TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN – ĐHQG HCM

KHOA CÔNG NGHỆ THÔNG TIN

BÁO CÁO
ĐỒ ÁN THỰC HÀNH - SOCKET

Sinh viên thực hiện: **Hồ Đình Minh** **1712591**

Lạc Tuấn Minh **1712593**

Nguyễn Trọng Nghĩa **1712615**

Đinh Văn Ngọc **1712616**

Môn học: Mạng máy tính

Lớp: 17CTT5

TP HỒ CHÍ MINH, 06/06/2019

1. THÔNG TIN THÀNH VIÊN

1.1 Danh sách thành viên:

STT	MSSV	Họ và tên	Email
1	1712591	Hồ Đình Minh	1712591@student.hcmus.edu.vn
2	1712593	Lạc Tuấn Minh	1712593@student.hcmus.edu.vn
3	1712615	Nguyễn Trọng Nghĩa	1712615@student.hcmus.edu.vn
4	1712616	Đinh Văn Ngọc	1712616@student.hcmus.edu.vn

1.2 Bảng phân công công việc

STT	Họ và tên	Nhiệm vụ chính	Mức độ hoàn thành
1	Hồ Đình Minh	• Chương trình hỗ trợ HTTP (1.0 và HTTP 1.1). • Chương trình cho phép Client truy cập website thông qua Proxy Server. • Proxy Server chạy trên port 8888.	100%
2	Lạc Tuấn Minh		
3	Nguyễn Trọng Nghĩa	• Proxy Server xử lý đồng thời được các request từ client. • Cấu hình 1 file blacklist.conf chặn tất cả các truy cập trùng với các domain trong file. • Proxy Server caching lại nội dung của trang web	100%
4	Đinh Văn Ngọc		

2. NHỮNG HÀM CHỨC NĂNG CHÍNH

```
int GetContent_Length(string a);
```

+Tham số đầu vào: string a là phần Header của gói response từ Websever đến proxy

+Chức năng: lấy thông số trường Content-Length

+Đầu ra: số bytes trong trường Content-Length

```
void send_403_forbidden_mess(const SOCKET &acceptSock);
```

+Tham số đầu vào: acceptSock là cổng socket phía Client

+Chức năng: Gửi nội dung của file 403.html cho acceptSock khi client truy cập các trang cấm trong blacklist

```
void send_404_notfound_mess(const SOCKET &acceptSock);
```

+tương tự hàm :void send_403_forbidden_mess(const SOCKET &acceptSock), thực hiện khi client truy cập trang web không tồn tại.

```
bool is_in_blacklist(const string &recvbuf);
```

+Tham số đầu vào: string recvbuf là chuỗi request từ Client đến proxy.

+Chức năng: kiểm tra xem host của gói request có thuộc file blacklist.conf không

+Đầu ra: true hoặc false

```
char* file_cache(char *buff);
```

+Tham số đầu vào: char *buff là chuỗi request từ Client đến proxy.

+Chức năng: Chuyển dòng đầu tiên của gói buff thành tên của file chứa dữ liệu trong quá trình cache gói request đầu vào.

+Đầu ra: Chuỗi có dạng cache/abc.txt

```
int Cache(SOCKET &AcceptSocket, FILE *fin);
```

+Tham số đầu vào: AcceptSocket là cổng socket phía Client, *fin là con trỏ file trỏ đến file chứa dữ liệu đã cache.

+Chức năng: Lấy thông tin tin file txt và gửi về cho socket client.

+Đầu ra: trả ra 1 nếu cache thành công, 0 nếu thất bại

```
WORD WINAPI MyThread(LPVOID a);
```

+Đầu vào: LPVOID a, với a được ép kiểu từ Socket về LPVOID, a là socket của Client.

+Chức năng: Nhận gói request từ Socket Client.

+ Nếu gói request được lưu sẵn trong cache thì gọi hàm char* file_cache(char *buff)

+ Nếu gói request không được lưu sẵn trong cache thì tạo 1 socket kết nối đến Websever, 1 file chứa dữ liệu sắp cache, ta tiến hành lấy dữ liệu từ Websever, sau đó vừa lưu dữ liệu đó vào file txt vừa gửi về cho Client

```
int main(int argc, char *argv);
```

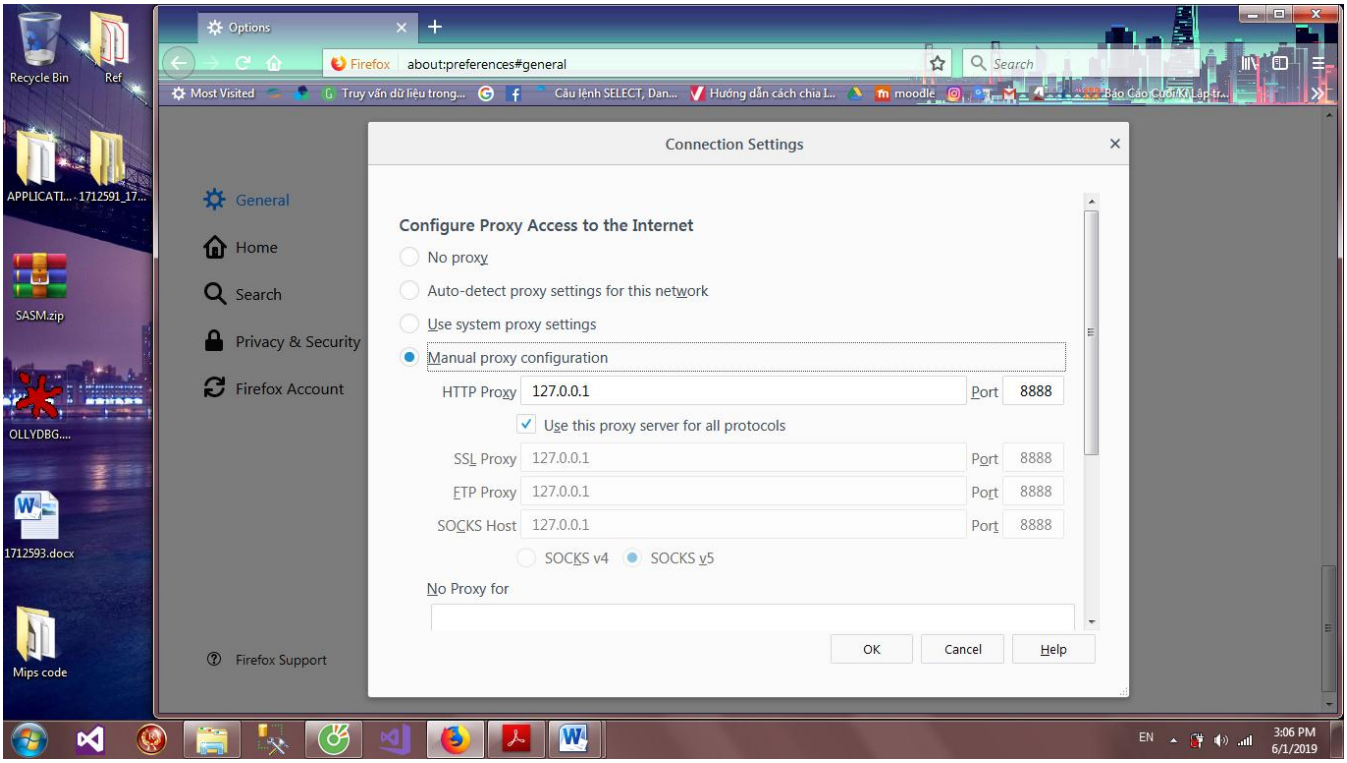
+Khởi tạo Winsock.

+Tạo socket listen để lắng nghe phía Client.

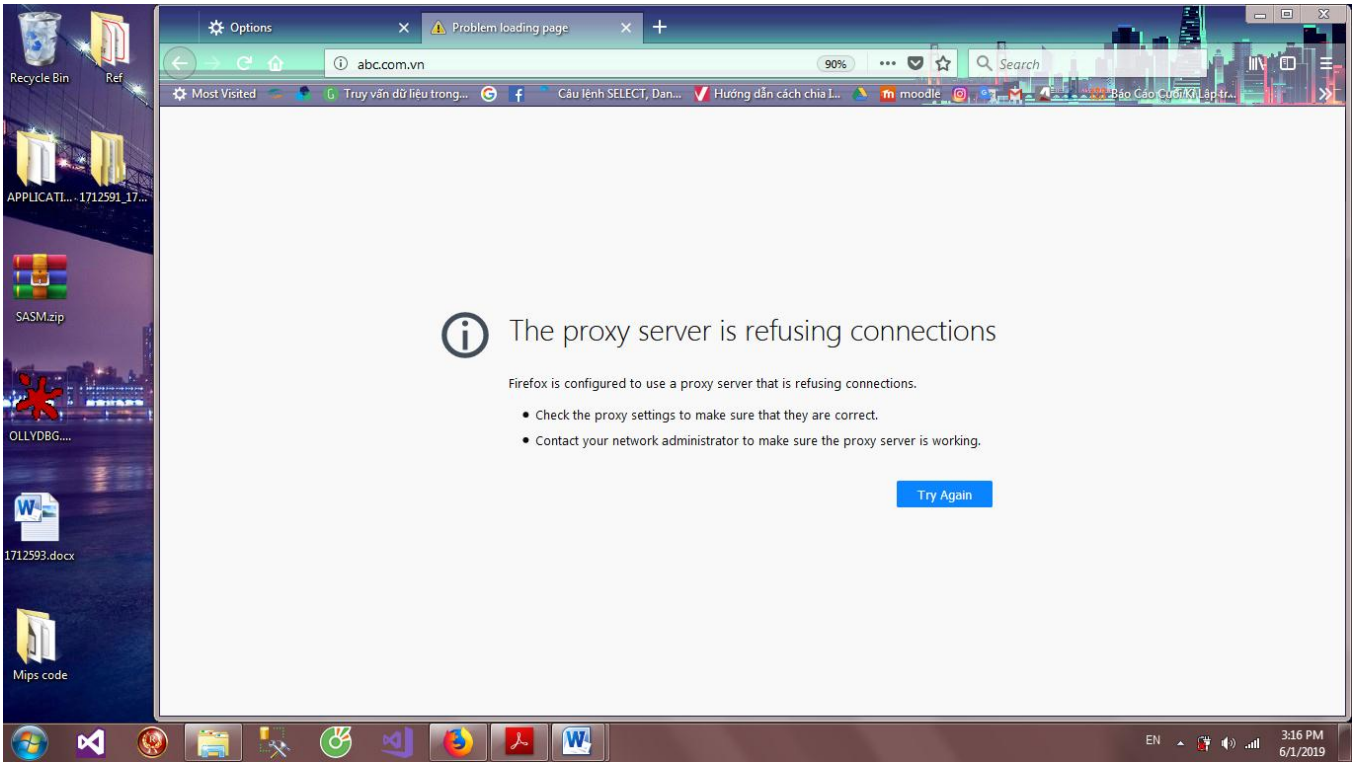
+Tạo 1 vòng while: trong mỗi vòng tiến hành accept các gói tin từ client và mở luồng xử lí thông tin.

3. CHẠY CHƯƠNG TRÌNH

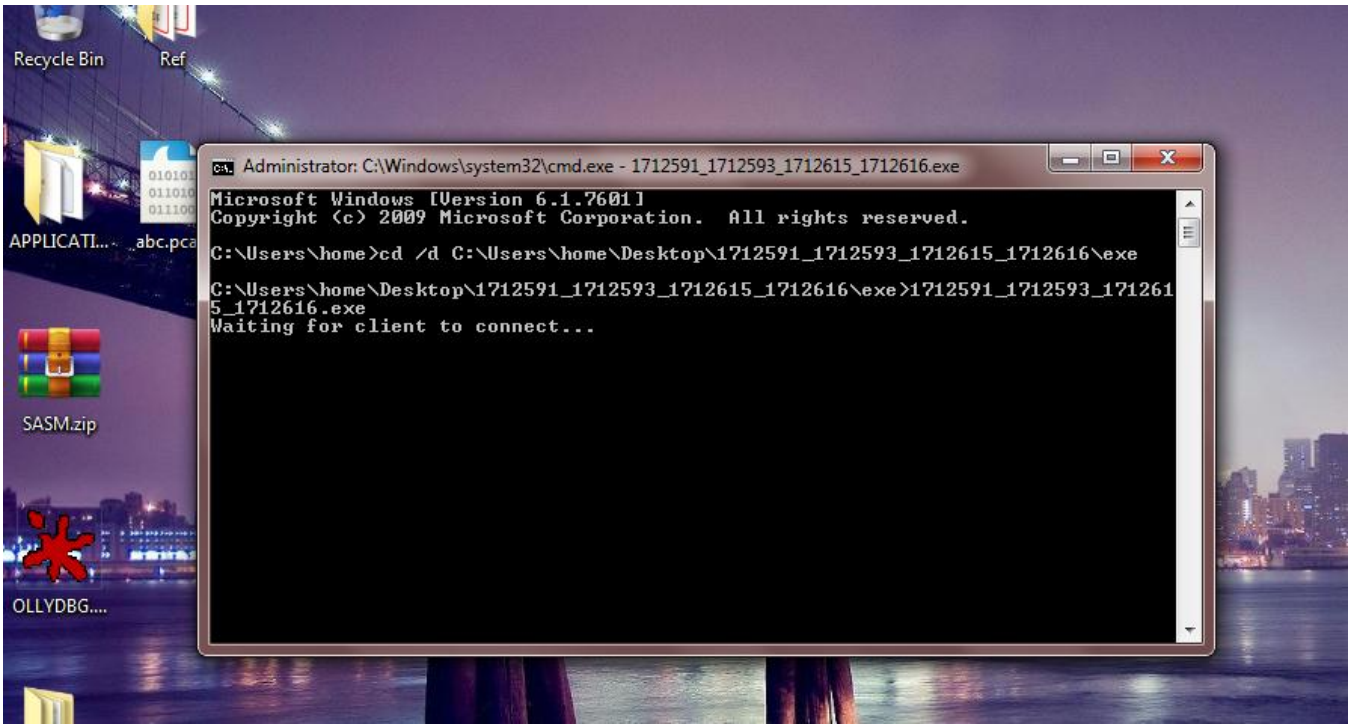
Bước 1: Sử dụng Firefox cấu hình proxy đến Proxy server có localhost là **127.0.0.1** và port là **8888**



Bước 2: Kiểm tra, khi chưa chạy Proxy server, truy cập abc.com.vn và không thể kết nối:



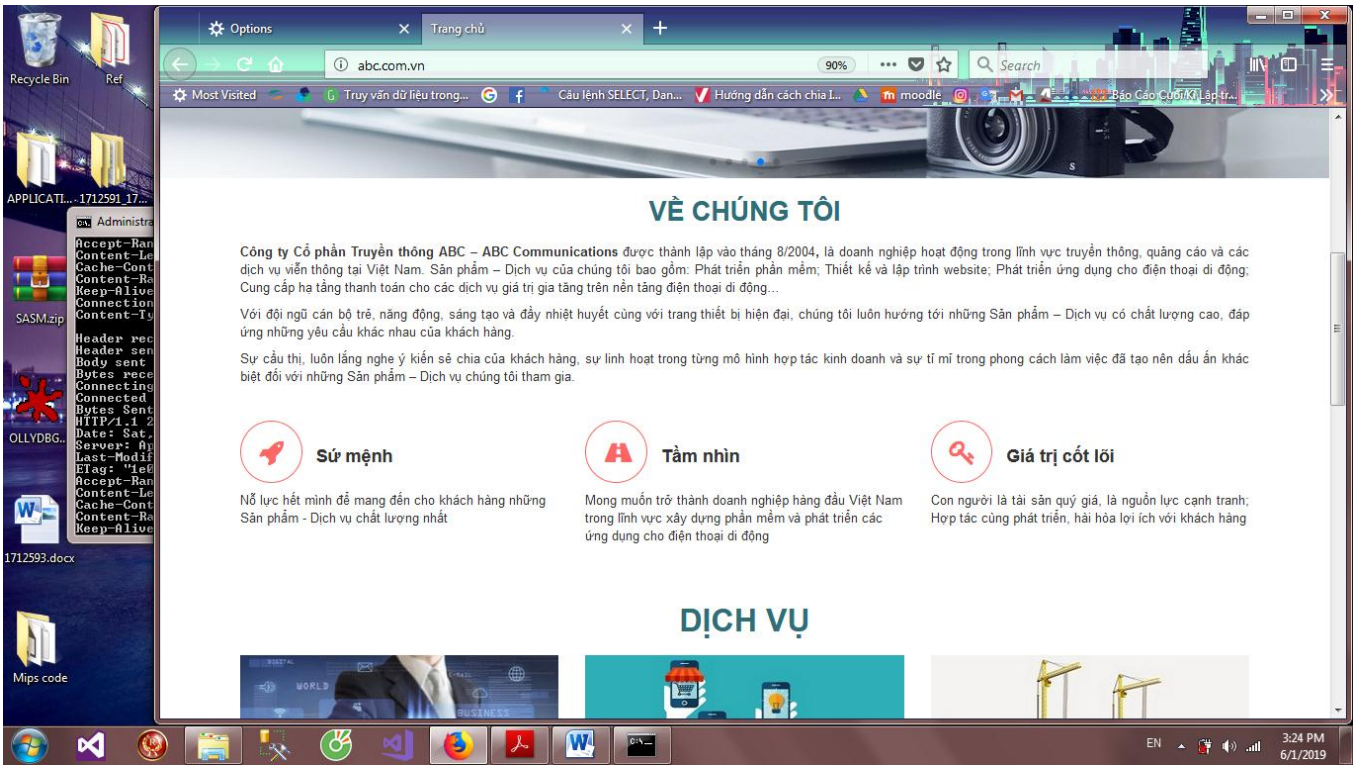
- Mở command line và nhập lệnh như sau để chạy chương trình proxy server (**lưu ý**: trong **thư mục exe** chứa file thực thi chương trình **phải có thư mục cache, tệp 403.html, 404.html đi kèm** để phục vụ việc caching và gửi các phản hồi cấm hoặc không tìm thấy cho client):

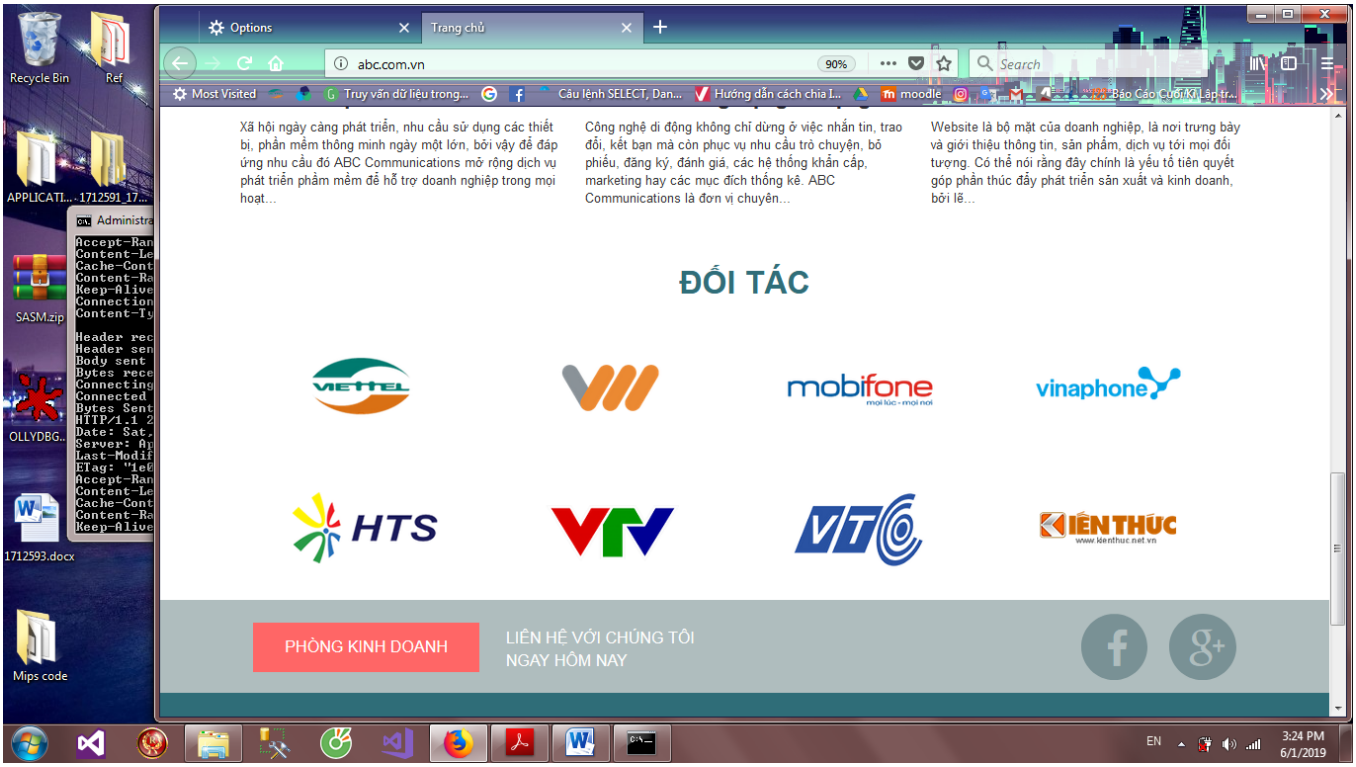


- Proxy sever đang lắng nghe client.

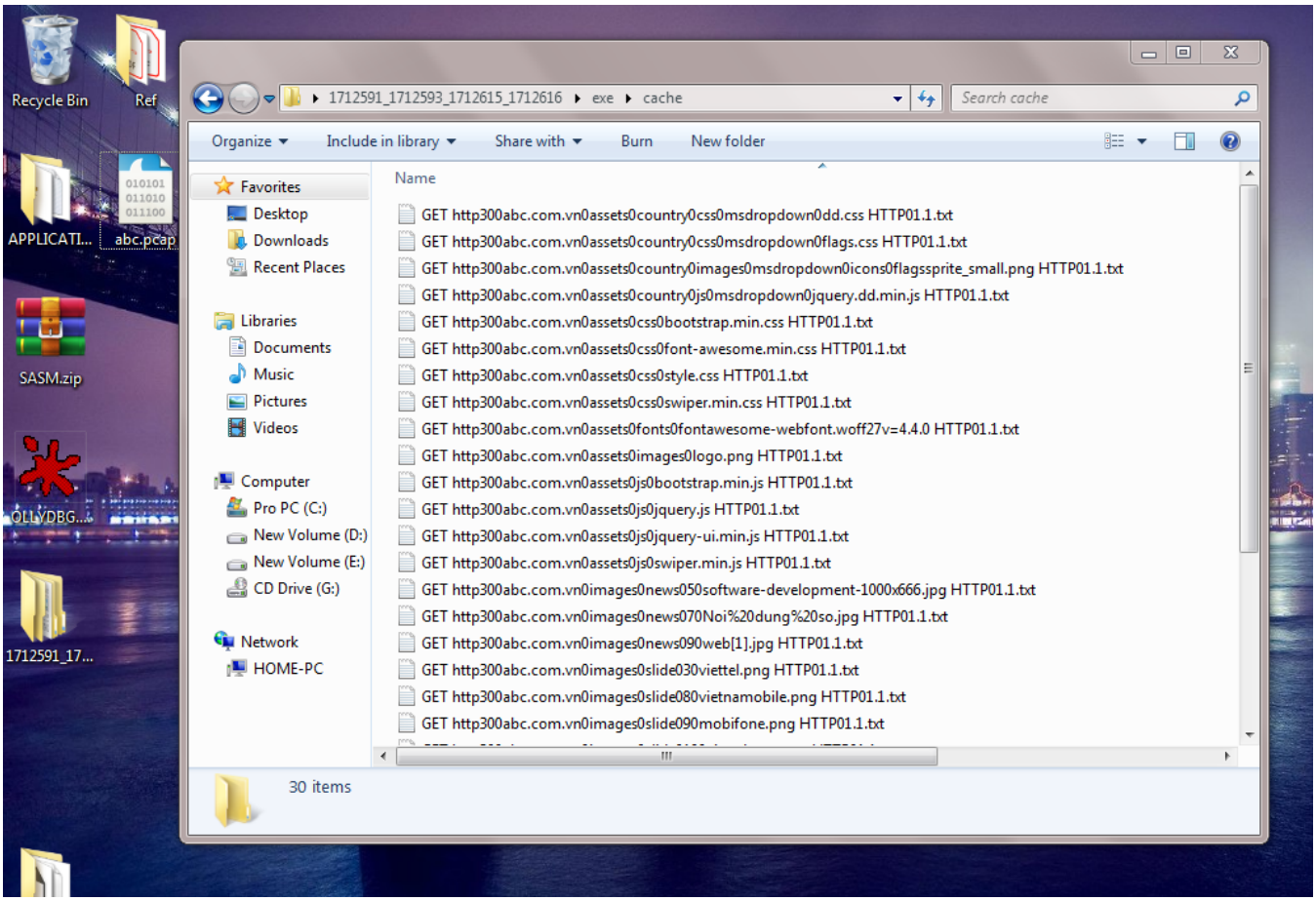
Bước 3: Truy cập trang web có giao thức HTTP trên firefox

- Truy cập trang **abc.com.vn** , ta load được trang web sau:

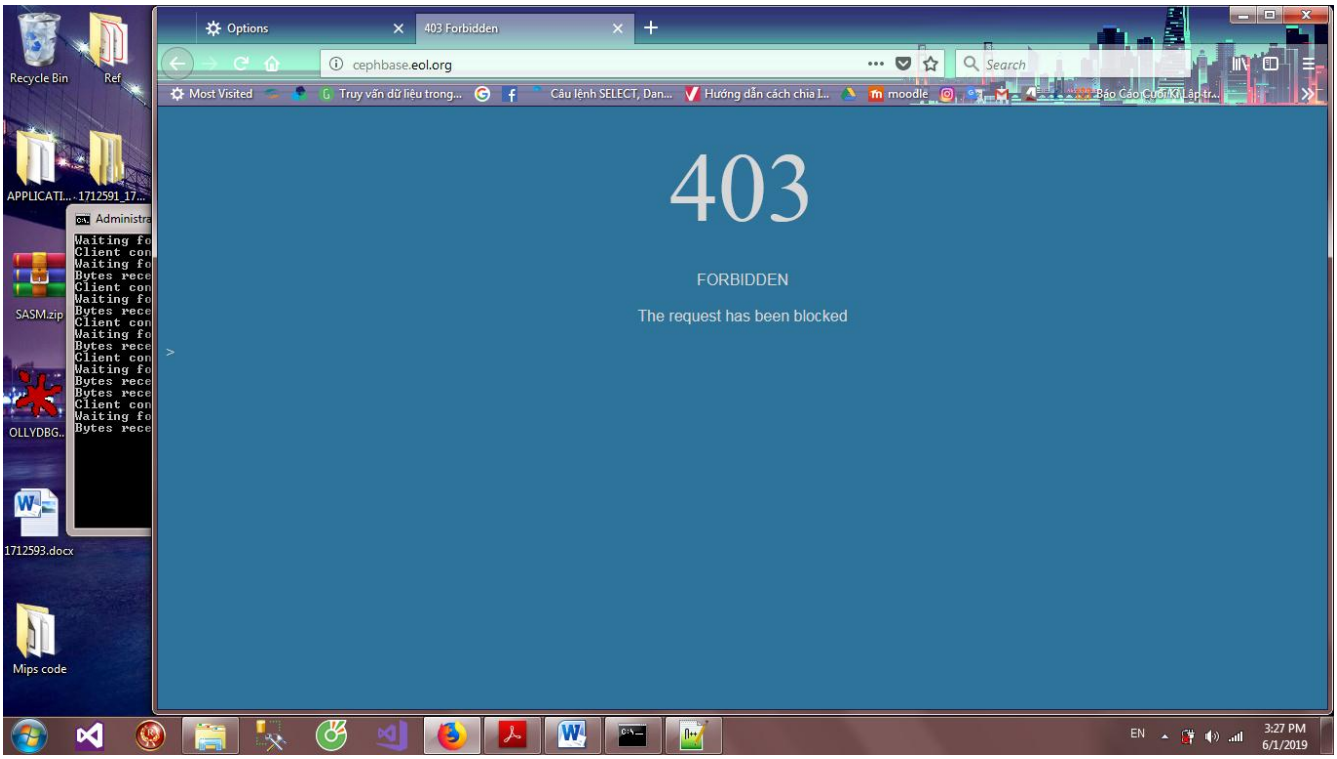




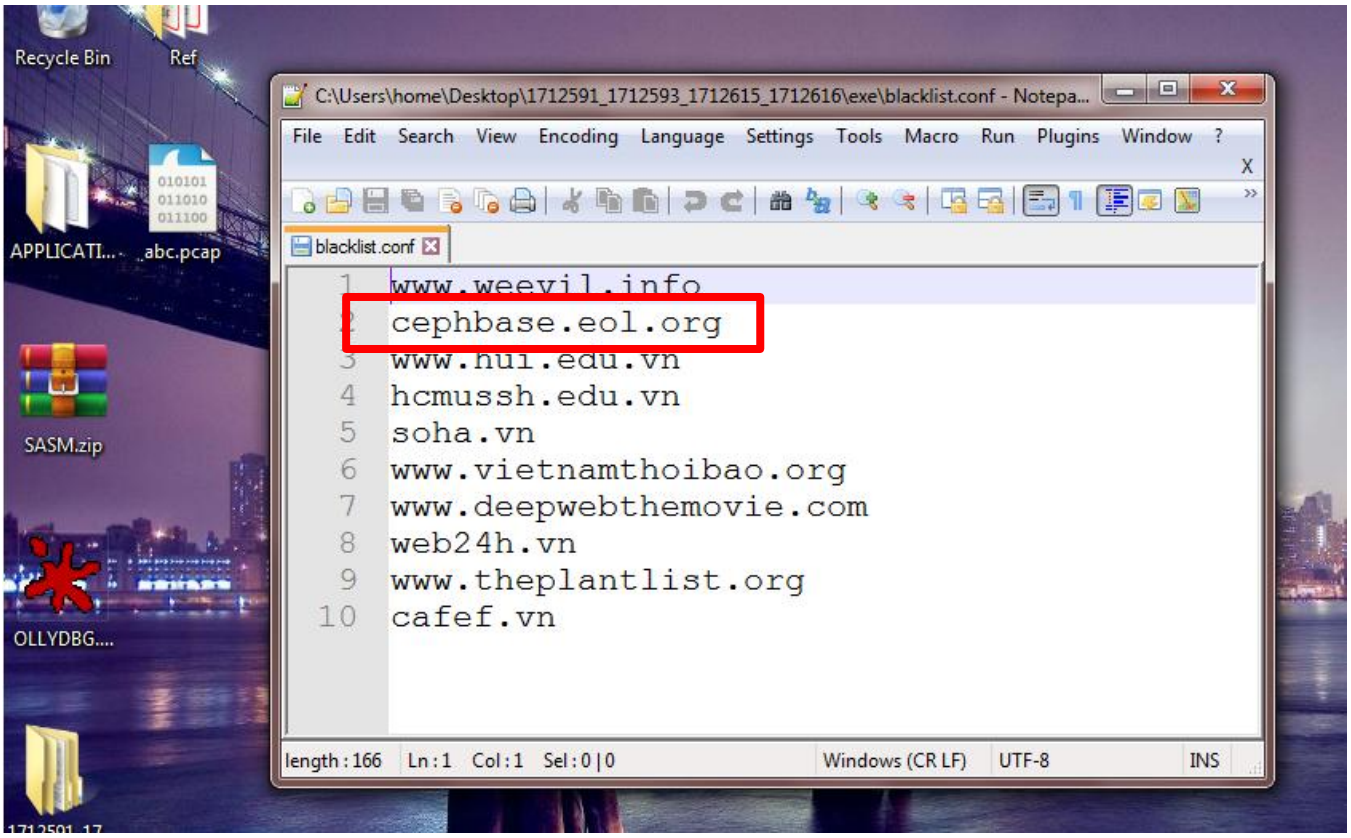
- **Mở thư mục cache trong thư mục exe**, ta thấy các gói tin response đã được cache lại thành các file text để phục vụ nhanh hơn trong lần truy cập sau:



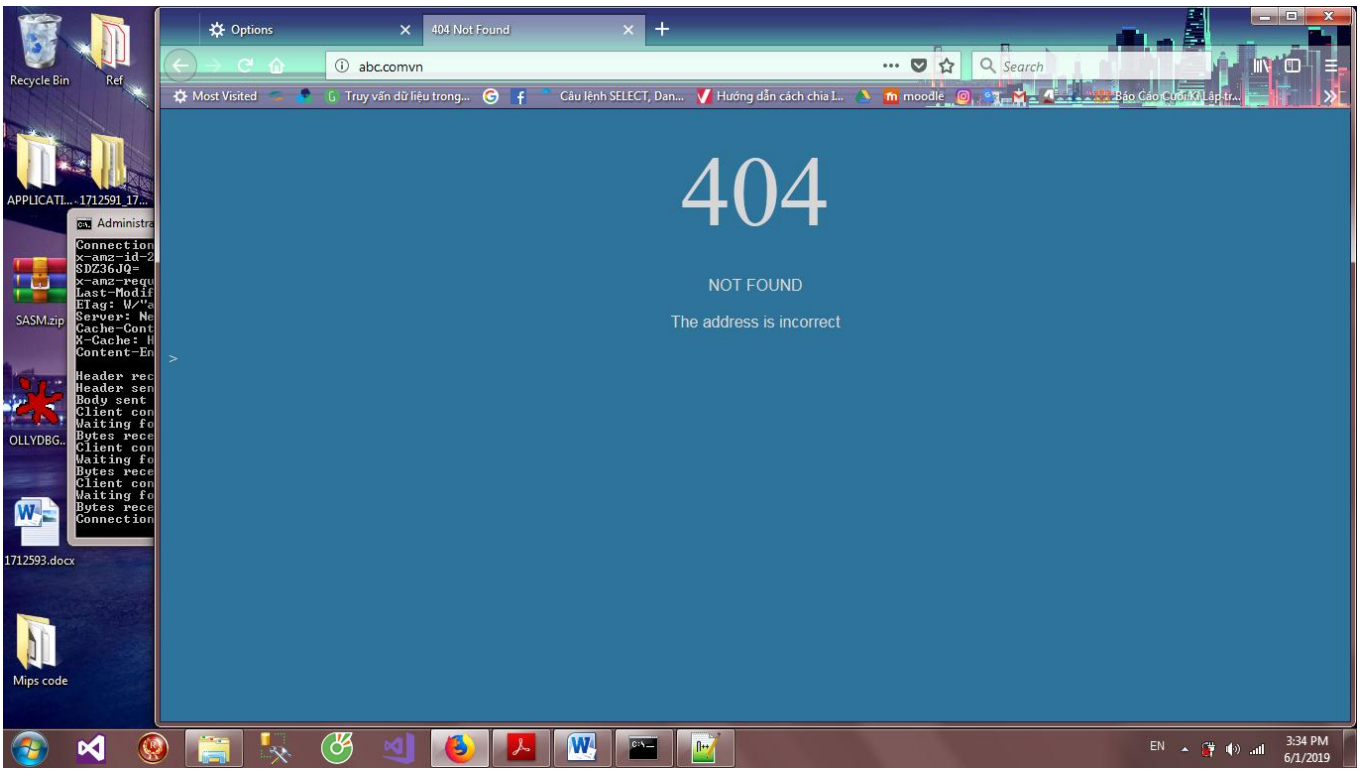
- Tiếp tục truy cập trang web: **cephbase.eol.org**, kết quả nhận được là 403 Forbidden do tên miền của trang web nằm trong file blacklist.conf



- Danh sách các domain bị cấm trong file blacklist.conf

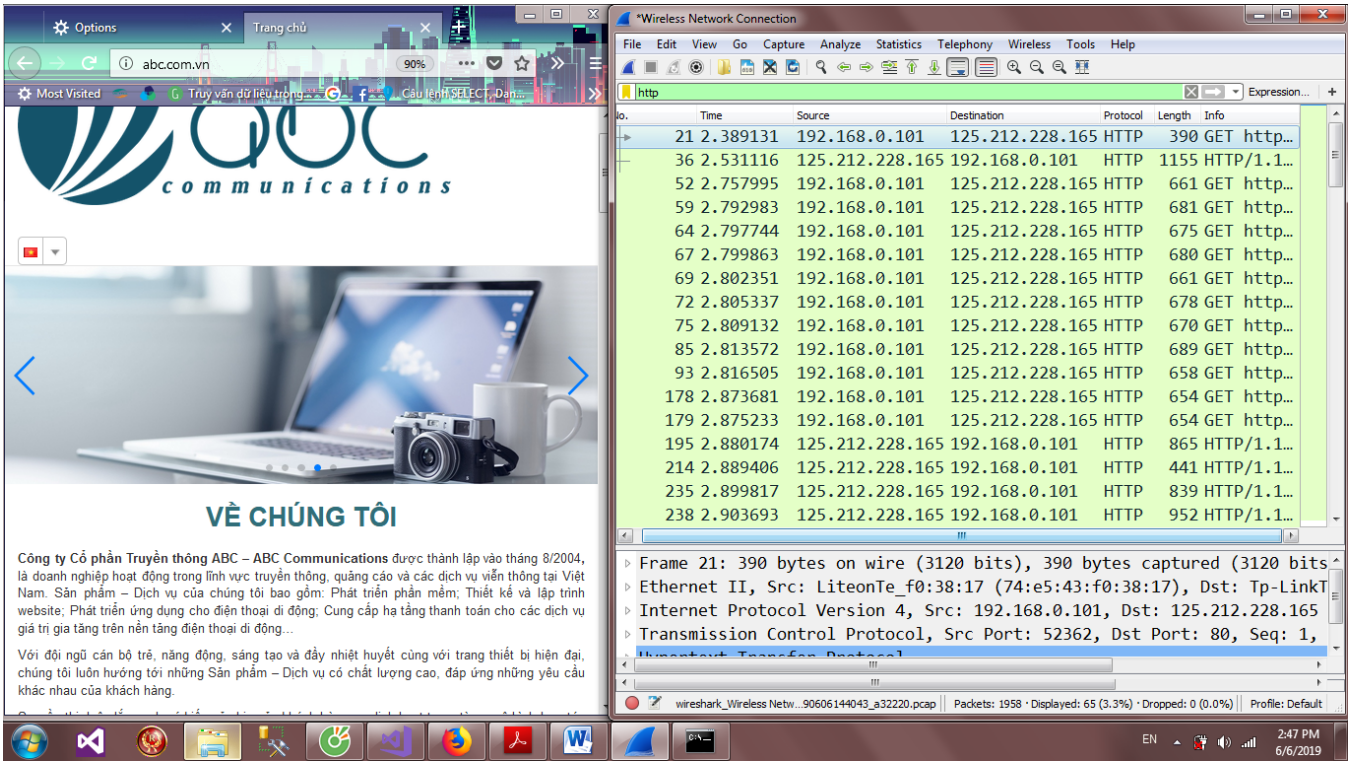


- Truy cập trang web: **abc.comvn**, kết quả nhận được là 404 Not found do tên miền không tồn tại:

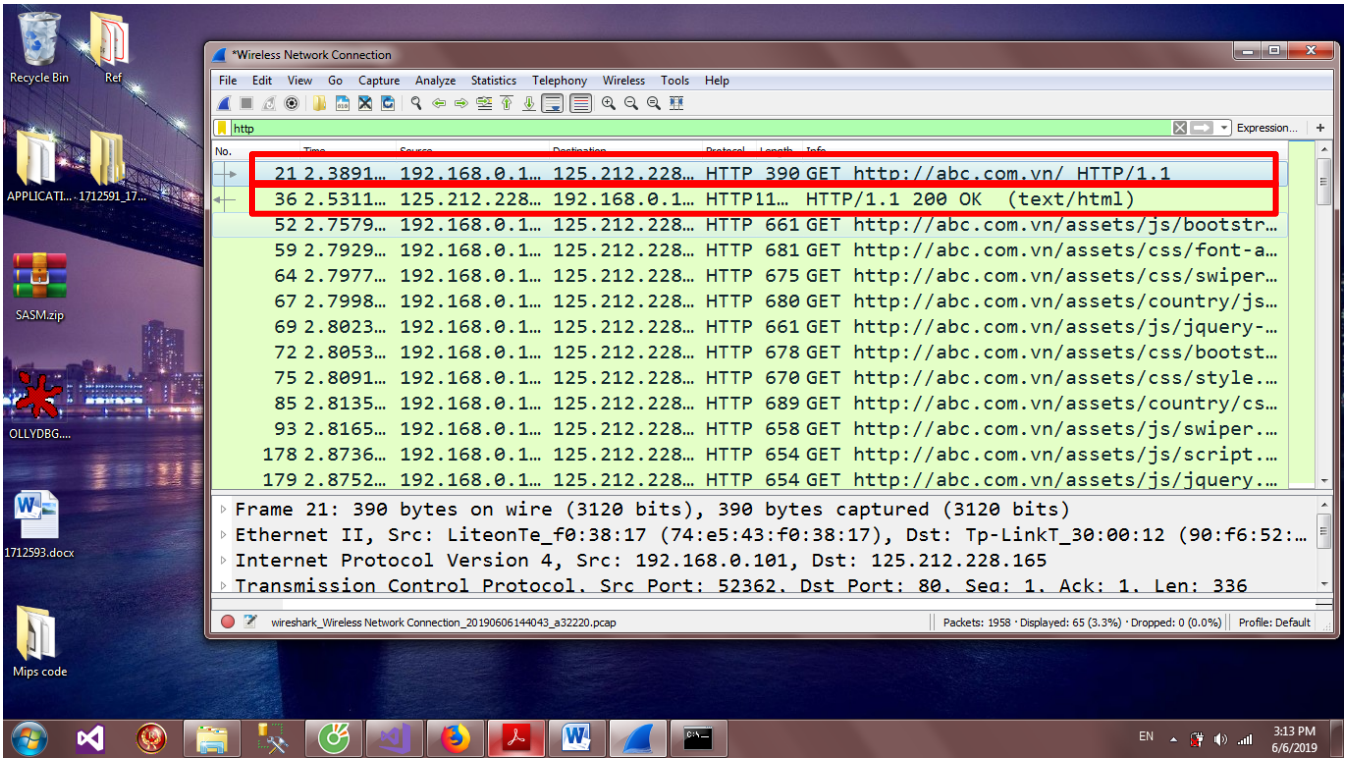


4. SỬ DỤNG WIRESHARK BẮT GÓI TIN TẠI PROXY SERVER

- Chạy proxy server và truy cập trang **abc.com.vn**, đồng thời sử dụng wireshark để bắt gói tin
- Lọc các gói tin có giao thức **http** ta được các gói sau:



- Quá trình nhận dữ liệu giữa Client - Proxy Server và Proxy Server – Web Server và ngược lại (chọn gói 21 và 36 để mô tả):



Tại gói tin số 21, ta thấy trình duyệt Firefox gửi request `GET http://abc.com.vn/ HTTP/1.1` cho proxy server.

Proxy server tiến hành kiểm tra tên miền có tồn tại hay không, nếu tồn tại thì kiểm tra có nằm trong blacklist hay không, và nếu không thì cuối cùng phân tích tên miền thành địa chỉ IP 125.212.228.165.

Sau đó proxy sẽ chuyển tiếp yêu cầu của người dùng đến web server có Destination IP là 125.212.228.165.

Tại gói tin số 36, proxy nhận được gói tin phản hồi `HTTP/1.1 200 OK` từ web server có Source IP là 125.212.228.165. Proxy sẽ chuyển ngược lần lượt header và body trong gói 36 cho browser (client).

5. GIẢI THÍCH Ý NGHĨA PROXY SERVER TRONG THỰC TẾ

Trong thực tế, proxy có tác dụng như ***một bộ lọc thông tin***. Những yêu cầu từ người dùng gửi sẽ qua trung gian là proxy trước khi đến web server thật sự. Tại đây, nhà cung cấp dịch vụ mạng sẽ sử dụng proxy để ngăn client truy cập các trang web, dịch vụ mạng có hại hoặc không phù hợp. Nếu trang web mà client yêu cầu không nằm trong danh sách "đen", thì yêu cầu sẽ được gửi đến web server và nhận lại phản hồi.

Proxy server có tác dụng lưu cục bộ những trang web đã truy cập vào bộ nhớ cache. Proxy server sẽ giúp ***giảm thời gian tìm kiếm*** vì cache của proxy server có thể đã sẵn chứa thông tin mà người dùng cần trong lần truy cập trước.

Tác dụng bảo mật, địa chỉ IP của proxy server sẽ được gửi đi (thay vì địa chỉ của client) trong các lần request, điều này tạo ra sự khó khăn cho bên ngoài nếu muốn tiếp cận hay tấn công máy của client, thông tin của client sẽ không bị tiết lộ.