Trường Đại học Khoa học Tự nhiên

Khoa Công Nghệ Thông Tin

BÁO CÁO ĐỒ ÁN

<u>ĐỒ ÁN 1:</u> LẬP TRÌNH SOCKET-PROXY SERVER.

<u>MÔN:</u> MẠNG MÁY TÍNH.

<u>Các thành viên trong nhóm:</u>

Đoàn Ngọc Nguyên.	**19120605.**
Lê Hồng Quân.	**19120629.**
Nguyên Anh Quốc.	**19120633.**

Mục Lụcx

I. Phân công công việc của nhóm:

STT	MSSV	Họ và tên	Công việc
1	19120605	Đoàn Ngọc Nguyên	• Thiết kế chương trình. • Cài đặt và tìm hiểu các method GET và POST • Cài đặt phần nhận và xử lý các thông tin từ gói tin request của client
2	19120629	Lê Hồng Quân	• Tìm hiểu giải pháp và các tài liệu hỗ trợ • Cài đặt phần chặn truy cập các trang web có tên miền thuộc file blacklist.conf. • Cài đặt phần chạy đa luồng, chạy Proxy Server (run Server).
3	19120633	Nguyễn Anh Quốc	• Tìm hiểu giải pháp và các tài liệu hỗ trợ. • Tổng hợp chương trình và viết báo cáo. • Cài đặt phần nhận gói tin response từ Web Server và trả về cho client.

II. Những hàm chức năng chính:

1. getWebInfor:

- Hàm: def getWebInfor(strData).
- Chức năng: Từ request nhận được từ Client gửi lên, hàm getWebInfor sẽ phân tích từ chuỗi request ra các thông tin như host, port, method, data và url.
- Các tham số:
  + strData: sẽ là một chuỗi ký tự thông tin của request từ Client gửi lên cách nhau bằng các khoảng trắng.

- Kết quả: Sau khi gọi hàm ta sẽ có các thông tin về Web Server mà Client gửi request như: host, port, method, data và url.

2. **loadBlackList:**
   - Hàm: def loadBlackList().
   - Chức năng: Mở và đọc file danh sách các tên miền bị chặn bởi Proxy Server (Black list).
   - Các tham số: Hàm này không có tham số.
   - Kết quả: Sau khi gọi hàm ta sẽ có các tên miền bị chặn trong file blacklist.conf.
3. **readResponse:**
   - Hàm: def readResponse(webServer).
   - Chức năng: nhận Response từ Web Server để gửi về cho Client
   - thông qua Socket webServer
   - Các tham số:
     + webServer: đây là Socket đã gửi request lên cho Proxy Server, Response (nhận được từ Web Server) sẽ được gửi trả về cho Client thông qua Socket này.
   - Kết quả: Sau khi gọi hàm ta sẽ có các thông tin về Web Server mà Client gửi request như: host, port, method, data và url.
4. **requestSendToWebServer:**
   - Hàm: def requestSendToWebServer(web).
   - Chức năng: kiểm tra method request của Client gửi lên và tạo request của Client tùy vào method. Ở đây method là GET và POST.
   - Các tham số:
     + web: đây là Socket gửi request lên cho Proxy Server.
   - Kết quả: Sau khi gọi hàm ta sẽ thay đổi request của Client dựa vào method GET hay POST.
5. **Process:**
   - Hàm: def Process(conn, client_addr).
   - Chức năng: Kiểm tra có phải nghi thức HTTP không? Kiểm tra tên miền có bị chặn hay không? Nếu web không bị chặn và là nghi thức HTTP thì gửi request lên Server và lấy reponse từ Server gửi về Client.
   - Các tham số:
     + conn: là đối tượng socket dùng để gửi và nhận dữ liệu kết nối.

+ client_addr: là địa chỉ liên kết socket ở đầu bên kia kết nối.

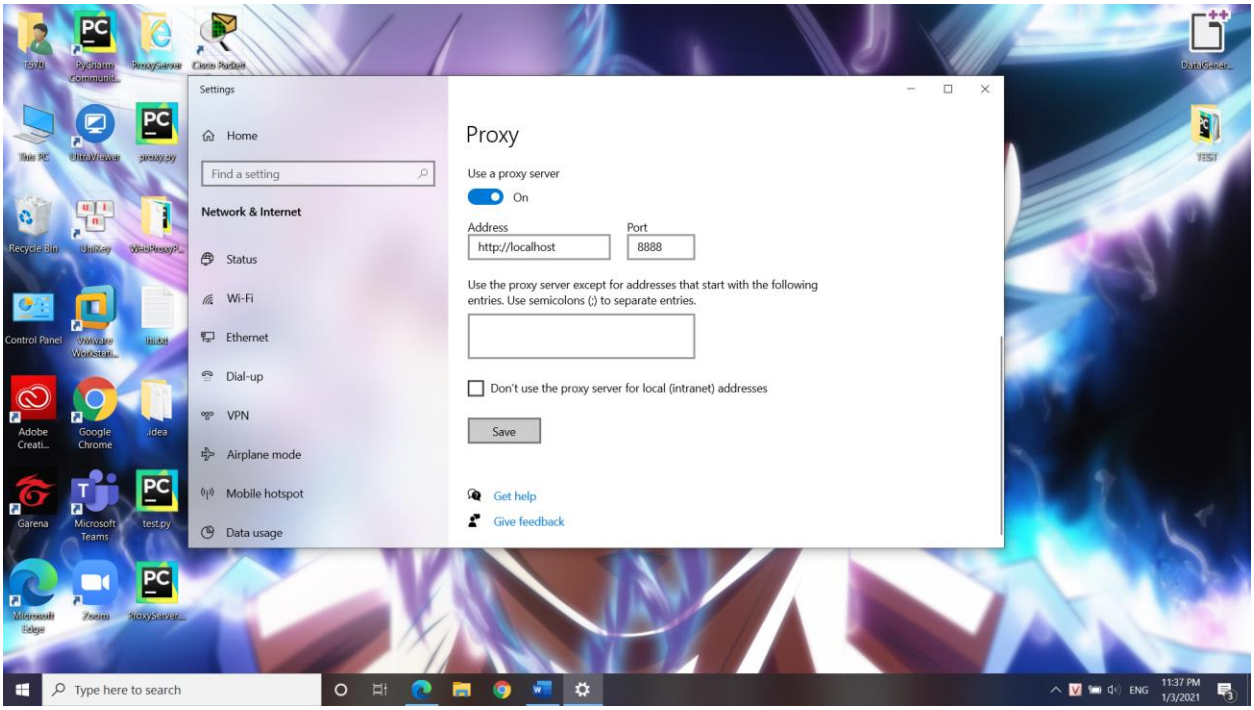
- Kết quả: Tắt kết nối khi trang truy cập không phải HTTP. Nếu truy cập địa chỉ trong blacklist thì gửi trang chặn về cho client. Nếu không thì client nhận được dữ liệu từ Server.

6. **isForbidden:**
   - Hàm: def isForbidden(host).
   - Chức năng: kiểm tra tền miền (chuỗi host) có nằm trong file blacklist.conf (bị cấm truy cập) hay không?
   - Các tham số:
     + host: tên miền cần kiểm tra.
   - Kết quả: nếu host nằm trong blacklist thì trả về true, ngược lại trả về false.

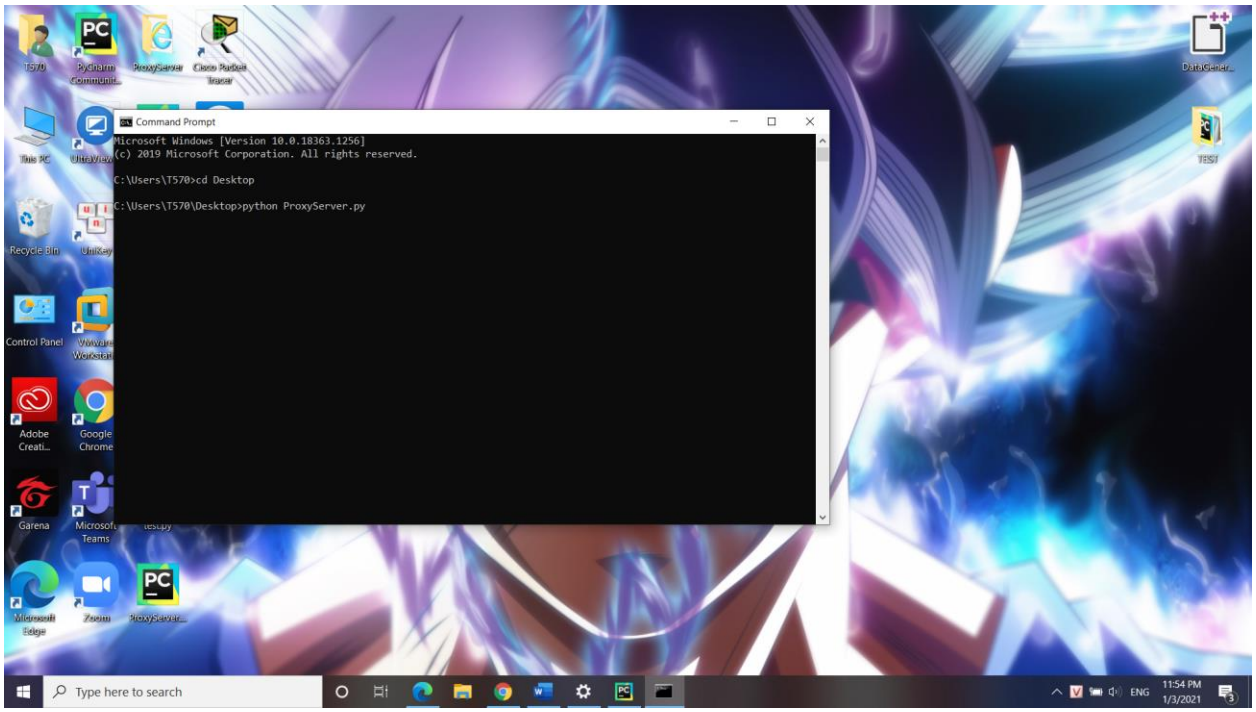
7. **main:**
   - Hàm: def main()
   - Chức năng: Tạo thread và tạo ProxyServer lắng nghe ở (HOST, PORT). Tạo queue lắng nghe yêu cầu ở client.
   - Các tham số: Không có.
   - Kết quả: Thực hiện công việc như ProxyServer.

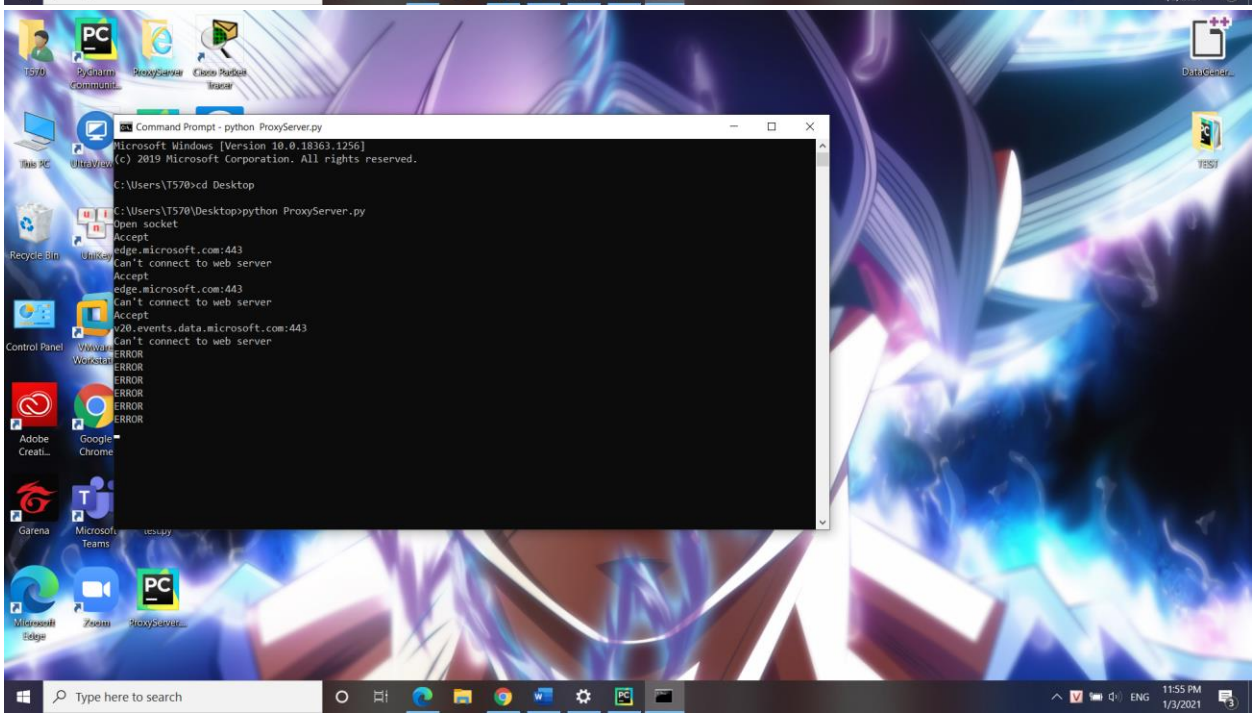
III. Cách chạy chương trình và kết quả chạy được:

- Mở trình duyệt lên và kết nối đến Proxy Server (IP: 127.0.0.1, Port: 8888):

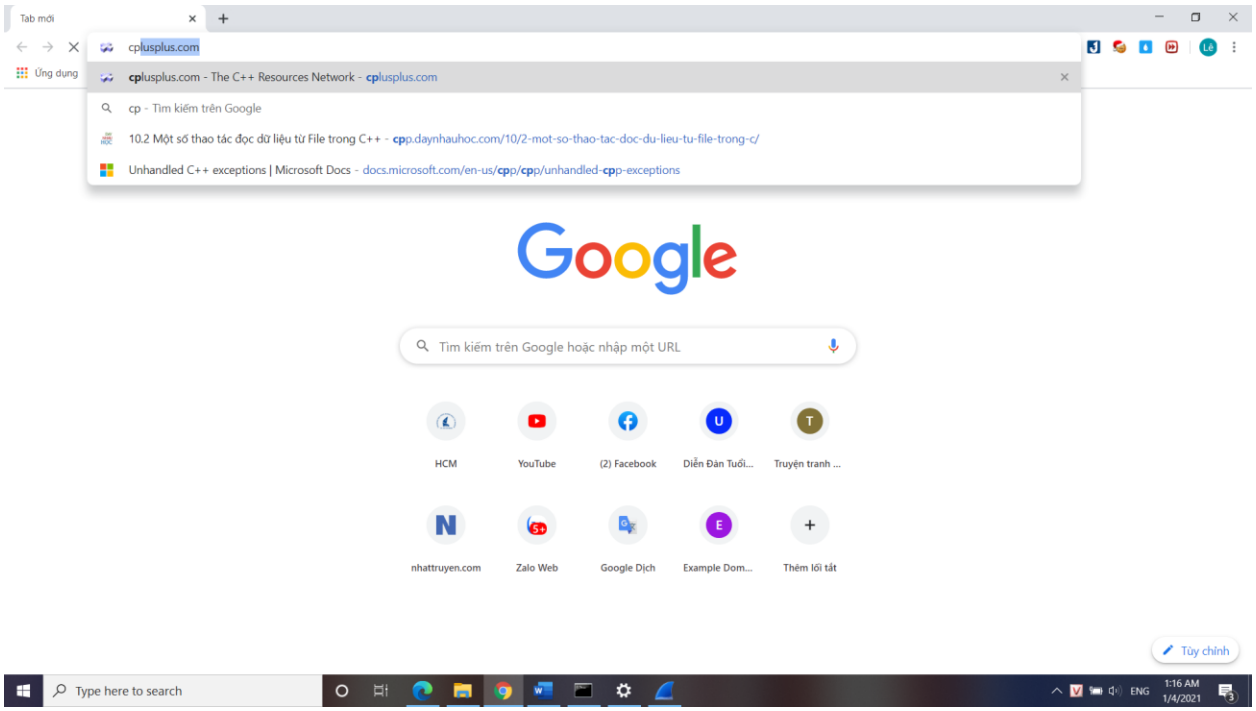


- Chạy chương trinh ProxyServer; cài đặt python cho máy; dùng cmd hay terminal. Ở cmd dùng lệnh cd để dẫn tới ổ đĩa và thư mục chưa file ProxyServer.py, và nhập lệnh: “python ProxyServer.py”.



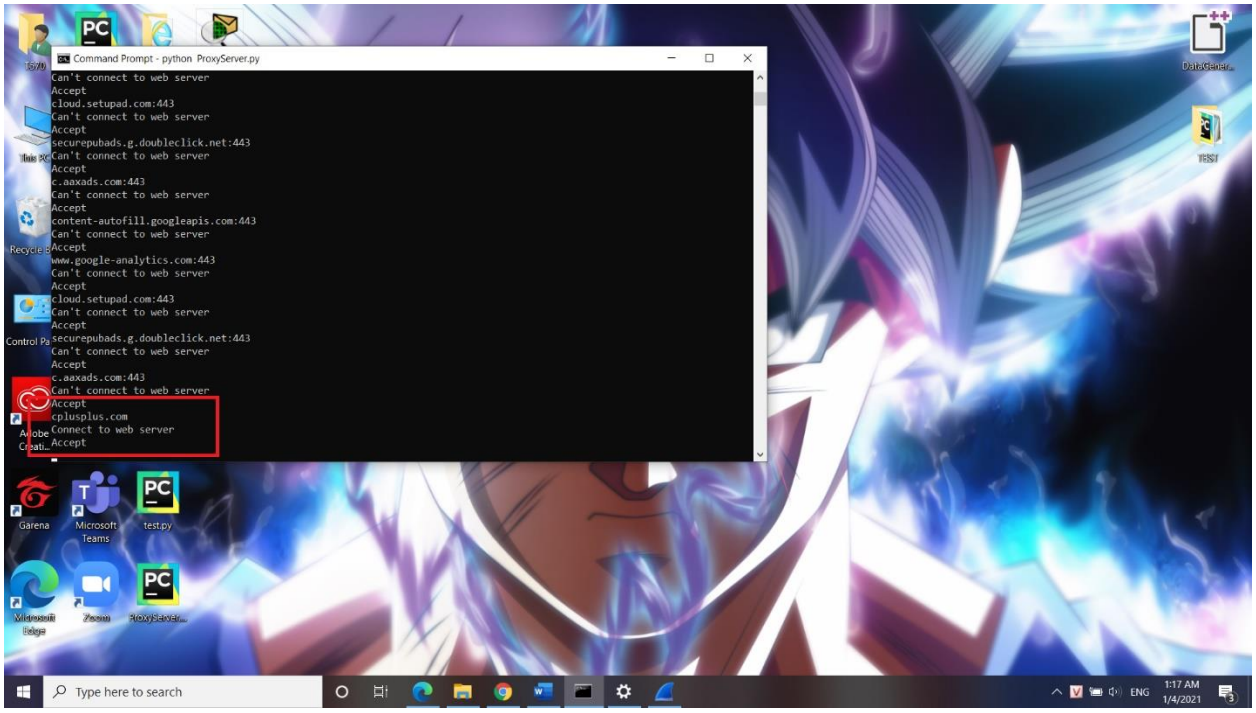


- Truy cập vào trang cplusplus.vn (hoặc các trang HTTP không nằm trong blacklist.conf)

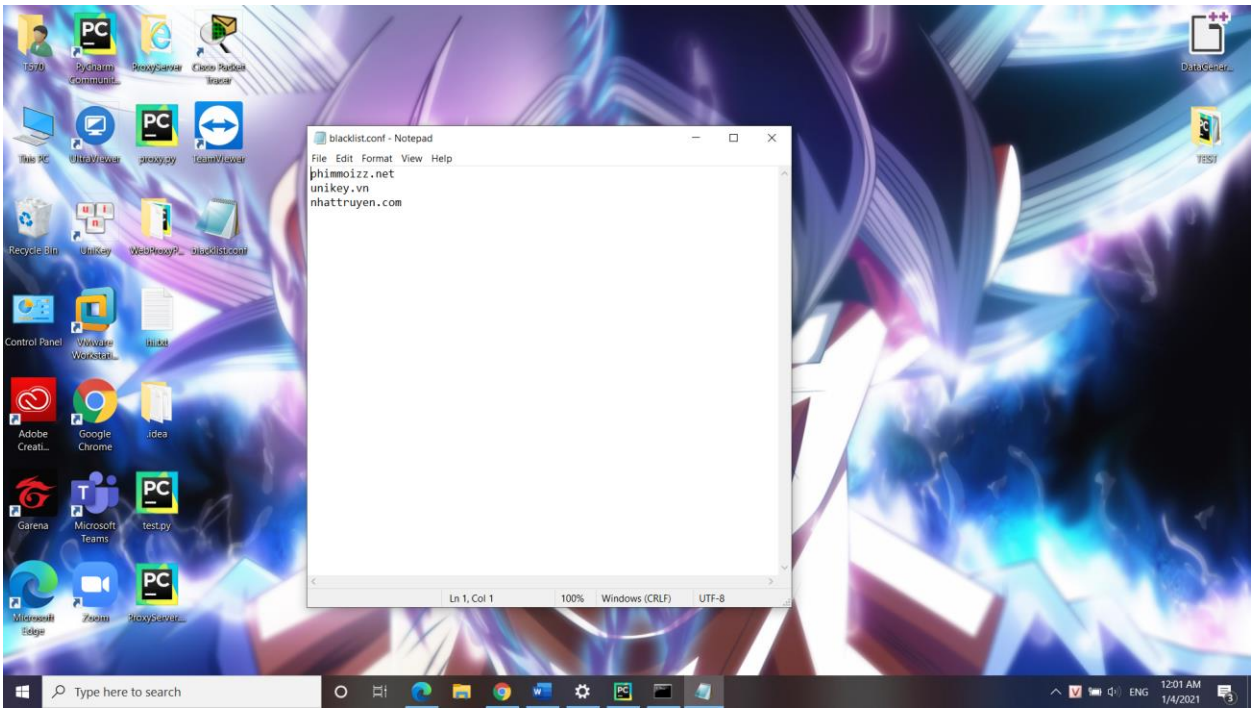


- Kết quả:

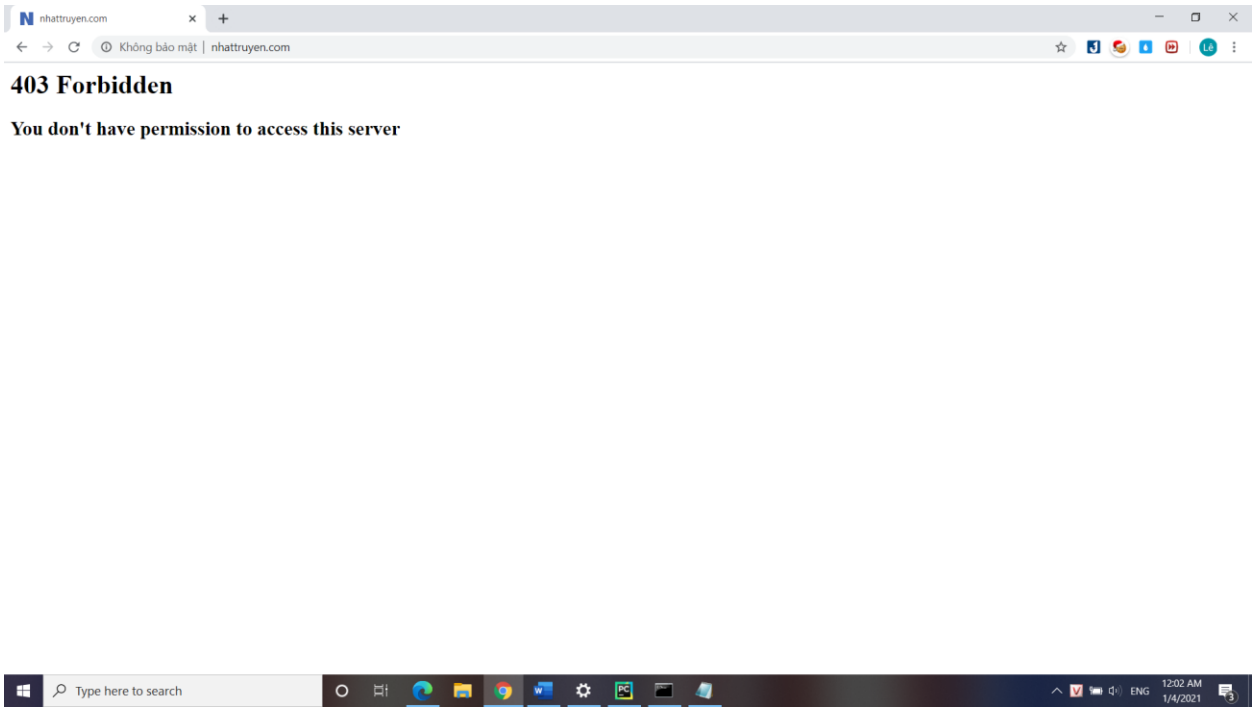
- Chương trình hiển thị:



- Thư mục blacklist.conf



- Truy cập trang web "nhattruyen.com":

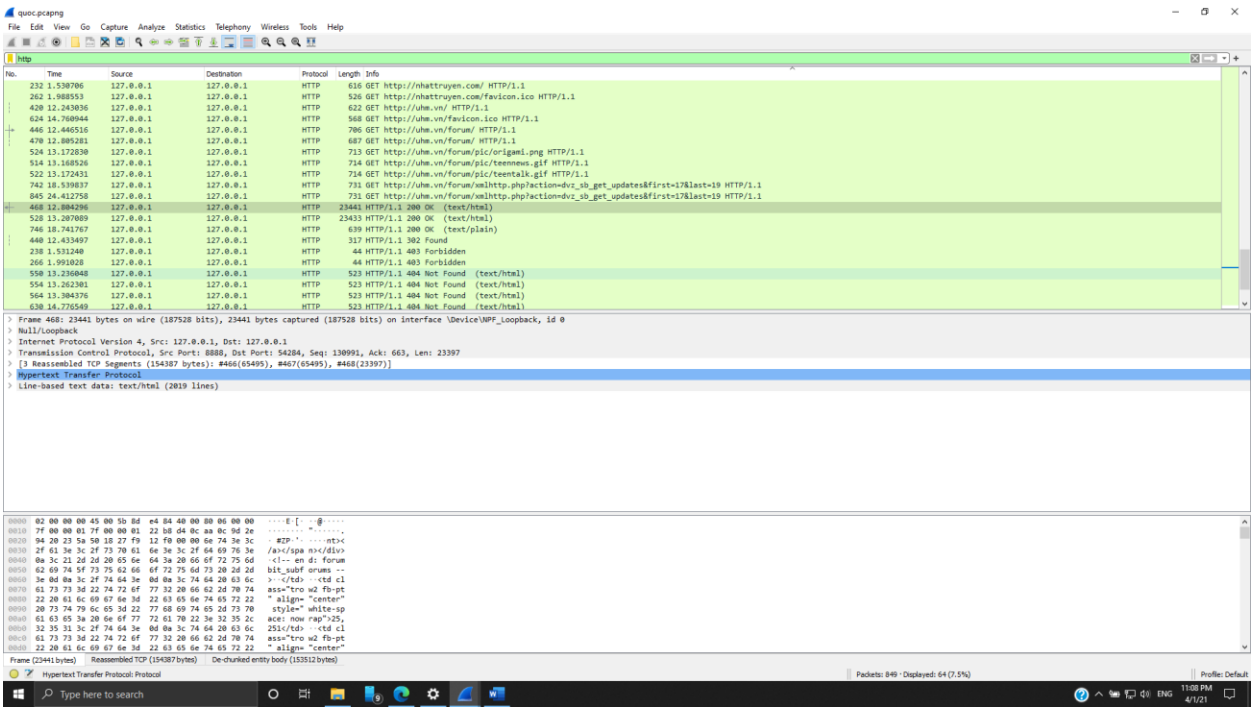


IV. Mức độ hoàn thành:

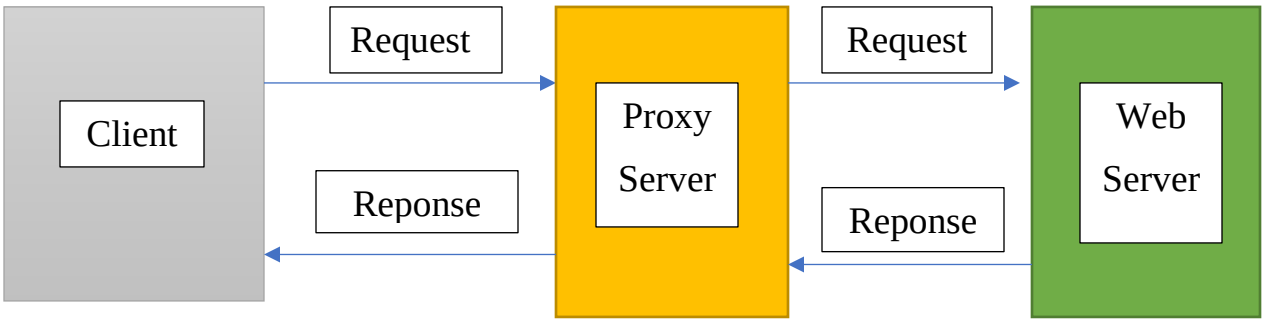
1. **Các chức năng làm được:**
   - Proxy Server chỉ hỗ trợ cho giao thức HTTP
   - Proxy Server cho phép Client truy cập website thông qua các method: GET, POST.
   - Proxy Server phải xử lý đồng thời được các request từ client.
   - Chặn tất cả các truy cập đến các website có tên miền (host) nằm trong file blacklist.conf.
2. **Các chức năng chưa làm được:** Không có
3. **Mức độ hoàn thanh đồ án:**
   Đã hoàn thanh 100% yêu cầu của đồ án.

V. Dùng Wireshark bắt gói tin. Mô tả quá trinh nhận và truyền dữ liệu.

- Các gói tin bắt được khi truy cập trang web “uhm.vn”:



- Quá trình gửi nhận dữ liệu giữa Client – Proxy Server và Proxy Server – Web Server.



  - Đầu tiên client sẽ gửi gói http request lên cho Proxy Server.
  - Từ gói tin http request nhận được từ client, Proxy Server sẽ lấy ra những thông tin cần thiết (như host, port, url). Proxy Server sẽ kiểm tra xem host có thuộc blacklist hay không? Nếu có sẽ gửi ngay gói tin http response 403 forbidden về client. Nếu không Proxy Server sẽ chuyển tiếp gói tin http request lên cho Web

Server (với thông tin host, port sau khi đã phân tích từ gói tin http request):

- Tiếp theo Proxy Server sẽ nhận gói tin http response từ Web Server, sau đó chuyển tiếp về cho Client, đồng thời cập nhật lại file cache.
- Sau đó, tương tự các bước ở trên Client sẽ tiếp tục gửi các gói tin request và nhận các đối tượng đầy đủ cho 1 trang web:

VI. Tại sao lại cần Proxy Server trong thực tế:

- **Dễ dàng kiểm soát việc sử dụng Internet của nhân viên và trẻ em:** Công ty và phụ huynh thiết lập máy chủ proxy để kiểm tra và giám sát nhân viên hoặc trẻ em sử dụng Internet.Phần lớn, các tổ chức không muốn nhân viên truy cập các trang web cụ thể trong thời gian cụ thể hoặc phụ huynh không mún con của mình truy cập các trang web không dành cho lứa tuổi của em.Vì thể họ có thể cấu hình một máy chủ proxy để ngăn chặn truy cập vào trang web cụ thể, điều hướng bạn bằng một ghi chú hoặc một nhắc nhở yêu cầu bạn không thể xem trang web này trên mạng này.Họ có thể giám sát và ghi lại tất cả các yêu cầu web.Vì vậy có thể không cần chặn họ vẫn có thể biết bạn dành thời gian cho những việc khác ngoài công việc.
- **Tiết kiệm băng thông và cải thiện tốc độ:** Các tổ chức cũng có thể nhận được hiệu suất mạng tổng thể tốt hơn khi sử dụng máy chủ proxy. Các máy chủ proxy có thể lưu vào bộ nhớ cache (lưu một bản sao trang web cục bộ) các trang web hay truy cập. Do đó khi yêu cầu trang google.com, máy chủ proxy sẽ kiểm tra xem có bản sao mới nhất của trang web này hay không và sau đó sẽ gửi cho bạn bản sao đã lưu. Điều này có nghĩa là khi hàng trăm người truy cập vào google.com cùng một thời điểm từ cùng một máy chủ proxy, máy chủ này chỉ cần gửi một yêu cầu đến google.com. Điều này giúp tiết kiệm băng thông của công ty và cải thiện hiệu suất mạng.
- **Bảo mật riêng tư:** Cá nhân và tổ chức cũng sử dụng máy chủ proxy để duyệt Internet riêng tư hơn. Một số máy chủ proxy sẽ thay đổi địa chỉ IP và thông tin nhận dạng khác. Điều này có nghĩa là máy chủ đích không biết ai thực sự đã thực hiện yêu cầu ban đầu, giúp giữ thông tin cá nhân và thói quen duyệt web của bạn riêng tư hơn.
- **Cải thiện bảo mật:** Bạn có thể cấu hình máy chủ proxy để mã hóa yêu cầu web để không ai có thể đọc được giao dịch của bạn. Ngoài ra, người dùng cũng có thể tránh các trang web độc hại thông qua máy chủ proxy. Các tổ chức có thể kết nối máy chủ proxy của họ với Mạng riêng ảo (VPN), do đó

người dùng từ xa có thể truy cập Internet thông qua proxy của công ty. VPN kết nối trực tiếp đến mạng công ty để có thể kiểm soát và xác minh người dùng của họ có quyền truy cập vào các tài nguyên họ cần (email, dữ liệu nội bộ) đồng thời cũng cung cấp kết nối an toàn cho người dùng để bảo vệ dữ liệu công ty.

- **Truy cập vào các tài nguyên bị chặn:** Máy chủ proxy cho phép người dùng phá vỡ các hạn chế nội dung do công ty hoặc một số tổ chức áp đặt. Nếu truy cập vào trang web bị chặn, bạn có thể đăng nhập vào máy chủ proxy ở nơi khác và xem từ đó. Máy chủ proxy khiến bạn giống như ở Mỹ nhưng thực ra bạn đang ở Việt Nam.