP của máy tính và của 1 website khác hay không? Hãy thực hiện ví dụ minh họa:

- Địa chỉ IP sẽ giúp các thiết bị trên mạng internet phân biệt và nhận ra nhau, từ đó có thể giao tiếp với nhau. Nó cung cấp danh tính của các thiết bị được kết nối mạng, tương tự như địa chỉ nhà hay doanh nghiệp trong thực tế đều có vị trí cụ thể.
- Có nhiều cách khác để xác định IP của máy tính và của 1 website.
- Cách xác định IP của máy tính với Terminal. Gõ lệnh `hostname -I`.



```
bach@bach-HP-ProBook-640-G2:~  
→ ~ hostname -I  
10.0.140.125  
→ ~
```

- Cách xác định IP của website với Command Prompt. Gõ lệnh `dig + <link website>`

```
bach@bach-HP-ProBook-640-G2:~  
→ ~ dig https://courses.uit.edu.vn/login/index.php  
; <<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> https://courses.uit.edu.vn/login/index.php  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 28112  
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:;; udp: 65494  
;; QUESTION SECTION:  
;https://courses.uit.edu.vn/login/index.php. IN A  
;; AUTHORITY SECTION:  
. 893 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2022100500 1800 900 604800 86400  
;; Query time: 16 msec  
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)  
;; WHEN: Wed Oct 05 21:53:26 +07 2022  
;; MSG SIZE rcvd: 146  
→ ~
```

HẾT