**BÁO CÁO**

**MÔN: MẠNG MÁY TÍNH**

**Đinh Nguyên Khánh – 19120087**

**Lớp 19CTT1**

**Trình bày nội dung báo cáo:**

**Phần 1**: ***Phân công công việc của nhóm, ghi cụ thể công việc của mỗi người.***

**Phần 2:** ***Những hàm chức năng chính (không copy code vào báo cáo, chỉ báo cáo tên hàm, các tham số cần truyền vào, chức năng của hàm, kết quả là gì sau khi gọi hàm)***

1. def main():

* *Tham số*: không có
* *Chức năng* :

+ Chờ xử lý hàng đợi

+ Tạo Socket

+ Kết nối Socket đến port and host

+ Tạo luồng xử lý yêu cầu

1. def printout(type, method, url, ver, clientAddr):

* *Tham số:*

+ type: kiểu có thể là Request, Response, BLOCKED SITE, …

+ method: phương thức có thể là GET, CONNECT, …

+ url: đường dẫn url

+ ver: version HTTP

+ clientAddr : địa chỉ của Client

* *Chức năng:*

+ In thông báo ra màn hình

1. def analyzeHeader(header, clientAddr):

* *Tham số:*

+ header: sau khi lấy request từ client thì header chính là dòng đầu tiên.

+ clientAddr : địa chỉ của client.

* *Chức năng:*

+ Phân tích header để tìm method, url, ver

+ Phân tích url để tìm HTTP position và Port position.

* *Kết quả sau khi gọi hàm:*

+ Trả về WebServer và Port

1. def Handle(connect, clientAddr):

* *Tham số:*

+ connect: nhận kết nối

+ clientAddr: địa chỉ của Client

* *Chức năng:*

+ Từ connect lấy ra request của Client

+ Kiểm tra Url có trong Blacklist hay không.

+ Gọi hàm Analyze Client Request (def analyzeHeader(header, clientAddr)) để lấy ra 2 giá trị webserver và port

+ Tạo một Socket kết nối tới webserver thật

+ Gửi một Client Request đến server đó.

+ Nhận Response từ server thông qua Socket.

+ Gửi phản hồi đó đến Client.

**Phần 3:** ***Chụp hình cách chạy chương trình và kết quả chạy được.***

**Quy trình:**

1. Cấu hình FireFox đến port 8888 và HTTP proxy.
2. Build chương trình trên VS
3. Truy cập vào các trang web và xem nội dung mà nó hiển thị

http://gaia.cs.umass.edu/

<http://www.example.org/>

<http://www.cs.toronto.edu/~arnold/>

1. Truy cập các trang bị cấm, xem thử Client có nhận được kết quả HTTP response với status code 403 (Forbidden) không?

facebook.com

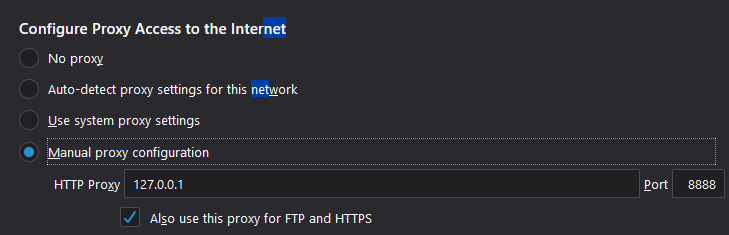
google.com

reddit.com

diendantoanhoc.net

**Thực hiện:**

*Bước 1: Cấu hình*

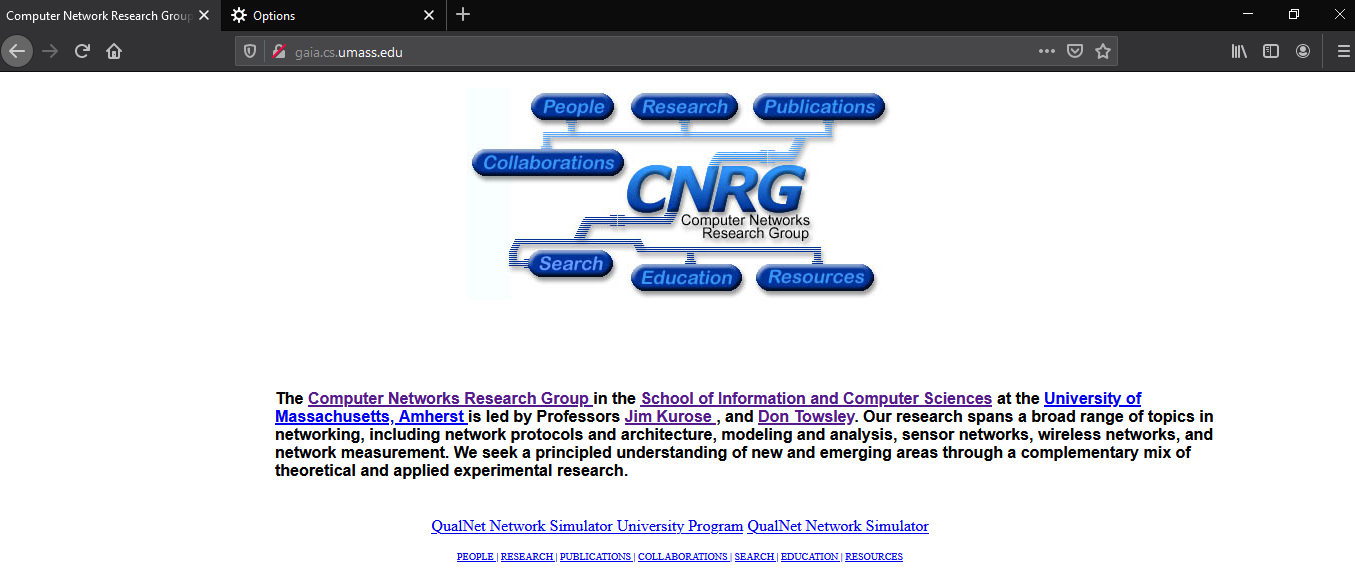


*Bước 2: Build*

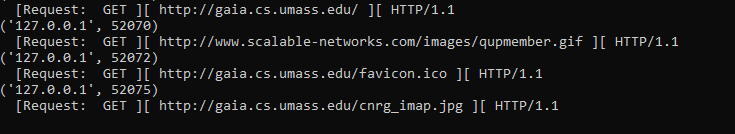


Đang lắng nghe tại port 8888

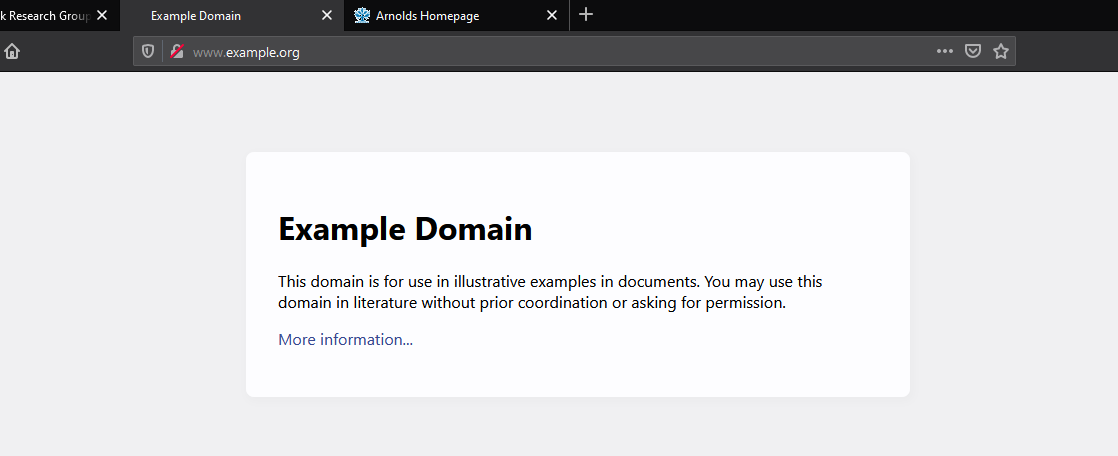
*Bước 3: Hiển thị nội dung trang web*

[http://gaia.cs.umass.edu/](http://gaia.cs.umass.edu/)

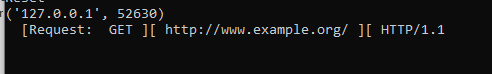
Những thứ nhận được trên màn hình build



http://www.example.org/



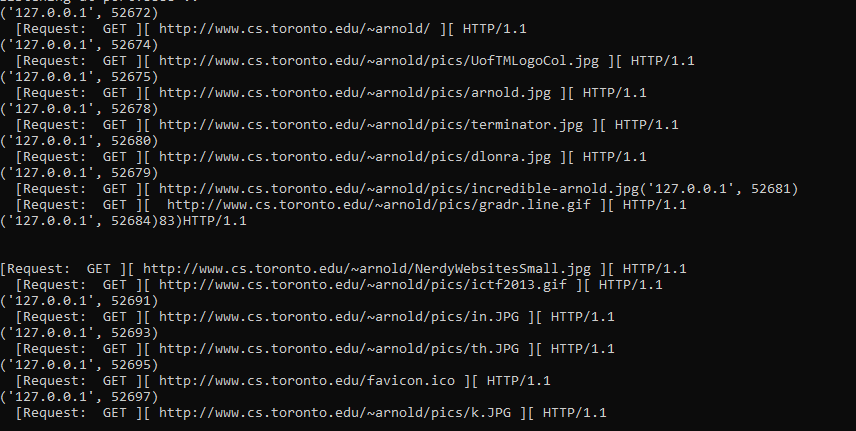
Một phần hiển thị trên màn hình build



<http://www.cs.toronto.edu/~arnold/>

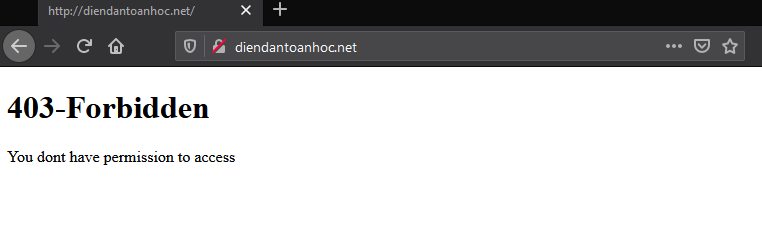


Những thứ hiển thị trên màn hình build

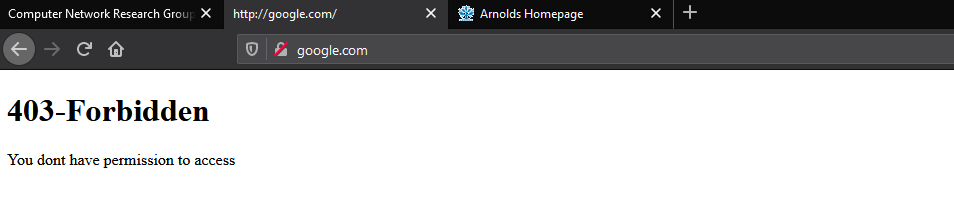


*Bước 4: Truy cập vào các trang web bị cấm*

diendantoanhoc.net



google.com



**Phần 4**: ***Chức năng làm được và chưa được. Mức độ hoàn thành (%).***

* Cho phép Client truy cập thông qua các method: GET, POST *(hoàn thành)*

- Hỗ trợ HTTP *(hoàn thành)*

- Xử lý đồng thời các yêu cầu từ Client *(hoàn thành)*

- Lắng nghe tại port 8888, chờ kết nối từ Client *(hoàn thành)*

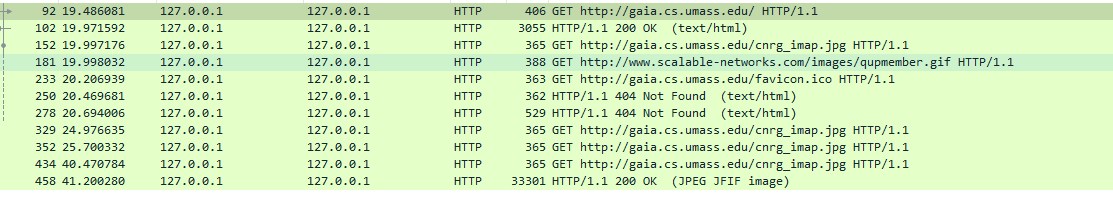
- Chặn tất cả các truy cập đến các domain có trong blacklist.conf *(hoàn thành)*

Mức độ hoàn thành 100%

**Phần 5:** ***Dùng Wireshark bắt gói tin tại Proxy Server, và mô tả lại quá trình nhận dữ liệu giữa Client - Proxy Server và Proxy Server – Web Server.***

Một ví dụ đơn giản cho đường link: <http://gaia.cs.umass.edu/>

Em dùng máy của mình để host nên địa chỉ ip của Proxy là **127.0.0.1** (hơi khó nhìn)



Hình ảnh cho thấy Client gửi yêu cầu đến Proxy và Proxy gửi HTTP Status về lại cho Client



Tại Port 8888



Sau khi GET thì dữ liệu sẽ được chuyển từ port 8888 của Proxy đến WebServer



Sau khi được phản hồi dữ liệu sẽ từ WebServer chuyển về cho port 8888 của Proxy

**Phần 6**: ***Giải thích được tại sao lại cần Proxy Server trong thực tế.***

- Để kiểm soát việc sử dụng Internet của nhân viên và trẻ em: Tổ chức và phụ huynh thiết lập máy chủ proxy để kiểm soát và giám sát nhân viên hoặc trẻ em sử dụng Internet. Hầu hết các tổ chức không muốn nhân viên của họ xem các trang web cụ thể trong thời gian làm việc và họ có thể cấu hình máy chủ proxy để từ chối truy cập vào trang web cụ thể, điều hướng bạn bằng một ghi chú yêu cầu bạn không xem các trang web này trên mạng công ty. Họ có thể giám sát và ghi lại tất cả các yêu cầu web, do đó mặc dù không chặn trang web nhưng họ vẫn biết thời gian bạn dành cho những việc làm 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.

- 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.

**HẾT**