

1

BÁO CÁO THỰC HÀNH

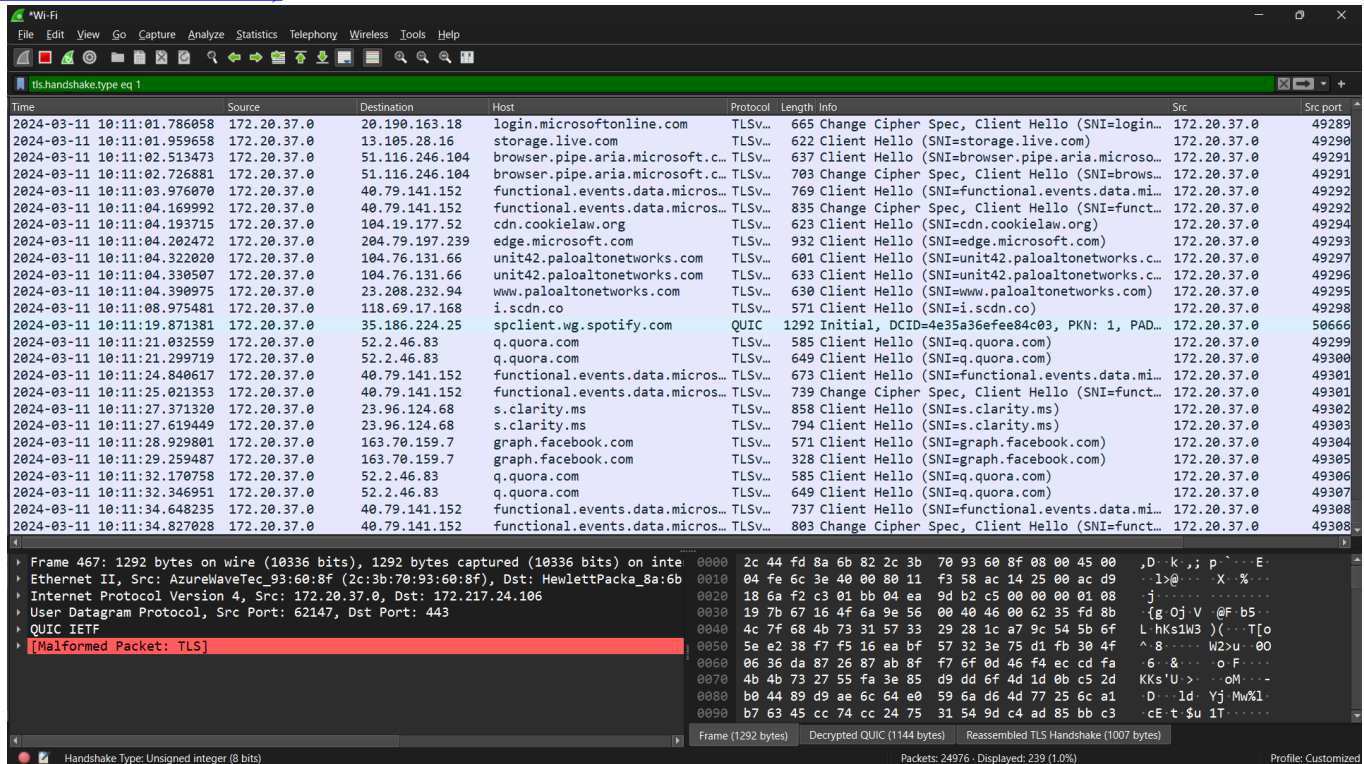
Môn học: Nhập môn mạng máy tính
Buổi báo cáo: Lab 01
Tên chủ đề: Làm quen với Wireshark
GVHD: Ngô Khánh Khoa
Ngày thực hiện: 06/03/2024
Ngày nộp báo cáo: 20/03/2024
1. THÔNG TIN CHUNG:
Lớp: IT005.O21.CTTN.1

STT	Họ và tên	MSSV	Email
1	Đoàn Đức Anh	23520041	23520041@gm.uit.edu.vn

BÁO CÁO CHI TIẾT

1. Thiết kế wireshark:

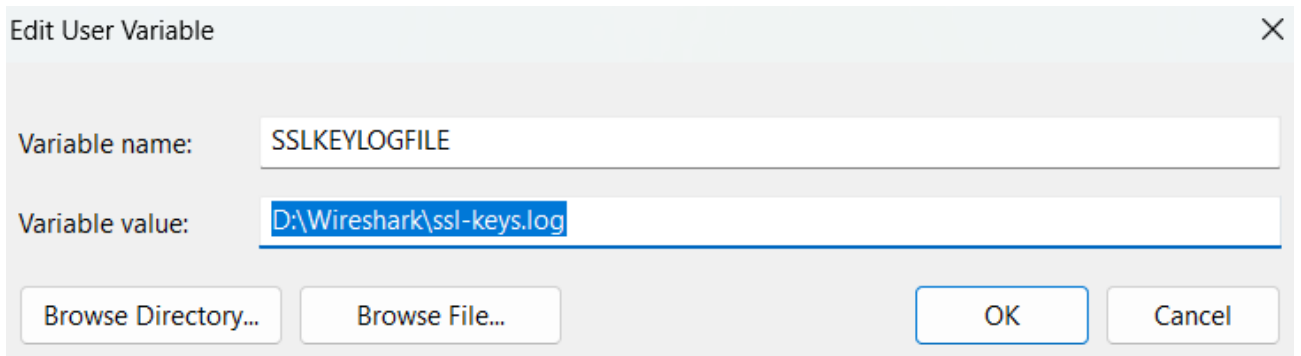
-Làm theo các bước ở website: [Wireshark Tutorial: Changing Your Column Display \(paloaltonetworks.com\)](https://www.paloaltonetworks.com/wireshark-tutorial/changing-your-column-display).



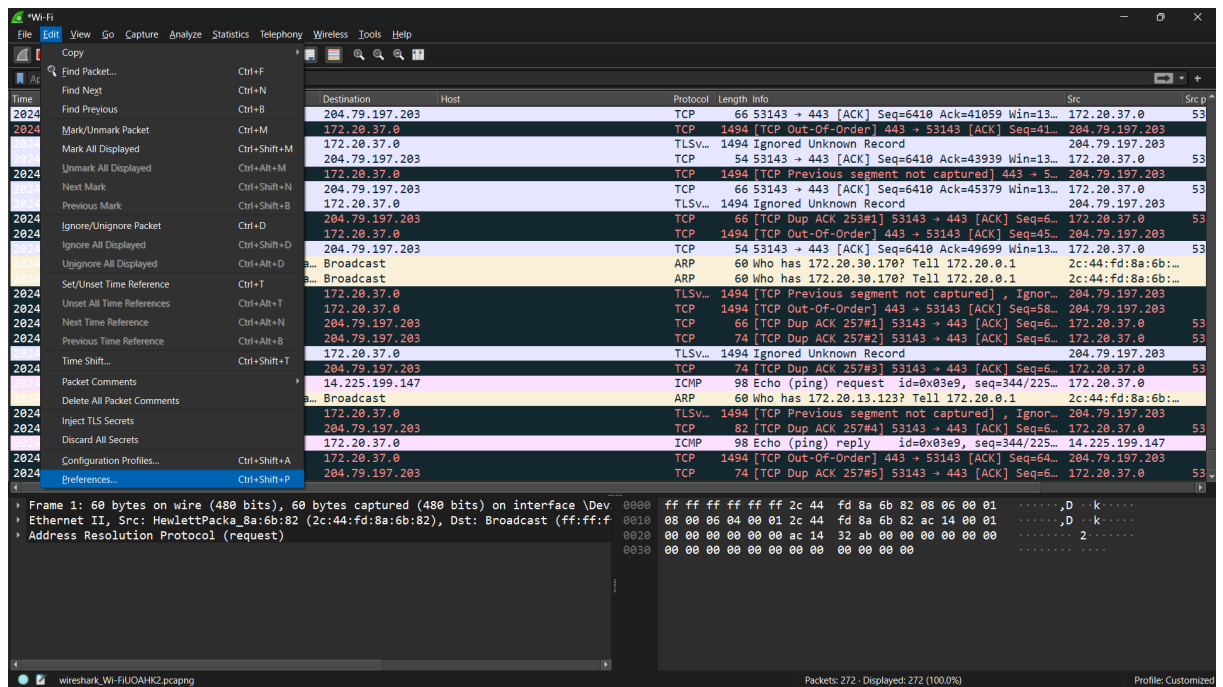
-Ta có được sự quan sát các packet chi tiết, rõ ràng và nhanh chóng hơn.

2. Xem được giao thức https(decryption):

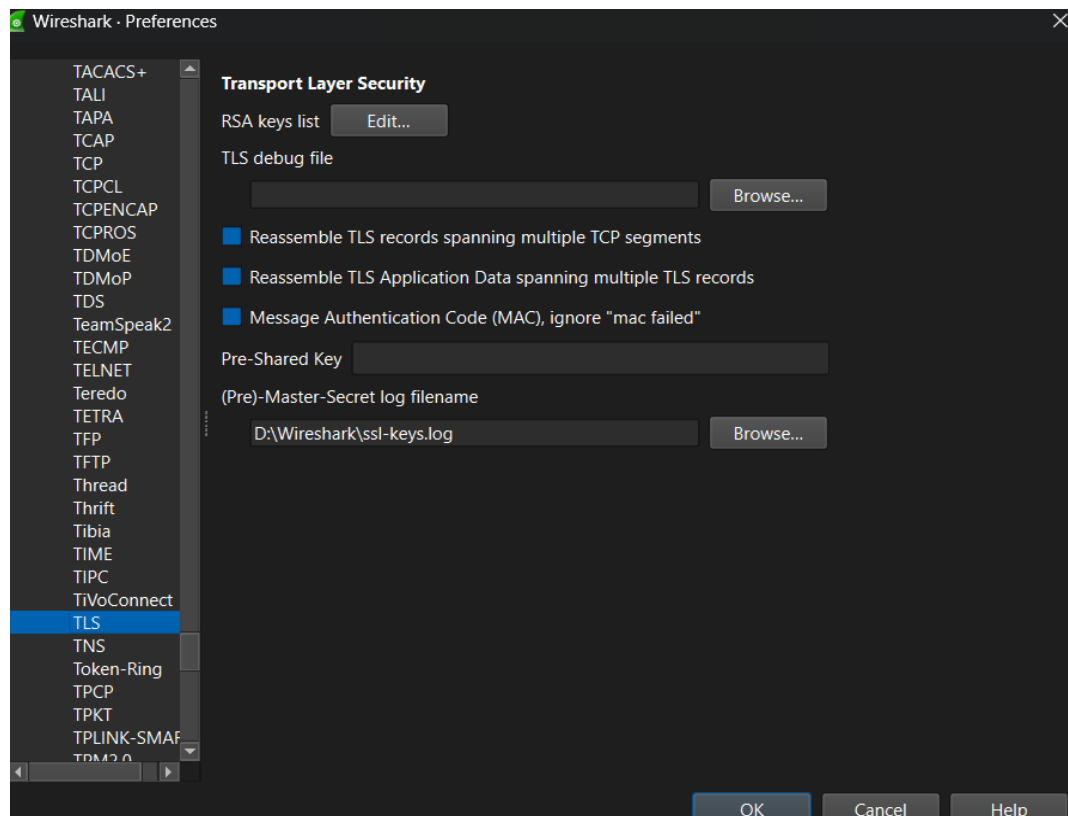
-Đầu tiên ta tạo một file có tên là **ssl-keys.log** , sau đó set environment variabale, với đường dẫn tới file trên.



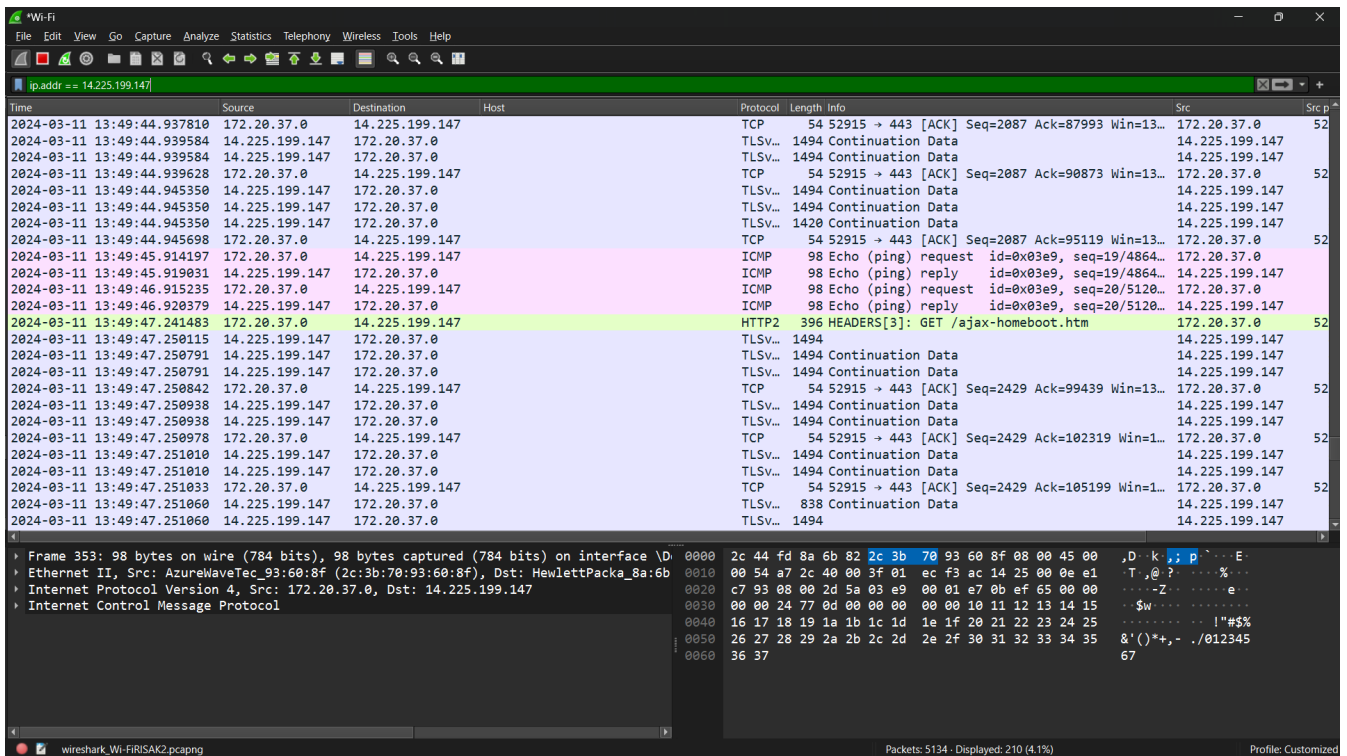
-Ta tiến hành các bước để set SSLKEYLOGFILE



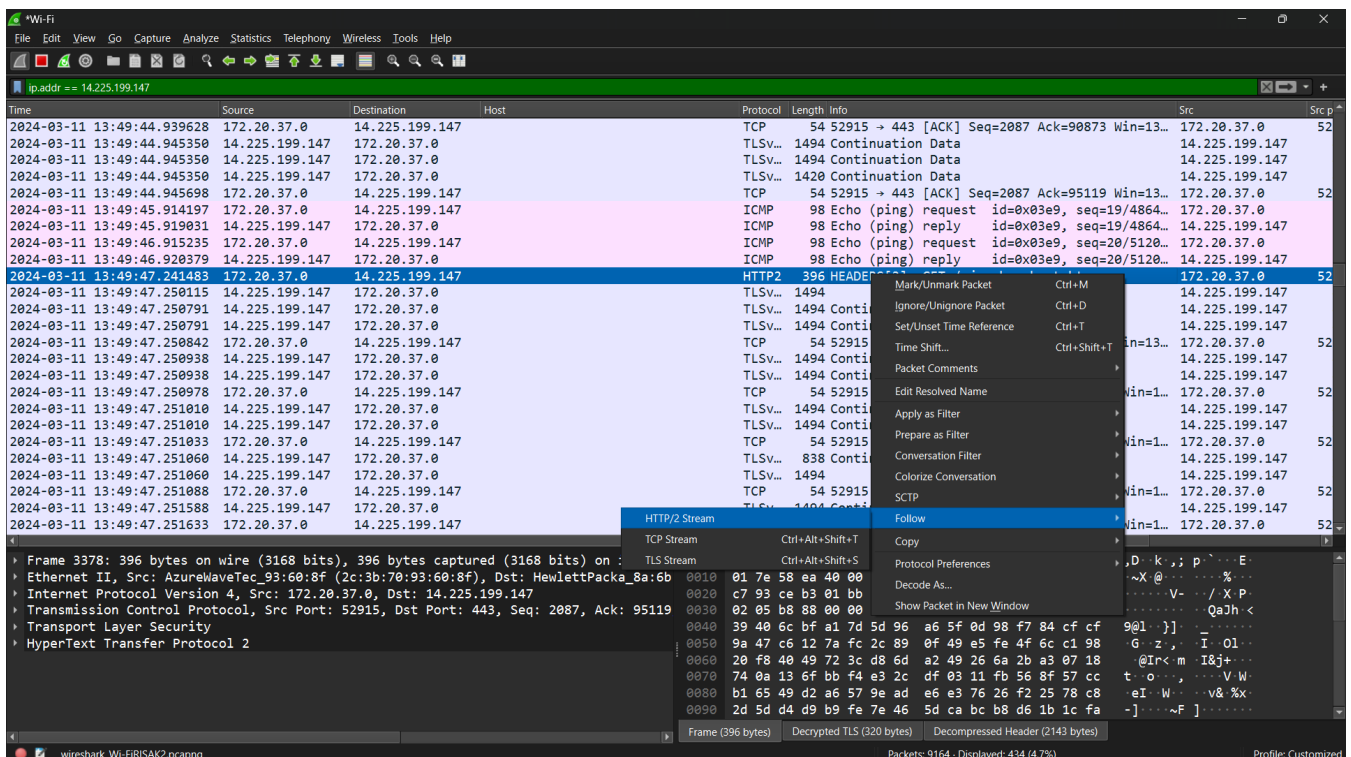
-Edit -> Preference -> protocol -> TLS và chọn đường dẫn đến file ssl-keys.log.



-Sau đó, ta tiến hành mở wireshark và capture packet, ở đây em sẽ capture packet trên web [Báo Tuổi Trẻ - Tin tức mới nhất, tin nhanh, tin nóng 24h \(tuoitre.vn\)](http://Báo Tuổi Trẻ - Tin tức mới nhất, tin nhanh, tin nóng 24h (tuoitre.vn))



-Có thể thấy có packet với protocol là HTTP2, ta check HTTP/2 Stream :



-Ta đã có được thông tin cần thiết:

Wireshark - Follow HTTP2 Stream (tcp.stream eq 27 and http2.streamid eq 3) - Wi-Fi

File Edit View Go Capture Analyze

tcp.stream eq 27 and http2.streamid eq 3

Time

2024-03-11 13:49:47.241483

Frame 3378: 396 bytes on wire (3168 bits) captured (3168 bits) on interface 0

Ethernet II, Src: AzureWave, Dst: 172.20.37.0

Internet Protocol Version 4, Src: 172.20.37.0, Dst: 172.20.37.0

Transmission Control Protocol, Src Port: 5291, Dst Port: 443

Transport Layer Security, Src: 172.20.37.0, Dst: 172.20.37.0

HyperText Transfer Protocol

method: GET
authority: tuoitre.vn
scheme: https
path: /ajax-homeboot.htm
sec-ch-ua: "Chromium";v="122", "Not(A:Brand";v="24", "Microsoft Edge";v="122"
accept: */*
x-requested-with: XMLHttpRequest
sec-ch-ua-mobile: ?0
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0
sec-ch-ua-platform: "Windows"
sec-fetch-site: same-origin
sec-fetch-mode: cors
sec-fetch-dest: empty
referrer: https://tuoitre.vn/
accept-encoding: gzip, deflate, br
accept-language: en-US,en;q=0.9,vi;q=0.8
cookie: __uidac=0165e9c88075bbbdecac107039a2f8a6
cookie: __admUTMTIME=1709820034
cookie: dtdz=87ccfc45-8ec7-5d3c-b0e1-e03cfc13fa80
cookie: __R=3
cookie: __stoffs=MA=
cookie: __ck_islogin=false
cookie: __ck_user=false
cookie: __ck_isTTSao=false
cookie: __tb=0
cookie: __stp=eyJ2aXNpdCI6InJldHVybm1uZyIsInVlaWQ1OiIyZjknJmZlODZlZTRjN2ItYmM0ZS02YTFhMGQ1NDVlNzIiOiF0=
cookie: __ttsid=73cd5d74c4fbc0c07b2e585f51f7bd90705afc9f1836d6bbbf36b7759289cd5
cookie: __gid=GA1.2.1458374319.1710163544
cookie: __sts=eyJ2aXNpdCI6InJldHVybm1uZyIsInVlaWQ1OiIyZjknJmZlODZlZTRjN2ItYmM0ZS02YTFhMGQ1NDVlNzIiOiF0=
cookie: __stgeo=IjA=
cookie: FCNEC=5585B522AKsRo19MRWYLSjLL4R74r0bZLC3cFafKdfqVh_8kLpGFTSZ3-QvYhWDSrv3ad8D9nkD1bc-wo5HDum5Tzv1qdBvqZ-HtZbgv53To5j-PXwIIdLLF4
KafIU6pgW8DLTErVHv9_b195rLW8URZ1pVOWjM06ZuXpeZw%3D%3D%22%5D%5D
cookie: __ga_1C330Q30Z4=GS1.1.1710163593.1.0.1710163593.0.0.0
cookie: __uidcms=6032854651286991300
cookie: __ga_G45HSW80Y9=GS1.1.1710163543.1.1.1710164985.59.0.0
cookie: __gat_UA-46730129-1=i
cookie: __gat_tto_vcc=1
cookie: __ga_8KQ37PQ0JH=GS1.1.1710163543.1.1.1710164985.59.0.0
cookie: __ga=GA1.1.1568419324.1710163543
cookie: __ga_G67558668B=GS1.2.1710163544.1.1.1710164986.0.0.0
cookie: __RC=58
cookie: __uif= uid%3A6032854651286991300%7C ui%3A-137C create%3A1710163545

Packet 3378: 396 bytes (3168 bits) captured (3168 bits) on interface 0

Entire conversation (1934 bytes) Show data as ASCII Stream 27 Substream 3

Find: Find Next

Filter Out This Stream Print Save as... Back Close Help

Profile: Customized