

# Lab 1: Làm quen với Wireshark

Sinh viên : Bùi Thị Như Quỳnh

Lớp : 10DH\_CNMP1

## Task 1

- Kể tên các loại thiết bị liên quan đến Mạng mà bạn biết hoặc đang sử dụng (kèm ảnh minh họa).

- **Router (Bộ định tuyến):** Kết nối các mạng với nhau và chuyển tiếp dữ liệu giữa chúng.
- **Switch (Bộ chuyển mạch):** Kết nối các thiết bị trong cùng một mạng nội bộ (LAN).
- **Modem:** Chuyển đổi tín hiệu số từ nhà cung cấp dịch vụ internet (ISP) thành tín hiệu có thể sử dụng cho mạng nội bộ.
- **Access Point (Điểm truy cập):** Mở rộng phạm vi Wi-Fi, cho phép nhiều thiết bị kết nối không dây.
- **Firewall (Tường lửa):** Bảo vệ mạng khỏi các truy cập trái phép và các mối đe dọa bên ngoài.
- **Network Cable (Cáp mạng, ví dụ: cáp Ethernet):** Kết nối vật lý giữa các thiết bị mạng.
- **Network Interface Card (NIC - Card mạng):** Cho phép thiết bị kết nối với mạng.
- **Server (Máy chủ):** Lưu trữ và quản lý tài nguyên mạng, cung cấp dịch vụ cho các thiết bị khác.
- **Repeater (Bộ lặp):** Khuếch đại tín hiệu mạng để truyền xa hơn.

- Những vấn đề gì có thể xảy ra nếu không có kết nối Internet trong 5 phút?

Trong công việc:

- Mất kết nối trong các cuộc họp trực tuyến, gây gián đoạn giao tiếp.
- Không thể truy cập các tài liệu trực tuyến hoặc ứng dụng trên cloud.
- Ngưng trệ các quy trình phụ thuộc vào hệ thống phần mềm trực tuyến.

Trong học tập:

- Không thể truy cập tài liệu học tập trực tuyến, video hướng dẫn.
- Gián đoạn trong các buổi học trực tuyến.

Trong cuộc sống hàng ngày:

- Không thể sử dụng các dịch vụ giải trí trực tuyến như xem phim, nghe nhạc.
- Các thiết bị nhà thông minh có thể bị ảnh hưởng (ví dụ: camera an ninh, hệ thống điều khiển từ xa).

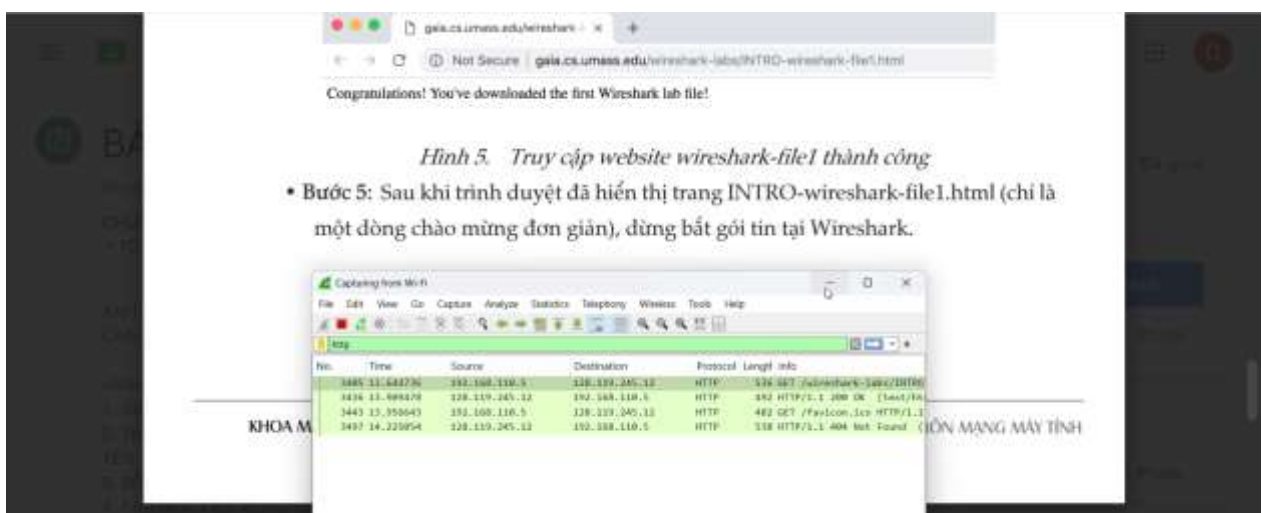
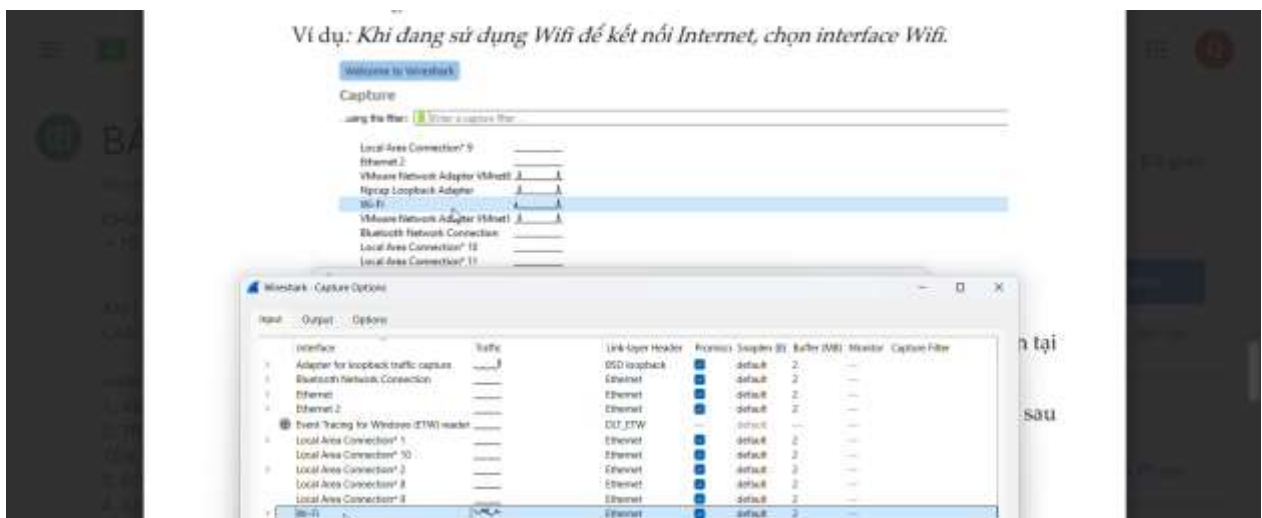
Gián đoạn các dịch vụ thanh toán điện tử hoặc mua sắm trực tuyến.

- Mục tiêu về kiến thức sau khi hoàn thành môn học Nhập môn Mạng máy tính của bạn là

gi?

- Hiểu rõ các khái niệm cơ bản về mạng máy tính và các mô hình mạng (ví dụ: OSI, TCP/IP).
- Nắm được cách thức hoạt động của các thiết bị mạng và vai trò của chúng trong hệ thống.
- Biết cách thiết lập và cấu hình các thiết bị mạng cơ bản (Router, Switch, Access Point,...).
- Hiểu về các giao thức mạng phổ biến (TCP, UDP, HTTP, FTP,...).
- Có khả năng phân tích và xử lý các sự cố mạng thông thường.
- Nâng cao nhận thức về bảo mật mạng và các biện pháp phòng chống tấn công mạng.
- Áp dụng kiến thức vào các dự án thực tế, ví dụ như thiết kế và triển khai một mạng nội bộ nhỏ.

Task 2: Làm quen với Wireshark và thử nghiệm bắt gói tin trong mạng



gaia.cs.umass.edu server (tìm trong packet-listing window đoạn chứa GET theo sau bởi gaia.cs.umass.edu) và HTTP 200 OK được trả về từ server đến máy tính

ethernet frame,

KHOA MÁY TÍNH

W

packet-header

hiện tại. Sau khi chọn thông điệp HTTP GET, các thông tin về Ethernet frame,

KHOA MÁY TÍNH

W

packet-header

lần truy cập



161 giây bắt được 37684 gói

The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. A filter bar at the top of the packet list shows 'Apply a display filter ... <Ctrl-/>'. The packet list table has columns for No., Time, Source, Destination, Protocol, Length, and Info. Packet 37683 is selected, showing it is a UDP packet from 52.114.82.131 to 192.168.110.5, port 3481 to 50045. The packet details pane on the right shows the structure of the selected packet: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and HiPerConTracer Trace Service. The packet bytes pane shows the raw data in hexadecimal and ASCII. The status bar at the bottom indicates 'Ready to load or capture', 'Packets: 37684 · Dropped: 0 (0.0%)', and 'Profile: Default'.

No.	Time	Source	Destination	Protocol	Length	Info
37676	161.914547	52.114.82.131	192.168.110.5	UDP, H...	1216	3481 → 50045 Len=11
37677	161.914547	52.114.82.131	192.168.110.5	UDP, H...	1216	3481 → 50045 Len=11
37678	161.914592	52.114.82.131	192.168.110.5	UDP, H...	1216	3481 → 50045 Len=11
37679	161.914592	52.114.82.131	192.168.110.5	UDP, H...	1216	3481 → 50045 Len=11
37680	161.914613	52.114.82.131	192.168.110.5	UDP, H...	1216	3481 → 50045 Len=11
37681	161.914613	52.114.82.131	192.168.110.5	UDP, H...	1216	3481 → 50045 Len=11
37682	161.914613	52.114.82.131	192.168.110.5	UDP, H...	1216	3481 → 50045 Len=11
37683	161.914613	52.114.82.131	192.168.110.5	UDP, H...	1190	3481 → 50045 Len=11
37684	161.915719	192.168.110.5	52.114.54.227	STUN	264	Allocate Request ba

Packet 37683 details:

- > Frame 37683: 1190 bytes on wire (9520 bits), 1190 captured (PKTLEN=1190 on interface)
- > Ethernet II, Src: RuijieNetwork\_02:91:2a (48:81:d4:91:2a:02), Dst: 02:00:00:00:00:00
- > Internet Protocol Version 4, Src: 52.114.82.131, Dst: 192.168.110.5
- > User Datagram Protocol, Src Port: 3481, Dst Port: 50045
- > HiPerConTracer Trace Service

Packet bytes (hex): 0000 2c 3b 70 de 24 a3 48 81 d4 02 91 2a 08 00 00 04 98 7e 94 00 00 71 11 10 fe 34 72 52 83 0020 6e 05 0d 99 c3 7d 04 84 3e 51 91 7d 2c a4 0030 01 e3 00 06 80 be 00 00 00 d4 be de 00 01 0040 e3 b1 a3 aa 29 b5 a1 68 f2 f0 12 dd 6c 31 0050 40 ee 2d 45 81 9b 1d c0 d9 a4 73 96 9a ad 0060 b3 de 6e 63 70 d0 54 4a a1 84 ba df cb 12 0070 24 8b 8c f1 8e 09 47 87 a5 c7 94 54 b0 25 0080 31 fd 13 4e cc 43 10 d7 13 85 1a af c8 97 0090 30 16 b1 86 7c 2d 53 0e 32 e4 b4 25 71 cf 00a0 c3 3e c8 11 4d 3f d7 2e 0a 23 31 a1 73 12 00b0 6b a3 22 c2 d3 bc 5e 57 48 3d d9 9e 68 f4 00c0 6f 53 06 01 b0 1e 33 d4 42 8d 02 3c f3 cc 00d0 d6 05 28 30 7a dc 93 99 41 13 7b 8f be da

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.

DNS (Domain Name System) Chuyển đổi tên miền thành địa chỉ IP.

TCP (Transmission Control Protocol) :Kết nối có hướng, đảm bảo truyền dữ liệu chính xác và theo thứ tự.

UDP (User Datagram Protocol) : Kết nối không hướng, truyền dữ liệu nhanh chóng nhưng không đảm bảo thứ tự.

HTTPS (Hypertext Transfer Protocol Secure): Giao thức truyền tải nội dung web an toàn, mã hóa qua TLS/SSL.

ARP (Address Resolution Protocol)

RTCP

TLSv1.2

MDNS

QUIC