Báo cáo bài tập phân tích gói tin

bằng công cụ Wireshark

Giáo viên giảng dạy: Đỗ Hoàng Hiển

Học viên thực hiện: Nguyễn Đức Luân

Đề bài : Bắt gói tin của các giao thức TCP, UDP, ICMP, ARP, HTTP và phân tích các yêu cầu sau:

1. Gói tin có đầy đủ các tầng đã học hay không? Nếu thiếu giải thích lý do.

2. Xem xét địa chỉ MAC nguồn, MAC đích và trường Type khác nhau như thế nào ở các gói tin.

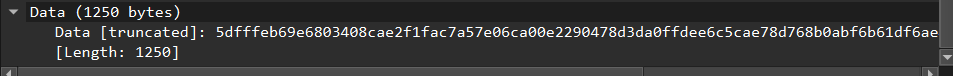
Bài làm

a)Giao thức UDP:

A screenshot of a computer

Description automatically generated

data :



segment:

A black screen with white text

Description automatically generated

packet:

A computer screen shot of a black screen

Description automatically generated

Frame :

A computer screen shot of a black screen

Description automatically generated

A screen shot of a computer

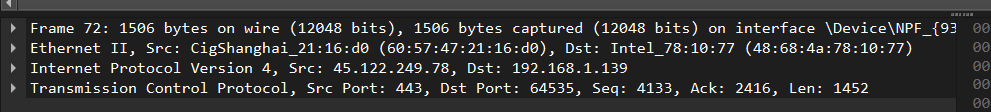
Description automatically generated

b) Giao thức TCP:

A screenshot of a computer

Description automatically generated

data: không có



Giải thích: nhìn vào hình đầu ta có thể thấy gói tin này dùng để thực hiện việc kết thúc kết nối bắt tay ba bước [FIN, ACK], nên sẽ không chứa data. Trong nếu không nhằm mục đích thực hiện kết nối bắt tay ba bước thì giao thức này vẫn có thể chứa data.

segment :

A computer screen shot of a black screen

Description automatically generated

packet:

A screenshot of a computer

Description automatically generated

Frame :

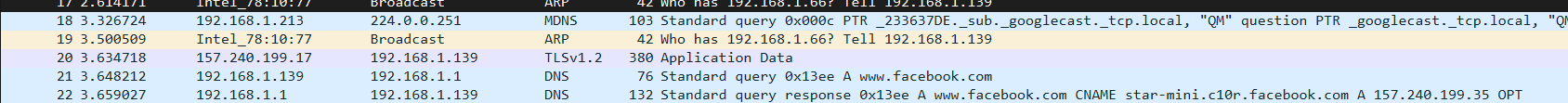
A computer screen with white text

Description automatically generated

A screen shot of a computer

Description automatically generated

c) Giao thức ARP:



data: không có

A computer screen with a white background

Description automatically generated with medium confidence

segment :không có

A computer screen with a white background

Description automatically generated with medium confidence

Packet: không có

A screenshot of a computer program

Description automatically generated

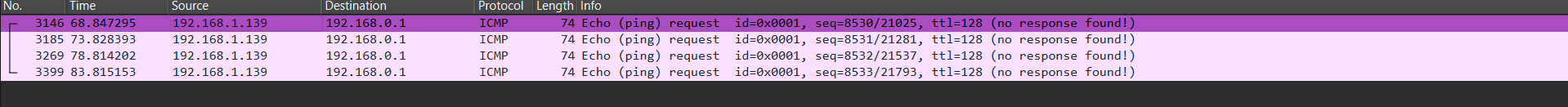
Frame :

A computer screen shot of a black screen

Description automatically generated

Giải thích : Giao thức ARP (Address Resolution Protocol) hoạt động ở tầng liên kết dữ liệu (Data Link Layer)

d) Giao thức ICMP



Data:



Segment :

A black and yellow rectangle

Description automatically generated

Packet:

A screen shot of a computer

Description automatically generated

Frame :

A computer screen shot of a black screen

Description automatically generated

A screen shot of a computer

Description automatically generated

e) HTTP:

A screen shot of a computer

Description automatically generated

Data :

A screenshot of a computer

Description automatically generated

Segment:

A computer screen shot of a black screen

Description automatically generated

Packet :

A computer screen shot of a black screen

Description automatically generated

Frame:  
A screenshot of a computer program

Description automatically generated

Tổng kết:

TCP:

Địa chỉ MAC nguồn và đích: Được sử dụng để định tuyến gói tin trong mạng LAN.

Trường Type: Được đặt là 0x0800 (IPv4) trong Ethernet.

UDP:

Địa chỉ MAC nguồn và đích: Tương tự TCP, sử dụng để định tuyến gói tin trong mạng LAN.

Trường Type: Được đặt là 0x0800 (IPv4) trong Ethernet.

ICMP:

Địa chỉ MAC nguồn và đích: Tương tự các giao thức khác, được sử dụng để định tuyến trong mạng LAN.

Trường Type: Được đặt là 0x0800 (IPv4) trong Ethernet.

ARP:

Địa chỉ MAC nguồn và đích: Địa chỉ MAC nguồn và đích được chỉ định rõ ràng trong ARP Request và ARP Reply.

Trường Type: Được đặt là 0x0806 (ARP) trong Ethernet.

HTTP:

Địa chỉ MAC nguồn và đích: Sử dụng để định tuyến trong mạng LAN.

Trường Type: Được đặt là 0x0800 (IPv4) trong Ethernet.