ডার্ক ওয়েব

dark web

মুহাম্মাদ সাইফুল ইসলাম

সতর্কীকরণ

এই বইটি শুধুমাত্র ডার্ক ওয়েবের সাথে সঠিকভাবে পরিচয় করিয়ে দেওয়ার জন্য।
এরপরও কেউ যদি খারাপ কাজ করে তবে, সেই দায়-দায়িত্ব একান্তই তার নিজের।
আমার উদ্দেশ্য- মানুষকে ডার্ক ওয়েবের সাথে সঠিকভাবে পরিচয় করিয়ে দেওয়া।
যাতে করে, সঠিক দিক নির্দেশনা ছাড়াই ডার্ক ওয়েবে
গিয়ে কেউ ক্ষতির স্বীকার না হয়।

- মুহাম্মাদ সাইফুল ইসলাম

ডার্ক ওয়েব

মুহাম্মাদ সাইফুল ইসলাম
মোঃ আবদুল্লাহ

প্রকাশকাল : জুন ২০২৩

ভূমিকা

ডার্ক ওয়েব বলতে সাধারণত TOR নেটওয়ার্কের ওয়েবসাইট সমূহকে বোঝানো হয়। যদিও, এরকম রহস্যে ঘেরা নেটওয়ার্ক আরও অনেক রয়েছে। রহস্যময় সেই ইন্টারনেট জগতের সাথেই আমরা পরিচিত হবো। তবে, এই পরিচিত হওয়ার মূল উদ্দেশ্য কি, জানেন? প্রায়ই এই ধরনের নেটওয়ার্কে প্রবেশ করে অনেক মানুষ ক্ষতির সম্মুখীন হয়। তার কারণ একটাই- এই নেটওয়ার্ক সম্বন্ধে তাদের সঠিক জ্ঞান নেই। এরপর তারা মনের আক্ষেপে ডার্ক ওয়েবকে খারাপ বলে মানুষের কাছে প্রচার করে। ফলে, তাদের কথা শুনে মানুষ মনে করে- ডার্ক ওয়েব হচ্ছে রাতের অন্ধকারে ডাকাতি করার মতো ভয়ানক জায়গা। অথচ, ডার্ক ওয়েবে ঘটে চলা খারাপ কাজকে অস্বীকার করা না গেলেও, আমরা যেই সাধারণ ইন্টারনেট ব্যাবহার করি, তার চেয়ে ডার্ক ওয়েব অধিক নিরাপদ। নিচে তার কারণ উল্লেখ করা হলো-

পরিচয় গোপন থাকে

আমরা যখন সাধারণ ইন্টারনেট ব্যাবহার করে কোন ওয়েবসাইটে প্রবেশ করি, তখন সেই ওয়েবসাইটের কাছে আমাদের ডিভাইসের অনেক তথ্য চলে যায়। যেমনঃ

- আমরা কোন ওয়েব ব্রাউজার ব্যাবহার করছি,
- আমাদের কম্পিউটারের অপারেটিং সিস্টেম কোনটি,
- আমাদের আইপি এড্রেস,
- আমাদের ঠিকানা।

এছাড়াও আরও অনেক তথ্যই ওয়েবসাইট সংগ্রহ করতে পারে। কিন্তু, আপনি যখন ডার্ক ওয়েব ব্যাবহার করবেন তখন আপনার ডিভাইসের এসব তথ্য ওয়েবসাইট সংগ্রহ করতে পারবে না। বরং, ওয়েবসাইট জানবেই না যে, আপনি ওয়েবসাইটে প্রবেশ করেছেন। কারণ, ডার্ক ওয়েব বা, TOR নেটওয়ার্ক ব্যাবহার করলে আপনি সরাসরি আপনার ডিভাইস দিয়ে ওয়েবসাইটের সাথে connect হবেন না। বরং, আপনার কম্পিউটার পর্যায়ক্রমে ৩ টি TOR নেটওয়ার্কের কম্পিউটারের সাথে connect হবে। এরপর সেই ৩য় কম্পিউটারটি connect হবে ওয়েবসাইটের সাথে। ফলে, ওয়েবসাইট মনে করবে- ডার্ক ওয়েবের সেই ৩য় কম্পিউটারটিই ওয়েবসাইটে প্রবেশ করেছে। ফলে, আপনার পরিচয় গোপন থাকবে।

ডার্ক ওয়েবে কিভাবে প্রবেশ করবো?

ডার্ক ওয়েব সম্বন্ধে যারা একদমই জানেন না, তারা অতি আগ্রহ নিয়ে অপেক্ষা করছেন- ডার্ক ওয়েবে প্রবেশের পদ্ধতি জানার জন্য। তাদের জন্যই ডার্ক ওয়েব সম্বন্ধে বিস্তারিত আলোচনা না করেই ডার্ক ওয়েবে প্রবেশের পদ্ধতি জানিয়ে দিচ্ছি। এরপর বিস্তারিত ও জরুরি আলোচনা করবো। তবে, আপনি একদমই নতুন হলে বইয়ে দেখানো কোনকিছু এখনই এখনই নিজে থেকে করতে যাবেন না। প্রথমে বইটি শেষ পর্যন্ত পড়ুন। তারপর নিজে থেকে বইয়ে দেখানো পদ্ধতি অনুসরণ করতে পারেন।

TOR ব্রাউজার ডাউনলোড

ডার্ক ওয়েবের ওয়েবসাইটগুলো রয়েছে TOR নেটওয়ার্কে। আর, TOR নেটওয়ার্কে প্রবেশ করতে চাইলে আপনাকে TOR ব্রাউজার ডাউনলোড করতে হবে। নিচের লিংকে ক্লিক করলে ছবির web page টি আসবে।

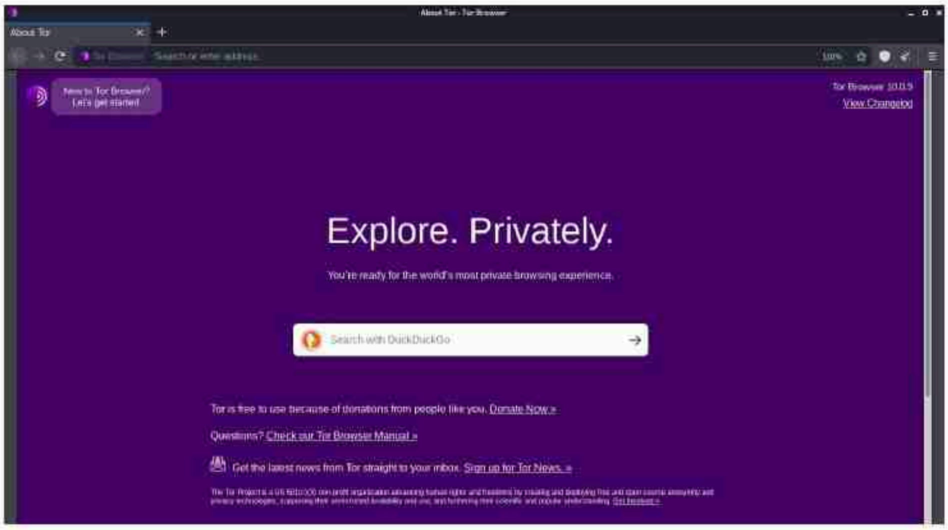
লিংকঃ https://www.torproject.org/download/

উপরের ছবিতে দেখতে পাচ্ছেন- Windows, OS X, Linux, Android চারটি অপশন রয়েছে। আপনার কম্পিউটারের অপারেটিং সিস্টেম অনুযায়ী ডাউনলোড করে নিন।

ডার্ক ওয়েবে প্রবেশ

TOR ব্রাউজার ডাউনলোড হয়ে গেলে install করুন। এখন TOR ব্রাউজারের আইকনে ক্লিক করে open করুন। তবে, TOR ব্রাউজার open হওয়ার আগে নিচের ছবির মতো কিছুক্ষণ loading হবে। এই সময় আপনার কম্পিউটারকে TOR নেটওয়ার্কের সাথে connect করিয়ে দেওয়া হয়।

এরপর নিচের ছবির মতো TOR ব্রাউজার open হবে।

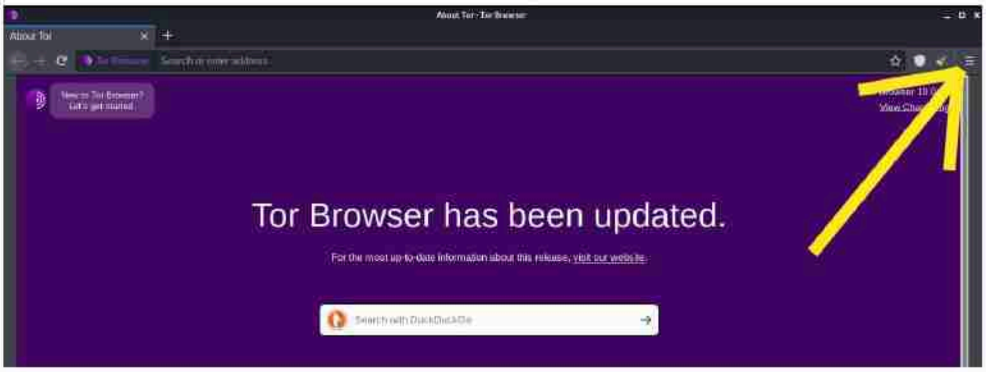


TOR ব্রাউজারের জরুরী **settings** পরিবর্তন

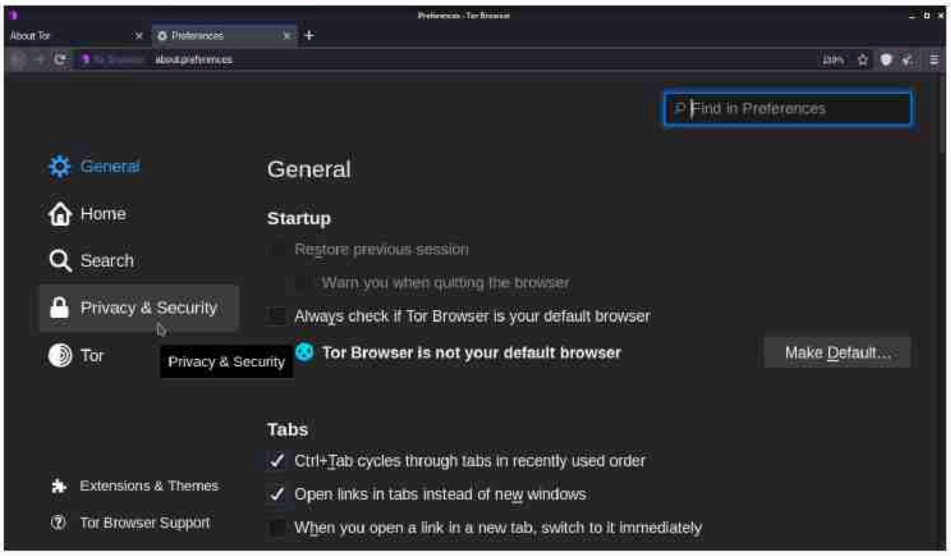
TOR ব্রাউজারের মাধ্যমে আমরা ডার্ক ওয়েবে প্রবেশ করবো। তবে, ডার্ক ওয়েবে আপনি যদি খারাপ কোন ওয়েবসাইটে প্রবেশ করে ফেলেন, তখন আপনি নিচে উল্লেখ করা বিপদ সমূহের সম্মুখীন হতে পারেন-

- ওয়েবসাইট আপনার কম্পিউটারের ক্যামেরা চালু করিয়ে দিতে পারে।
- আপনার কম্পিউটারের মাইক্রোফোন চালু করিয়ে দিতে পারে।
- আপনার বর্তমান ঠিকানা track করতে পারে।

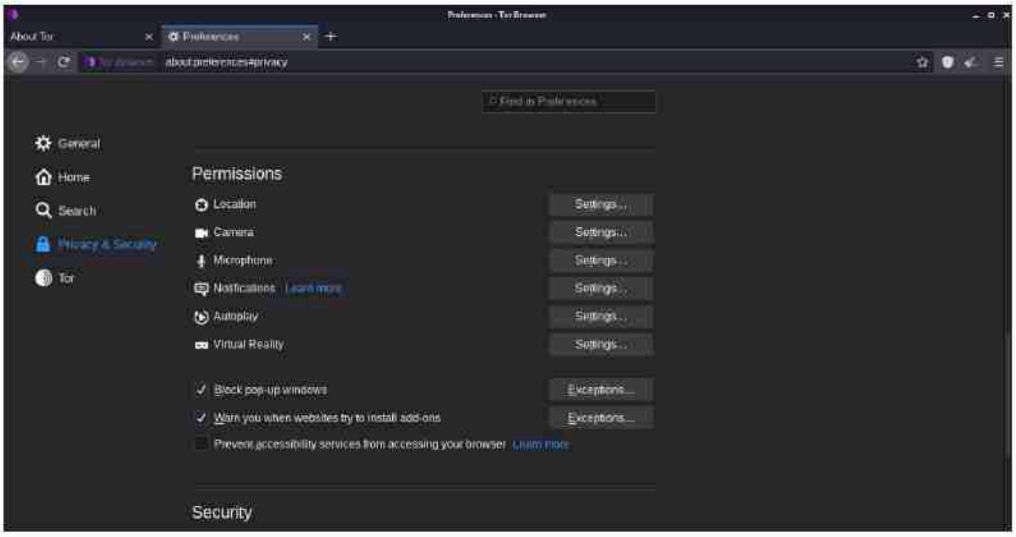
তাই, শুরুতেই কিছু settings পরিবর্তন করতে হবে। যাতে করে ওয়েবসাইটগুলো আপনার কম্পিউটারের ক্যামেরা, মাইক্রোফোন, ঠিকানা ইত্যাদি access করতে না পারে। এজন্য প্রথমেই নিচের ছবিতে তীর চিহ্ন দিয়ে দেখানো **menu** তে ক্লিক করুন।



এরপর **Preferences** এ ক্লিক করলে নিচের ছবির মতো page আসবে।

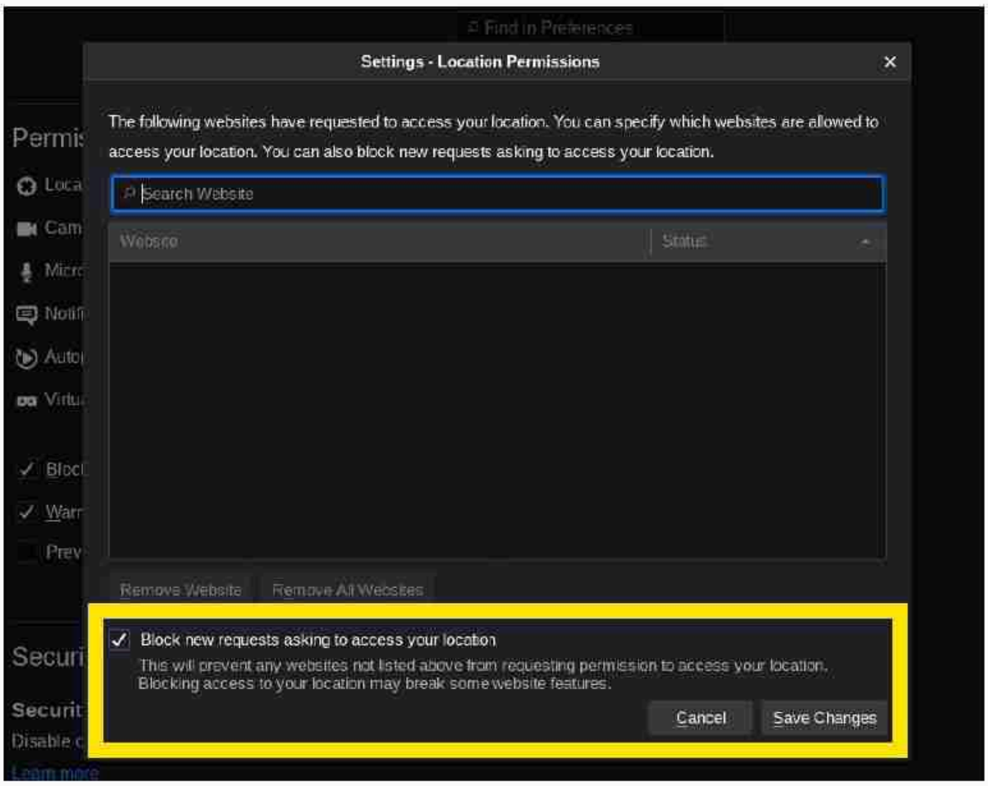


এখন **Privacy & Security** তে ক্লিক করুন। তারপর নিচের দিকে (scroll down করে) গেলেই ছবির মতো কিছু অপশন দেখতে পারবেন।



এখানে Location, Camera থেকে শুরু করে যেগুলোর ডান পাশে **Settings..** লেখা দেখতে পাচ্ছেন, সেই **Settings..** এর ওপর ক্লিক করলে নিচের ছবির মতো লেখা আসবে।

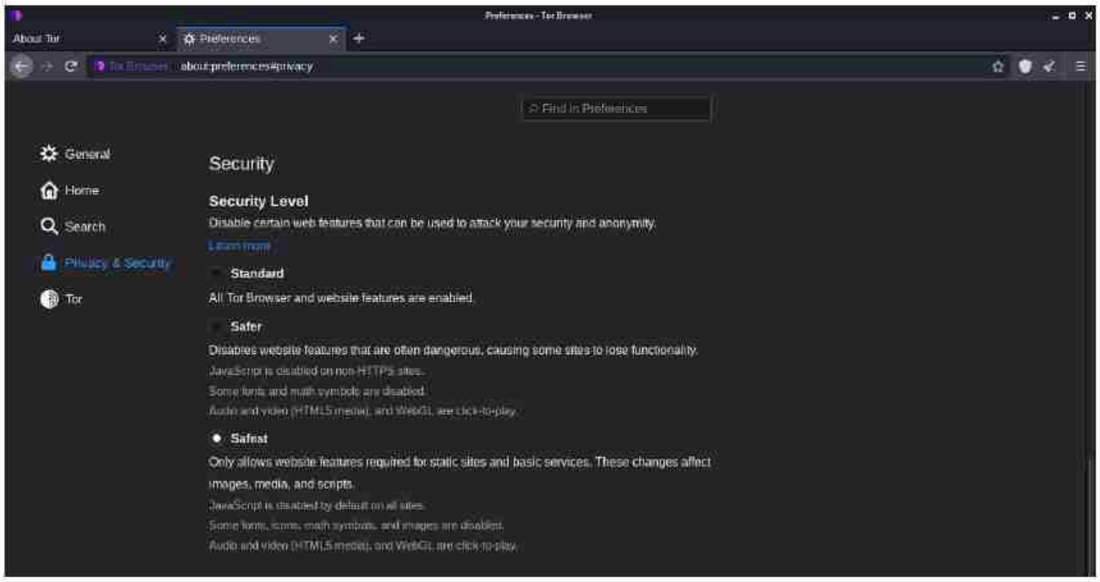
s



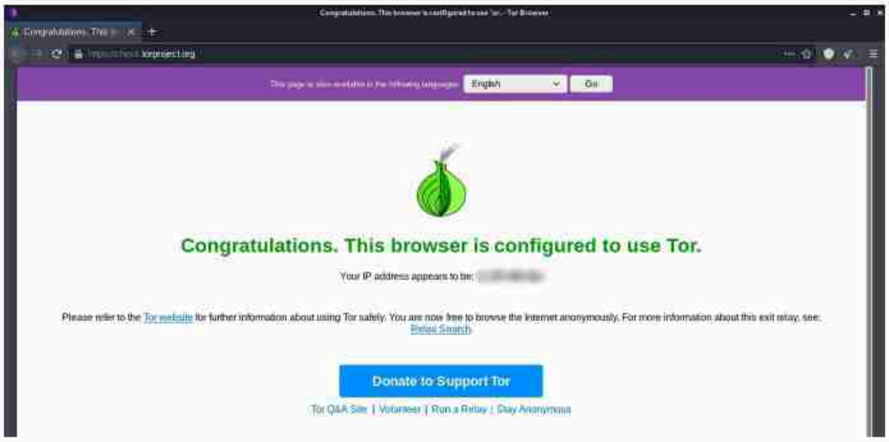
সবগুলো **Settings..** এ ক্লিক করে ছবির মতো নিচে টিক চিহ্ন দিয়ে **Save Changes** এ ক্লিক করুন।

JavaScript অচল করুন

এখনও একটি জরুরি settings পরিবর্তন করা বাকি আছে। আর, তা হচ্ছে জাভাস্ক্রিপ্ট disable করা। সেই জন্যে একটু আগে দেখানো পদ্ধতিতে **Privacy & Security** তে আবার ক্লিক করুন। এরপর (scroll down করে) কিছুটা নিচে গেলেই দেখতে পাবেন ছবির মতো **Security Level** নামের একটি অপশন চলে এসেছে। এখানে **Safest** অপশনটি select করুন।



এখন TOR ব্রাউজার দিয়ে এই লিংকে যান- check.torproject.org

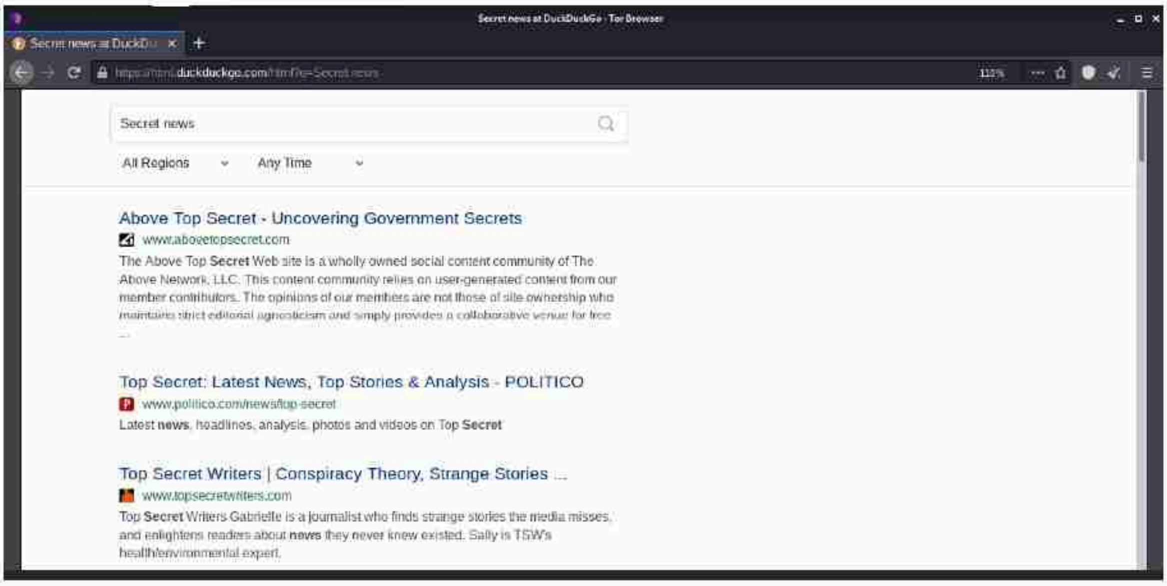


আপনাকে কি উপরের মতো **Congratulations** জানানো হচ্ছে? তাহলে স্বাগতম!

এখন আপনি TOR ব্রাউজার দিয়ে ডার্ক ওয়েবে প্রবেশ করার জন্য প্রস্তুত।

ডার্ক ওয়েবের ওয়েবসাইটে প্রবেশ করবো কিভাবে?

TOR ব্রাউজারে কিছু লিখে search দিলে দেখতে পারবেন- সাধারণ ইন্টারনেটের ওয়েবসাইট গুলোই আসবে। যেমনঃ নিচের ছবিতে দেখতে পাচ্ছেন- TOR ব্রাউজারে **Secret news** লিখে search দেওয়ায় যেসব ওয়েবসাইট এসেছে, যেগুলোর লিংকে সাধারণ ইন্টারনেটের ওয়েবসাইটের মতোই .com লেখা রয়েছে। অথচ, ডার্ক ওয়েবের ওয়েবসাইটের লিংকের শেষে .onion লেখা থাকে।



কিভাবে সার্চ করলে শুধুমাত্র ডার্ক ওয়েবের ওয়েবসাইটের লিংক আসবে? এর জন্য আমাদেরকে ডার্ক ওয়েবের সার্চ ইঞ্জিন ব্যাবহার করতে হবে। সাধারণ ইন্টারনেটে আমরা যেভাবে Google সার্চ ইঞ্জিন ব্যাবহার করে সার্চ করি, ডার্ক ওয়েবেরও সেরকম সার্চ ইঞ্জিন আছে। সেখানে সার্চ করলে ডার্ক ওয়েবের ওয়েবসাইট পাওয়া যায়।

এর মধ্যে উল্লেখযোগ্য কিছু ডার্ক ওয়েব সার্চ ইঞ্জিন হচ্ছে-

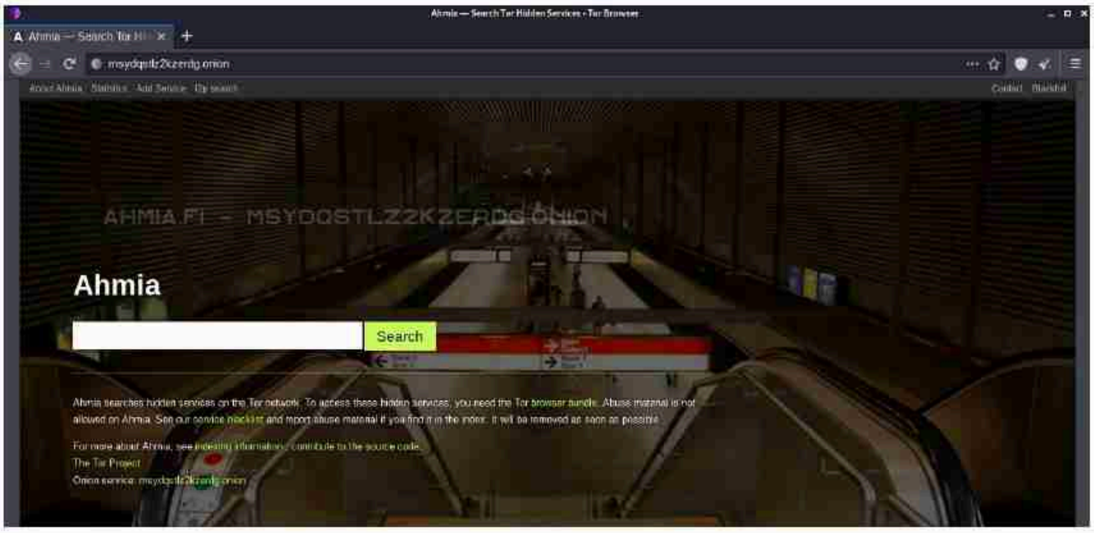
- **Ahmia**

  লিংকঃ msydqstlz2kzerdg.onion

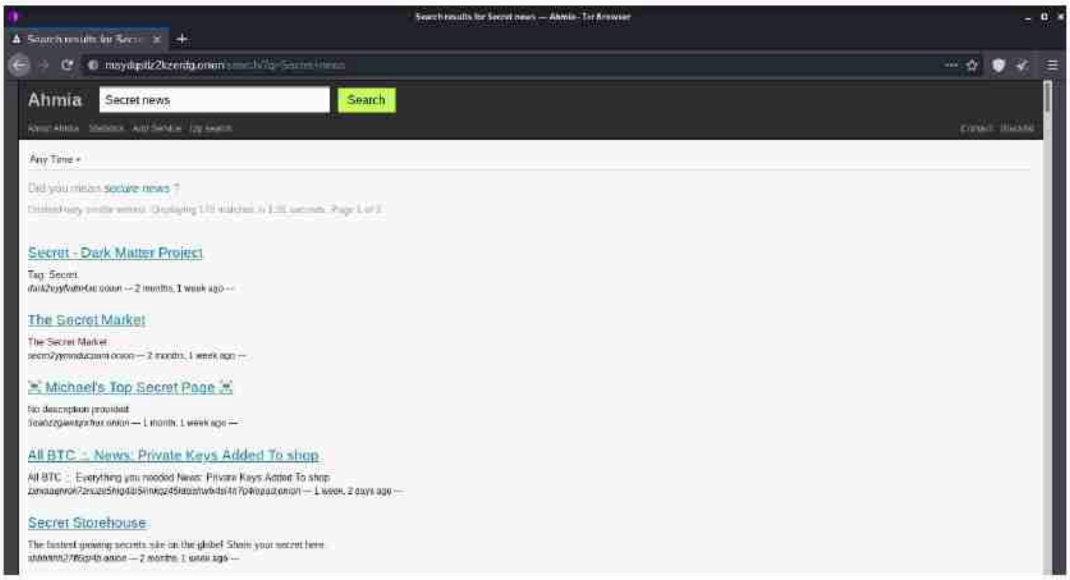
- **Torch**

  লিংকঃ cnkj6nippubgycuj.onion

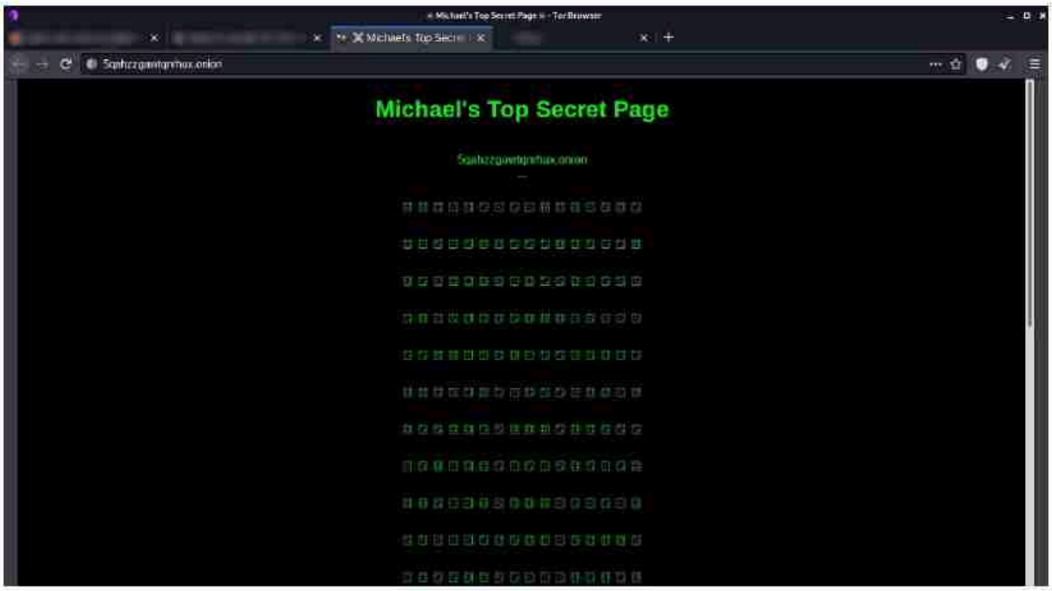
এখন আমরা **Ahmia** সার্চ ইঞ্জিন দিয়ে ডার্ক ওয়েবে সার্চ করবো। নিচের ছবিতে দেখতে পাচ্ছেন- আমরা TOR ব্রাউজার দিয়ে **Ahmia** সার্চ ইঞ্জিনে চলে এসেছি।



একটু আগে আমরা TOR ব্রাউজারে **Secret news** লিখে সার্চ দেওয়ার পর সাধারণ ইন্টারনেটের ওয়েবসাইট গুলোই এসেছিলো। কিন্তু, এইবার আমরা **Ahmia** সার্চ ইঞ্জিনে **Secret news** লিখে সার্চ দিয়েছি। নিচের ছবিতে দেখতে পাচ্ছেন- **Ahmia** আমাদেরকে সাধারণ ইন্টারনেটের ওয়েবসাইট না দেখিয়ে ডার্ক ওয়েবের ওয়েবসাইটের লিংক দেখাচ্ছে।



উপরের ছবিতে দেখানো সার্চ রেজাল্ট থেকে যখন আমরা ৩য় লিংকে ক্লিক করলাম, তখন নিচের ছবির মতো অদ্ভুত একটি web page দেখতে পেলাম। এর নিচের দিকে কিছু হেক্সাডেসিম্যাল সংখ্যাও লেখা রয়েছে।



সে যাই হোক, ডার্ক ওয়েবে প্রথম প্রথম এসে অনেকেই উত্তেজিত হয়ে পড়ে। এটা মোটেও উচিত না। মাথা ঠাণ্ডা না রাখলে ডার্ক ওয়েবের অন্ধকার গর্তে পড়ে যাবেন। আপনি ডার্ক ওয়েবের পথ-ঘাট চিনুন কিন্তু, ডার্ক ওয়েবের পথ-ঘাট যেনো আপনাকে চিনতে না পারে। ডার্ক ওয়েব থেকে কিছু নিতে এসেছেন, দিতে নয়- এটা মাথায় রেখে চলুন। অবশ্য আমি শুধুমাত্র এই বই লেখার জন্যই ডার্ক ওয়েবে এসেছি। এছাড়া ডার্ক ওয়েবে আসাই হয় না।

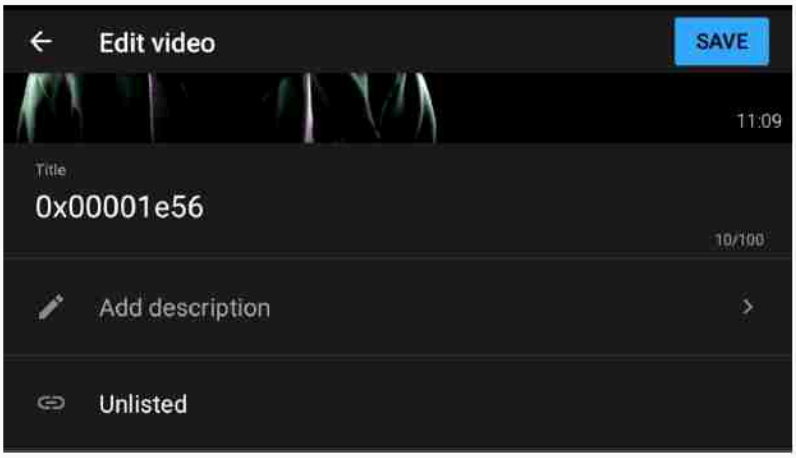
এক দেশের গোয়েন্দা সংস্থায় চাকরি করার শর্ত হচ্ছে- "তুমি যা করেছো, তা মানুষকে জানাতে পারবে না। এমনকি গুরুত্বপূর্ণ অপারেশনে successful হলেও সেটা মানুষকে জানিয়ে বাহ বা নেওয়া যাবে না।" এই শর্তের কারণে অনেকেই গোয়েন্দার চাকরি করতে নিরুৎসাহিত হয়ে চলে গিয়েছে। অপরদিকে, যারা গোয়ান্দা হিসেবে দায়িত্ব পালন করছেন তাদের ঘরের মানুষও জানে না যে, তারা গোয়ান্দা। এটাই গোপনীয়তা, আর গোপনীয়তার জন্যই ডার্ক ওয়েবের জন্ম।

আমি আশা করি- এই বই যারা পড়বেন তারা যথেষ্ট চালাক ও বোধ-সম্পন্ন।

ওয়েব পরিচিতি

আমরা যেই সাধারন ইন্টারনেট ব্যাবহার করি, তাকে surface web বলা হয়। ইন্টারনেটের এই অংশের ওয়েবসাইট ও তথ্য Google এর মতো সার্চ ইঞ্জিন দিয়েই খুঁজে পাওয়া যায় যেমন Youtube ভিডিও। কিন্তু, ধারনা করা হয়- সম্পুর্ন ইন্টারনেটের তুলনায় সাধারন ইন্টারনেট (surface web) কেবলমাত্র ৪% এর মতো। বাকি সিংহ ভাগই হচ্ছে ডিপ ওয়েব এবং ডার্ক ওয়েব। ডিপ ওয়েবের তথ্য Google এর মতো সার্চ ইঞ্জিন দিয়ে সরাসরি খুঁজে পাওয়া যায় না। যেমনঃ Gmail এর উপাদান (আমাদের ইমেইল) হচ্ছে ডিপ ওয়েবের অংশ। এই কারনেই ইমেইল গুলো Google সার্চ করে খুঁজে পাওয়া যায় না।।

আবার, অনেক Youtube ভিডিও ডিপ ওয়েবের অংশ। যেমনঃ নিচের ছবিতে দেখতে পাচ্ছেন আমার Youtube চ্যানেলের একটি ভিডিও আমি **Unlisted** করে রেখেছি। এর মানে হচ্ছে- এই ভিডিও শুধুমাত্র তারাই দেখতে পারবে, যাদের কাছে এই ভিডিওর লিংক থাকবে। কিন্তু, লিংক ছাড়া এই ভিডিও কেউ দেখতে পারবে না। এমনকি সার্চ করেও এই ভিডিও খুঁজে পাওয়া যাবে না।



একজন ব্যক্তি চাইলে তার Youtube ভিডিও বাংলাদেশ বা, অন্য কোন দেশে block করে দিতে পারে। তখন block করে দেওয়া দেশের মানুষ সেই Youtube ভিডিও দেখতে পারবে না। তবে, এই ধরনের ভিডিও কিন্তু ডিপ ওয়েবের অংশ না। কারন, যেসব দেশে block করা হয় নি, সেসব দেশের মানুষ ঠিকই সেই ভিডিও সার্চ করে খুঁজে পাবে।

ডার্ক ওয়েব ব্যাবহারবিধি ও সঠিক ধারনা

আপনি যখন TOR ব্রাউজার open করবেন, তখন ব্রাউজারটি full-screen না হয়ে ছোট window নিয়ে open হবে। আপনি কখনো TOR ব্রাউজার full-screen করবেন না। বরং, যেভাবে থাকে সেভাবেই ব্যাবহার করুন। কারন, full-screen করলে ডার্ক ওয়েবের ওয়েবসাইট আপনার কম্পিউটার screen এর resolution জানতে পারবে।

ডার্ক ওয়েব সম্বন্ধে ধারনা

- মনে রাখবেন- TOR ব্রাউজার এবং TOR নেটওয়ার্ক সম্পুর্ন আলাদা বিষয়। প্রথমে আমেরিকান নৌ-বাহিনীর রিসার্চ ল্যাবরেটরিতে TOR নেটওয়ার্ক তৈরি করা হয়েছিলো এবং তাদের উদ্দেশ্য ছিলো- শুধুমাত্র তারাই TOR নেটওয়ার্ক ব্যাবহার করবে। ফলে, ইন্টারনেটে একদম গোপনভাবে তারা কাজ করতে পারবে। কিন্তু, শীঘ্রই তারা বুঝতে পারলো- এই নেটওয়ার্ক যদি শুধুমাত্র তারাই ব্যাবহার করে তাহলে, এই নেটওয়ার্ক ব্যাবহার করে তারা কোন ওয়েবসাইটে প্রবেশ করলেই ওয়েবসাইটের মালিক বুঝতে পারবে যে, TOR নেটওয়ার্ক ব্যাবহার করে আমেরিকান নৌ-বাহিনী তার ওয়েবসাইটে প্রবেশ করেছে। তাই, তখন তারা সাধারন মানুষের ব্যাবহারের জন্য TOR নেটওয়ার্ক উন্মুক্ত করে দেয়। ফলে, ওয়েবসাইটের মালিক যখন দেখবে- তার ওয়েবসাইটে TOR নেটওয়ার্ক থেকে কেউ প্রবেশ করেছে, তখন তিনি বুঝতে পারবেন না যে, তার ওয়েবসাইটে গোয়েন্দা প্রবেশ করেছে নাকি, সাধারণ মানুষ প্রবেশ করেছে। যদিও আমেরিকার গোয়েন্দাদের জন্য **SIPRnet, JWICS, NSANet** ইত্যাদি অনেক নেটওয়ার্ক রয়েছে। তবে, TOR নেটওয়ার্ক হচ্ছে অন্যতম। TOR নেটওয়ার্ক পরিচালিত হচ্ছে অসংখ্য স্বেচ্ছাসেবী লোকের কম্পিউটারের মাধ্যমে। সব মিলিয়ে এটাকে circuit বলা হয়। TOR ব্যাবহার করে আপনি যখন কোন ওয়েবসাইটে প্রবেশ করেন, তখন মূলত TOR নেটওয়ার্কের কম্পিউটারের মাধ্যমেই ওয়েবসাইটে প্রবেশ করেন। তো, এই কম্পিউটারগুলো দিয়ে গঠিত নেটওয়ার্ক হচ্ছে TOR নেটওয়ার্ক আর, সেই নেটওয়ার্কে connect হওয়ার জন্য ব্যাবহার করতে হয় TOR ব্রাউজার।
- সাধারন ইন্টারনেটে চাইলেই আপনার আইপি এড্রেস, ঠিকানা থেকে শুরু করে অনেক তথ্য সংগ্রহ করা সম্ভব। কিন্তু, ডার্ক ওয়েবে আপনার তথ্য সংগ্রহ করা বলা যায় অসম্ভব।

- TOR ব্রাউজার দিয়ে আপনি সাধারণ ইন্টারনেটও ব্যাবহার করতে পারবেন। সেক্ষেত্রেও, আপনার পরিচয় গোপন থাকবে।
- TOR ব্রাউজার ব্যাবহার করে ইন্টারনেট ব্যাবহার করলে slow কাজ করে। কারন, আপনার কম্পিউটার সরাসরি ওয়েবসাইটের সাথে connect না হয়ে প্রথমে TOR নেটওয়ার্কের ৩ টি কম্পিউটারের সাথে connect হবে। এরপর, ৩য় কম্পিউটারটি connect হবে ওয়েবসাইটের সাথে। তাই কোনকিছু load হতে দেরি হয়।

ডার্ক ওয়েবে গিয়ে ডার্ক ওয়েবের সার্চ ইঞ্জিনে সার্চ করেই আপনি সব তথ্য পেয়ে যাবেন, সকল রহস্য জেনে যাবেন- এমন কিন্তু না। বরং, ডার্ক ওয়েবে এমন কিছু ওয়েবসাইট আছে যেখানে প্রবেশ করতে অনুমতি নিতে হয় কিংবা, টাকা দিতে হয়। আবার, ফেসবুকের মতো ডার্ক ওয়েবেও বেশকিছু social media রয়েছে। এমনকি ফেসবুকেরও ডার্ক ওয়েবের লিংক আছে। সব মিলিয়ে ডার্ক ওয়েব এক বিশাল সমুদ্র। বিভিন্ন তথ্য রয়েছে বিভিন্ন জায়গায়। এখানে অনেক কিছুই হচ্ছে প্রতিনিয়ত। কিন্তু, জ্ঞান, বুদ্ধি ও অভিজ্ঞতা না থাকলে কোনকিছুই দেখতে পাবেন না।

ডার্ক ওয়েবের ফাঁদ

ডার্ক ওয়েবে আমেরিকান গোয়েন্দা সংস্থা ১০০% সফল হতে পারে নি। দিনের পর দিন ডার্ক ওয়েবে অনেক খারাপ কাজ হচ্ছে এবং অবৈধ পণ্যের মার্কেট তাদের কাজ ঠিকই করেই যাচ্ছে। মাঝে মাঝে **Silk Road** জব্দ করার মতো ঘটনা ঘটলেও আমেরিকান গোয়েন্দাদের চোখের সামনেই অসংখ্য ওয়েবসাইটে খারাপ কাজ ঘটে চলেছে। কিন্তু, ডার্ক ওয়েবে অপরাধের মূল হোতাদেরকে নির্মুল করতে না পারলেও মানুষ যেনো এসব অপরাধমূলক সেবা ক্রয় করতে ভয় পায়, সেই পদক্ষেপ তারা ঠিকই নিয়েছে। তারা নিজেরাই খারাপ কাজের ওয়েবসাইট খুলে বসে থাকে। এভাবে তাদেরকে অপরাধী ভেবে কেউ যদি তাদের কাছে খারাপ কিছু চাইতে আসে তখন তাকে গ্রেফতার করে। ফলে, ডার্ক ওয়েবে কেউ খারাপ কিছু করতে চাইলেও অনেকটা ভয়ের মধ্যে থাকে। তবে, আশা করি- আপনি এই ভয়ের মধ্যে থাকবেন না কারন, আপনি খারাপ কাজ করতে যাবেন না। এমনকি Firefox ব্রাউজারের একটি ত্রুটির সুযোগ নিয়ে আমেরিকান গোয়েন্দা সংস্থা NSA একসময় TOR ব্যাবহারকারীদের ওপর নজরদারী করেছিলো বলেও শোনা যায়।

তাই, কম্পিউটার নেটওয়ার্ক ও সাইবার সিকিউরিটির ওপর প্রাথমিক জ্ঞান না থাকলে ডার্ক ওয়েবের ওয়েবসাইটে প্রবেশ করা উচিত না।

.clos এবং .loky লিংকের ওয়েবসাইট

অনেকের কাছে ডার্ক ওয়েব খুব সাধারন একটি জায়গা। তাদের কাছে রহস্যময় ইন্টারনেট জগত হচ্ছে- Mariana's ওয়েব। যদিও, বাস্তবে সেই Mariana's ওয়েবের অস্তিত্ব আজও পাওয়া যায় নি। তবে, ধারনা করা হয়- আমেরিকা সরকারের গোপন তথ্য সহ বিশ্বের রাজনৈতিক ও ঐতিহাসিক অসংখ্য তথ্য রয়েছে এই Mariana's ওয়েবে। আবার, Mariana's ওয়েবের সাথে এখন .clos এবং .loky লিংকের ওয়েবসাইটের কথাও শোনা যাচ্ছে। আরও শোনা যাচ্ছে .lll এবং .rdos লিংকের ওয়েবসাইটের কথা। এই সবকিছুকে সাধারনত গুজব বলা হয়। অন্ততপক্ষে, এসবের কোন প্রমান কেউ দেখাতে পারে নি। এই বিষয়গুলো প্রচার করার একটি কারন হতে পারে- মানুষকে ধোঁকা দেওয়া। যেমনঃ এই ধরনের লিংকের ওয়েবসাইটে প্রবেশ করার সফটওয়্যার বিক্রি করার নামে ডার্ক ওয়েবে ভাইরাস যুক্ত সফটওয়্যার বিক্রি করা হয় বলে অভিযোগ আছে। আর, আপনি প্রায়ই বিভিন্ন রহস্যময় নেটওয়ার্কের কথা শুনতে পাবেন। প্রথমতো, যারা এসব প্রচার করা শুরু করে, তাদের আসল পরিচয়ই পাওয়া যায় না। দ্বিতীয়ত, এসব নেটওয়ার্ক বা, ওয়েবে প্রবেশ করার কোন পদ্ধতিই তারা বলতে পারে না। সাইবার জগত নিয়ে খোঁজ-খবর রাখলে আপনি নিশ্চয়ই জেনে থাকবেন যে, ডার্ক ওয়েবের ড্রাগ মার্কেট Silk Road যখন বন্ধ হয়, তার পরপরেই ইন্টারনেটে একটি ছবি ছড়িয়ে পরে যাতে ডিপ ওয়েব ও ডার্ক ওয়েব ছাড়াও ওয়েবের আরও অনেক level আছে বলে প্রচার করা হয়। সেই প্রচারণা অনুযায়ী সাধারন ওয়েবের ওয়েবসাইটগুলো হচ্ছে level 0 বা, common ওয়েব। এছাড়াও Bergie Web, Charter Web, Closed Shell System সহ আরও অনেক ওয়েব আছে বলে প্রচার করা হয়। পরবর্তীতে এগুলোকে কেউ গুজব বলেছেন আবার, কেউ কেউ এসবের ভিন্ন সংজ্ঞা দেখিয়ে বাস্তব implementation (নেটওয়ার্ক implementation) করে দেখানোর চেষ্টা করেছে। তবে, আপনাকে সবসময় যেই কথা মাথায় রাখতে হবে তা হচ্ছে- মানুষের আবেগ কিংবা কৌতূহলকে কাজে লাগিয়ে তাকে ফাঁদে ফেলা যায়। তাই, সবসময় অনলাইন কমিউনিটি গুলোর সাথে আপডেট থাকবেন। যেকোন নতুন বিষয় সামনে আসলে প্রথমে অভিজ্ঞদের মতামত জানুন। আপনি নিজেই যদি অভিজ্ঞ হয়ে থাকেন সেক্ষেত্রেও অভিজ্ঞদের সাথে পরামর্শ করে নিন।

TOR এবং VPN

আপনি চাইলে TOR এবং VPN একসাথে ব্যাবহার করতে পারবেন। TOR এবং VPN একসাথে ব্যাবহার করার পদ্ধতি হতে পারে ২টি যথা-

- প্রথমে TOR ব্রাউজার দিয়ে TOR নেটওয়ার্কে connect হয়ে তারপর VPN চালু করা।
- প্রথমে VPN চালু করে তারপর TOR ব্রাউজার দিয়ে TOR নেটওয়ার্কে connect হওয়া।

প্রথমে TOR ব্রাউজার দিয়ে TOR নেটওয়ার্কে connect হয়ে তারপর VPN চালু করলে আপনার ইন্টারনেট সার্ভিস প্রোভাইডার (ISP) বুঝতে পারবে যে, আপনি TOR ব্রাউজার ব্যাবহার করছেন। কিন্তু, এই পদ্ধতি অবলম্বন করলে যেই উপকার হবে তা হচ্ছে- TOR নেটওয়ার্কের ৩য় কম্পিউটারের মাধ্যমে ওয়েবসাইটে প্রবেশ করার সময় data encrypted না থাকলেও VPN ব্যাবহার করার ফলে একটি encrypted tunnel তৈরি হবে।

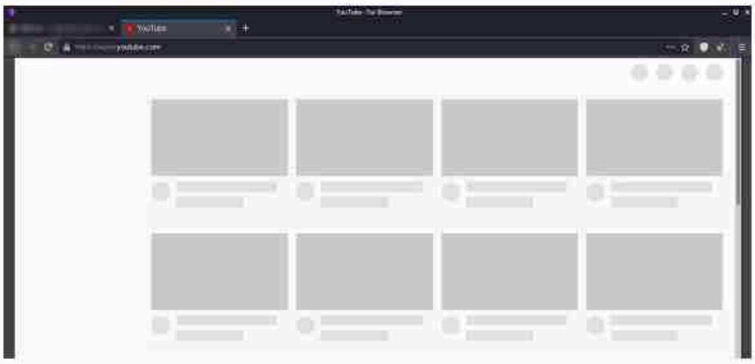
আবার, প্রথমে VPN চালু করে তারপর TOR ব্রাউজার দিয়ে TOR নেটওয়ার্কে connect হওয়ার উপকারিতা হচ্ছে যে, ISP বুঝতে পারবে না- আপনি TOR ব্যাবহার করছেন। তবে, এক্ষেত্রে TOR নেটওয়ার্কের ৩য় কম্পিউটারের মাধ্যমে ওয়েবসাইটে প্রবেশ করার সময় data encrypted থাকবে না। যেহেতু, ডার্ক ওয়েবের ওয়েবসাইটগুলোতে https ব্যাবহার না করে http ব্যাবহার করা হয়ে থাকে তাই, কিছুটা শঙ্কা থেকেই যায়।

Red Room | রেড রুম

ডার্ক ওয়েবে রহস্যে মোড়ানো যাকিছু আছে, তার মধ্যে অন্যতম হচ্ছে- রেড রুম। রেড রুমে ক্যামেরার সামনে একজনকে অত্যাচার করতে করতে মেরে ফেলা হয়। রেড রুমে অত্যাচার করা দেখতে চাইলে টাকা দিয়ে নির্দিষ্ট সময়ের আগেই membership কিনতে হয়। যদিও, অত্যাচার করার live ভিডিওতে comment করে নিজের কথামতো অত্যাচার করাতে চাইলে বেশি টাকা দিয়ে membership কিনতে হয়।

সতর্কতা

রেড রুমের নামে ধোঁকা খাবেন না। আজ পর্যন্ত রেড রুমের বাস্তব প্রমাণ পাওয়া যায় নি। বরং, রেড রুমের কথা বলে মানুষের থেকে টাকা নিয়ে প্রতারণা করা হয় বলেই অভিযোগ পাওয়া যায়। তাছাড়া, আপনি জানেন- TOR ব্রাউজারে কোনকিছু load হতে দেরি হয়। নিচের ছবিতে দেখতে পাচ্ছেন- ৩০ মিনিট ধরে অপেক্ষা করার পরেও Youtube এখনও load হচ্ছে।

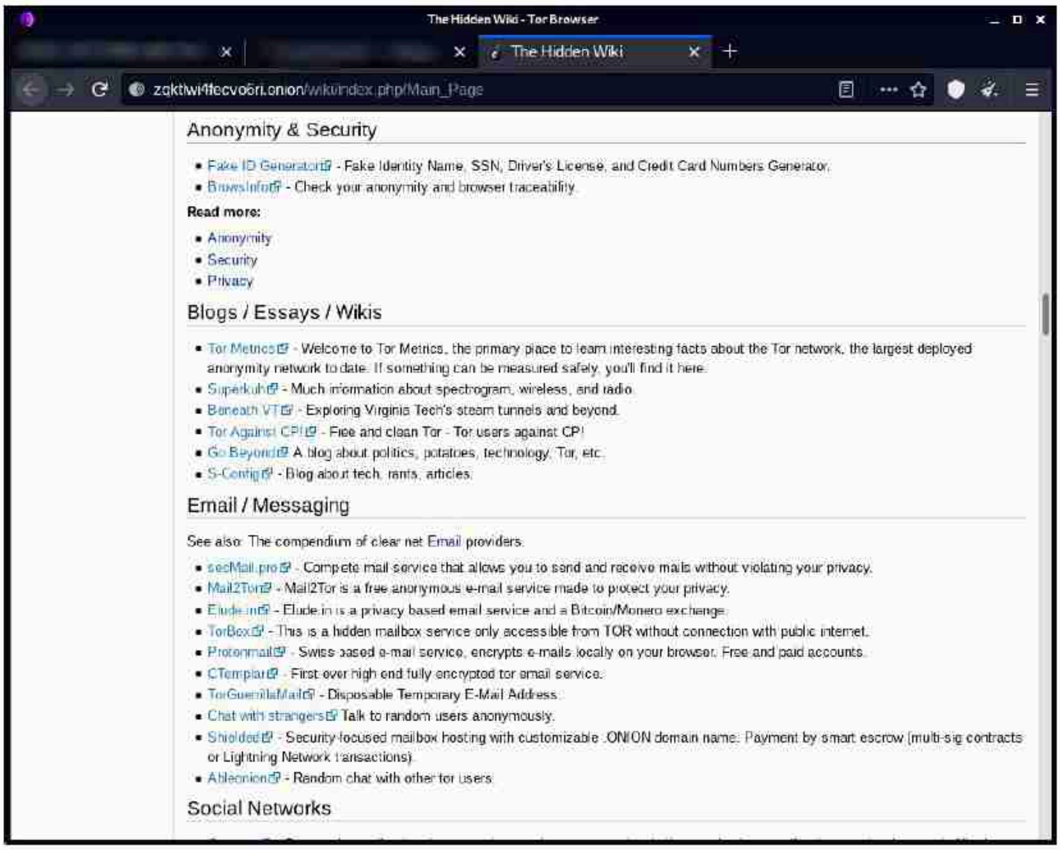


তাই, বুঝতেই পারছেন- ডার্ক ওয়েবে রেড রুমের live ভিডিও দেখা সম্ভবই না।

The Hidden Wiki

ডার্ক ওয়েবের অসংখ্য ওয়েবসাইটের লিংক রয়েছে The Hidden Wiki সাইটে।

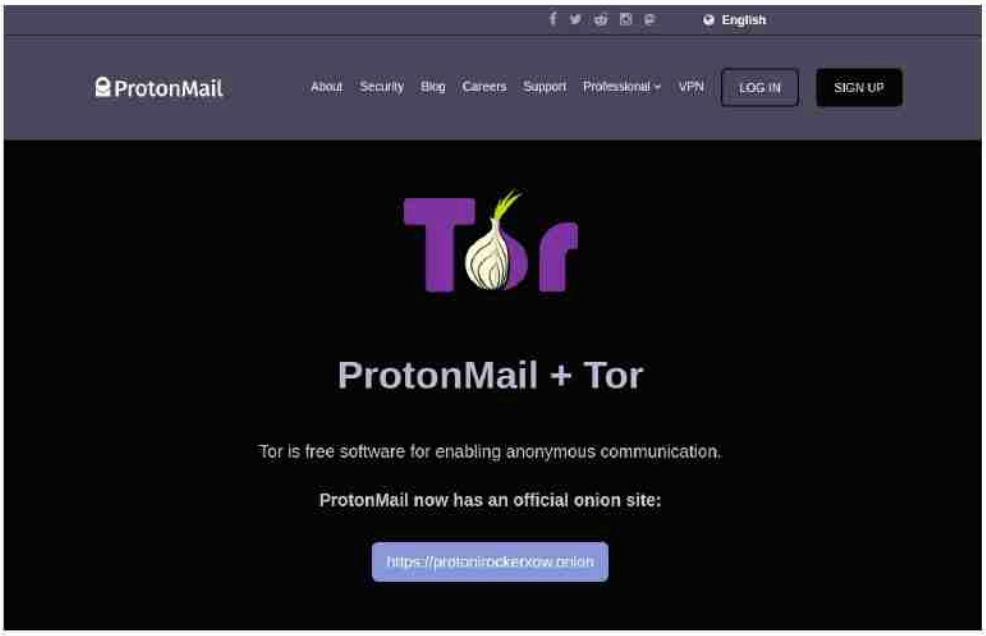
লিংকঃ zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page



উপরের ছবিতে The Hidden Wiki -র কিছু অংশ দেখতে পাচ্ছেন। এখানে বিষয়ভিত্তিক সাজিয়ে বিভিন্ন ওয়েবসাইটের লিংক দেওয়া আছে।

ProtonMail

ডার্ক ওয়েব ব্যাবহার করার মূল লক্ষ্য হচ্ছে- পরিচয় গোপন রাখা। আর, যদি ওয়েব ডার্ক ওয়েবেরই কোন বিশ্বস্ত ইমেইল সার্ভিস ব্যাবহার করা যায় তাহলে প্রাইভেসি অনেক গুণ বৃদ্ধি পায়। এক্ষেত্রে, ডার্ক ওয়েবের মেইল সার্ভিস ProtonMail হতে পারে আপনার প্রথম পছন্দ। এজন্য প্রথমে এই লিংকে ক্লিক করে ProtonMail এর অফিসিয়াল ওয়েবসাইটে প্রবেশ করুন।

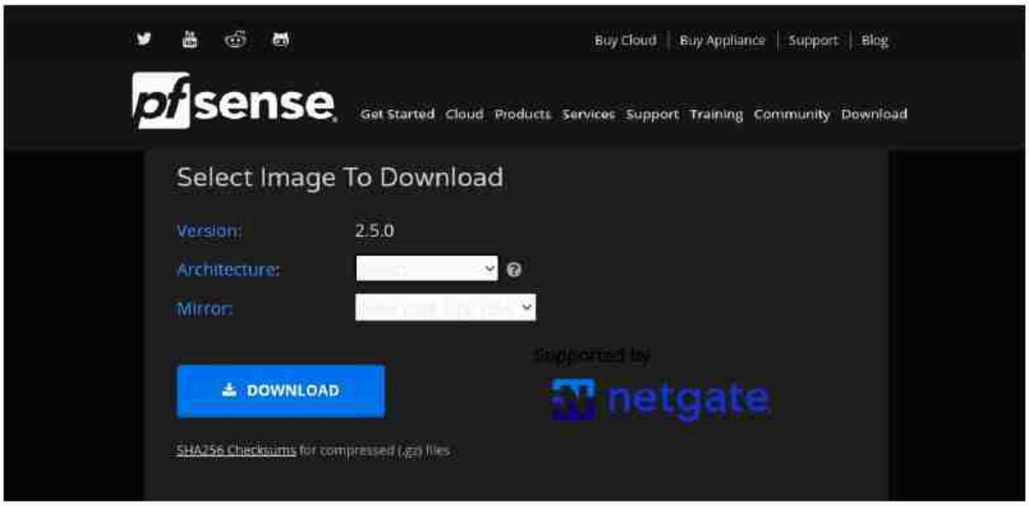


এরপর উপরের ছবির মতো ওয়েব পেইজটি আসলে সেখানে দেওয়া অফিসিয়াল .onion লিংকটি copy করে TOR ব্রাউজারে সার্চ করুন। এরপর sign up করার অপশন আসলে sign up করুন।

নিজেই নিজের **Tor** ভার্চুয়াল নেটওয়ার্ক তৈরি করুন

আপনি হয়তো ভার্চুয়াল মেশিনে Tor ব্যাবহার করেন। কিন্তু, আপনি চাইলে এমন একটি ভার্চুয়াল নেটওয়ার্ক তৈরি করতে পারবেন- যার মাধ্যমে ইন্টারনেটে আপনার সকল কাজই TOR নেটওয়ার্কের মাধ্যমে হবে।

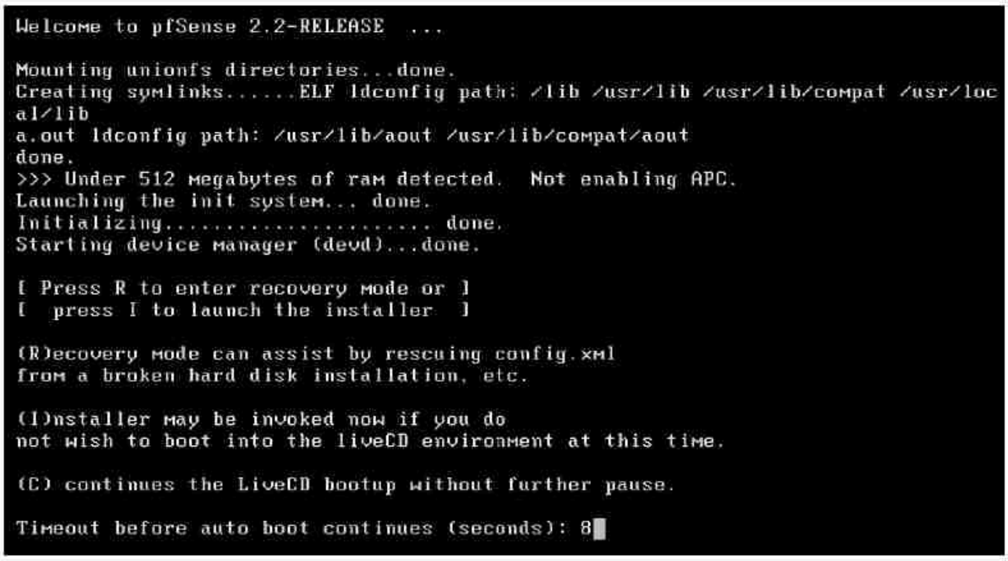
এটি setup করার জন্য আমরা pfSense রাউটার ব্যাবহার করবো। তাই, শুরুতেই pfSense এর অফিসিয়াল ওয়েবসাইটের এই লিংকে যান। তখন নিচের ছবির মতো ওয়েব পেইজটি আসবে। এখন আপনার কম্পিউটারের মাইক্রো প্রসেসর 64 bit হলে Architecture হিসেবে **AMD64 (64-bit)** অপশনটি select করুন এবং Installer হিসেবে **USB Memstick** অপশনটি select করুন।



আপনার যদি VirtualBox ডাউনলোড করা না থাকে তাহলে, এই লিংকে যান। এরপর আপনার কম্পিউটারের অপারেটিং সিস্টেম অনুযায়ী ডাউনলোড করে নিন। এরপর ভার্চুয়াল বক্সে **new** এ ক্লিক করে pfSense রাউটারের ISO file সিলেক্ট করুন। এক্ষেত্রে Network Settings টি অবশ্যই **NAT** করে রাখবেন। তবে, আপনি যদি আগে কখনো VirtualBox ব্যাবহার না করে থাকেন তাহলে, ভার্চুয়াল বক্সে একটি অপারেটিং সিস্টেম কিভাবে setup করতে হয়, সেই বিষয়ে অনলাইনে ভিডিও দেখে নিন।

এখন আপনি প্রস্তত। শুরুতেই ভার্চুয়াল বক্সে pfSense কে start করুন। যখন নিচের ছবির মতো দেখতে পারবেন তখন 1 চেপে Enter প্রেস করুন।

এরপর নিচের ছবির মতো আসলে ১০ সেকেন্ডের মধ্যে "I" প্রেস করুন (চাপুন)।



এরপর “Quick/Easy Install” এর আগে “Accept these Settings” -এ ক্লিক করে Ok করুন। এরপর কার্নেল install করতে বললে Standard Kernel সিলেক্ট করুন। এরপর সব হয়ে যাওয়ার পর reboot করার অনুমতি চাইলে reboot করুন।

আপনি যদি সবকিছু সঠিকভাবে করে থাকেন তাহলে, নিচের ছবির মতো দেখতে পারবেন।

এখন ভার্চুয়াল বক্সে ভার্চুয়াল মেশিন হিসেবে একটি অপারেটিং সিস্টেম start করুন। এরপর সেই ভার্চুয়াল মেশিনটি যেনো pfSense রাউটারের LAN এর সাথে connect হতে পারে সেজন্য virtual network adapter কে set করুন।

এরপর একটি ওয়েব ব্রাউজার open করে pfSense রাউটারের LAN আইপি এড্রেসে যান। আইপি এড্রেসটি pfSense ভার্চুয়াল মেশিনে লেখা থাকবে, সেখান থেকে দেখে নিবেন। যেমন উপরের ছবিতে দেখতে পাচ্ছেন- আমার LAN আইপি এড্রেস হিসেবে **192.168.1.1** লেখা আছে। তাই, ভার্চুয়াল মেশিনের ওয়েব ব্রাউজারে আমি **192.168.1.1** লিখে সার্চ দিবো।

এরপর login পেইজ আসলে username:admin এবং password:pfsense লিখে login করুন। এরপর Services এ গিয়ে DNS Resolver এ যান। সেখানে দেখতে পারবেন- DNS Resolver অপশনটি চালু করা আছে। কিন্তু, আমরা DNS resolver হিসেবে TOR ব্যাবহার করবো। যাতে করে আমাদের সকল অনলাইন কাজ TOR দিয়ে হয়। তাই, Enable DNS Resolver অপশনটি uncheck করে দিন।

এখন পুনরায় pfSense এর ভার্চুয়াল মেশিনে যান। সেখানে গেলে উপরের ছবির মতো দেখতে পারবেন। এখন আমরা TOR ইন্সটল করার জন্য 8 প্রেস করবো।

এখন পর্যায়ক্রমে নিচের দুইটি command লিখে Enter প্রেস করুন।

- pkg install tor
- rm -rf /usr/local/etc/tor/torrc

এখন /usr/local/etc/tor/torrc ফাইল open করে নিচের অংশটুকু লিখে save করুন।

```
DNSPort 53
DNSListenAddress YOUR_PFSENSE_LAN_IP_HERE
VirtualAddrNetworkIPv4 10.192.0.0/11
AutomapHostsOnResolve 1
RunAsDaemon 1
TransPort 9040
```

এরপর পর্যায়ক্রমে নিচের command গুলো লিখে Enter চাপুন।

- touch /usr/local/etc/rc.d/tor.sh
- cd /usr/local/etc/rc.d/
- echo “/usr/local/bin/tor” >> tor.sh && chmod +x tor.sh
- /usr/local/bin/tor

এখন আপনি Firewall সেটআপ করে নিন। তাহলেই আপনার pfSense রাউটারটি ব্যাবহার করতে পারবেন এবং আপনার দ্বিতীয় ভার্চুয়াল মেশিন দিয়ে ইন্টারনেটে যাকিছুই করবেন, সেগুলো TOR নেটওয়ার্ক ব্যাবহার করে কাজ করবে।

ডার্ক ওয়েবে তথ্য সংগ্রহ

টাকার মূল্য নিশ্চয়ই জানেন। ডার্ক ওয়েবেও টাকার ছড়াছড়ি। আপনি যদি ডার্ক ওয়েবে গোপন ও মূল্যবান তথ্য সংগ্রহ করতে চান তাহলে অবশ্যই পারবেন। এমনকি, সাধারন ইন্টারনেটে যেই তথ্য সংগ্রহ করতে পারবেন না, ডার্ক ওয়েবে সেই তথ্য পাবেন। কিন্তু, এখানে একটি 'কিন্তু' আছে। আর, তা হচ্ছে- ডার্ক ওয়েবে যেসকল forrum থেকে ভালো তথ্য পাওয়া যায়, সেগুলোর প্রায় সবগুলোতে join করতেই টাকা লাগে। যদিও, ডার্ক ওয়েবে search দিয়ে ফ্রিতেও অনেক তথ্য সংগ্রহ করা সম্ভব। এমনকি ডার্ক ওয়েবে ফ্রিতেও অনেক দরকারি তথ্য সংগ্রহ করা যায়।

যেমন ধরুন, Illuminati সম্পর্কে বলা হয় যে, তাদের কাছে HAARP নামের একটি মেশিন আছে, যেটি দিয়ে তারা ঘুর্ণিঝড় তৈরি করতে পারে। এখন, এই বিষয়ে বিস্তারিত জানতে সাধারন ইন্টারনেটে ঘাটাঘাটি করে অনেক তথ্য পাবেন। কিন্তু, ডার্ক ওয়েবে যদি এই বিষয়ে জানতে চান তাহলে প্রচুর তথ্য না পেলেও অনেক মূল্যবান তথ্য পেতে পারেন। ডার্ক ওয়েবে তথ্য সংগ্রহের জন্য নিচের পদক্ষেপসমূহ গ্রহন করতে পারেন-

- ডার্ক ওয়েবের সার্চ ইঞ্জিন ব্যাবহার করে সার্চ করা।
- ডার্ক ওয়েবের social media তে যোগ্য কারও কাছে জানতে চাওয়া।

ডার্ক ওয়েবে আপনি যদি কাউকে প্রশ্ন করেন তাহলে তিনি সত্য তথ্য প্রকাশ করতে ভয় পাবেন না; কারন, ডার্ক ওয়েবে পরিচয় গোপন থাকে। যদিও, ডার্ক ওয়েবে এমন অনেক খারাপ মানুষও থাকে, যাদের কাছে কিছু জানতে চাইলে ইচ্ছা করেই ভুল তথ্য দিবে। এজন্যেই বলে থাকি, অনলাইনে নিজেকে ব্যতীত নিজের ছায়াকেও বিশ্বাস করতে নেই।

তবে, ডার্ক ওয়েবে কাউকে কোন প্রশ্ন না করাই যদি আপনি ভালো মনে করেন তাহলে, তাই করুন।

mortis.com এবং Cthulhu.net

যদিও mortis.com ওয়েবসাইটটি ডার্ক ওয়েবের না, তারপরও রহস্যময় ওয়েবসাইট আসলে কি ধরনের হতে পারে- সেই সম্বন্ধে ধারনা দেওয়ার জন্যই mortis.com নিয়ে আলোচনা করা হচ্ছে। যদিও এই রহস্যময় ওয়েবসাইটটি এখন আর নেই।

সর্বপ্রথম একজন 4chan ইউজার এই ওয়েবসাইটটি খুঁজে পেয়েছিলেন। এই ওয়েবসাইটটির শুধুমাত্র একটি page ছিলো যেখানে login করতে হতো অথচ, এটি কয়েক terabyte পরিমাণ তথ্য host করতো! সেই ওয়েবসাইটের মালিককে নির্দিষ্টভাবে চেনা যায় নি। এমনকি সেই ওয়েবসাইটটি কেন বন্ধ করা হলো, সেটাও অজানা।

Cthulhu.net নামের আরেকটি ওয়েবসাইট ছিলো, যার শুধু একটি page ছিলো। সেখানে কালো background এর ওপর সাদা রঙে লেখা ছিলো- “dead but dreaming”।

ডার্ক ওয়েব নিয়ে কিছু প্রশ্ন-উত্তর

প্রশ্নঃ ০১

একটি দেশের নাগরিক ফেসবুকে খারাপ কাজ করলে অনেক সময় সেই দেশের সরকার তার ফেসবুক আইডির তথ্য চেয়ে ফেসবুকের কাছে আবেদন করে। এমনকি কোন দেশের সরকারকে ফেসবুক কি পরিমান একাউন্টের তথ্য দিচ্ছে, সেই বিষয়ে ফেসবুক নিজেই এই লিংকে তথ্য প্রকাশ করে। কিন্তু, ডার্ক ওয়েবের সামাজিক যোগাযোগ মাধ্যমগুলোতে অপরাধীরা তো সবার সামনেই তাদের অপরাধ সম্বন্ধে আলোচনা করে। এই যেমন- সম্প্রতি Cyberpunk 2077 এর source code হ্যাক হয়ে গেলো; হ্যাকাররা ডার্ক ওয়েবের একটি ফোরামে (forrum) সেটা বিক্রিও করে দিলো। তারপরও প্রশাসন তাদেরকে ধরতে পারে না কেনো?

উত্তরঃ এটা ঠিক যে, ডার্ক ওয়েবে অপরাধীরা বিভিন্ন ফোরামে (forrum) তাদের অপরাধ নিয়ে আলোচনা করে যেমনঃ

- হ্যাক করা একাউন্ট বিক্রি করা,
- বড় বড় কোম্পানির পণ্যের source code হ্যাক করে নিলামে তোলা ইত্যাদি।

কিন্তু, ডার্ক ওয়েবে তারা যাকিছুই করছে, সেগুলো তাদের কম্পিউটার দিয়ে সরাসরি connect হয়ে করছে না। বরং, TOR ব্যাবহার করায় তাদের কম্পিউটার ও ওয়েবসাইটের মাঝে TOR নেটওয়ার্কের ৩ টি কম্পিউটার connected থাকে। ফলে, তাদের প্রকৃত পরিচয় পাওয়া সম্ভব হয় না। আর, তারা যেই ডার্ক ওয়েবের সামাজিক যোগাযোগ মাধ্যম বা, ফোরামে এসব অপরাধ করছে সেসব ফোরামের মালিকের থেকে অপরাধীদের একাউন্টের তথ্য সংগ্রহ করলেও কোন ফায়দা নেই। কারন, ডার্ক ওয়েবে কেউই নিজের আসল পরিচয় দিয়ে একাউন্ট খোলে না। ফলে, অপরাধীদের আসল পরিচয় না পাওয়ায় প্রশাসন তাদেরকে ধরতেও পারে না।

তবে হ্যাঁ, কয়েক বছরের চেষ্টায় মাঝে মাঝে কিছু অপরাধীকে ধরেও ফেলে প্রশাসন। আবার, অনেক সময় অপরাধী নিজে থেকেই অপরাধ করা বন্ধ করে। যেমনঃ ডার্ক ওয়েবের JokerStash মার্কেটে চুরি হওয়া ক্রেডিট কার্ড বিক্রি করা হতো। কিন্তু, ক্রিপ্টোকারেন্সিতে প্রায় ১ বিলিয়ন ডলার আয় করার পর সেই মার্কেটের মালিক নিজে থেকেই মার্কেটটি বন্ধ করে দিচ্ছে। যদিও, এই ধরনের ঘটনা সচরাচর ঘটে না।

প্রশ্নঃ ০২

ডার্ক ওয়েবে খারাপ কাজ করার কারনেই নাকি এই ওয়েবকে ডার্ক (dark) ওয়েব বলা হয়। অথচ, আপনি বলেন- ডার্ক ওয়েব নিরাপদ। বিষয়টা একটু ব্যাখ্যা করবেন কি?

উত্তরঃ ডার্ক ওয়েবে খারাপ কাজ করার কারনেই একে ডার্ক ওয়েব বলা হয়- এই কথাটাই ভুল। বরং, অন্ধকারে যেরকম কাউকে চেনা যায় না, ডার্ক ওয়েবেও কাউকে চেনা যায় না। সবার পরিচয় গোপন থাকে। সেই কারনেই একে ডার্ক (dark) ওয়েব বলা হয়।

মূলত, ডিপ ওয়েব এবং ডার্ক ওয়েবের নামের মধ্যেই এদের পরিচয় পাওয়া যায়। যেমন- ডিপ (deep) ওয়েব অর্থ গভীর ওয়েব। ফলে, সাধারন ইন্টারনেটের তুলনায় ডিপ ওয়েব এতোটাই গভীরে অবস্থিত যে, সেখানে সাধারন ওয়েবের মতো সহজেই যাওয়া যায় না। কিন্তু, একজন ব্যক্তি যখন সেখানে পৌঁছে যাবেন, তখন সবকিছু আলোকিত ও পরিষ্কার দেখতে পাবেন।

অপরদিকে, ডার্ক (dark) ওয়েব এমন এক ওয়েব- যা শুধু গভীরেই অবস্থিত না বরং, এর সম্পূর্ন অংশ অন্ধকারে ঢাকা। এখানে সবার পরিচয় গোপন থাকে। তাই, এখানে প্রাইভেসি সুরক্ষিত থাকে। ফলে, নিরাপত্তা বেশি। প্রাইভেসি সুরক্ষিত থাকার কারনেই সারা বিশ্বের বিভিন্ন শ্রেণী-পেশার মানুষ Tor ব্যাবহার করে যেমন- সাংবাদিক, আইন প্রয়োগকারী কর্মকর্তা সহ আরও অনেকে।

প্রশ্নঃ ০৩

VPN ছাড়া TOR ব্যাবহার করা কতোটা নিরাপদ?

উত্তরঃ VPN সিস্টেম যদিও অনলাইনে নিরাপত্তা দেওয়ার জন্য তৈরি করা হয় নি তবুও, এখন VPN এর ব্যাবসায়িক প্রচারণাগুলোতে অনলাইন নিরাপত্তার বিষয়টাই মুখ্য হিসেবে প্রচার করা হয়। সাইবার সিকিউরিটি নিয়ে সচেতন অনেক ব্যক্তি VPN ব্যাবহার করা থেকে মানুষকে নিরুৎসাহিত করেন (এক্ষেত্রে রাষ্ট্রীয় কিংবা, ব্যাবসায়িক কারন থাকলে তা একান্তই তাদের ব্যক্তিগত বিষয়)। আবার, সিকিউরিটি নিয়ে একদম অনভিজ্ঞ ব্যক্তিরা VPN ব্যাবহার করেই নিজেকে খারাপ হ্যাকার থেকে নিরাপদ মনে করেন। কিন্তু, এই বিপরীতধর্মী দৃষ্টিভঙ্গি এক প্রান্তিকতার সৃষ্টি করেছে। আর, এই প্রান্তিকতার মাঝখানেই রয়েছে সঠিক দৃষ্টিভঙ্গি। আর, তা হচ্ছে-

আমরা VPN ব্যাবহার করবো এবং এটা অবশ্যই

আমাদের প্রাইভেসি রক্ষায় যথেষ্ট ভূমিকা রাখে।

তবে, VPN এমন কোন কাজ করে না যেটি

আমাদেরকে হ্যাকারের attack থেকে রক্ষা করবে।

অর্থাৎ, VPN আপনার পরিচয় কিছুটা গোপন করার পরেও হ্যাকার আপনাকে আক্রমণ করতে পারে। আবার, মনে করুন- আপনি ডার্ক ওয়েবে একটি mail একাউন্ট খুললেন; যাতে করে সেই একাউন্ট ব্যাবহার করে গোপনীয়তার সাথে মানুষের কাছে মেইল পাঠাতে পারেন। এই কাজ করতে আপনার জন্য শুধুমাত্র TOR ব্রাউজারই যথেষ্ট। কিন্তু, সেই মেইল এড্রেস যদি আপনি ফেসবুকে সবাইকে জানিয়ে দেন তাহলে তো VPN সহ TOR ব্যাবহার করেও কোন লাভ নেই। কারন, এটা যে আপনারই মেইল এড্রেস, তা সবাই জেনে গেছে।

তাই, VPN সহ TOR ব্যাবহার করলে কিছুটা উপকার অবশ্যই হবে। কিন্তু, আপনার ব্যাবহার বিধির ভিত্তিতেই আপনার নিরাপত্তা অন্যের তুলনায় কম বা বেশি হবে।

প্রশ্নঃ ০৪

অনেকে বলে- “Tor ব্রাউজার ব্যাবহার করা অনিরাপদ।" তাই, ভার্চুয়াল মেশিন ছাড়া মূল কম্পিউটারে TOR ব্রাউজার ব্যাবহার করতে তারা নিষেধ করে থাকে। এটা কি সঠিক?

উত্তরঃ যারা অনলাইন জগতে একদমই নতুন এবং সিকিউরিটি ও প্রাইভেসি নিয়ে যাদের প্রাথমিক জ্ঞান নেই, তারা শুধু ডার্ক ওয়েব না বরং, সাধারন ইন্টারনেটেও ক্ষতির সম্মুখীন হবেন। এক্ষেত্রে শুধু শুধু Tor ব্রাউজারকে দোষ দেওয়া ভুল। তাছাড়া, Brave ব্রাউজারেও তো ডার্ক ওয়েবে প্রবেশ করার জন্য Tor mode নামের একটি feature আছে। তাহলে কি Brave ব্রাউজার ব্যাবহার করতেও তারা নিষেধ করবে? যেখানে Tor নেটওয়ার্কের খরচ চালাতে আমেরিকান সরকার কখনো কখনো শতভাগ খরচ বহন করছে, সেই ওয়েব ব্রাউজার ক্ষতি করবে? আমাকে বলুন, Tor ব্রাউজার কার কি ক্ষতি করেছে?

দেখুন- privacy নিয়ে যারা সচেতন, তাদের অনেকে সাধারন ওয়েব ব্রাউজার হিসেবেও Epic Browser, SRWare Iron, Comodo Dragon ইত্যাদি ওয়েব ব্রাউজার ব্যাবহার করে থাকেন। অথচ, Tor ব্রাউজার তো এসবের থেকে অনেক বেশি নিরাপদ। কারন, Tor ব্রাউজার Tor নেটওয়ার্কের সাথে connect হয়ে কাজ করে।

তাই, যারা খুব বেশি জ্ঞান রাখেন না তাদের জন্য ডার্ক ওয়েবের ওয়েবসাইটে প্রবেশ করাই অনুচিত; সেটা মূল কম্পিউটারের Tor ব্রাউজার দিয়েই হোক কিংবা, ভার্চুয়াল মেশিনের Tor ব্রাউজার দিয়েই হোক। কিন্তু, Tor ব্রাউজার নিজে থেকে কোন ক্ষতি করবে না; সেটা মূল কম্পিউটারের Tor ব্রাউজারই হোক কিংবা, ভার্চুয়াল মেশিনের Tor ব্রাউজারই হোক। এমনকি অনলাইন নিরাপত্তার জন্য যেই Qubes অপারেটিং সিস্টেম ব্যাবহার করা হয়, সেই অপারেটিং সিস্টেমের সকল আপডেট Tor ব্যাবহার করেই download করা হয়।

কিছু দিকনির্দেশনা

অনেক সময় এমন হতে পারে যে, আপনি যেখানে আছেন সেখানে Tor ব্রাউজার block করে দেওয়া আছে। সেক্ষেত্রে আপনি Tor ব্রাউজারের bridge ব্যাবহার করতে পারেন। যদিও, যাদের দেশে Tor ব্রাউজার ব্যাবহার করা নিষিদ্ধ, তারা Tor ব্রাউজার ব্যাবহার করলে অপরাধ হবে। তাই, তাদের দেশের আইন মেনে চলা উচিত।

ডার্ক ওয়েবে কোথাও sign up করার প্রয়োজন হলে আপনার আসল পরিচয় কখনোই দিবেন না। সেক্ষেত্রে প্রথমে VPN ব্যাবহার করে temp-mail.org/en/ থেকে একটি temporary mail নিন। এরপর সেই মেইল এড্রেস দিয়ে sign up করুন।

ডার্ক ওয়েবের ওয়েবসাইটগুলোর ads এ ক্লিক না করাই আপনার জন্য উত্তম।

পরিশেষে কিছু কথা

ডার্ক ওয়েব বলতে সাধারনত Tor নেটওয়ার্কের ওয়েবসাইটগুলোকে বোঝানো হয়। এই ডার্ক ওয়েব প্রতিষ্ঠিত আছে ডার্কনেটের ওপর। ডার্কনেটের ওপর আরও অনেক নেটওয়ার্ক প্রতিষ্ঠিত আছে যেমনঃ I2P, Freenet ইত্যাদি। এছাড়াও আছে GNUnet, Zeronet, dn42 ইত্যাদি।

এই বইটিতে ডার্ক ওয়েব এর ওপর তত্ত্ববহুল আলোচনার পাশাপাশি practical আলোচনার ওপর গুরুত্ব দেওয়া হয়েছে।

প্রায়ই অনেককে দেখা যায়- ডার্ক ওয়েবের ওপর বাংলা ভাষায় বিস্তারিত জানার চেষ্টা করেন। কিন্তু, বাংলায় সেরকম কোন রিসোর্স তারা পান না। এখন আশা করি- আমার এই বইটি তাদের উপকারে আসবে।

ভালো কাজ করে অন্তরে তৃপ্তি পাওয়া যায়। তাই, মানুষের কল্যানে সঠিক দিক-নির্দেশনা দেওয়ার জন্য বিনামূল্যে প্রচার করতে এই বইটি লেখা হয়েছে। একজন ব্যক্তিও যদি বইটি পড়ে উপকৃত হন তাহলে নিজেকে সার্থক মনে করবো।

এই বইয়ের যাবতীয় সকল তথ্য-ই অনলাইন থেকে সংগৃহীত। অতএব এর থেকে ভাল আইডিয়া জানা থাকলে আপনি এড়িয়ে যেতে পারেন।

কৃতজ্ঞতা : আবদুল্লাহ আল মামুন