**MSSV**: 21521924

**Họ và tên**: Ngô Phúc Danh

**Lớp:** IT005.N16

Bài lab: 1

# Bài báo cáo Lab 1: Wireshark Getting started

## Bài 1:

Tổng thời gian bắt gói tin:			6.990573				
Tổng số gói tin bắt	được:		744				
■ *Wi-Fi	•			- 0 ×			
File Edit View Go Capture Analyze Statistics T	Telephony Wireless Tools Help						
■ Ø	= e e e =						
Apply a display filter <ctrl-></ctrl->							
No. Time Source	Destination Protoco	Length Info					
734 6.825700 192.168.152.35	20.60.59.131 TCP		9 Ack=1 Win=512 Len=1339 [TCP segment of a reassembled PDU]				
	2402:800:be32:8f10: OUIC	921 Protected Pavload (KP0)	, , , , , , , , , , , , , , , , , , , ,				
736 6.848403 2404:6800:4005:81a:.	2402:800:be32:8f10: QUIC	184 Protected Payload (KP0)					
737 6.848917 2402:800:be32:8f10:.	2404:6800:4005:81a: QUIC	95 Protected Payload (KP0), DC	ID=b882fabb198363e9				
738 6.879933 2404:6800:4005:815:.	2402:800:be32:8f10: QUIC	88 Protected Payload (KP0)		_			
	2402:800:be32:8f10: QUIC	87 Protected Payload (KP0)		=			
	2402:800:be32:8f10: QUIC	183 Protected Payload (KP0)					
	2404:6800:4005:80d: QUIC	97 Protected Payload (KP0), DC					
742 6.915923 20.60.59.131	192.168.152.35 TCP		4102 [ACK] Seq=1 Ack=171478 Win=2050 Len=0 SLE=142020 SRE=143359				
	2404:6800:4005:814: TCP 2402:800:be32:8f10: TCP		=64800 Len=0 MSS=1440 WS=256 SACK_PERM=1 0 Ack=1 Win=65535 Len=0 MSS=1319 SACK PERM=1 WS=256				
744 6.990576 2404:0800:4005:814:.	2402:800:De32:8T10: TCP	80 443 → 0411/ [SYN, ACK] Seq=	0 VCK=1 MJU=00030 FGU=0 W22=131A 2VCK AFKW=1 M2=500				
3000 88 d8 2e 5d f6 42 ea 9b dd a1 11 af 3010 90 28 00 20 06 78 24 04 68 00 40 05 3020 00 00 00 00 20 03 24 02 08 00 be 32 3030 36 8d 62 59 17 7d 10 1bb fa 75 9e dd 3040 2b d1 80 12 ff ff 26 5d 00 00 02 04	6 08 14 00 00	\$% (-					
0050 04 02 01 03 03 08							
● ② wireshark_Wi-FiY3F8T1.pcapng			Packets: 744 · Displayed: 744 (100.0%) · Dropped: 0 (0.0%)	Profile: Defa			
		ı 📋 🔤 📭 6 6	o ◆ ☆ ⋈ × d · ∰ ▼ · ﴿				

**Hình 1.1:** Hình tổng gói tin và thời gian

## Bài 2:

Tên giao thức	Chức năng chính		hức	Tên giac
TCP	Kiểm soát mức độ tin cậy của việc truyền dữ liệu.			TCP
90 1.115629 24	:4005:809: 2402:800:be32:8f10: TCP	2404:6800:40	29 2404:6800	90 1.11

Hình 2.1: Minh họa giao thức TCP.

Tên giao thức	Chức năng chính			
TLSv1.3	Cung cấp sự riêng tư đảm bảo sự nguyên vẹn cho dữ liệu giữa hai ứng			
	dụng trong môi trường mạng.			
93 1.154801	2404:6800:4005:80c: 2402:800:be32:8f10: TLSv1.3 720 Application Data			

**Hình 2.2:** Minh họa giao thức TLSv1.3

Tên giao thức	Chức năng chính
QUIC	Giảm đáng kể thời gian kết nối, sửa lỗi chuyển tiếp, cải thiện khả năng kiểm soát tắc nghẽn.
206 2 600254	2/0/-6900-4005-900- 2/02-900-bo22-9f10- OUTC 97 Protected Payload (VDG)

Hình 2.3: Minh họa giao thức QUIC

Tên giao tl	ıức	Chức năng chính				
DNS		Giúp liên kết với các trang thiết bị mạng cho các mục đích định vị và chỉ hóa các thiết bị trên Internet.				
156 1 760727	102 160 152 25	102 169 152 252	DNC	OF Standard guary AvEs77 AAAA salah masaansh gaagla sam		

Hình 2.4: Minh họa giao thức DNS

Tên giao thức	Chức năng chính
ARP	Chuyển địa chỉ từ tầng mạng(Internet layer) sang tầng liên kết dữ liệu theo mô hình OSI.
	tiles iiis iiiiii esii

42 Who has 192.168.152.35? Tell 192.168.152.253 196 2.045941 ea:9b:dd:a1:11:af IntelCor\_5d:f6:42 ARP

Hình 2.5: Minh họa giao thức ARP

#### Bài 3:

Đối với website: gaia.cs.umass Thời gian HTTP GET: 1.110937

89 1.110937 192.168.152.35 128.119.245.12 HTTP 560 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Hình 3.1: Hình HTTP GET của wireshark

Thời gian HTTP 200 OK: 1.525004

136 1.525004 128.119.245.12 192.168.152.35 HTTP 492 HTTP/1.1 200 OK (text/html)

Hình 3.2: Hình HTTP 200 OK

⇒ Thời gian: 0.414067

Đối với website http: iuh.edu.vn

Thời gian HTTP GET: 4.67018

192.168.152.35 489 4.670184 220.231.93.18 HTTP 565 GET / HTTP/1.1

Hình 3.3: Hình HTTP GET của IUH.edu.vn

Thời gian HTTP 200 OK: 5.713714

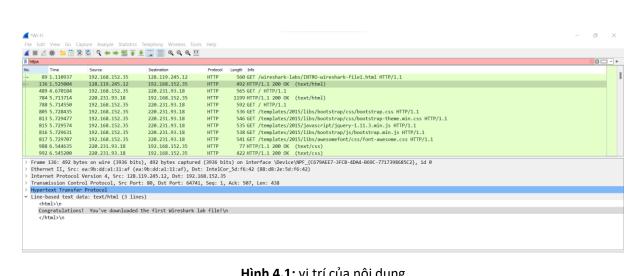
784 5.713714 220.231.93.18 192.168.152.35 HTTP 1199 HTTP/1.1 200 OK (text/html)

Hình 3.4: Hình HTTP 200 OK của IUH.edu.vn

## Bài 4:

Có nằm trong gói tin bắt được không: có nằm trong gói tin bắt được.

Tìm và xác định vị trí:



Hình 4.1: vị trí của nội dung

## Bài 5:

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

**Địa chỉ IP http**: 220.231.93.18

Địa chỉ IP của máy tính đang sữ dụng: 192.168.152.35

No.	Time	Source	Destination	Protocol	Length Info
-	89 1.110937	192.168.152.35	128.119.245.12	HTTP	560 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
<b>←</b> 1	36 1.525004	128.119.245.12	192.168.152.35	HTTP	492 HTTP/1.1 200 OK (text/html)

Hình 5.1: Địa chỉ IP của gaia.cs.umass và địa chỉ IP của máy tính đang dùng.

489 4.670184	192.168.152.35	220.231.93.18	HTTP	565 GET / HTTP/1.1	
784 5.713714	220.231.93.18	192.168.152.35	HTTP	1199 HTTP/1.1 200 OK	(text/html)

Hình 5.2: Địa chỉ IP của IUH và địa chỉ IP của máy tính đang dùng.