

MSSV: 22520751

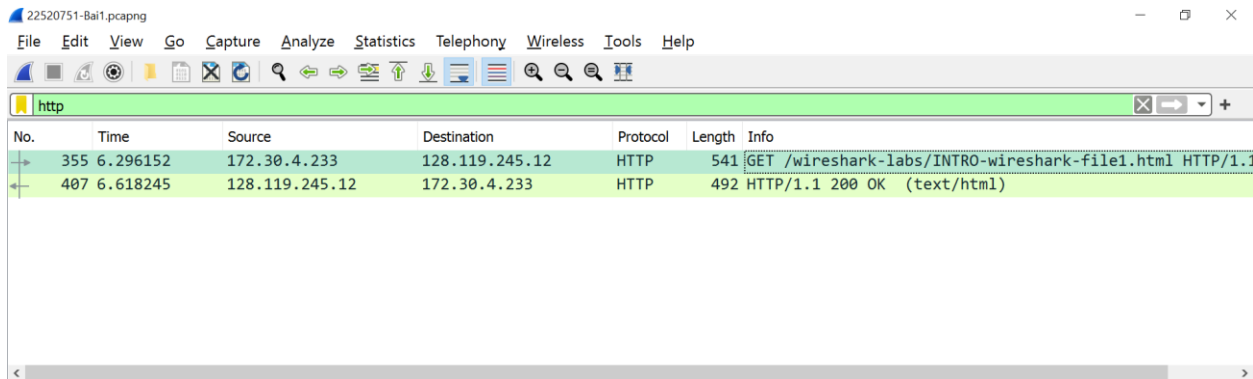
Họ Tên: Đỗ Thanh Liêm

Bài Thực Hành 1

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?

Tổng thời gian bắt gói tin trong trang web <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html> là: 0,322093 giây

Tổng số gói tin bắt được là: 2



No.	Time	Source	Destination	Protocol	Length	Info
355	6.296152	172.30.4.233	128.119.245.12	HTTP	541	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
407	6.618245	128.119.245.12	172.30.4.233	HTTP	492	HTTP/1.1 200 OK (text/html)

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.

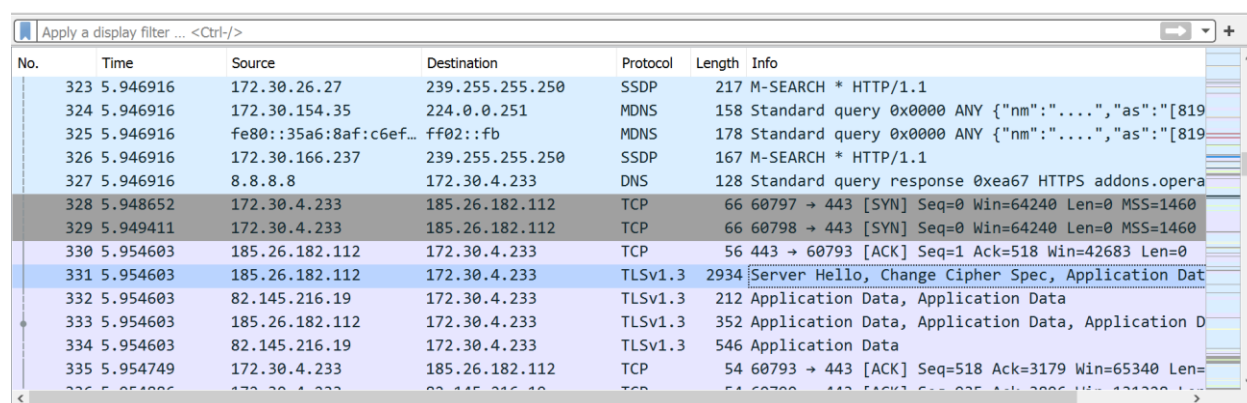
MDNS: giao thức mDNS (Multicast DNS) là một giao thức mạng được sử dụng để tự động phát hiện và liên kết các thiết bị trên mạng cục bộ (LAN) mà không cần sử dụng máy chủ DNS truyền thống

SSDP: giao thức SSDP (Simple Service Discovery Protocol) là một giao thức mạng được sử dụng để phát hiện và truy cập các dịch vụ, thiết bị và tài nguyên mạng khác trong mạng cục bộ (LAN)

DNS: Domain Name System (DNS)- hệ thống phân giải tên miền. Hệ thống này là một hệ thống cho phép thiết lập tương ứng giữa địa chỉ IP và tên miền trên internet. Nhờ giao thức này nên có thể chuyển đổi tên miền thành địa chỉ IP.

TCP: Transmission Control Protocol (TCP) là giao thức điều khiển truyền vận. Chúng là giao thức cốt lõi của Internet Protocol Suite (bộ giao thức liên mạng). Với nhiệm vụ thực thi mạng, bổ sung cho Internet Protocol. Giao thức này đảm bảo chuyển giao dữ liệu tới nơi nhận một cách đáng tin cậy và đúng thứ tự.

TLSv1.3: TLS (Transport Layer Security) và là sự kế thừa cho SSL (Secure Sockets Layer). TLS thì cung cấp giao tiếp an toàn giữa các trình duyệt web và máy chủ Server. Các kết nối này sẽ được bảo mật bằng cách sử dụng mật mã đối xứng để mã hóa dữ liệu được truyền đi. Các keys thì được tạo ra duy nhất cho mỗi kết nối và dựa trên một chia sẻ bí mật ở đầu phiên kết nối, còn được gọi TLS handshake (bắt tay TLS).

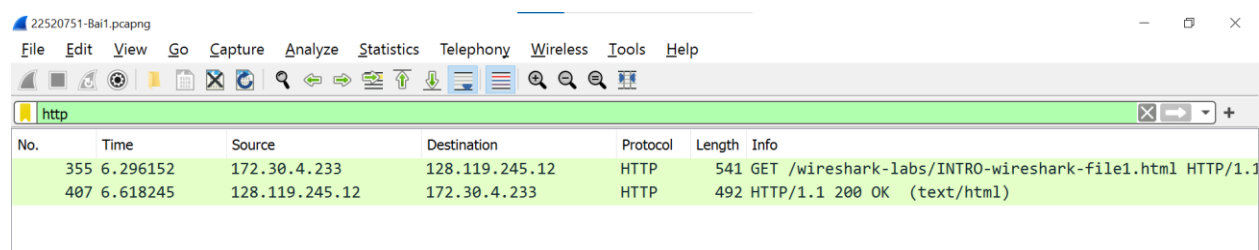


Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
323	5.946916	172.30.26.27	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
324	5.946916	172.30.154.35	224.0.0.251	MDNS	158	Standard query 0x0000 ANY {"nm": "...", "as": "[819
325	5.946916	fe80::35a6:8af:c6ef...	ff02::fb	MDNS	178	Standard query 0x0000 ANY {"nm": "...", "as": "[819
326	5.946916	172.30.166.237	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
327	5.946916	8.8.8.8	172.30.4.233	DNS	128	Standard query response 0xea67 HTTPS addons.opera
328	5.948652	172.30.4.233	185.26.182.112	TCP	66	60797 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
329	5.949411	172.30.4.233	185.26.182.112	TCP	66	60798 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
330	5.954603	185.26.182.112	172.30.4.233	TCP	56	443 → 60793 [ACK] Seq=1 Ack=518 Win=42683 Len=0
331	5.954603	185.26.182.112	172.30.4.233	TLSv1.3	2934	Server Hello, Change Cipher Spec, Application Data
332	5.954603	82.145.216.19	172.30.4.233	TLSv1.3	212	Application Data, Application Data
333	5.954603	185.26.182.112	172.30.4.233	TLSv1.3	352	Application Data, Application Data, Application Data
334	5.954603	82.145.216.19	172.30.4.233	TLSv1.3	546	Application Data
335	5.954749	172.30.4.233	185.26.182.112	TCP	54	60793 → 443 [ACK] Seq=518 Ack=3179 Win=65340 Len=0

Câu 3: Mất bao lâu 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.

Mất 0,322093 giây kể từ khi gói tin HTTP GET đầu tiên được gửi cho đến khi HTTP 200 OK đầu tiên được nhận



22520751-Bai1.pcapng

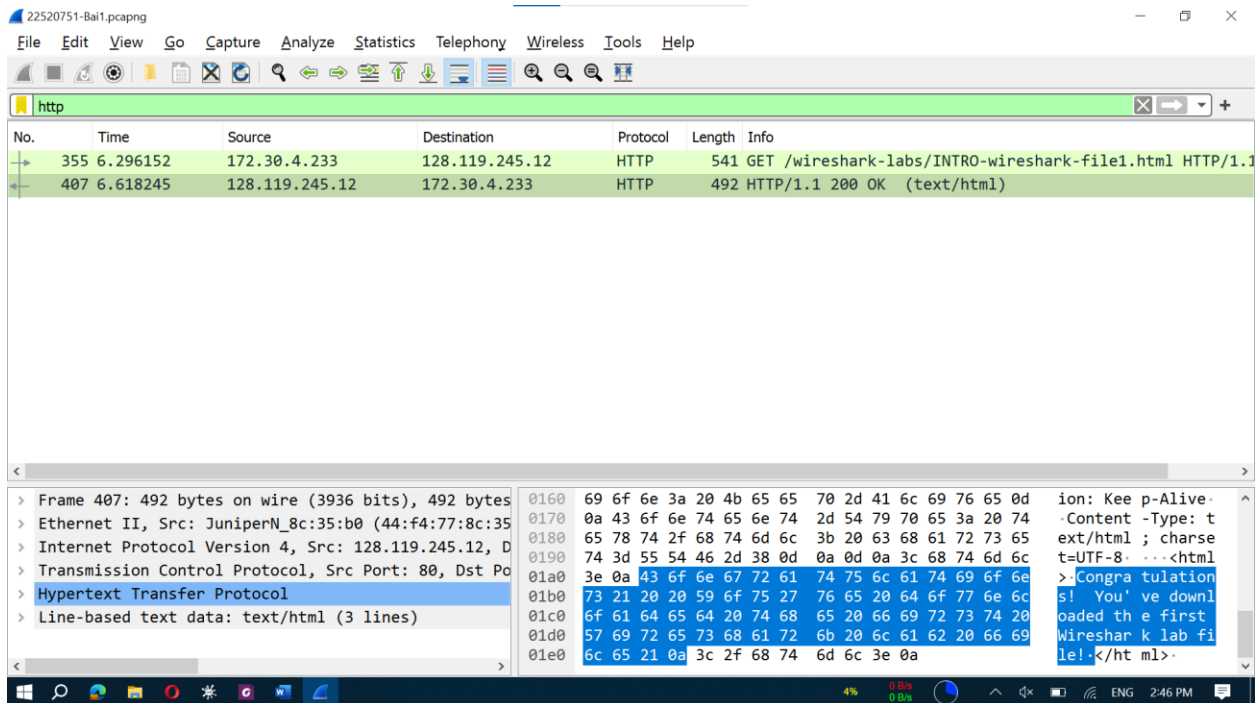
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
355	6.296152	172.30.4.233	128.119.245.12	HTTP	541	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
407	6.618245	128.119.245.12	172.30.4.233	HTTP	492	HTTP/1.1 200 OK (text/html)

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.

Nội dung có hiển thị trong gói tin HTTP 200 OK. Nội dung nằm trong Packet Raw Data.



**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?**

Địa chỉ IP của gaia.cs.umass.edu là: 128.119.245.12

Địa chỉ IP của máy tính đang sử dụng là: 172.30.4.233

No.	Time	Source	Destination
355	6.296152	172.30.4.233	128.119.245.12
407	6.618245	128.119.245.12	172.30.4.233

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.

Khi nhập URL vào trình duyệt và bấm Enter, trình duyệt sẽ chuyển đổi URL thành 1 địa chỉ IP. Sau đó, trình duyệt gửi 1 yêu cầu HTTP đến máy chủ Web tại địa chỉ IP đã được xác định. Máy chủ sẽ phản hồi với 1 mã trạng thái HTTP, nếu mã là 200 nghĩa là quá trình diễn ra suôn sẻ và máy chủ gửi nội dung về trình duyệt và hiển thị trang web.

