

## FINAL LAB PRACTICE

14/4/2025

### Task:

Create and test a phishing website using XAMPP. You must capture login credentials and redirect the user to a fake loading page.

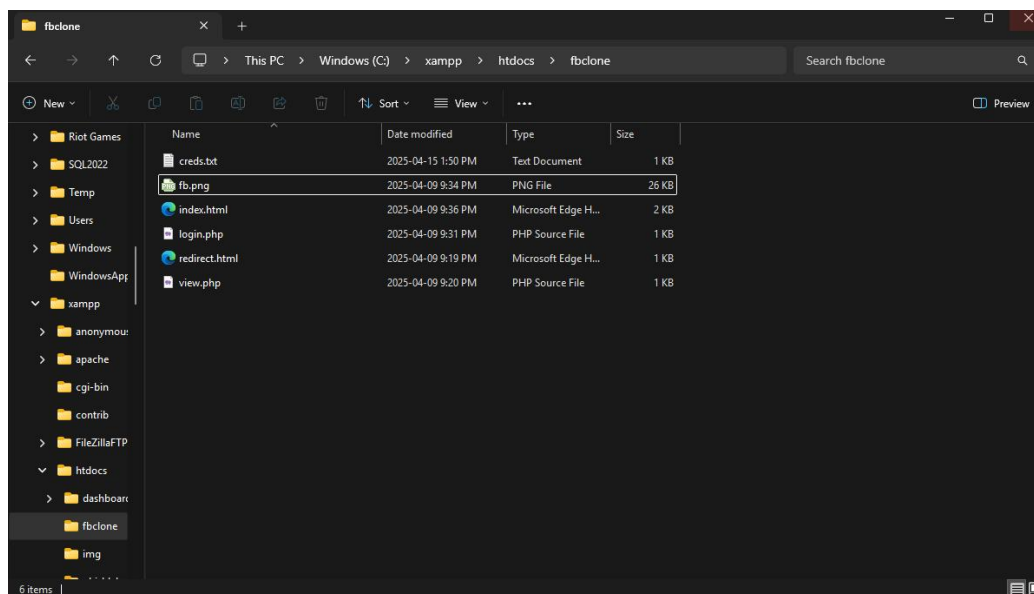
### Step-by-Step Instructions:

#### 1. Create Your Project Folder

- Name the folder fbclone
- Place it inside C:\xampp\htdocs

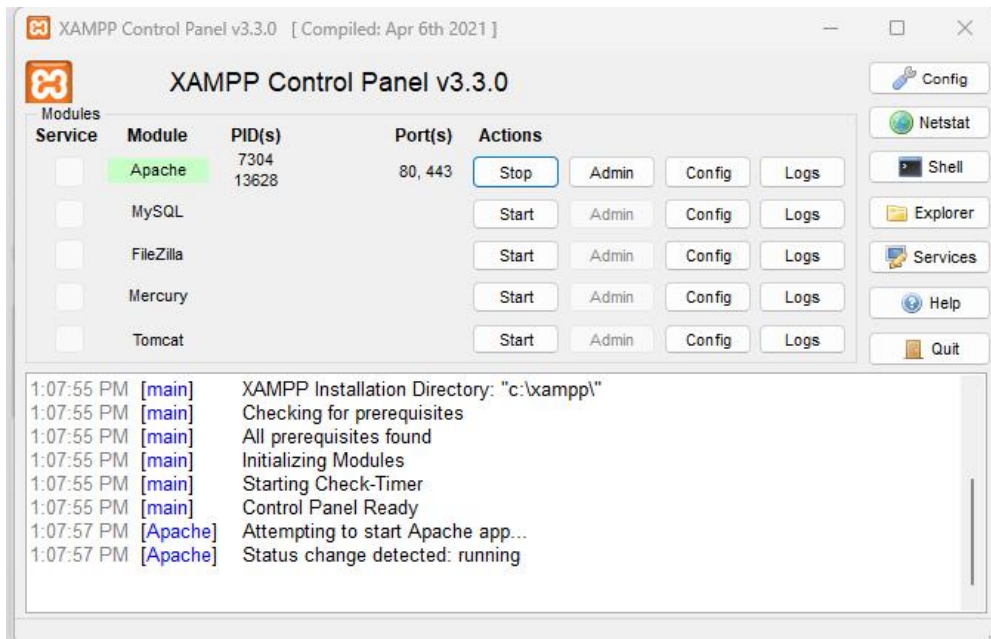
#### 2. Inside fbclone, create the following files:

- index.html – Fake Facebook login page
- login.php – Handles form submission and writes credentials to a file
- redirect.html – A fake redirect page (e.g., “Loading...” or “Connecting...”)
- view.php – Displays captured login credentials
- creds.txt – Leave this blank; it will store captured usernames and passwords
- fb.png – Facebook logo for realism



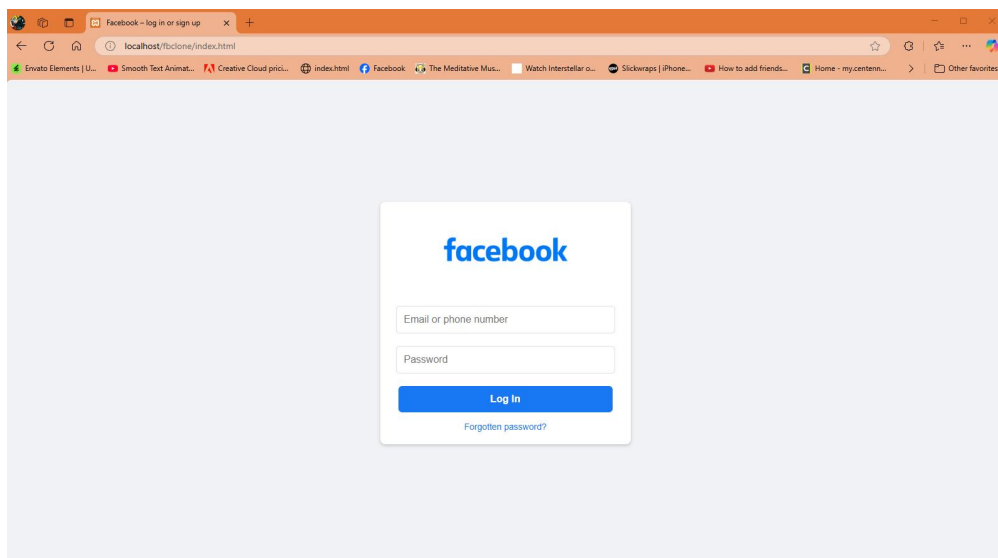
### 3. Start XAMPP

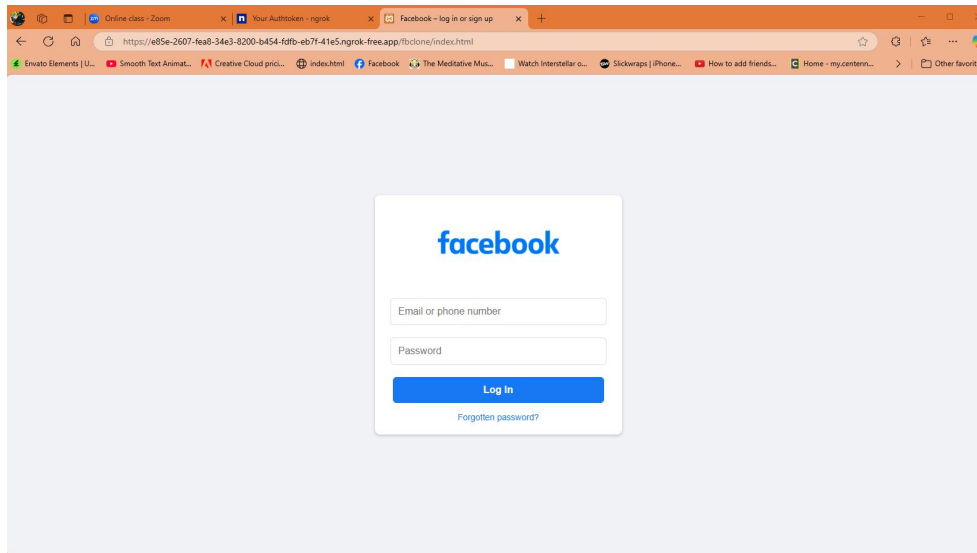
- Open **XAMPP Control Panel**
- Start the **Apache** module only
- Confirm it shows “Running” in green



### 4. Test on Browser

- Go to <http://localhost/fbclone/index.html>
- Enter any test credentials (e.g., dummy email and password)
- After clicking **Log In**, you should land on [redirect.html](#)
- Visit <http://localhost/fbclone/view.php> to confirm the captured data





## 5. Use Ngrok to Share Your Site (Bonus Task)

- Open **Command Prompt**
- Navigate to your XAMPP htdocs directory or just run:

nginx

ngrok http 80

- Copy the public HTTPS link generated by ngrok
- Test the phishing site from another device or browser tab
- Credentials from remote submissions will still be stored in creds.txt

```
C:\Users\elure\Desktop\XAMPP > ngrok http 80

USAGE:
  ngrok [command] [flags]

COMMANDS:
  config      update or migrate ngrok's configuration file
  http        start an HTTP tunnel
  tcp         start a TCP tunnel
  tunnel      start a tunnel for use with a tunnel-group backend

EXAMPLES:
  ngrok http 80                                # secure public URL for port 80 web server
  ngrok http --url baz.ngrok.dev 8080          # port 8080 available at baz.ngrok.dev
  ngrok tcp 22                                  # tunnel arbitrary TCP traffic to port 22
  ngrok http 80 --oauth=google --oauth-allow-email=foo@foo.com # secure your app with oauth

Paid Features:
  ngrok http 80 --url mydomain.com              # run ngrok with your own custom domain
  ngrok http 80 --cidr=allow 2600:8c00::a03c:91ee:fe69:9695/32 # run ngrok with IP policy restrictions
  Upgrade your account at https://dashboard.ngrok.com/billing/subscription to access paid features

Upgrade your account at https://dashboard.ngrok.com/billing/subscription to access paid features

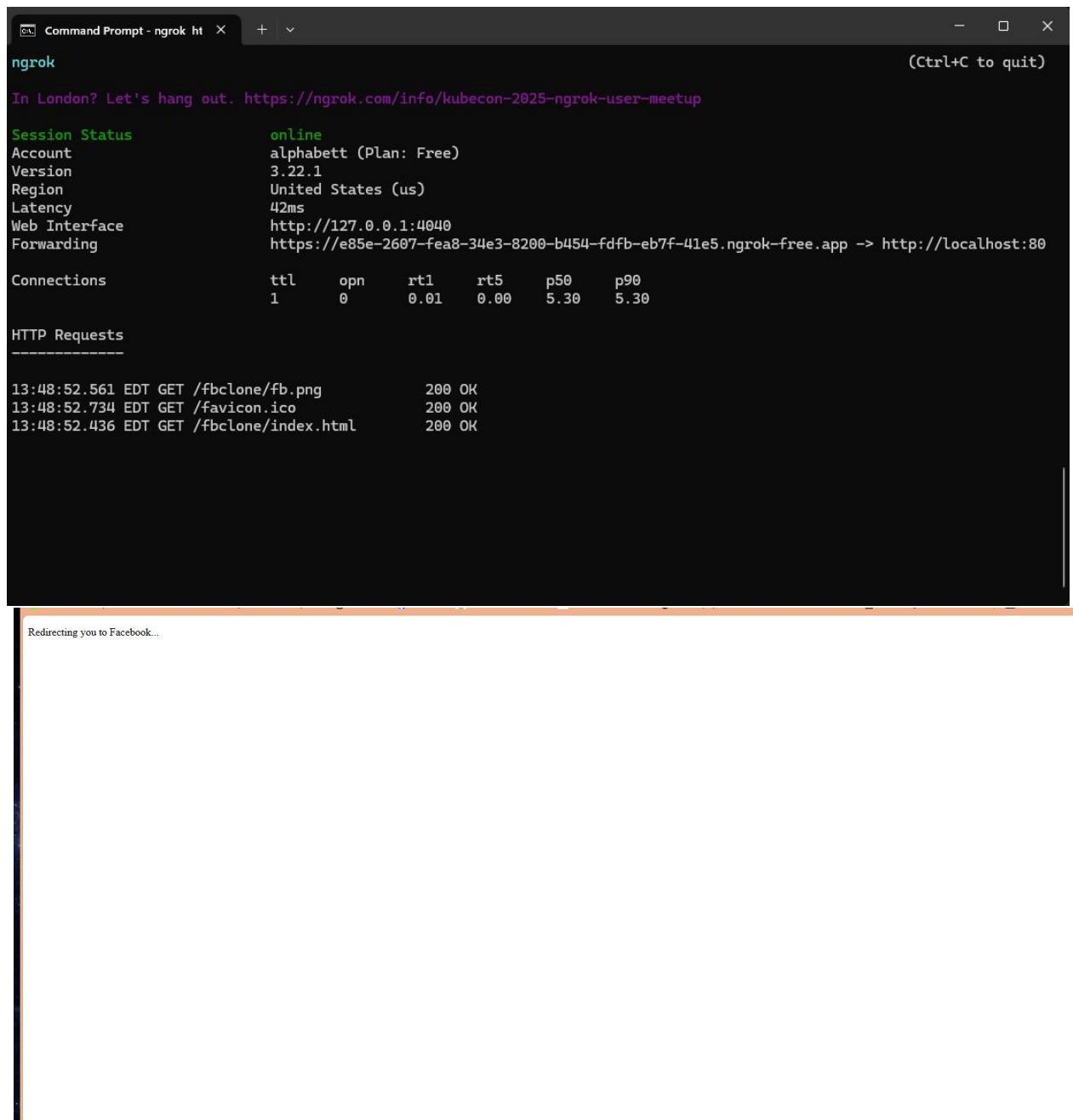
Flags:
  -h, --help      help for ngrok

Use "ngrok [command] --help" for more information about a command.

ngrok is a command line application, try typing 'ngrok.exe http 80'
at this terminal prompt to expose port 80.
C:\Users\elure\Desktop\XAMPP FILES\ngrok-v3-stable-windows-amd64>ngrok http 80
```

✓ Submit:

- Screenshot of the phishing login page -
- Screenshot of view.php showing the captured credentials
- Screenshot of redirect.html in browser
- Screenshot of your folder showing all the required files
- If using Ngrok: a screenshot of your terminal with the generated link -



The image shows a Windows Command Prompt window titled "Command Prompt - ngrok ht" with a dark background. The ngrok application is running, displaying its status and session information. Below the status, it shows a table of connections and a list of HTTP requests. The browser window below the terminal shows a message "Redirecting you to Facebook..." in a white box on a dark background.

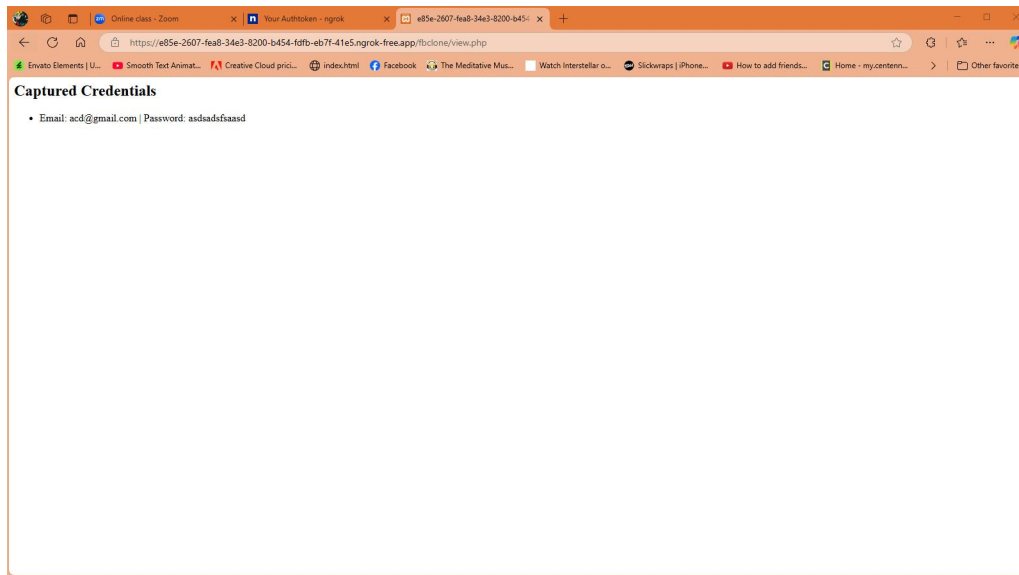
```
ngrok (Ctrl+C to quit)
In London? Let's hang out. https://ngrok.com/info/kubecon-2025-ngrok-user-meetup

Session Status      online
Account             alphabett (Plan: Free)
Version             3.22.1
Region              United States (us)
Latency              42ms
Web Interface        http://127.0.0.1:4040
Forwarding            https://e85e-2607-fea8-34e3-8200-b454-fdfb-eb7f-41e5.ngrok-free.app -> http://localhost:80

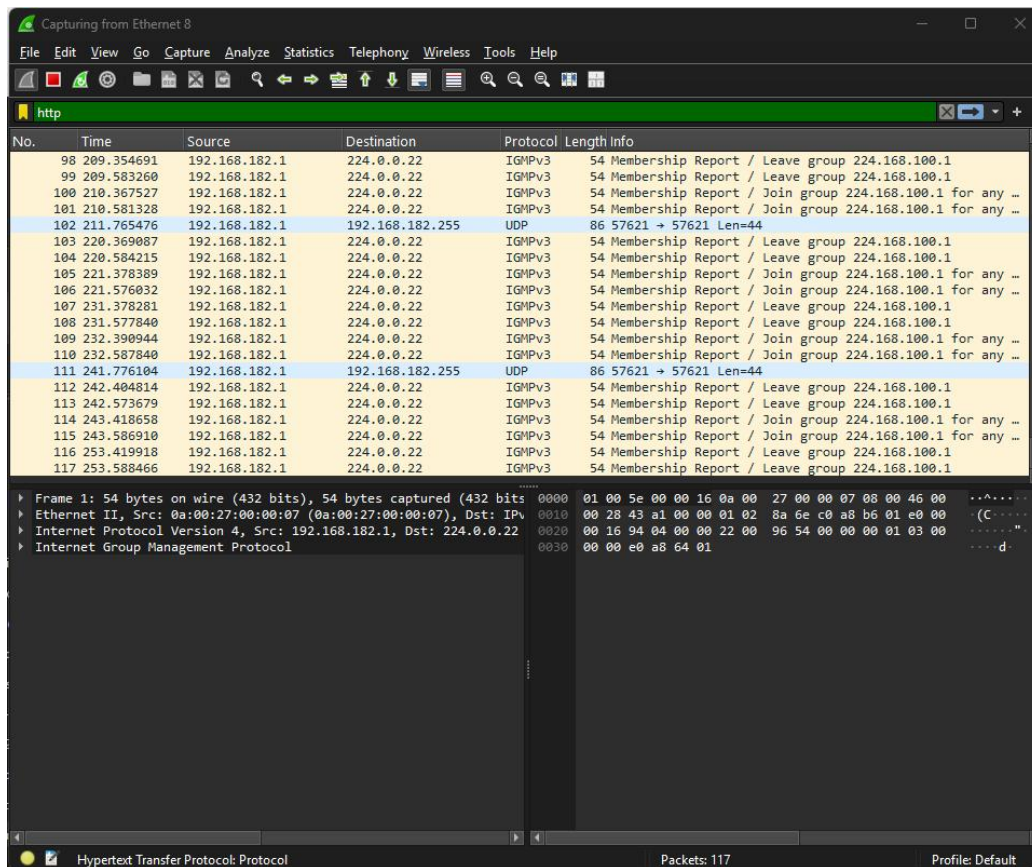
Connections          ttl    opn    rt1    rt5    p50    p90
1                    0      0.01   0.00   5.30   5.30

HTTP Requests
-----
13:48:52.561 EDT GET /fbclone/fb.png          200 OK
13:48:52.734 EDT GET /favicon.ico              200 OK
13:48:52.436 EDT GET /fbclone/index.html       200 OK

Redirecting you to Facebook...
```



Wireshark analyzing http for academic/defensive education only



The image shows a Wireshark packet capture window. 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 display filter bar shows 'Apply a display filter ... <Ctrl-/>'. The main packet list table contains 26 entries, each with a number, time, source, destination, protocol, and length. The first packet is an IGMPv3 Membership Report. The details pane for the first packet shows the frame structure: Ethernet II, Internet Protocol Version 4, and Internet Group Management Protocol. The packet bytes are displayed in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
7	11.077282	192.168.182.1	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.168.100.1
8	12.027803	192.168.182.1	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.168.100.1 for any ...
9	12.087414	192.168.182.1	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.168.100.1 for any ...
10	21.282254	192.168.182.1	239.255.255.250	SSDP	212	M-SEARCH * HTTP/1.1
11	22.042181	192.168.182.1	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.168.100.1
12	22.087375	192.168.182.1	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.168.100.1
13	22.286926	192.168.182.1	239.255.255.250	SSDP	212	M-SEARCH * HTTP/1.1
14	23.054766	192.168.182.1	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.168.100.1 for any ...
15	23.084750	192.168.182.1	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.168.100.1 for any ...
16	23.299827	192.168.182.1	239.255.255.250	SSDP	212	M-SEARCH * HTTP/1.1
17	24.312864	192.168.182.1	239.255.255.250	SSDP	212	M-SEARCH * HTTP/1.1
18	31.662707	192.168.182.1	192.168.182.255	UDP	86	57621 → 57621 Len=44
19	33.061772	192.168.182.1	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.168.100.1
20	33.076653	192.168.182.1	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.168.100.1
21	34.076948	192.168.182.1	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.168.100.1 for any ...
22	34.581622	192.168.182.1	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.168.100.1 for any ...
23	44.084092	192.168.182.1	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.168.100.1
24	44.575462	192.168.182.1	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.168.100.1
25	45.098014	192.168.182.1	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.168.100.1 for any ...
26	45.573728	192.168.182.1	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.168.100.1 for any ...

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0  
Ethernet II, Src: 0a:00:27:00:00:07 (0a:00:27:00:00:07), Dst: IPv4  
Internet Protocol Version 4, Src: 192.168.182.1, Dst: 224.0.0.22  
Internet Group Management Protocol

0000 01 00 5e 00 00 16 0a 00 27 00 00 07 08 00 46 00  
0010 00 28 43 a1 00 00 01 02 8a 6e c0 a8 b6 01 e0 00  
0020 00 16 94 04 00 00 22 00 96 54 00 00 00 01 03 00  
0030 00 00 e0 a8 64 01

wireshark: Ethernet 8K46K52.pcapng Packets: 26 Profile: Default