

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN



Môn học: An toàn mạng

Báo Cáo Bài Tập 2

Cài đặt dịch vụ và phân tích gói tin FTP, DNS

Họ và tên: Trần Thị Thu Phương

Mã sinh viên: B21DCAT151

Nhóm môn học: 04

Giảng viên: Nguyễn Ngọc Điệp

Hà Nội, 8/2024

Mục lục

1. Bài thực hành số 1: Cài đặt và thử nghiệm một số ứng dụng web, ftp, dns	3
a. Cài đặt thử nghiệm web	3
b. Cài đặt thử nghiệm ứng dụng ftp	4
c. Cài đặt và thử nghiệm dns	6
2. Bài thực hành số 2: Sử dụng công cụ Wireshark để phân tích giao thức HTTP/FTP/DNS	7
a. Phân tích tương tác HTTP GET/response đơn giản	7
b. Phân tích tương tác FTP đơn giản.....	9
c. Phân tích tương tác DNS đơn giản	9

1. Bài thực hành số 1: Cài đặt và thử nghiệm một số ứng dụng web, ftp, dns

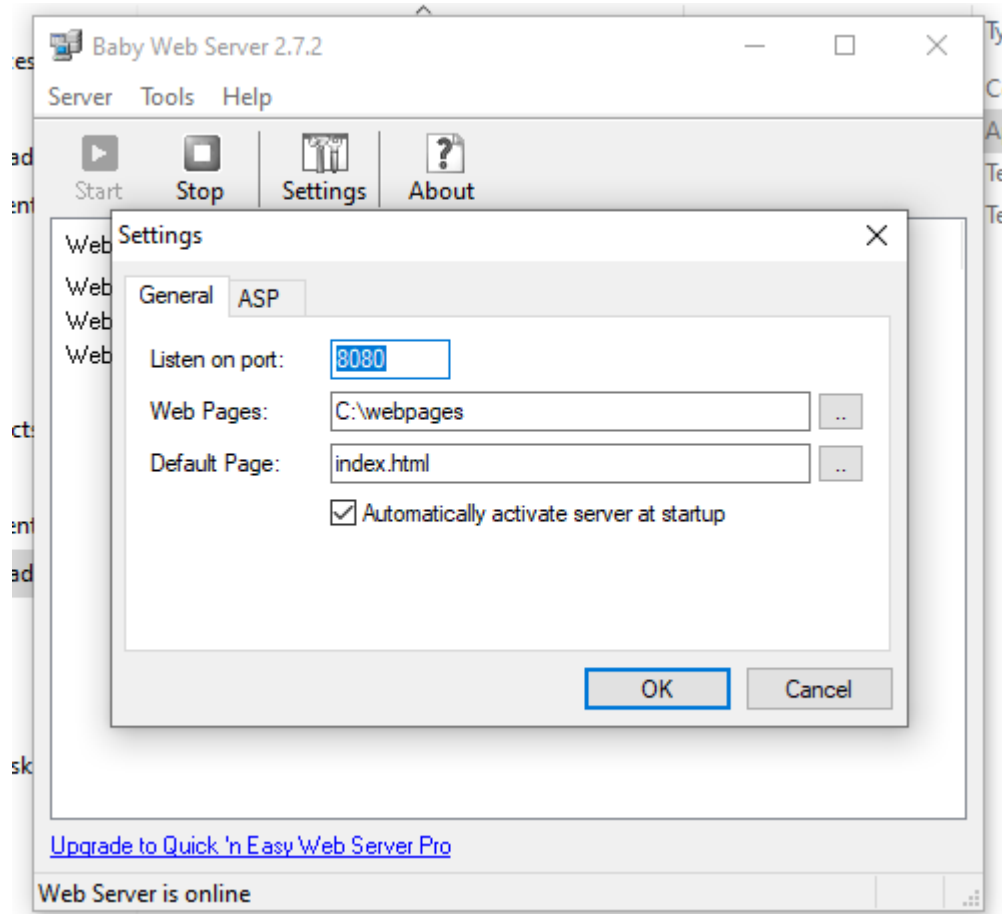
a. Cài đặt thử nghiệm web

Bước 1: Chạy chương trình Baby Web server

Bước 2: Tạo một file index.html với nội dung bất kỳ, ví dụ:

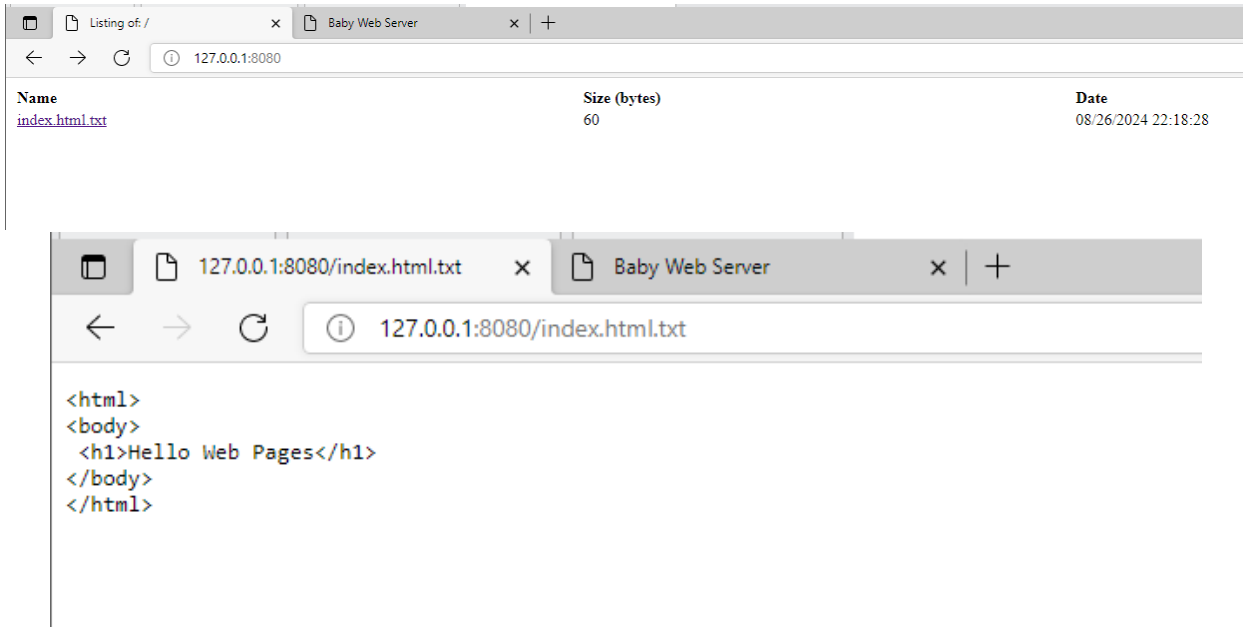
```
<html>
<body>
  <h1>Hello Web Pages</h1>
</body>
</html>
```

Bước 3: Thiết lập trang web:



- Vào mục Settings để chọn cổng cho web server và thiết lập đường dẫn tới trang web
- Bấm Start
- Vào trình duyệt bất kỳ gõ: “ip của máy tính chạy web server:cổng tương ứng đã thiết lập”, hoặc bỏ cổng nếu dùng cổng 80. Nếu cài đặt trên cùng máy với trình duyệt thì gõ “localhost:cổng tương ứng đã thiết lập” hoặc “127.0.0.1:cổng tương ứng đã thiết lập”

Bước 4: Xem trang web

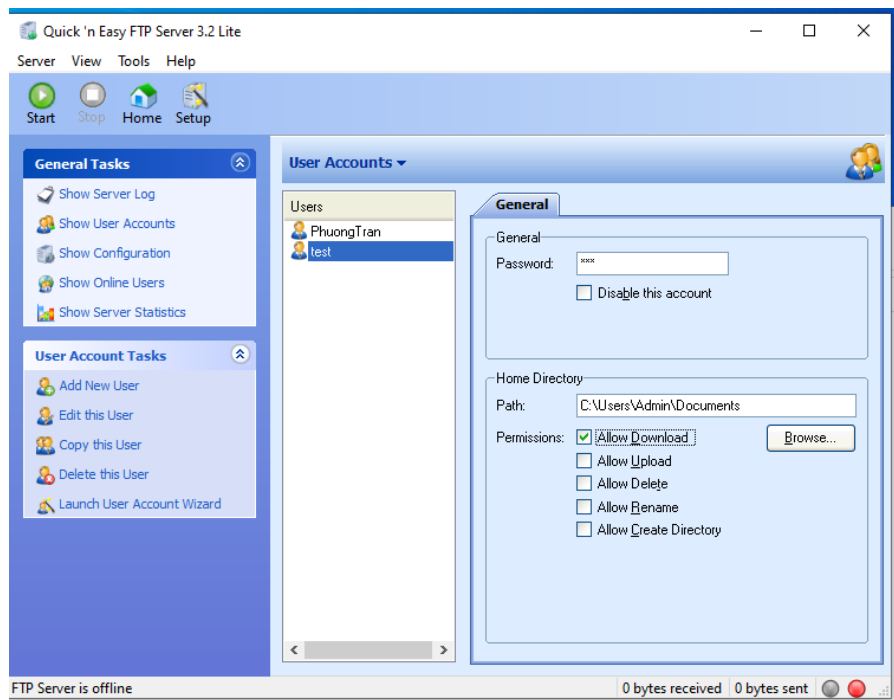


b. Cài đặt thử nghiệm ứng dụng ftp

Bước 1: Chạy chương trình Quick 'n Easy FTP Server

Bước 2: Vào Show User Accounts để tạo account

- Chọn “Add New User”: với username là test, password là 123
- Tại ô “Path”, ta chọn thư mục mong muốn chia sẻ các file, chọn các quyền tương ứng

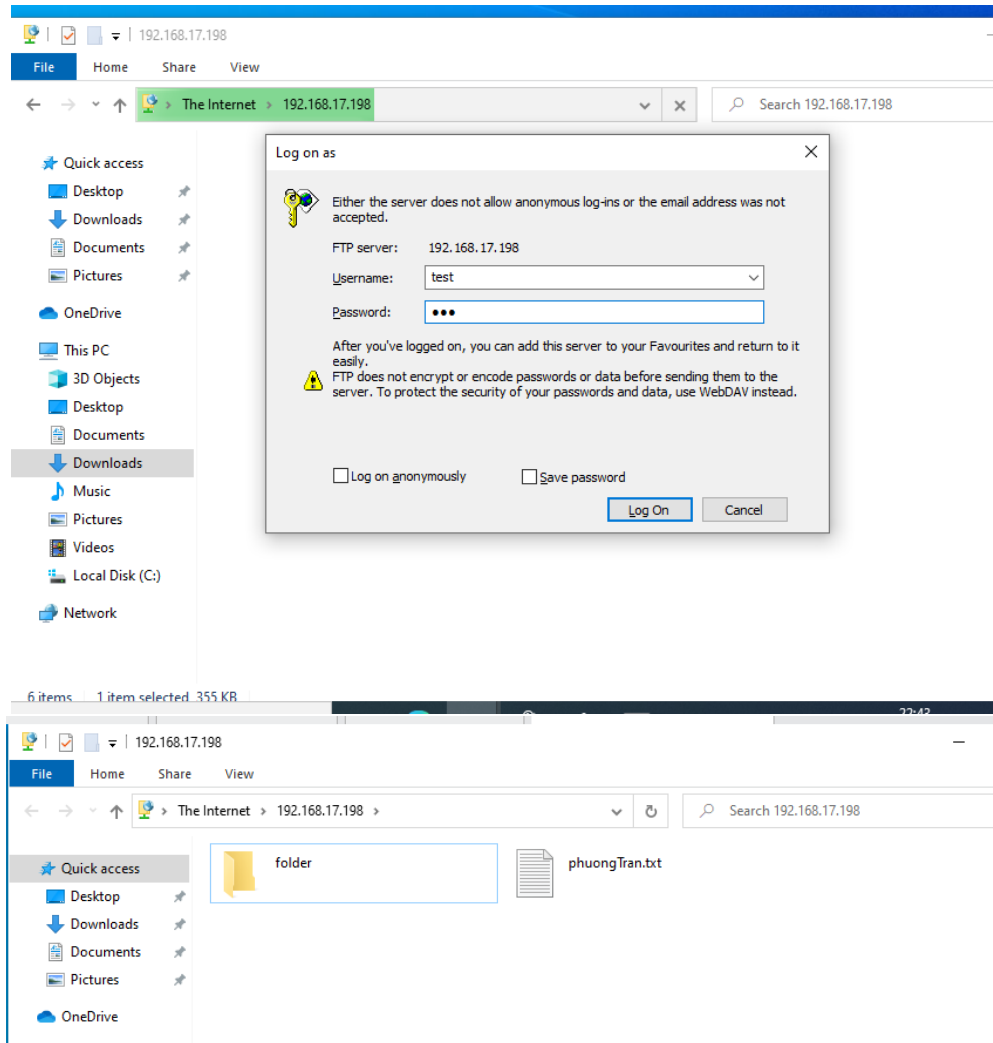


Bước 3: Chạy server

- Bấm vào nút Start để chạy server

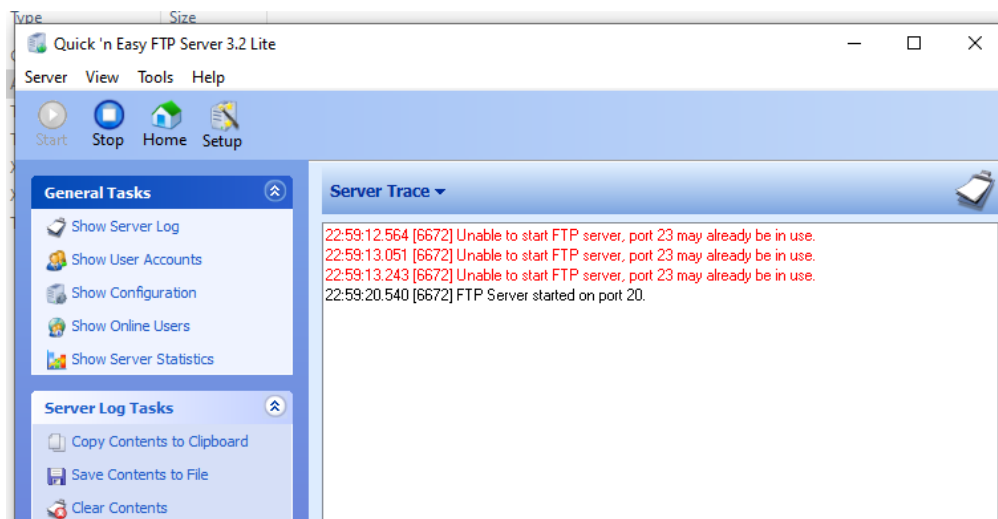
Bước 4: Thử copy file từ ftp server từ máy tính bất kỳ trong mạng

- Sử dụng Windows Explorer làm ftp client đơn giản. Gõ “ftp://địa chỉ ip của ftp server”
- Nhập username và password vừa thiết lập ở bước trên
- Nếu vào được thư mục ftp, thử copy một file về máy tính của mình

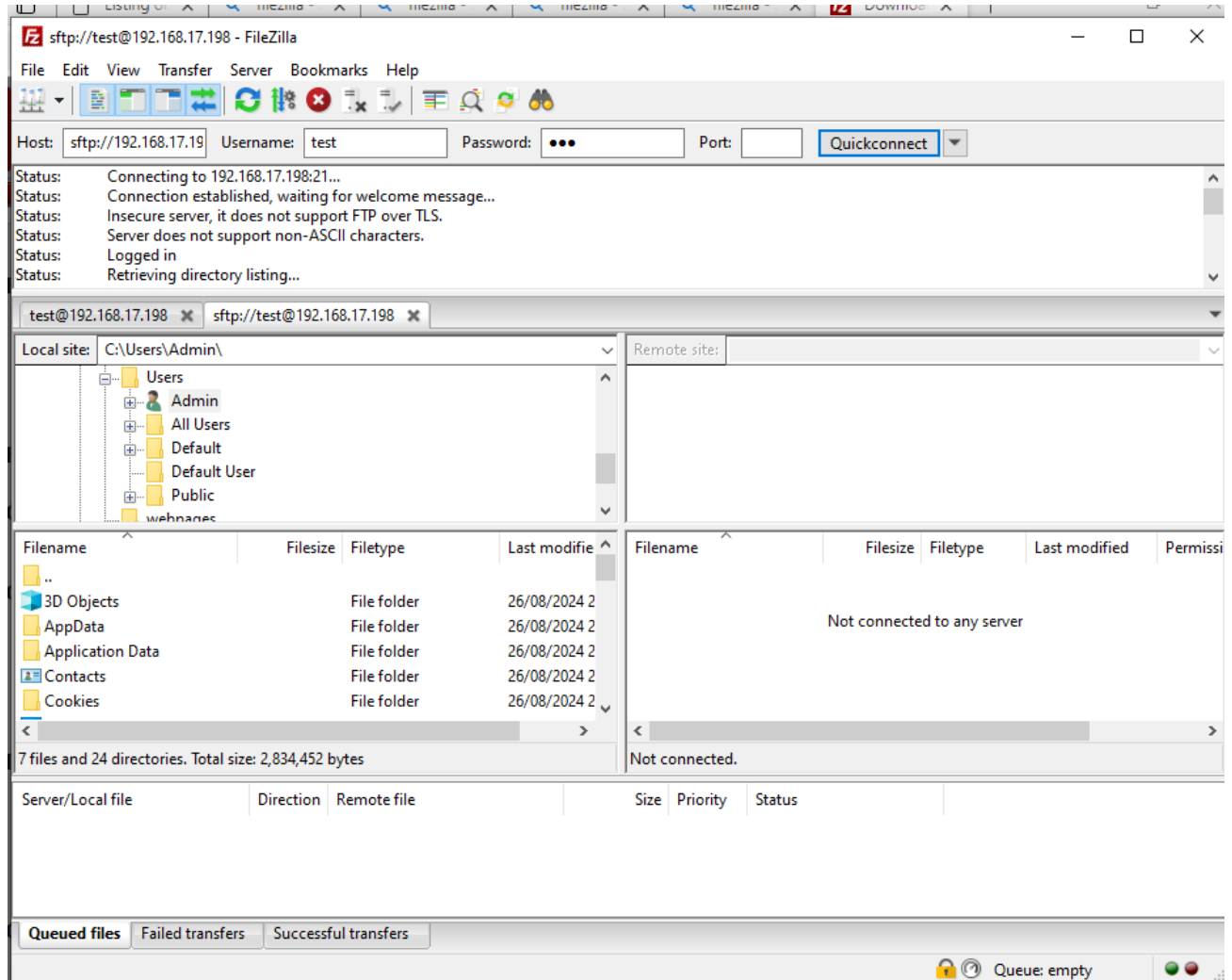


Bước 5: Ghi nhận kết quả và phân tích

- Vào ftp server, mục Show Configuration để xem cấu hình: cổng nào?
- Ghi nhận các câu lệnh tương ứng trong cửa sổ Show Server Log



Bước 6 (thực hiện thêm): Download chương trình ftp client như FileZilla để thử nghiệm các chức năng ftp



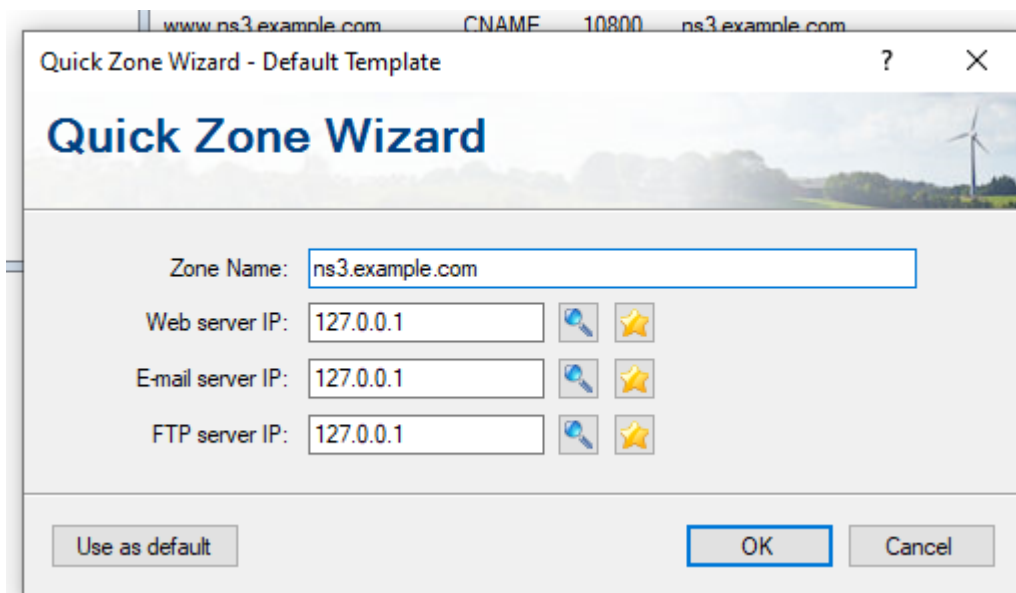
c. Cài đặt và thử nghiệm dns

Bước 1: Chạy chương trình Simple DNS

Bước 2: Cấu hình một tên miền chạy cục bộ trước thử nghiệm, trước khi đăng ký tên miền thật trên Internet

- Xem địa chỉ IP kết nối ra gateway của máy tính đang chạy bằng lệnh ipconfig
- Bấm nút Records
- Chọn Quick Zone Wizard và chọn tên zone cùng địa chỉ IP vừa có cho các server Web FTP, Email nếu có. (Một zone tương ứng với tên miền hoặc các tên miền con

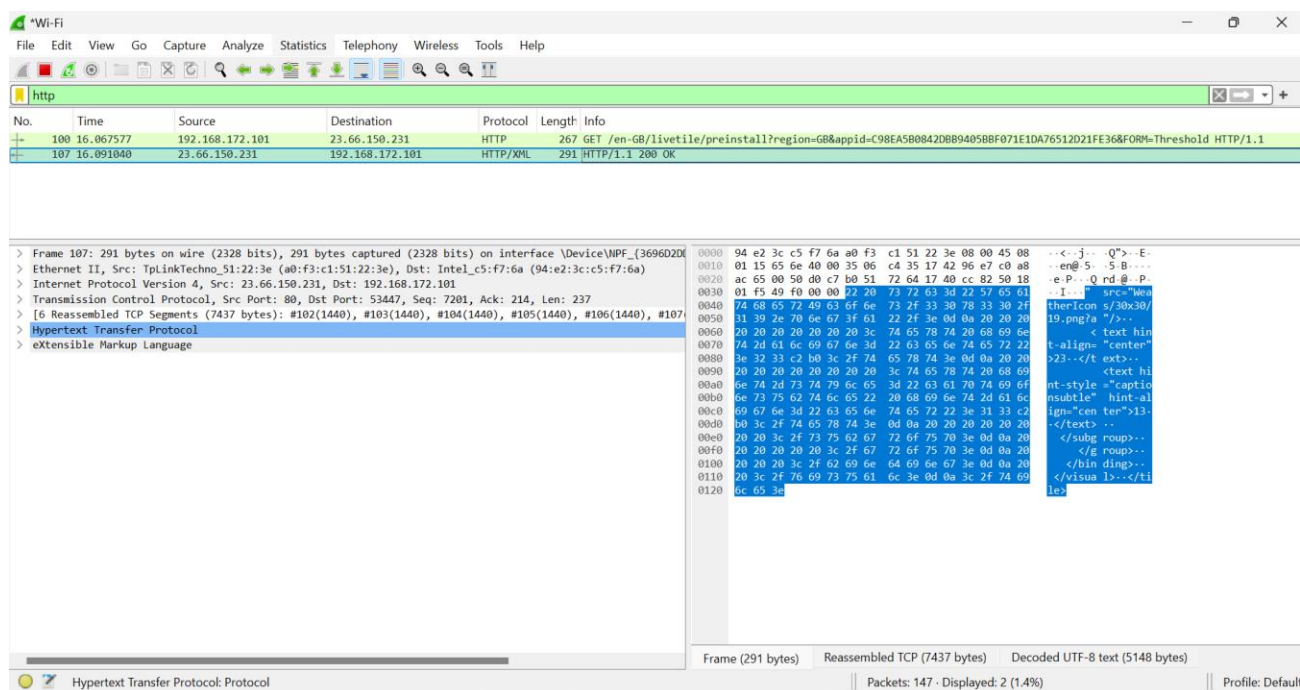
Ví dụ: tên zone là ns2.example.com và ip cho các server là 127.0.0.1, sẽ sinh ra các bản ghi:



ns3.example.com					
Name	Type	TTL	Data	Comments	
www.ns3.example.com	CNAME	10800	ns3.example.com		
ns3.example.com	A	10800	127.0.0.1		
ns3.example.com	MX	10800	[10] mail.ns3.example.com		
ns3.example.com	SOA	10800	desktop-9jtb0hm [2024082...		
ns3.example.com	NS	10800	desktop-9jtb0hm		
mail.ns3.example.com	A	10800	127.0.0.1		
ftp.ns3.example.com	A	10800	127.0.0.1		

2. Bài thực hành số 2: Sử dụng công cụ Wireshark để phân tích giao thức HTTP/FTP/DNS

a. Phân tích tương tác HTTP GET/response đơn giản



Xem bản tin HTTP GET (trên), và bản tin HTTP response dưới để trả lời các câu hỏi sau:

1. Trình duyệt chạy version HTTP nào?

Trình duyệt chạy HTTP 1.1

- ✓ Hypertext Transfer Protocol
 - ✓ GET /en-GB/livetile/preinstall?region=GB&appid=C98EA5B0842DBB9405BBF071E1
 - > [Expert Info (Chat/Sequence): GET /en-GB/livetile/preinstall?region=GB
 - Request Method: GET
 - ✓ Request URI: /en-GB/livetile/preinstall?region=GB&appid=C98EA5B0842DBB
 - Request URI Path: /en-GB/livetile/preinstall
 - > Request URI Query: region=GB&appid=C98EA5B0842DBB9405BBF071E1DA7651
 - Request Version: HTTP/1.1
 - Connection: Keep-Alive\r\n
 - User-Agent: Microsoft-WNS/10.0\r\n
 - Host: tile-service.weather.microsoft.com\r\n\r\n
 - [Full request URI: <http://tile-service.weather.microsoft.com/en-GB/liveti>
 - [HTTP request 1/1]
 - [Response in frame: 107]

2. Server chạy version HTTP nào?

Server chạy HTTP version 1.1

- ✓ Hypertext Transfer Protocol
 - ✓ HTTP/1.1 200 OK\r\n
 - > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
 - Response Version: HTTP/1.1
 - Status Code: 200
 - [Status Code Description: OK]
 - Response Phrase: OK
 - Content-Type: application/xml; charset=utf-8\r\n
 - Access-Control-Allow-Credentials: true\r\n
 - [truncated]Access-Control-Allow-Headers: TicketType, RequestContinuationKey, AuthTake

3. Địa chỉ IP của máy tính bạn và của server?

Ip máy tính: 192.168.172.101

Ip server: 23.66.150.231

4. Mã trạng thái trả về là gì? (status code)

Status code: 200 OK

5. Có bao nhiêu byte trả về từ server?

Có 5148 byte trả về

Date: Mon, 26 Aug 2024 16:28:55 GMT\r

✓ Content-Length: 5148\r\n

[Content length: 5148]

Connection: keep-alive\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.023463000 seco

b. Phân tích tương tác FTP đơn giản

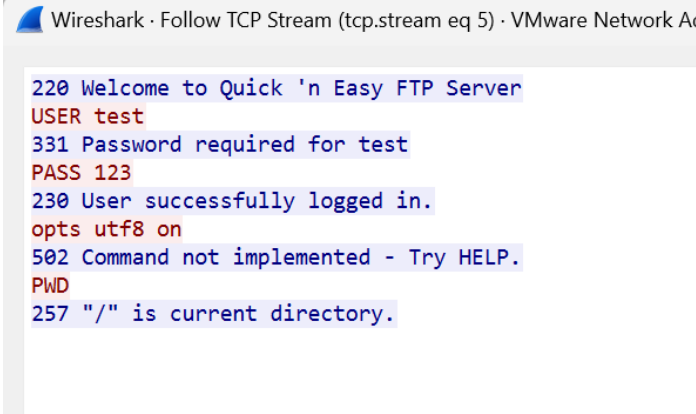
Xem các gói tin trong Wireshark và:

1. Hãy mô tả số hiệu cổng của server và cổng của máy tính hiện tại

Cổng của server: 21

Cổng của máy tính: 54115

2. Nhấn chuột phải vào một gói tin ftp và chọn Follow TCP Stream để xem các bản tin trao đổi giữa client và server



```
Wireshark · Follow TCP Stream (tcp.stream eq 5) · VMware Network Ad...

220 Welcome to Quick 'n Easy FTP Server
USER test
331 Password required for test
PASS 123
230 User successfully logged in.
opts utf8 on
502 Command not implemented - Try HELP.
PWD
257 "/" is current directory.
```

c. Phân tích tương tác DNS đơn giản

Thực hiện các truy vấn đơn giản với nslookup để tìm địa chỉ Ip thông qua tên miền và tìm tên miền thông qua địa chỉ IP

