Phụ lục

[I. GIỚI THIỆU DEEPWEB 3](#_Toc521078189)

[1. Các cấp độ của Internet và vị trí của Deep Web 3](#_Toc521078190)

[Cấp 0: Common Web 3](#_Toc521078191)

[Cấp 1: Surface Web 3](#_Toc521078192)

[Cấp 2: Bergie Web 3](#_Toc521078193)

[Cấp 3: Deep Web 3](#_Toc521078194)

[Cấp 4: Charter Web 4](#_Toc521078195)

[Cấp 5: Marianas Web 4](#_Toc521078196)

[Cấp 6: ? 4](#_Toc521078197)

[Cấp 7: The Fog/Virus Soup 4](#_Toc521078198)

[Cấp 8: The Primarch System 4](#_Toc521078199)

[2. Các hệ thống mạng DeepWeb 4](#_Toc521078200)

[1. Tor 4](#_Toc521078201)

[2. I2P 5](#_Toc521078202)

[3. Freenet 5](#_Toc521078203)

[Freenet 5](#_Toc521078204)

[4. GNUnet 5](#_Toc521078205)

[5. Zeronet 5](#_Toc521078206)

[6. Syndie 5](#_Toc521078207)

[7. OneSwarm 5](#_Toc521078208)

[8. Tribble 5](#_Toc521078209)

[9. AllPeers 5](#_Toc521078210)

[10. anoNet 6](#_Toc521078211)

[11. F2F turtle 6](#_Toc521078212)

[12. WASTE 6](#_Toc521078213)

[3. HỆ THỐNG TOR 6](#_Toc521078214)

[Chức năng của Tor 6](#_Toc521078215)

[Cách sử dụng Tor 6](#_Toc521078216)

[Tor Browser 6](#_Toc521078217)

[Hạn chế của Tor 7](#_Toc521078218)

[Sử dụng Tor Browser 7](#_Toc521078219)

[Tải Trình Duyệt Tor 7](#_Toc521078220)

[Cài đặt Tor Browser: 8](#_Toc521078221)

[Sử dụng Trình Duyệt Tor 9](#_Toc521078222)

[II. PHÁT TRIỂN HỆ THỐNG DEEPWEB VỚI TOR 11](#_Toc521078223)

[1. Mô hình truy cập 11](#_Toc521078224)

[1. Hệ thống web thông thường 11](#_Toc521078225)

[2. Mạng Tor 12](#_Toc521078226)

[2. Thiết lập Dịch vụ 13](#_Toc521078227)

[I. Thiết lập dịch vụ IIS 13](#_Toc521078228)

[II. Thiết lập dịch vụ Tor. 14](#_Toc521078229)

[3. Tor.net 18](#_Toc521078230)

[1) Ý tưởng 18](#_Toc521078231)

[2) Cấu hình project 19](#_Toc521078232)

[a. Yêu cầu: 19](#_Toc521078233)

[b. Sử dụng 20](#_Toc521078234)

# GIỚI THIỆU DEEPWEB

Về bản chất, Deep Web là những trang web không được lập chỉ mục bởi những công cụ tìm kiếm như Google, Bing.

## Các cấp độ của Internet và vị trí của Deep Web

Internet có thể chia thành 8 cấp độ như sau, àng xuống cấp độ sâu hơn, nội dung của những trang web trong đó càng khó tiếp cận.



### Cấp 0: Common Web

Mức này chính là những nội dung web mà bạn duyệt hàng ngày như YouTube, Facebook, Quantrimang.com và những trang web nổi tiếng, dễ truy cập khác.

### Cấp 1: Surface Web

Mức này vẫn có thể truy cập thông qua những phương tiện thông thường, nhưng có chứa những trang web "tối hơn" như Reddit.

### Cấp 2: Bergie Web

Mức này là mức cuối cùng có thể truy cập theo cách thông thường: Tất cả các cấp phía sau phải được truy cập bằng proxy, Tor hoặc bằng cách thay đổi phần cứng của bạn. Ở cấp này, bạn có thể tìm thấy một số web ngầm nhưng chúng vẫn được lập chỉ mục, chẳng hạn như 4chan.

### Cấp 3: Deep Web

Phần đầu tiên của cấp độ này phải được truy cập với proxy. Nó có chứa hình ảnh child porn, máu me, hack website... Đây chính là cấp độ mà Deep Web bắt đầu. Phần thứ hai của cấp độ này chỉ có thể truy cập thông qua Tor và có chứa nhiều thông tin nhạy cảm, ghê hơn.

### Cấp 4: Charter Web

Mức này cũng được chia thành hai phần. Phần đầu có thể truy cập qua Tor, những thứ như ma túy, buôn bán người, phim ảnh bị cấm, chợ đen đều tồn tại ở đây. Phần thứ hai có thể được truy cập bằng cách sửa đổi phần cứng: Closed Shell System. Ở đây, nội dung phát triển theo chiều hướng tệ hơn rất nhiều. Những nội dung bị cấm, những thông tin đen tối, Law of 13 (một tổ chức tội phạm nguy hiểm), thí nghiệm trong chiến tranh thế giới thứ 2, tài liệu dị giáo bị cấm, thậm chí cả vị trí của Atlantis.

### Cấp 5: Marianas Web

Bạn sẽ cảm thấy thật may mắn khi tìm thấy bất cứ ai biết về nó, vì ở cấp độ này có thể có tài liệu bí mật liên quan đến chính phủ Mỹ và nhiều quốc gia lớn.

### Cấp 6: ?

Giống như một hàng rào ngăn cách giữa cấp 5 với cấp 7, 8, ngăn chặn các cá nhân thâm nhập vào cấp cao hơn.

### Cấp 7: The Fog/Virus Soup

Đây có thể ví như vùng chiến tranh, nơi diễn ra những đơn hàng mua bán giá trị cực cao, là vùng đất của virus, các cao thủ, những người không thích có kẻ tọc mạch nào xía vào chuyện của mình và sẵn sàng cho kẻ lắm chuyện "ăn đủ". Mọi người ở cấp này thì cố gắng tiến vào cấp 8 và ngăn chặn những người khác tiến đến đó. Cấp này cũng được tạo ra để bảo vệ cấp độ 8.

### Cấp 8: The Primarch System

Primarch System là hệ thống kiểm soát Internet. Không có chính phủ, tổ chức nào có quyền kiểm soát nó. Được phát hiện vào năm 2000, nhưng không ai biết thực sự trong này chứa những thông tin, hoạt động gì. Nó không phản hồi, nhưng gửi đi những lệnh không thể thay đổi cho toàn bộ mạng, một cách ngẫu nhiên. Cấp 8 được cho là bị ngăn cách bởi "level 17 quantum t.r.001 level function lock" mà máy tính của chúng ta hầu như không thể phá vỡ. Hiện tại nó được gọi là Boss cuối cùng của Internet.

## Các hệ thống mạng DeepWeb

### Tor

Ban đầu viết tắt của chữ The Onion Router là một phần mềm mã nguồn mở và miễn phí. Tor thực hiện giao thức phân tuyến kiểu củ hành (onion routing) thế hệ thứ hai. Hệ thống này sử dụng một hệ thống proxy tình nguyện ẩn danh, bao gồm hơn bảy nghìn hệ thống relay để che giấu vị trí và cách sử dụng của người dùng, tránh giám sát mạng hoặc phân tích lưu lượng truy cập. Sử dụng Tor giúp người dùng truy cập Internet ẩn danh, không cho thống kê "lượt truy cập vào các trang web, bài đăng trực tuyến, tin nhắn trực tuyến và các dạng giao tiếp khác

### I2P

Invisible Internet Project, có nghĩa là “dự án Internet tàng hình” là dự án phần mềm được xây dựng nhằm mục đích tạo ra một mạng máy tính “ẩn danh” trên nền mạng Internet. Một mạng được xây dựng trên nền một mạng khác như thế còn được gọi là một overlay network. (Mạng I2P là một mạng đồng đẳng, phân tán, tự tổ chức, sử dụng bảng băm phân tán (DHT – Distributed Hash Table) Kademlia cải tiến.

### Freenet

Freenet là phần mềm miễn phí cho phép bạn ẩn danh chia sẻ tập tin, duyệt và xuất bản "freesites" (các trang web chỉ truy cập thông qua Freenet) và trò chuyện trên diễn đàn, mà không sợ kiểm duyệt. Freenet được phân cấp để làm cho nó ít bị tấn công hơn, và nếu được sử dụng trong chế độ "darknet", nơi người dùng chỉ kết nối với bạn bè của họ, rất khó phát hiện.Truyền thông bởi các nút Freenet được mã hóa và được định tuyến thông qua các nút khác để làm cho nó vô cùng khó khăn để xác định ai đang yêu cầu thông tin và nội dung của nó là gì. Người dùng đóng góp cho mạng bằng cách cho băng thông và một phần của ổ đĩa cứng của họ (được gọi là "lưu trữ dữ liệu") để lưu trữ các tệp. Các tệp được tự động lưu giữ hoặc bị xóa tùy thuộc vào mức độ phổ biến của chúng, với mức phổ biến nhất bị loại bỏ để nhường chỗ cho nội dung mới hơn hoặc phổ biến hơn. Các tập tin được mã hóa, vì vậy nói chung người dùng không thể dễ dàng khám phá những gì có trong kho dữ liệu của mình, và hy vọng không thể chịu trách nhiệm về nó.

RetroShare là một dịch vụ giao tiếp ít thông qua server, giúp cung cấp chia sẻ file, forums, channels và chat; thuộc bản quyền của GnuPG và mã hóa bằng OpenSSL. Với secure mail, Video hoặc VoID và các tính năng chia sẻ khác, ứng dụng mạnh mẽ này cho phép bạn giao tiếp thông qua nhiều hình thức khác nhau mà không sợ gặp phải những rủi ro bảo mật không mong muốn.

### GNUnet

### Zeronet

### Syndie

### OneSwarm

### Tribble

### AllPeers

### anoNet

### F2F turtle

### WASTE

Tổng kết:

Đến nay, trong số các hệ thống hỗ trợ ẩn danh trên mạng, đáng kể nhất chỉ có Tor và I2P. Trong khi Tor hướng đến việc đảm bảo ẩn danh cho người sử dụng các tài nguyên mở thì I2P lại tập trung vào việc đảm bảo ẩn danh cho người đăng tải các tài nguyên bằng việc xây dựng một mạng mới tách biệt với mạng Internet. Nếu chính quyền có thể hạn chế hoạt động của Tor bằng cách ngăn chặn các website- tracker (thực tế đã xảy ra ở Trung Quốc, Nga) thì điều đó là không khả thi với I2P. Việc đưa các website có nội dung “chống đối” lên mạng I2P sẽ khiến cho các cơ quan chức năng không thể tìm ra được nơi đăng tải để có biện pháp ngăn chặn thích hợp mặc dù trên thực tế có thể website được đặt ở một máy chủ trong nước.

## HỆ THỐNG TOR

### Chức năng của Tor

Tor là phần mềm máy tính có chức năng xóa dấu vết, ẩn địa chỉ [IP] xuất xứ của máy truy cập Internet khi gửi hay nhận thông tin qua mạng Internet. Các thông tin trao đổi qua Tor được mã hóa và truyền qua nhiều máy chủ trung gian khác nhau. Nếu một máy trung gian Tor bị truy cập trộm, kẻ trộm cũng không thể đọc được các thông tin của người sử dụng do các thông tin đã được mã hóa.

Tor là công cụ giúp người ở những nơi bị ngăn chặn thông tin có thể vượt tường lửa để tiếp cận với những luồng thông tin tự do và khách quan hơn ở bên ngoài. Bản chất của Tor là tự động và liên tục thay đổi proxy để bảo mật dữ liệu.

### Cách sử dụng Tor

Tor hoạt động tốt với trình duyệt Firefox , với trình duyệt này chỉ cần thao tác ở một nút phía dưới góc phải màn hình: đồng ý (enabled) hoặc không đồng ý (disabled), cũng có thể làm việc chung với tiện ích Foxyproxylà một extension (tiện ích) của trình duyệt Firefox. Người ta đã tích hợp sẵn trình duyệt Opera với Tor thành trình duyệt [Opera Tor](http://letwist.net/operator).  
Tor là một gói phần mềm sau khi cài đặt sẽ có hai biểu tượng shortcut có tên: Vidalia và Privoxy. Nếu đường truyền Internet đủ mạnh và muốn tình nguyện chia tải cho mạng Tor, nhấp chuột phải vào biểu tượng củ hành và chọn Configure -> Server, đánh dấu "Relay trafic for the Tor network". Nếu không, người sử dụng chỉ cần chọn "Start" và chờ củ hành biến thành màu xanh lá là đã vào mạng Tor.

### Tor Browser

Tor Browser là phần mềm mới, hiện tại bản mới nhất là bản 7.5.4 (tháng 5 năm 2018) kèm theo bản Firefox 31.7.0 thành trình duyệt Tor. Có thể dùng nó trong ổ USB nếu không muốn cài đặt. Nó được dùng để ngăn chặn trường hợp bị theo dõi để tìm ra các trang mà bạn xem, hoặc tìm kiếm vị trí máy bạn đang sử dụng, và cũng giúp bạn vào được những trang web bị đặt tường lửa

### Hạn chế của Tor

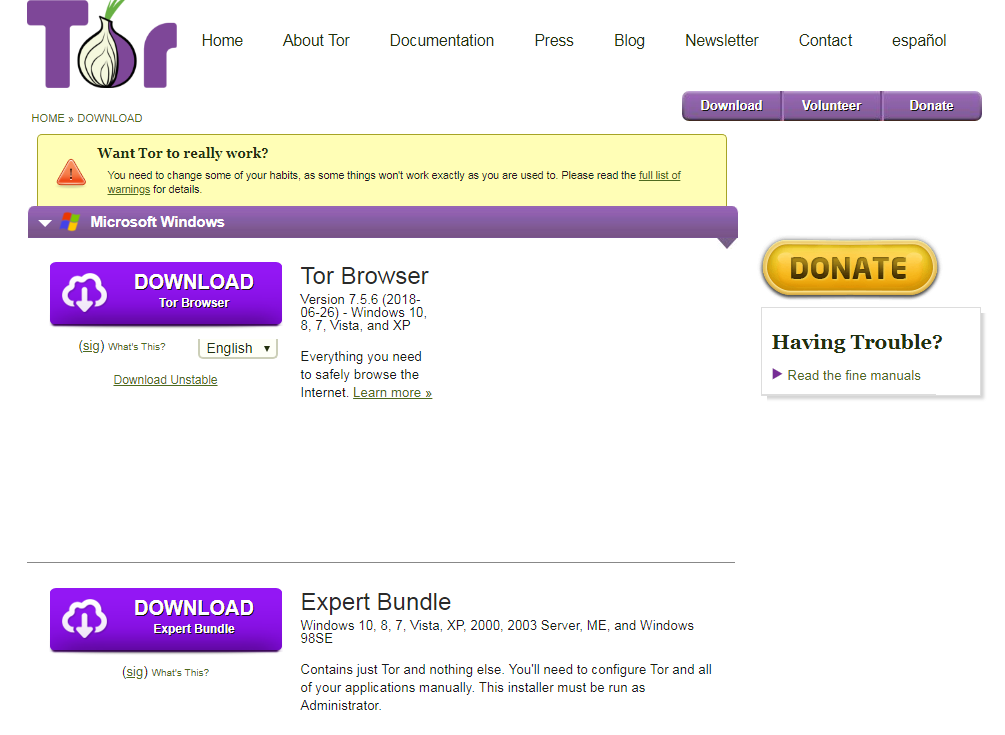
Do mạng Tor hoạt động thông qua nhiều máy chủ trung gian và liên tục thay đổi các máy chủ này nên khi sử dụng phần mềm Tor tốc độ truy cập Internet có thể sẽ bị chậm hơn so với bình thường, để khắc phục phần nào nhược điểm này người ta đang tìm cách nâng cấp hệ thống máy chủ.

Giống như tất cả các mạng vô danh tiềm tàng khác, theo lý thuyết Tor có nhược điểm là nếu như một phần mềm theo dõi mạng được cài đặt tại 2 máy cuối trong mạng Tor, nó có thể phân tích các thông tin được trao đổi từ 2 máy đó qua mạng Tor. Nhưng cũng rất khó khăn bởi Tor liên tục tự động thay đổi máy chủ, cả máy đầu và máy cuối trong mạng, và dữ liệu cũng đã được mã hóa.

### Sử dụng Tor Browser

### Tải Trình Duyệt Tor

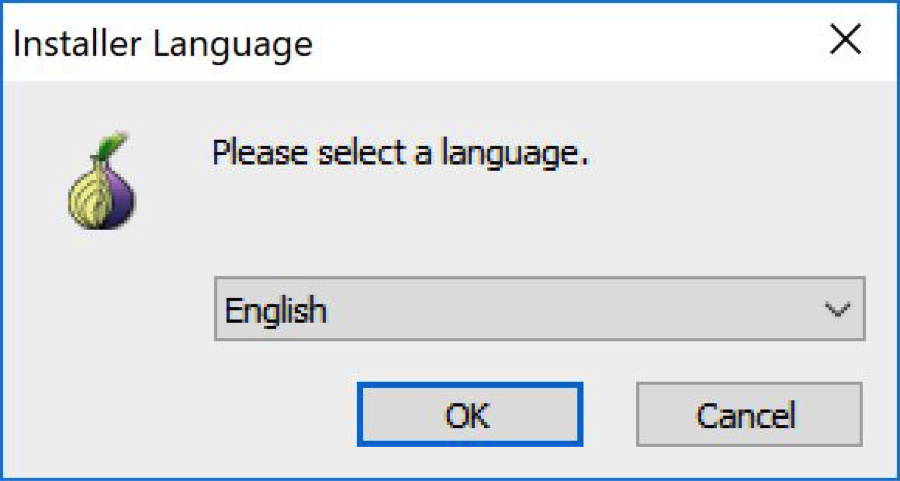
<https://www.torproject.org/download/download.html.en>



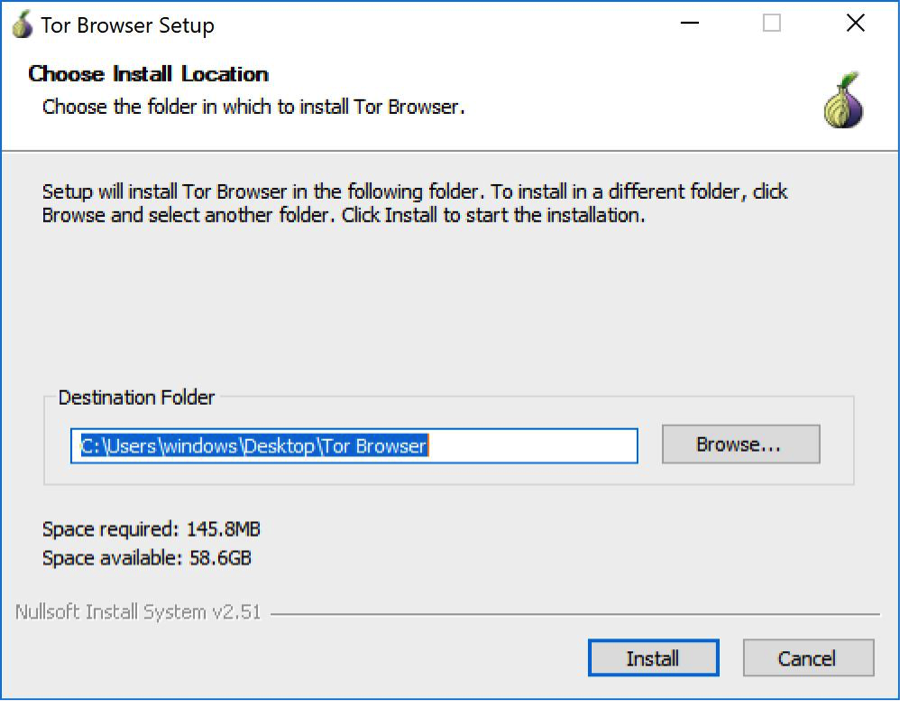
Tại đây có 2 phiên bản là Tor Browser và Expert bundle. Tor Browser sẽ sử dụng như một trình duyệt web thông thường thường. Expert bundle được dùng cho các chuyên gia và phải cấu hình bằng tay.

### Cài đặt Tor Browser:

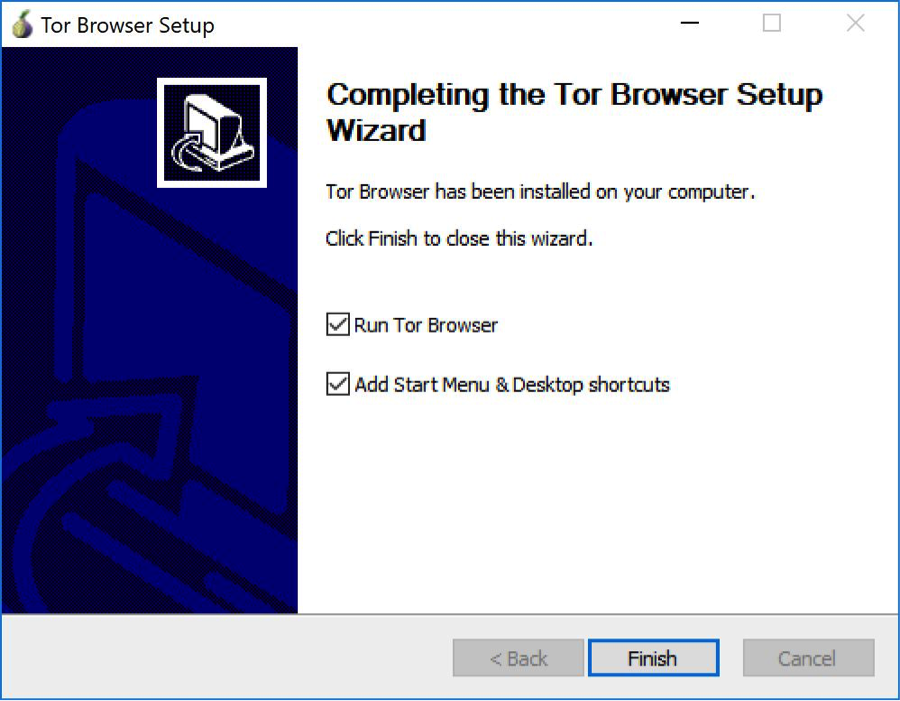
Sau khi tải được trình duyệt Tor Browser, ta mở file cài đặt. Một cửa sổ nhỏ mở ra và hỏi bạn về ngôn ngữ bạn sẽ sử dụng cho Trình Duyệt Tor. Sẽ có nhiều chọn lựa. Chọn ngôn ngữ bạn muốn rồi nhấn vào nút OK.



Bạn sẽ thấy một cửa sổ mới cho bạn biết nơi mà Trình Duyệt Tor được cài đặt. Vị trí mặc định là bàn làm việc (desktop). Bạn có thể thay đổi nơi khác mà bạn muốn, nhưng bây giờ cứ giữ mặc định.

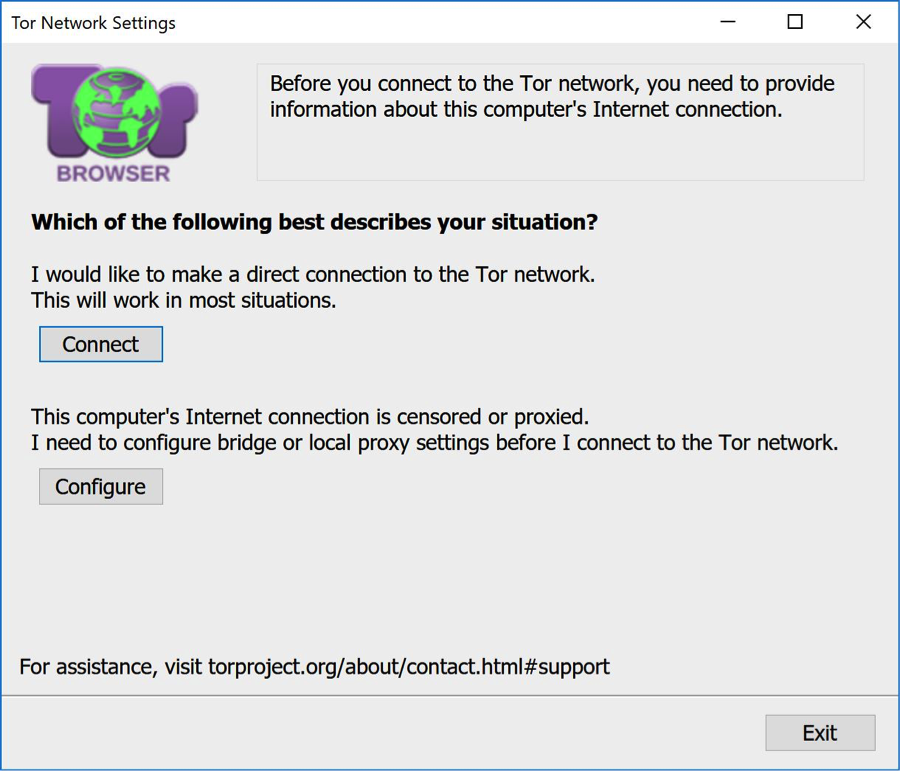


Quá trình cài đặt hoàn tất khi bạn thấy một cửa sổ thông báo hoàn thành quá trình cài đặt. Nếu bạn nhấp vào nút Finish (Kết thúc), Trình Duyệt Tor sẽ bắt đầu ngay lập tức và lối tắt “Start Tor Browser” (Bắt Đầu Trình Duyệt Tor) sẽ được thêm vào Menu Start (Bắt đầu) và trên Bàn làm việc (desktop)

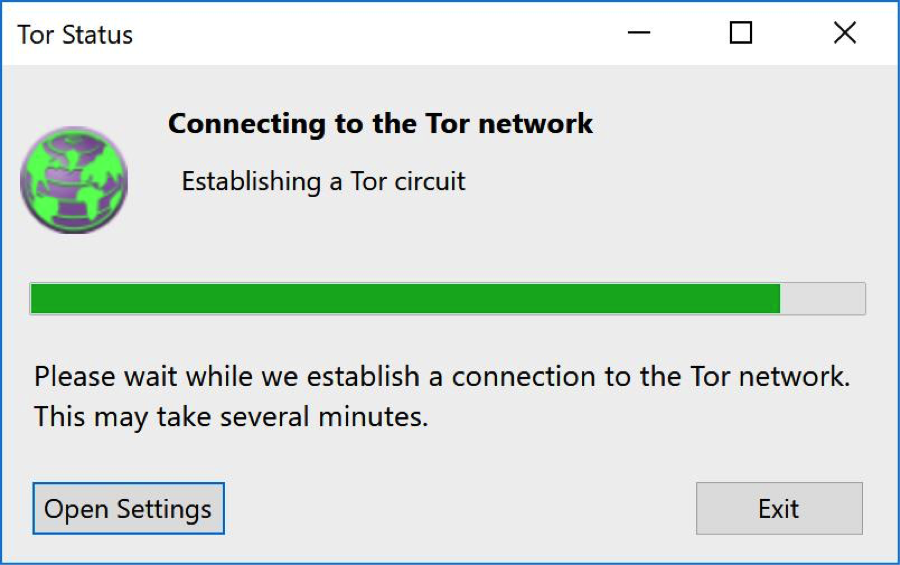


### Sử dụng Trình Duyệt Tor

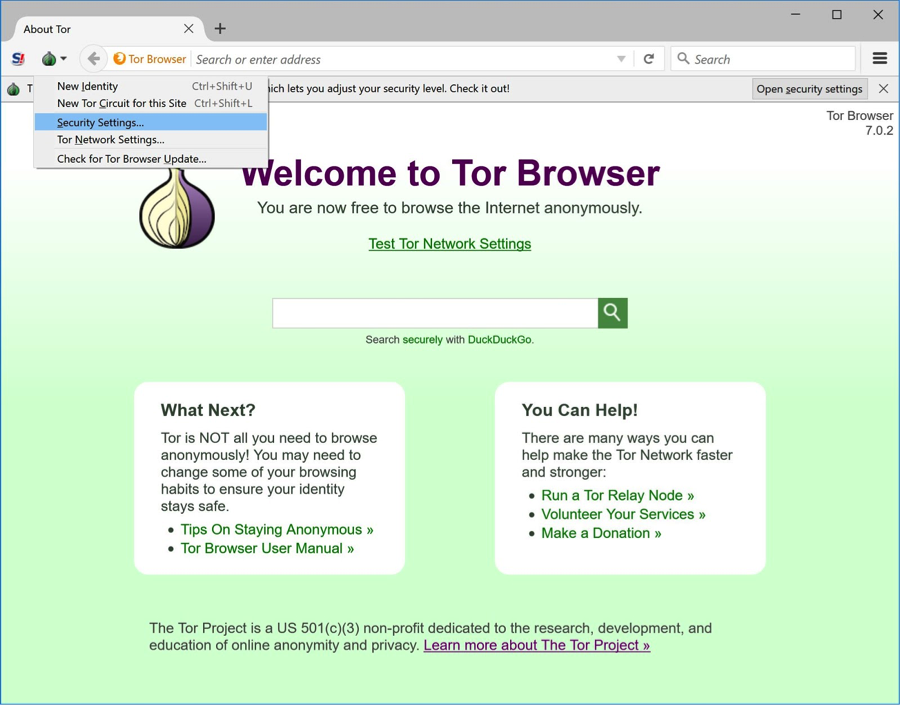
Khi Trình Duyệt Tor chạy lần đầu tiên, bạn sẽ thấy một cửa sổ cho phép thay đổi một số thiết đặt nếu thấy cần. Bạn có thể trở lại và thay đổi một số cấu hình cài đặt, nhưng cứ tiếp tục và thử kết nối với mạng Tor bằng cách nhấn vào nút Connect (Kết nối)



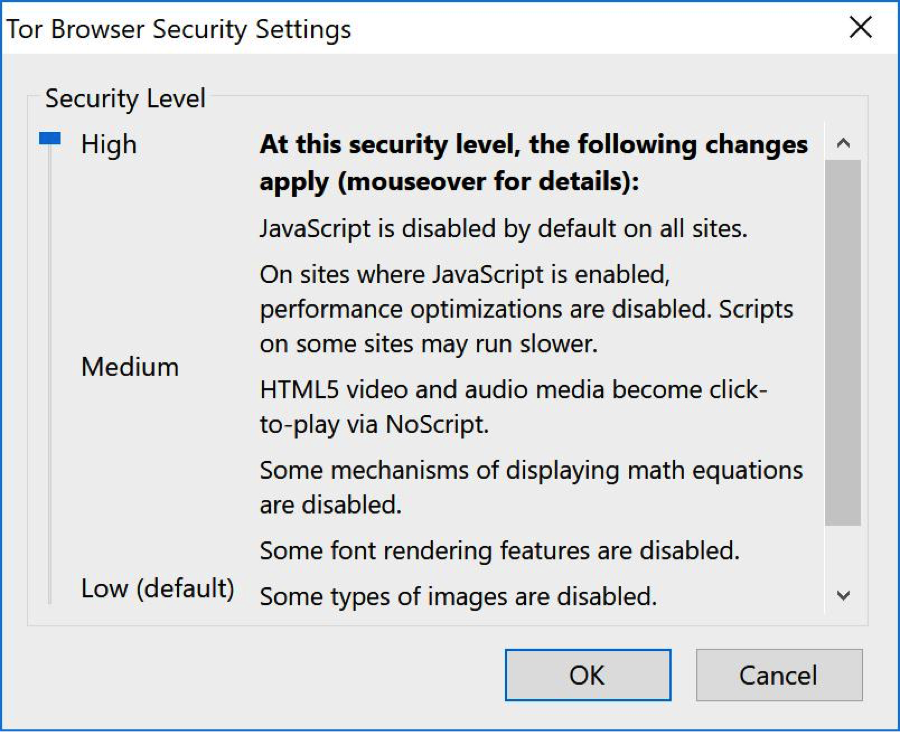
Một cửa sổ mới xuất hiện với một thanh công cụ màu xanh lá minh hoạ tiếnt triển kết nối của Trình duyệt Tor vào mạng Tor



Lần đầu tiên khi Tor Browser chạy có thể lâu hơn bình thường, nhưng hãy kiên nhẫn, trong vài phút sẽ xong và Trình duyệt Tor sẽ mở ra để chúc mừng bạn. Bấm vào biểu tượng Củ Hành Tor ở góc trái bên trên của Trình duyệt Tor, rồi chọn Privacy and Security Setting (Thiết đặt Riêng Tư và Bảo Mật).



Một số chức năng của một trình duyệt bình thường có thể gây ra yếu điểm để bị lối tấn công của kẻ-trung-gian. Những chức năng khác trước đây có lỗi làm tiết lộ danh tính của người dùng. Nâng độ bảo mật lên nấc cao hơn để tắt các chức năng này đi. Điều này sẽ giúp bạn an toàn hơn không bị kẻ tấn công dồi dào tài lực xen lấn vào đường kết nối mạng hoặc dùng những lỗi chưa ai biết trong các chức năng này. Điều đáng tiếc là khi tắt các chức năng này đi có thể không xem được một số trang mạng. Thiết đặt mặc định thấp chấp nhận được cho việc bảo vệ riêng tư thường nhật, nhưng bạn có thể dùng thiết đặt cao hơn nếu lo ngại về các đối thủ tinh vi, hoặc nếu bạn không màng là một số trang web không hiển thị đúng.

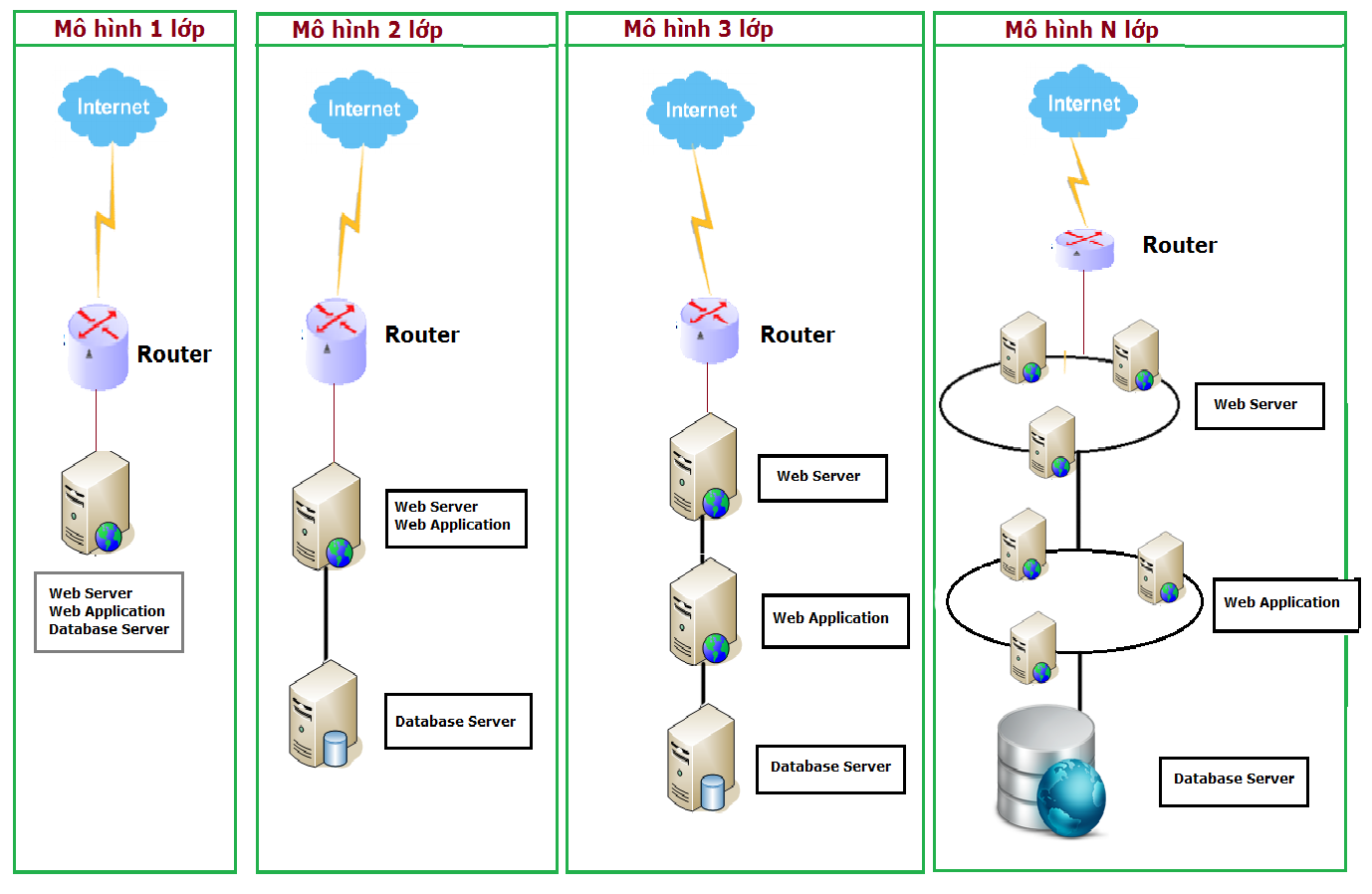


Sau khi thiết lập mức độ bảo mật bạn đã có thể lướt web trên mạng và được ẩn danh về thông tin cá nhân.

# PHÁT TRIỂN HỆ THỐNG DEEPWEB VỚI TOR

## Mô hình truy cập

### Hệ thống web thông thường



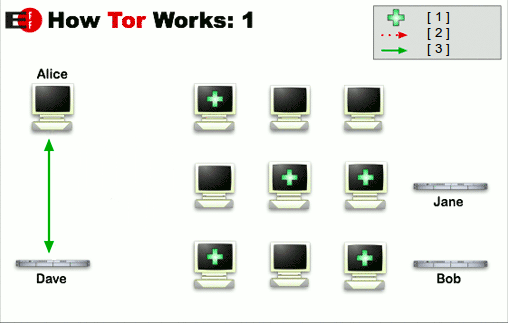
Client sẽ truy cập tới internet và tới hệ thống router và kết nối tới webserver và thao tác trực tiếp với các dịch vụ mà webserver cung cấp. Các router có thể có hoặc không có các luật(tường lửa) truy cập webserver.

### Mạng Tor

Những bước sau đây cho thấy cách mà Tor Browser hoạt động khi máy tính của Alice sử dụng Tor Browser để kết nối với máy trạm/máy chủ của Bob:

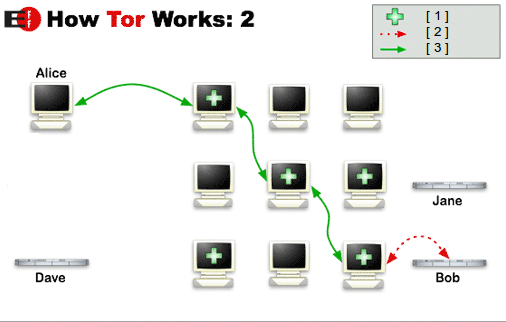
**Cách 1**

Tor Browser của Alice có chứa các điểm hoặc giao dịch Tor **[1]** từ thư mục máy trạm của Tor (**Dave**)



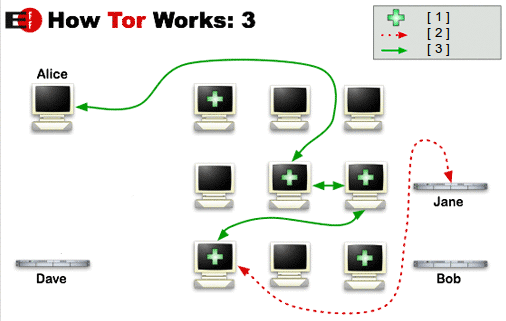
**Cách 2:**

Tor Browser của Alice chọn một đường đi ngẫu nhiên thông qua mạng Tor đến máy trạm cần đến (**Bob**). Toàn bộ các kết nối bên trong mạng Tor được mã hóa (xanh lá **[3]**). Trong ví dụ này, kết nối cuối cùng không được mã hóa (đỏ **[2]**). Kết nối cuối cùng sẽ được mã hóa nếu Alice truy cập vào trang web **https**.



**Cách 3**

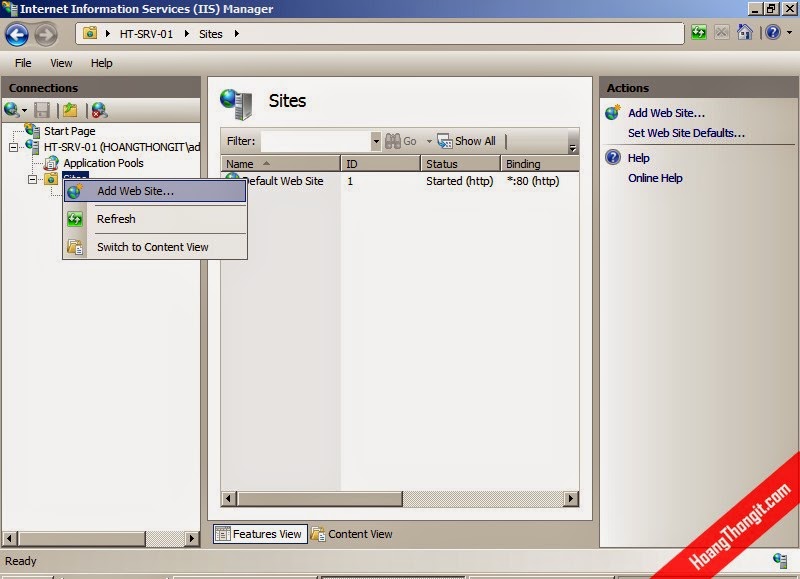
Nếu tại một thời điểm sau đó, Alice truy cập vào một máy trạm khác (**Jane**), Tor Browser của Alice lựa chọn một đường đi ngẫu nhiên khác.



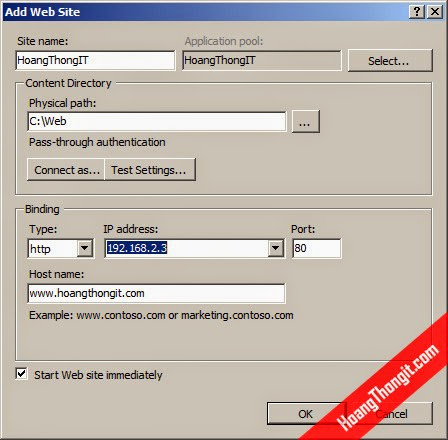
## Thiết lập Dịch vụ

### Thiết lập dịch vụ IIS

Mở **Internet Information Service (IIS) Manager** từ Administrative Tools. Sau đó chuột phải vào **Site** chọn **Add Web Site…**

****

Trên màn hình **Add Web Site** nhập **ThongHoangit**vào ô **Site** **name**. Trong ô **Physical Path** trỏ đường dẫn đến **C:\ ThongHoangit**. Trong ô **Type** chọn **http**. Trong ô **Host** **name** nhập www.thonghoangit.vn, sau đó chọn **OK**

****

Để client có thể truy cập qua internet tới site vừa dựng thì IP address phải là IP public của Server. Cổng nên sử dụng cổng mặc định là 80( Không sử dụng https cổng 443, 8443 vì dịch vụ tor không sử dụng được https).

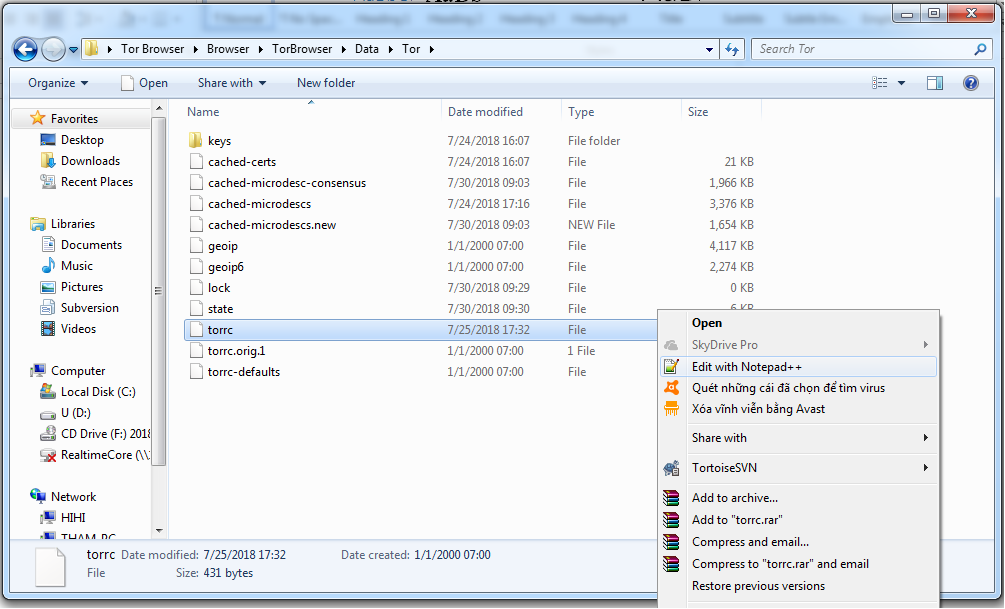
### Thiết lập dịch vụ Tor.

#### Cách 1: Sử dụng Tor Browse

##### Mở thư mục :

C:\Users\TranDuyThanh\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor

Mở file torrc bằng notepad++



##### Thêm cấu hình dịch vụ tor

Thêm 2 dòng vào cuối file “torrc”:

**HiddenServiceDir D:\public\hidden**

**HiddenServicePort 80 127.0.0.1:8080**

**HiddenServiceDir**: Đường dẫn tới thư mục của web đã được cấu hình trên IIS

**HiddenServicePort**: Port của dịch vụ sẽ sử dụng. Định mạng theo mẫu

**HiddenServicePort** <**port tor**> <**Địa chỉ web mở bằng IIS**>

Lưu lại và đóng file torrc.

Mở trình duyệt Tor Browser.

Tại thư mục của web đã được cấu hình IIS xuất hiện 2 file là hostname và private\_key

##### Tạo hostname và private key

Tải và giải nén file scallion theo link:

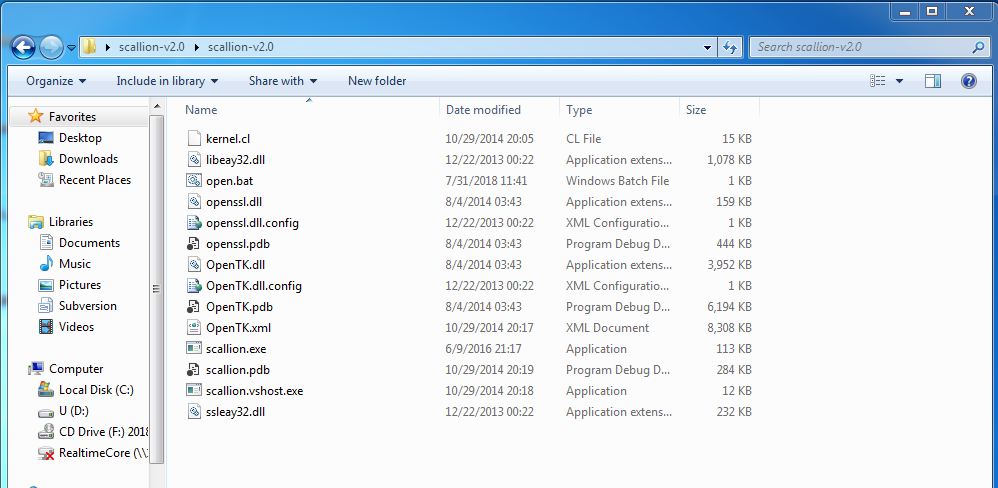
<https://github.com/lachesis/scallion/raw/binaries/scallion-v2.0.zip>

Trong thư mục scallion vừa giải nén. Mở file open.bat và edit lại thông tin của domain tor sẽ sử dụng.

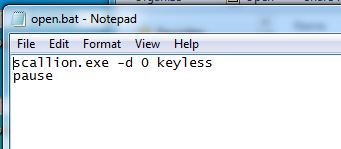
scallion.exe -d 0 <ytut>

ytut: là domain tor sẽ được sử dụng.

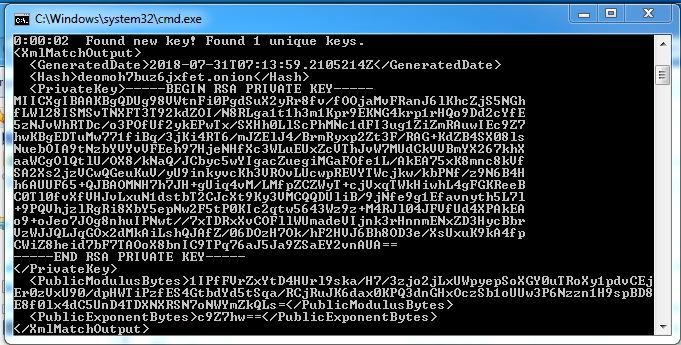
vd:



Lưu và run file open.bat.



Commad line sẽ chạy và sẽ tự động tạo ra hostname và private\_key tương ứng với host đã được cấu hình. Lưu ý: hostname càng dài thời gian run để tạo ra được hostname và private\_key sẽ càng lâu. Server phải kết nối với internet để scallion tạo hostname và private\_key.



Với domain deomo sau khi sử chạy sẽ sinh ra hash “deomoh7buz6jxfet.onion” là domain tor dùng để truy cập qua tor browser. PrivateKey là mã hóa của domain sau khi mã hóa.

-----BEGIN RSA PRIVATE KEY-----

MIICXgIBAAKBgQDUg98VWtnFi0PgdSuX2yRr8fv/fOOjaMvFRanJ6lKhcZjS5NGh

fLWl28ISMSvTNXFT3T92kdZOI/N8RLga1t1h3m1Kpr9EKNG4krp1rHQo9Dd2cYfE

5zNJvWhRTDc/o3POfUf2ykEPwTx/SXHh0LlScPhMNc1dFI3ug1ZiZmRAuwIEc9Z7

hwKBgEDTuMw771fiBq/3jKi4RT6/mJZElJ4/BrmRyxp2Zt3F/RAG+KdZB4SX08ls

NuebOIA9tNzbYVYvVFEeh97HjeNHfXc3WLuEUxZcVThJvW7MUdCkVVBmYX267khX

aaWCgOlQtlU/OX8/kNaQ/JCbyc5wYIgacZuegiMGaFOfe1L/AkEA75xK8mnc8kVf

SA2Xs2jzVCwQGeuKuV/yU9inkyvcKh3VROvLUcwpREVYTWcjkw/kbPNf/z9N6B4H

h6AUUF65+QJBAOMNH7h7JH+gUiq4vM/LMfpZCZWyT+cjVxqTWkHiwhL4gFGKReeB

C0Tl0fvXfVHJvLxuN1dstbT2CJcXt9Ky3VMCQQDUliB/9jNfe9g1Efavnyth5L7l

+9PQVhjzlRgRi8XbY5epNw2F5tP0KIc2qtw5643Wz9z+M4RJl04JFVfUd4XPAkEA

o9+oJeo7JOg8nhuIPNwt//7xTDRxXvCOFllWUmadeVIjnk3rHnnmENxZD3HycBbr

VzWJJQLJqGOx2dMkAiLshQJAfZ/06DOzH7Ok/hF2HVJ6Bh8OD3e/XsUxuK9kA4fp

CWiZ8heid7bF7TAOoX8bnIC9TPq76aJ5Ja9ZSaEY2vnAUA==

-----END RSA PRIVATE KEY-----

##### Cấu hình tor host

Thay nội dung file hostname bằng hash đã tạo ra, nội dung file private\_key bằng PrivateKey có được khi hash.

Test dịch vụ đã cấu hình.

Mở trình duyệt Tor và dán đường link(hash) và kiểm tra kết quả.

#### Cách 2: Sử dụng Tor Bundle

##### Thiết lập Tor Bundle

Giải nén file tor-win32-0.3.3.7.zip ra desktop hoặc thư mục lưu trữ.

Tạo file torrc trong thư thư mục Tor\Tor (C:\Users\TranDuyThanh\Desktop\tor-win32-0.3.3.7\Tor)

##### Thiết lập cấu hình dịch vụ

Eidt file torrc. Thêm các dòng dòng sau:

DataDirectory C:\Users\TranDuyThanh\Desktop\tor-win32-0.3.3.7\Data\Tor

GeoIPFile C:\Users\TranDuyThanh\Desktop\tor-win32-0.3.3.7\Data\Tor\geoip

GeoIPv6File C:\Users\TranDuyThanh\Desktop\tor-win32-0.3.3.7\Data\Tor\geoip6

HiddenServiceDir D:\public\hidden

HiddenServicePort 80 127.0.0.1:80

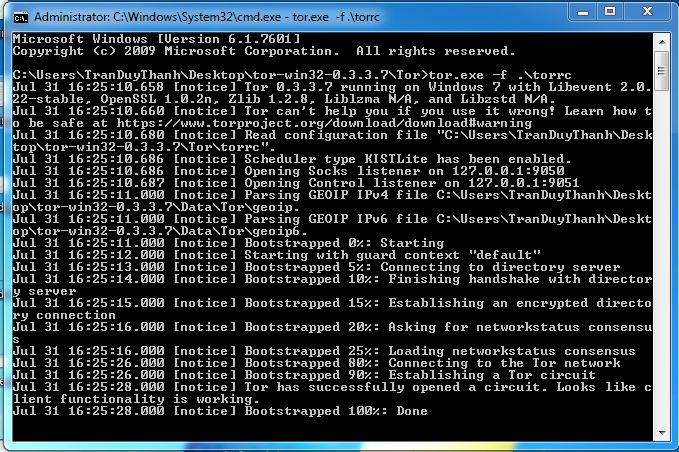
DataDirectory: Là thư mục chứa file tor.exe

GeoIPFile: Là đường dẫn file geoip

GeoIPv6File: Là đường dẫn file geoip6

##### Tạo dịch vụ tor

Mở cmd.exe và trỏ đường dẫn tới thư mục chứa file tor.exe và gõ lệnh: “tor.exe –f .\torrc”.



Sau khi chạy được 100%, tắt tiến trình hiện tại và bước [3 và 4 cách 1](#_Tạo_hostname_và). Trước khi test cần thực hiện lại bước [3 cách 2](#_Tạo_dịch_vụ)

## Tor.net

### Ý tưởng

Tại sao không thể sử dụng Tor trực tiếp như một proxy HTTP?

Đây là một quan niệm sai lầm phổ biến. Một số người cố gắng khởi động tiến trình Tor trên máy cục bộ của họ, đưa ra quy trình một số cổng cho cổng SOCKS, và sau đó cấu hình trình duyệt của họ để trỏ đến tiến trình Tor. Điều này sẽ không hoạt động.

Tor là một SOCKS proxy có nghĩa là nó có thể kết nối với các địa chỉ IP và các cổng, nhưng nó không hiểu các yêu cầu HTTP. Proxy SOCKS có một loạt các giao thức phải được theo dõi một cách rõ ràng trước khi kết nối có thể được thiết lập. Trong các proxy SOCKS điển hình, có thể có xác thực bổ sung (sử dụng các thông tin xác thực) sẽ được yêu cầu trước khi bất kỳ nỗ lực kết nối nào thậm chí có thể bắt đầu. Tor, tuy nhiên, không yêu cầu bất kỳ thông tin đăng nhập nào khi kết nối.

Sự khác biệt chính giữa proxy SOCKS và proxy HTTP là sau này hiểu được các yêu cầu HTTP. Một proxy HTTP có khả năng phân tích các tiêu đề của một yêu cầu HTTP để xác định nơi thông tin sẽ được định tuyến và thực hiện tất cả các hoạt động liên quan đến việc truyền dữ liệu HTTP đến và từ một máy chủ.

Proxy SOCKS chỉ có thể thực hiện khi được hướng dẫn. Nó được thông báo rằng một kết nối được yêu cầu đến một địa chỉ nhất định, sau đó nó sẽ cố gắng để thiết lập kết nối. Nếu kết nối thất bại, nó sẽ phản hồi với một gói lỗi được cấu trúc theo giao thức SOCKS. Nếu kết nối thành công, nó sẽ đóng vai trò như một luồng "đệm" nằm giữa máy khách và máy chủ. Khi proxy SOCKS nhận dữ liệu, nó sẽ chuyển nội dung đó ngay lập tức tới kết nối đối lập.

Như đã đề cập trước đó, mạng Tor không được thiết kế cho các giao tiếp HTTP proxy ngay lập tức. Thay vào đó, một proxy web phải được thực hiện. Thư viện Tor.NET thực hiện một hệ thống proxy tùy chỉnh để xử lý việc chuyển đổi từ các truyền thông SOCKS chuẩn sang HTTP.

### Cấu hình project

Để sử dụng được thư viện Tor.Net cho một project cần thêm cấu hình trong file config gồm có các thông tin:

### Yêu cầu:

Project sử dụng với .NET 4.0 trở lên( Nên sử dụng ở .NET 4.5)

Thư viện [Tor Bundle](https://www.torproject.org/dist/torbrowser/7.5.6/tor-win32-0.3.3.7.zip).

Cấu hình trong file config của project với các tham số:

1. ControlPassword: Password dùng để remote tor client
2. ControlPort: Port sẽ dùng để remote tor client
3. SocketPort: Port để tor client sử dụng để truy cập mạng tor
4. TorPath: Đường dẫn tới thư mục chứa thư thư viện TorBundle
5. Profile: Tài khoản sử dụng tor client
6. License: Key tài khoản tor client

Vd:

<add key="ControlPassword" value="123456789" />

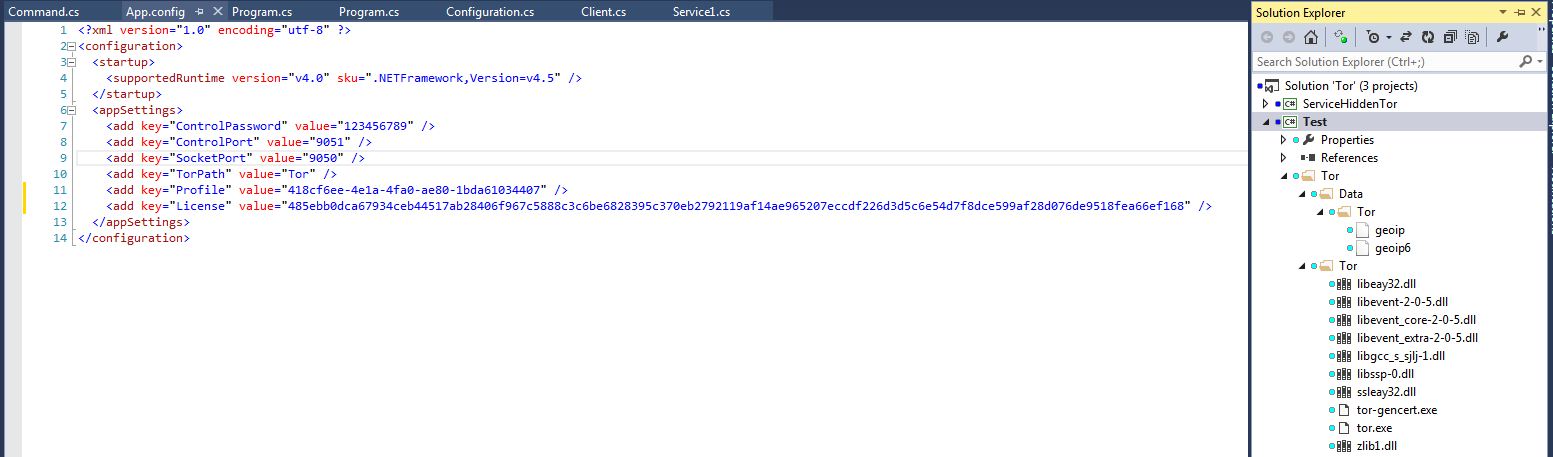
<add key="ControlPort" value="9051" />

<add key="SocketPort" value="9050" />

<add key="TorPath" value="Tor" />  
<add key="Profile" value="L6PP7-JYMJB-KVSG9-AXRN1-LX2R4-7WCPE" />

<add key="License" value="2HNE3-DYDMF-18N09-DH3K4-CBS97-GH4M5" />

Lưu ý: Các port tránh trùng với các port đã sử dụng của Server. Profile và License không được phép sửa. Các file nằm trong folder Tor phải được set thuộc tính “Build Action” là Content và Copy to output là “Copy if newer”



Add 2 referent có tên “SecurityCode.dll” và “tor.dll”.

### Sử dụng

Sau khi cấu hình các thông tin như hướng dẫn. Để gọi Web API cần khởi tạo client Tor trước khi sử dụng.

##### Các hàm thao tác:

public static string HTTPGetAPI(string uri, Client client = null, Dictionary<string, string> queryParams = null, int port = -1);

public static string HTTPGetAPI(Uri uri, Client client = null, Dictionary<string, string> queryParams = null, int port = -1);

public static string HTTPPostAPI(string url, Client client = null, Dictionary<string, string> para = null, int port = -1);

public static string HTTPPostAPI(Uri url, Client client = null, Dictionary<string, string> para = null, int port = -1);

uri: Link get/post API,

client: Nếu sử dụng tor để call API thì phải truyền tham số tor client.

queryParams/para : Danh sách các paramater dùng trong việc gọi web api.

Port: port để gọi web api nếu khác cổng mặc định 80.

##### Demo code:

Tor.Clients.Client tor= Tor.Clients.Client.Instance(); // Khởi tạo Tor client

string a= Tor.Clients.Client.HTTPGetAPI("https://www.torproject.org/download/download.html.en",tor); // Kết quả trả về là string