Sumário

1.Apresentação

Formações

Criptografia 0x65 Desec Security
Introdução ao Hacking e Pentest Solyd
Linux Módulo 0 Estodonauta
Linux Módulo 1 Estodonauta
Linux Módulo 2 Estodonauta
Linux Módulo 3 Estodonauta
Linux Módulo 4 Estodonauta
Linux Módulo 5 Estodonauta
Redes Módulo 0 Estudonauta
Redes Módulo 1 Estudonauta
Redes Módulo 2 Estudonauta
Redes Módulo 3 Estudonauta
Redes Módulo 4 Estudonauta
Redes Módulo 5 Estudonauta
Mysql Estudonauta
Mysql Digital Innovation One
Python Básico Solyd
Python Segurança da informação Digital Innovation One
Python 1 Estudonauta
Python 2 Estudonauta
Python 3 Estudonauta

Github: https://github.com/shadowgh0s7

2.Introdução

O que é privacidade

Privacidade é o direito a reserva de informações pessoais e da própria vida pessoal. Na internet significa não revelar suas atividades a terceiros.

Aqui vai um exemplo, privacidade é como se fosse um banheiro, você pode até saber quem está dentro, porém não sabe oque a pessoa está fazendo lá.

O que é Anonimato

Anonimato é a qualidade ou condição daquilo que é anonimo, sem nome ou assinatura, na internet significa manter a identidade escondida de terceiros

Ainda no exemplo do banheiro, com o anonimato você não sabe quem está dentro do banheiro.

Em outras palavras tendo anonimato e privacidade, você não sabe quem está dentro do banheiro e muito menos sabe oque o mesmo está fazendo dentro.

Quem nos observa

Provedores de internet (ISP)
Administrador da sua rede
Sistemas operacionais
Websites de motores de busca (Google, Bing e etc)
Apps
Governos
Hackers

O que eles podem ver e fazer

- Sites e mídias sociais que você visita e para quem você envia e-mails;
- Detalhes sobre suas informações financeiras e de sua família;
- Salvar seus dados por meses ou anos, dependendo da legislação local;

- Sua localização, informações da conta, endereço de e-mail;
- Seu histórico de pesquisa (resultados de pesquisa);
- Pedir ao seu provedor seus dados de navegação, limitar a liberdade de expressão.

Por que se preocupar com sua privacidade na internet ?

- Coleta de dados sem sua consciêntização
- Comércio de dados sem sua consciêntização
- Intrusão desnecessária (Ad, Trackers, Fingerprint e etc)

Noticia sobre Coleta de dados:

Mensagens do WhatsApp podem ser lidas por funcionários, afirma investigação jornalística: segundo o grupo ProPublica, revisores utilizam um software especial do Facebook para obter acesso a conteúdo privado quando mensagens são relatadas como impróprias por usuários. O sistema encaminha cinco mensagens para revisão: a supostamente ofensiva junto de quatro anteriores, incluindo imagens e vídeos. Um sistema de inteligência artificial também verifica os dados não criptografados que o WhatsApp coleta de usuários como nomes, imagens de perfil, número de telefone, mensagem de status, nível de bateria do telefone, idioma, fuso horário, endereço IP, intensidade do sinal sem fio, contas relacionadas do Facebook e Instagram. Carl Woog, diretor de comunicações do WhatsApp, confirmou que o aplicativo possui equipes que revisam mensagens para identificar e remover conteúdo impróprio, mas que a empresa não considera esse trabalho como de moderação ativa.

Noticia tirada da newsletter do filipe deschamps.

Edward Snowden e a NSA e CIA :

Edward Joseph Snowden é um ex Administrador de sistemas da CIA e ex-contratato da NSA, Snowden ficou famoso após revelar documentos que comprovam ah existência de programas feitos para espionagem em massa no qual eram utilizados para vigilância constante em cima da população mundial. Um exemplo de programa que eles usavam é o Xkeyscore que permite que os engenheiros efetuem pesquisas em Big-datas que contêm e-mails, conversas

online (Whatsapp, facebook, messenger e etc) e buscas de internet de milhões de pessoas ao redor do mundo.

Existe um filme chamado Snowden: Herói ou Traidor, no qual conta com detalhes sobre a história e os acontecimentos que levaram a essa revelação, Edward Snowden atualmente mora na Rússia ainda refugiado e procurado pelas autoridades dos EUA e também utilizando de diversas ferramentas de privacidades no qual serão abordadas nesse PDF.

Mais espera-la, e a LGPD ???:

Sobre a LGPD ou Lei Geral de Proteção de Dados, é um conjunto de normas válidos pelo território brasileiro (Porém, essa mesma lei foi aprovada em diversos países, tais como: Argentina, Austrália, Canadá e etc...) no qual diz respeito a como empresas, pessoas e órgãos públicos devem guardar, proteger e usar informações coletadas dos usuários, um exemplo de norma é a obrigação de empresas divulgarem vazamentos de dados e invasões que venham a ocorrer e afetar os dados dos clientes. Outra norma considerável é o fato de ser totalmente transparente pelo lado da

empresa que coleta os dados, dizer o por quê coleta e como está sendo utilizado. Agora por quê a LGPD é ineficaz ?, primeiro que o direito a privacidade digital vai ser garantido pela constituição federal ???, BALELA total, as big techs não precisam dos dados pessoais (como nome, RG, CPF e etc… embora elas também não reclamem em ter os mesmos...), basta eles observarem como nós agimos e coletar os metadados (data e hora, pra quem você enviou, marca e modelo do aparelho e etc).

Você é criminoso ??

Criminoso é o governo que rouba a população sistematicamente utilizando os impostos, e se defendem usando essas ferramentas de privacidade, agora eu ou você que se importa com sua privacidade online que é o criminoso…. Fica a reflexão

MAIS É CLARO, Privacidade e anonimato são NEUTROS, ou seja pode ser usado, tanto para o mau, quanto para o bem, isso vária de usuário para usuário, sendo assim não culpe a privacidade por conta dos atos mal intencionados de uma pessoa que usa a privacidade como um meio de se esconder e se manter ileso no qual cometeu atos ilícitos.

O QUE VOCÊ VAI VER NESSE PDF

+ O que devemos esconder na internet
+ VPN
+ Trackers e Cookies
+ Anúncios e como Bloquea-los
+ HTTPS
+ Guia Anônima, vantagens e desvantagens
+ E-mails seguros e privados
+ Mensageiros instantâneos e privados
+ Armazenamento em Nuvem Seguros
+ Buscadores de privacidade
+ Browsers de privacidade

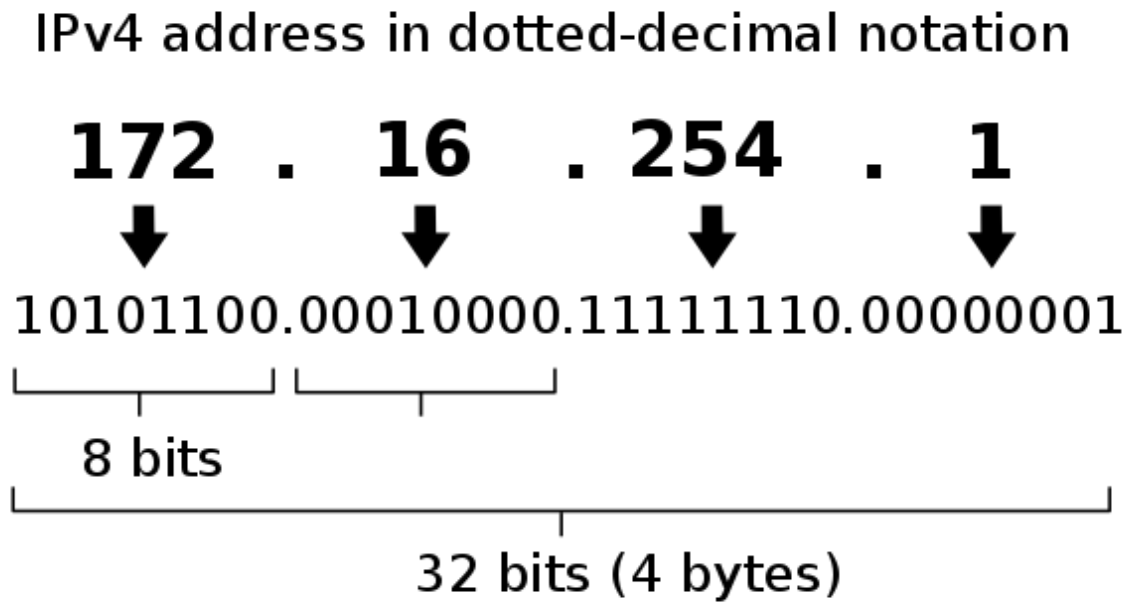
+ Alternativa ao googlemaps
+ Linux
+ Privacidade em smartphones e citação a um notebook privado
+ Privacidade em transações bancárias
+ Deep web, oque é, como funciona e redes da deep web
+ Rede Onion
+ Virtualização
+ Whonix
+ Tails

3.O que devemos esconder na internet ?

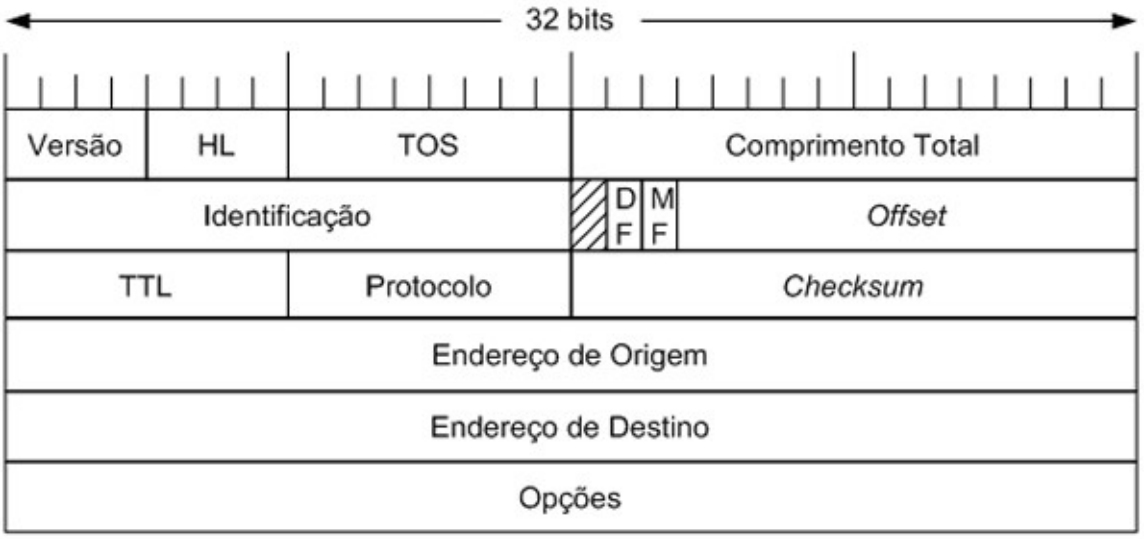
Na internet nós devemos esconder nosso endereço de IP

O IP é um protocolo de internet da camada de REDE do modelo OSI que serve para encapsular segmentos TCP, definir rotas de rede, endereçar uma rede e detectar possíveis erros.

Um endereço IP possui 32 bits ou 4 Bytes, utilizando números que vão de 0 a 255 que se baseiam por meio de octetos, por quê octetos ?, por quê se converter um endereço de IP para binário nota-se que cada número em binário possui 8 bits sendo assim não se deve passar de 255 se não passa a ter mais de 8 bits.

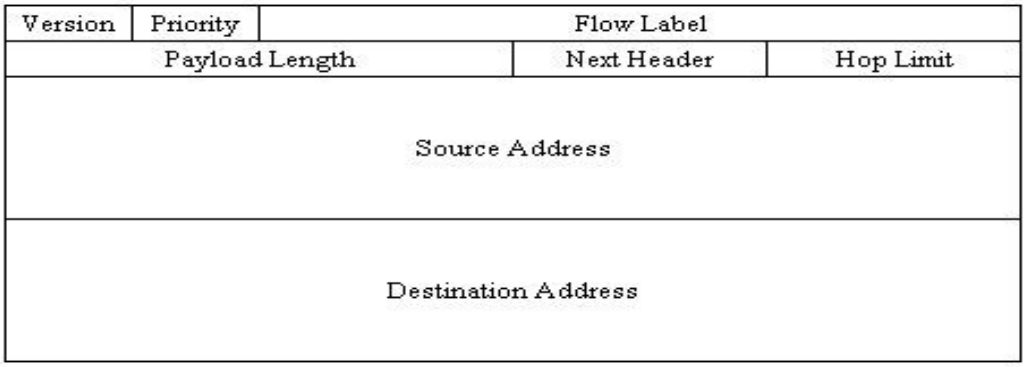


Um Pacote IP também possui um cabeçalho no qual serve para controle em uma rede, por exemplo, no cabeçalho possui um campo chamado flags no qual é usado para indicar se deve ou não fragmentar o pacote, não vou entrar em detalhes de cada um dos campos aqui nesse PDF, até por quê sai do escopo, porém caso tenha interesse, vou deixar links que explicam certinho como cada campo funciona.



4,29 bilhões de ips para o mundo todo e infelizmente as reservas de IPv4 já acabaram, porém já tem o IPv6 que está em processo de adoção, ele suporta 340 undecilhões de endereços, é um número confortável para a quantidade de aparelhos que existem no mundo, tão confortável que quando ele entrar em total vigor o NAT, as classes e o DHCP seram aposentados e cada interface de rede possuirá um IP próprio.

Cabeçalho IPv6:



Onde vejo meu endereço de IP público ?

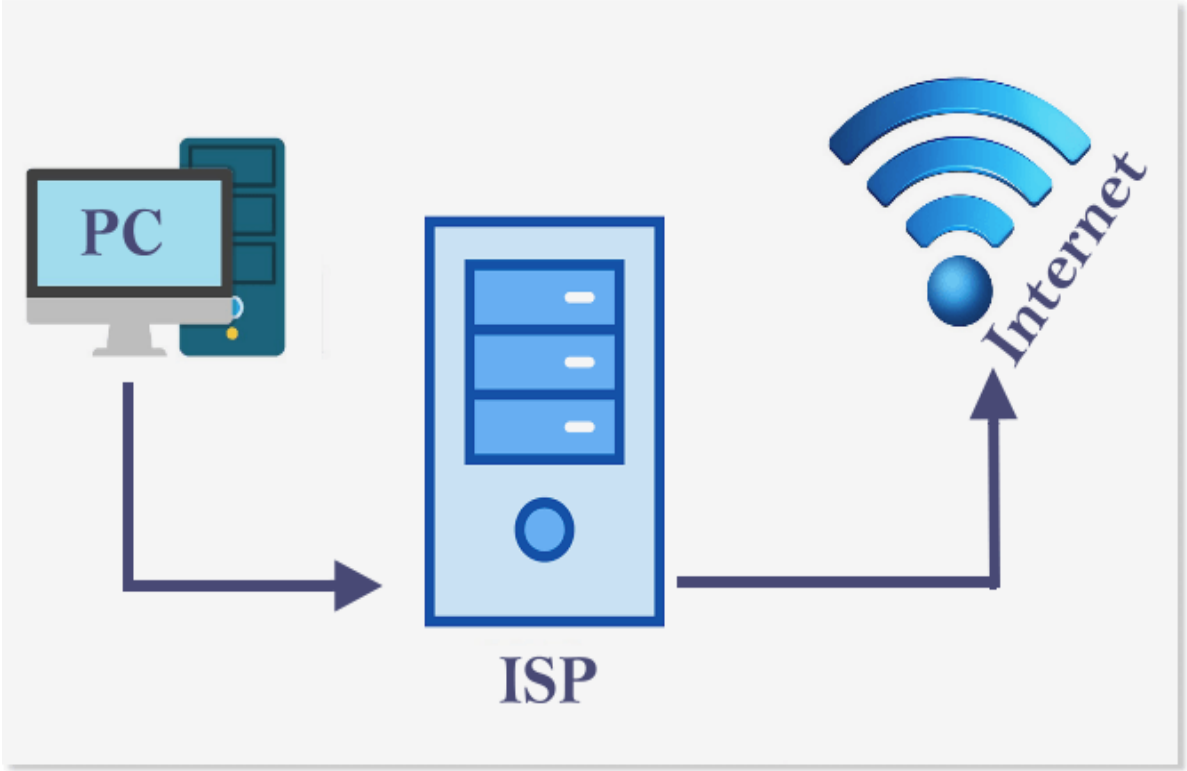
Existem diversas formas de descobrir o endereço IP público, a mais comum é entrando em um site que informa o endereço links abaixo:

ifconfig.me: https://ifconfig.me/ (de quebra ainda mosta os metadados abordaremos mais a frente)
whatsifmyipaddress: https://whatismyipaddress.com/

O que as pessoas podem saber a partir do IP ?

Antes de citar os motivos coloque uma coisa na sua cabeça, é inviável uma pessoa te hackear apenas tendo o seu endereço de IP, pelo simples fato de que o seu ip público ele na verdade não é seu, é do seu ISP, a grosso modo, a arquitetura para você acessar a internet é mais ou menos essa, você envia uma requisição da sua rede local

para o provedor e do provedor sua requisição é mandada para a internet, sendo assim, a internet enxerga seu ISP, não você ok ?…



4.Criptografia

Introdução a criptografia:

a Criptografia e a Criptoanálise faz parte da Criptologia, no qual engloba estudos de formas de escritas codificadas, Cifras, chaves, Algorítmos criptográficos, análise de cifras existentes e até mesmo formas de quebra de tais cifras.

A palavra Criptografia vem do grego Kryptós que significa “escondido”, e Gráphein que significa “escrita”, a tradução livre seria escrita escondida. Porém não faz tanto jus ao que realmente é, pois na verdade criptografia visa escritas codificadas de tal forma que não é possível ler sem a presença do algoritmo criptográfico e também da chave, o método que visa informações escondidas se chama esteganografia, a Criptografia visa também o ato de trafegar uma mensagem criptografada por meio de uma cifra que é um método de encriptação tais como a cifra de César e a cifra de

Vigenére, utilizando uma chave de encriptação que tal cifra suporte, ou então encriptando por meio de um algoritmo criptográfico no qual utiliza de diversos métodos e cifras de encriptação também com a presença de chaves.

Ao contrário da Criptografia existe a Criptoanálise no qual visa quebrar a Criptografia por meio de diversas técnicas, tais como análise de frequência, força bruta ou vulnerabilidades em algoritmos.

Cifra Clássica:

Vamos dar uma rápida olhada em uma cifra clássica, é simples e fácil de se quebrar porém possui um bom entendimento tanto da ideia como da prática do processo de encriptação, decriptação e criptoanálise no sentido de quebrar a cifra através de técnicas.

A cifra que vamos ver é a cifra de César, ela possui esse nome por quê segundo o escritor Suetônio essa cifra foi utiliza por Júlio César para se comunicar com seus generais, dessa forma protegendo as mensagens. A cifra de César é uma cifra de substituição na qual cada letra da mensagem é substituída por outra letra de acordo com a chave fornecida.

Cada letra do Alfabeto da cifra de César possui um número que vai de 0 a 25 ou seja fica algo dessa forma:

a b c d e f g h i j k l m n o p q r s t u v w x y z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

para encriptar é necessário uma chave, que pode ser qualquer número, inclusive maior que 25, pois caso seja maior que 25 começa-se a contar desde o começo de novo, por exemplo vamos supor que a chave é 27, ao chegar ao 25, começa-se a contar a partir de 0 de novo e segue em frente até o 1, calma eu sei que tá confuso mais continua lendo que logo mais você vai entender.

Agora que você já entendeu o alfabeto e a necessidade de uma chave, vamos encriptar e decriptar a seguinte mensagem: “shadow”, e usando a chave “5”, na qual indica o deslocamento que usaremos do alfabeto.

Sendo assim começaremos a encriptar letra por letra, no caso a letra “s” representa o número 18 no alfabeto, então 18 + 5 = 23 e o número 23 no alfabeto é o x, então trocaremos o “s” pelo “x”, agora a letra “h”, a letra “h” é igual a “7” no alfabeto então 7 + 5 = 12 e “12” é igual a “m” no alfabeto sendo assim vamos substituir “h” por “m”, agora o “a”, “a” é igual a “0”, e 0 + 5 = 5, sendo assim “a” virá “f”, e por ai em diante, vou colocar o processo de maneira ilustrativa agora:

a b c d e f g h i j k l m n o p q r s t u v w x y z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Chave = 5
Texto em claro = shadow

s = 18 + 5 = 23 = x

h = 7 + 5 = 12 = m

a = 0 + 5 = 5 = f

d = 3 + 5 = 8 = i

o = 14 + 5 = 19 = t

w = 22 + 5 = 27 = b (pois resetou a contagem)

Mensagem cifrada = xmfitb

Para decriptar é seguindo a mesma lógica porém subtraindo ao invés de adicionando:

a b c d e f g h i j k l m n o p q r s t u v w x y z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Key = 5
Texto cifrado = xmfitb

x = 23 – 5 = 18 = s

m = 12 – 5 = 7 = h

f = 5 - 5 = 0 = a

i = 8 – 5 = 3 = d

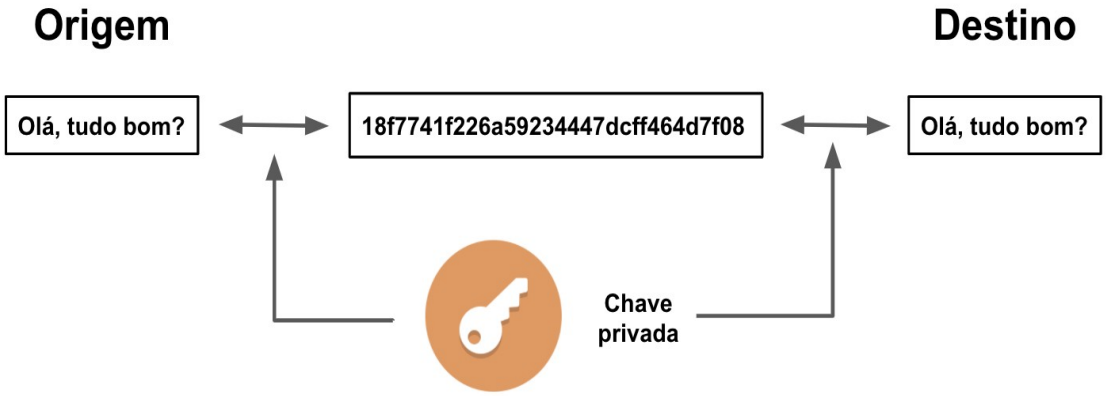
t = 19 – 5 = 14 = o

b = 1 – 5 = -4 = 22 = w

Mensagem decifrada = shadow

Agora que você já entendeu uma cifra clássica, e como funciona o processo de encriptação e decriptação, vamos entender como algoritmos criptográficos atuais funcionam.

Criptografia de chave simétrica, quando você ouvir falar que tal algoritmo criptográfico é simétrico ou de chave simétrica, quer dizer que na verdade ele usa apenas uma chave tanto pra encriptar quando para decriptar a mensagem, vamos usar um exemplo, vamos supor que João quer enviar uma mensagem para Julia via um chat que usa criptografia simétrica, sendo assim o João digita “Oi Julia, tudo bem ?”, e essa mensagem vai ser encriptada usando a chave “ABCD1234”, quando a mensagem chegar no chat de Julia ela será decriptada utilizando a mesma chave, ou seja “ABCD1234”.



Criptografia de chave Assimétrica, mesmo esquema, quando você ouvir alguém dizer que tal algoritmo é assimétrico ou de chave assimétrica, significa possui duas chaves, uma de encriptação no qual é a chave privada e outra de decriptação e também chave pública, detalhe a chave de decriptação não encripta e a chave de encriptação não decripta, sendo assim vamos ao exemplo, seguindo ainda o raciocínio do João com a Julia, quando o joão digitar e enviar uma mensagem via chat de criptografia assimétrica, sendo assim a mensagem será encriptada usando a chave pública de Julia, pois a mensagem está indo para ela, e ao chegar no chat de Julia a mensagem é decriptada por meio da chave privada de Julia, esse processo todo acontece devido ambas as chaves serem matematicamente relacionadas.

Criptografia de chave hibrida, essa é a união do melhor dos 2 mundos, possui tanto chave pública e privada que possuem a mesma finalidade de encriptar e decriptar, quanto chave simétrica, essa criptografia funciona da seguinte maneira, ainda no exemplo de João e Julia, ao João enviar uma mensagem para Julia, a mensagem é encriptada usando a criptografia de chave simétrica, após isso a mensagem e a chave simétrica é encriptada por meio da chave pública de Julia, sim são duas camadas de criptografia em cima da mensagem, quando a mensagem chegar até Julia, a primeira camada de criptografia e a chave simétrica é decriptada, e após isso a mensagem em si é decriptada por meio da chave simétrica, dessa forma a Julia conseguirá lera a mensagem de João.

5.*VPN*

O que é VPN

VPN na tradução livre fica Rede Virtual Privada, é uma forma de tunelamento de trafego, tunelamento esse que permite criptografar o trafego e ocultar o endereço IP.

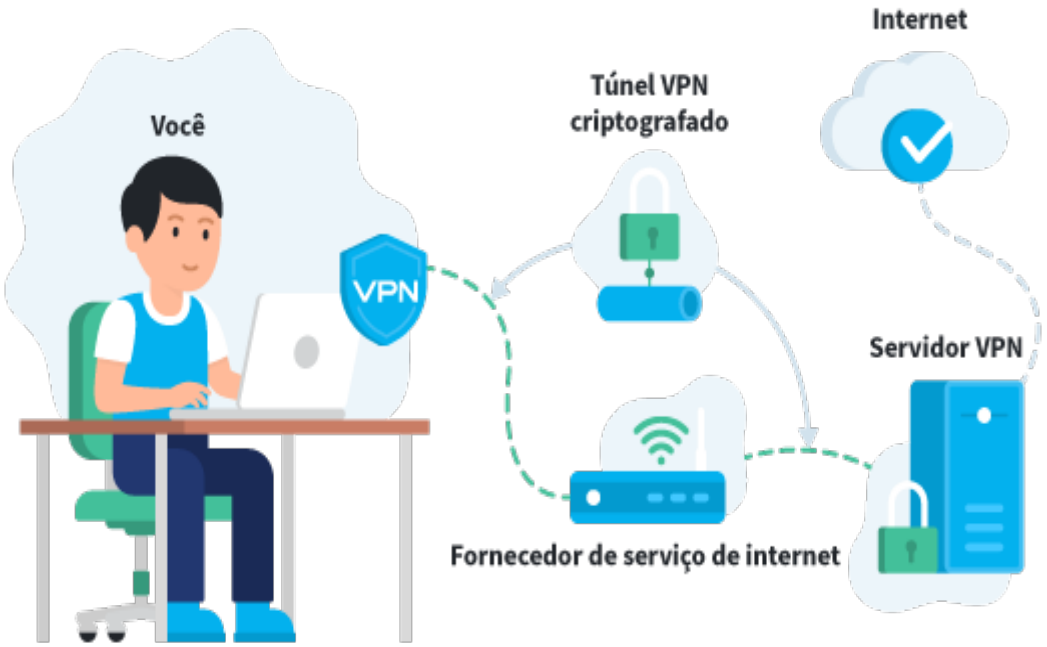
Como funciona ?

A VPN funciona da seguinte maneira, cria-se uma conexão privada entre seu computador e o provedor da vpn que por fim interliga você com internet, a grosso modo funciona como se fosse um proxy com a diferença de que o trafego da VPN é criptografado, o túnel criado pela VPN embaralha os dados para que nem um atacante externo que esteja sniffando a rede possa visualizar oque trafega dentro desse túnel.

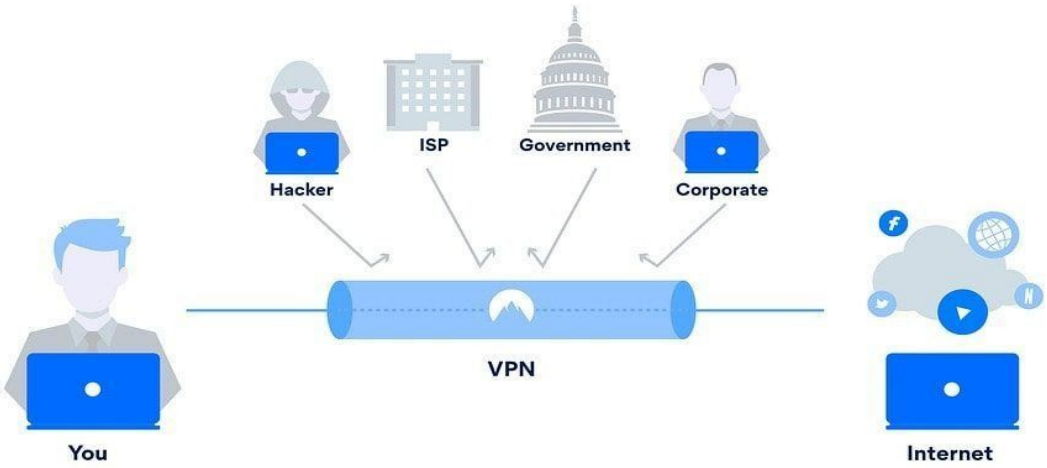
Aqui vai um exemplo de funcionamento da VPN, vamos supor que você deseja entrar no site da UOL, então você digita no seu

navegador uol.com.br, que então envia a requisição já encriptada, para o seu ISP e posteriormente para o servidor da VPN, que vai criar um túnel entre o servidor da UOL e o servidor da VPN dessa forma criptografando e privando seu endereço de ip e dados trafegados, de lá ele vai ir para o servidor da UOL, assim estabelecendo uma conexão com o servidor, enviando de volta o HTML da página pela conexão da VPN, sendo assim reenviando de volta para você.

IMAGEM ILUSTRATIVA LOGO A FRENTE



Dito tudo isso podemos concluir que, fica muito complicado para um hacker que está sniffando a rede saber o que está acontecendo devido a criptografia que está presente no túnel, também tem o fato de que ao ocultar seu endereço de IP fica difícil para terceiros, não só hackers, como também ISPs, Governos e etc, interceptarem seu trafego e saber o que está se passando ali, dessa forma mantendo o seu anonimato, privacidade e segurança



O que a VPN fornece ?

+ Privacidade de pacotes trafegados
+ Privacidade de endereço IP
+ Liberação de aplicações que estão bloqueados no país(Tlgd, quando o zap é bloqueado ?, é a VPN que tu usa para poder liberar o acesso.)

O que ela não fornece ?

+ Anonimato absoluto, pois o servidor da VPN armazena seu endereço real
+ Metadados e Fingerprints expostos

Mais ainda assim a VPN protege de maneira considerável sua privacidade.

O que se deve observar ante de usar uma VPN ?

+Reputação: Pesquise sobre a reputação a VPN, olhe em fóruns, o reddit é interessante para isso, mais em outras palavras não poupe pesquisa para VPN.

+Coleta de dados: A empresa mantém logs de pesquisa ?.

+Localização e Leis: importa bastante a localização na qual a VPN se localiza, pois tem países da Europa que obriga a empresa a enviar logs.

+Criptografia: priorize a VPN que utiliza de criptografia militar e de handshake como AES-256 e RSA-4086.

+Kill Switch: garante a privacidade e criptografia caso a conexão com o servidor da VPN venha a cair ou ter alguma outra falha.

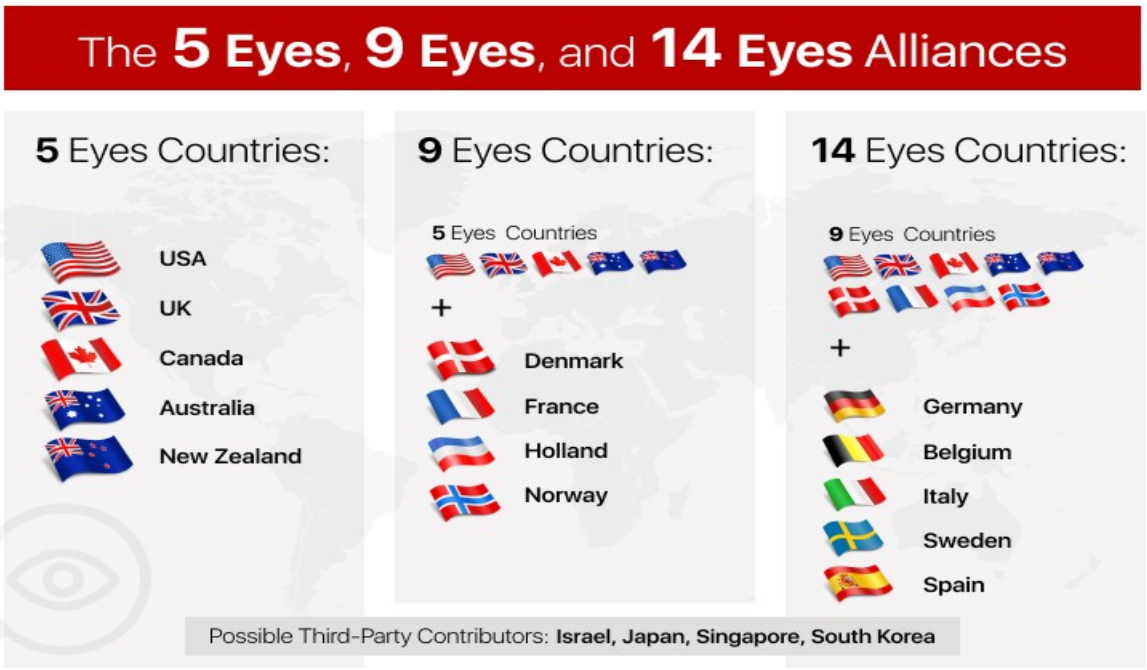
+Data split: pacotes divididos e enviados por servidores diferentes, dando um certo gostinho de descentralização e fortificando a segurança.

Para ajudar a selecionar a VPN, este site pode ser útil:
https://redditfavorites.com/vpns?order=anonymity_score

aliança dos 14 olhos

A aliança dos 14 olhos é um acordo feito em 14 países que visa o monitoramento da população, mais detalhes aqui.

Se alguma aplicação estiver situado em algum desses 14 países deve ser evitado ao máximo.



6.Trackers

Mesmo que você use VPN, ainda é possível rastreá-lo, existem diversas técnicas usadas por Big Techs e governos para te rastrear em um mundo online.

A VPN ajuda, porém como já dito anteriormente ela não oculta seus metadados, metadados esses que podem ser usados para criar um perfil exclusivo seu na internet e dessa forma poder identificá-lo em um mundo online. Uma dessas maneiras é usando trackers.

Trackers são scripts, códigos rastreadores com o objetivo de coletar informações sobre você no intuito de descobrir seus interesses e criar um perfil exclusivo sobre você na web, os mais famosos deles é o Google Analytics e o Hotjar, um é o google e o outro é uma criadora de Trackers.

Antes de irmos aos detalhes sobre os trackers, precisamos entender como que funciona a criação de um perfil digital sobre você na internet, também chamado de fingerprint ou impressão digital de navegador.

Como já dito anteriormente as Big Techs não precisam do seu Nome, RG, CPF e etc, basta elas coletarem os metadados anexados a sua requisição, tais como, data e hora do acesso, língua na qual está usando (Português, inglês e etc) e a localização do ISP, apenas coletando isso já da pra saber aproximadamente, de onde você é, e qual cidade você mora. Mais é claro que existem muitos outros metadados a serem coletados, metadados o suficiente para compor um perfil digital. Agora que você já está ciente da gravidade do problema, como ele funciona na realidade ?, é simples, todos os metadados coletados quando juntos formam uma informação, informação essa que é processada por IAs (inteligências artificiais) que posteriormente é armazenado em forma de um HASH.

HASH é um algoritmo matemático que gera um valor aleatório de tamanho fixo. Sendo assim a nossa informação é armazenada mais ou menos dessa maneira:

3f39588bb19e28051d9aedfbb170025c

Esse valor aleatório é único sendo assim, fica fácil identificar quem é quem de maneira precisa. Dessa forma criando uma impressão digital virtual exclusivamente sua.

Resumindo tudo, por um exemplo, vamos supor que você está acessando o google usando uma VPN, quando você acessa ou faz uma pesquisa você gera uma cadeia de metadados, metadados esses que vão gerar uma informação, essa informação vai ser processada por IAs (Inteligências Artificiais) que então vai ser convertido para um HASH, HASH esse que vai ser comparado com o HASH que já está nos servidores do google, caso ambos batam, o google acabou de identificar que é você que está acessando, mesmo usando VPN.

Agora você deve estar se perguntando, “então complicou por quê o google já tem minha impressão digital, dessa forma toda vez que eu acesso a WEB ele vai me identificar, tem como evitar isso ?”

Tem sim jovem, simples, as IAs do google e outras big techs atualizam os hashs de tempos em tempos, por quê eles sabem que o ser humano é um bicho mutável, estamos em constante mudança, dessa forma eles sempre sabem quem somos mesmo que você mude um pouco, então é simples, se você ir pro lado da privacidade hoje, daqui 1 mês (Número de exemplo) as big techs não saberão mais quem é você, pois eles terão um HASH antigo que não identifica mais você.

Para algumas empresas é interessante saber quem é que está acessando para melhor atendê-los, por exemplo, um site de noticias precisa saber de onde a pessoa está acessando para mostrar as noticiais locais, porém a maneira como eles ficam sabendo que é preocupante, já que eles compram essas informações de big techs, e só o fato da nossa informação estar sendo comercializada já é assustador por quê significa que qualquer um pode ir lá e comprar os nossos dados, e outra as políticas de privacidade das big techs deixam claros que coletam tais dados porém não perguntam a nós usuários se podem ou não vender os nossos dados que nós mesmo fornecemos a eles.

Para saber o quão identificável é seu navegador, faça o teste nesse site: https://coveryourtracks.eff.org/

Para saber o quão seu fingerprint é único use este site: https://amiunique.org/

Já este informa quais trackers te rastreiam em sites de noticias: https://trackography.org/

Agora que você já sabe de tudo isso, vamos aos trackers ou rastreadores.

Cookie Primário:

Arquivos de texto, armazenados no seu navegador, para tornar a navegação na WEB muito mais dinâmica e fácil. Geralmente são usados para armazenar configurações e login em sites.

Exemplo: quando você loga em um site você pode fechar o navegador e voltar ao site que ainda vai estar logado, devido ao cookie primário que está armazenado no seu navegador.

Eles são inofensivos pois podem ser excluidos a qualquer hora, porém os próximos da lista não são.

Cookie de Terceiros:

São arquivos carregados a partir de servidores de terceiros, por exemplo: um banner de anúncio está atrelado a um cookie de terceiro.

O Cookie de Terceiro mais comum é do google analytics no qual estima-se estar presente em **80% DOS SITES**

Não podem ser excluídos pelo fato de estarem sendo carregados a partir de servidores de terceiros, sendo assim é melhor bloquea-los antes da requisição do navegador (Veremos mais pra frente).

Supercookies ou “Cookies Zumbis”:

Baseados em Javascript ou flash, são cookies que são armazenados de diferentes formas no navegador do usuário, ele não só se instala de diversas formas como também ressuscita cookies expirados ou ausentes, é extremamente difícil de removê-los.

Impressão digital do navegador

Informação coletada ao interagir com o navegador de diversas formas, não só por metadados coletados, como também como você usa o navegador em si.

É uma lista extensa dos metadados coletados para formar uma impressão digital embora já tenhamos vistos exemplos anteriormente caso queira saber de maneira mais aprofundada segue os links a seguir:

Lista de metadados coletados: https://browserleaks.com/
Lista de metadados coletados 2:https://amiunique.org/faq

Trocar de navegador funciona ?:

NÃO !

Uma técnica chamada Cross-Browser Fingerprinting instrui aos navegadores executarem rotinas que por sua vez extrai dados ligeiramente diferentes para cada computador, porém 36 novos recursos funcionam independente do navegador especifico.

Sendo assim, trocar de navegador não é uma opção….. a não ser que você queira por outros motivos.

Biometria comportamental:

Coleta de informações sobre como você usa o aparelho em si, tipo interação com o dispositivo, sensores e como você se comporta quando está com o dispositivo na mão, frequência de toques ou cliques na tela e etc.

TUDO ISSO é composto para criar um perfil único nosso online !!!

Tenho uma má notícia

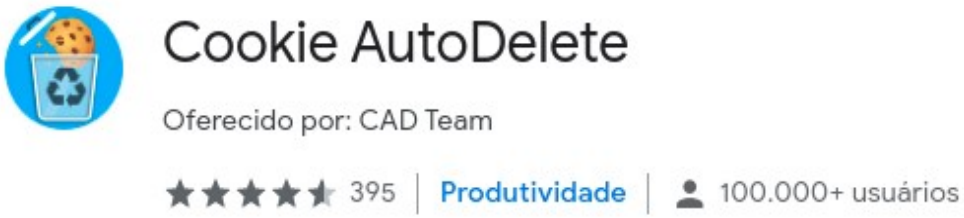
Não existe uma forma precisa que impede o rastreamento de trackers, principalmente o rastreamento via fingerprint, que é algo mais relacionado ao comportamento do ser humano. Porém existem métodos que podem ser aplicados e que dificultam e muito o rastreamento na internet, métodos esses que vamos ver agora.

Privacy Badger

Privacy Badger é um plug-in open-source que pode ser instalado no navegador, ele bloqueia cookies de rastreamento usando táticas de comportamento, ou seja, quanto mais você usa a extensão mais, ela aprende e fica mais efetiva conforme o tempo.

Cookie Autodelete

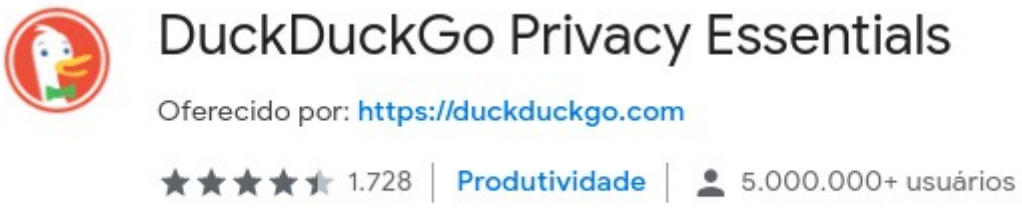
Só para garantir, caso o Privacy Badger falhe, esse plug-in open-source garante que todos os cookies do site sejam excluídos após o fechamento da aba do site.



DuckDuckGo Privacy Essentials

O famoso buscador com foco em privacidade também se juntou a luta contra os trackers, ele possui 3 vantagens

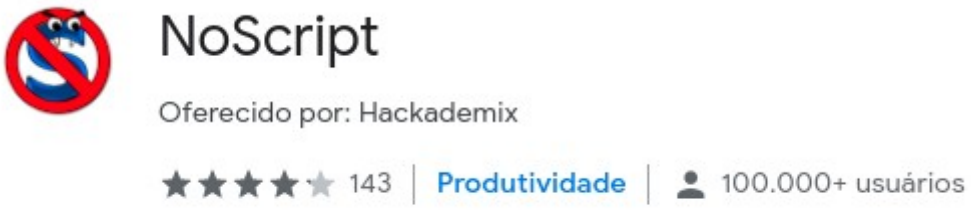
1. *Bloqueia Trackers*
2. *Informa se o site usa HTTPs*
3. *Informa a reputação de privacidade do site*



Saindo do “bloqueamento” de trackers e entrando na Cibersegurança

NoScript

Essa extensão é bem rígida, ela bloqueia qualquer Javascript e Flash que possui no site, sendo assim afeta drasticamente a navegação.

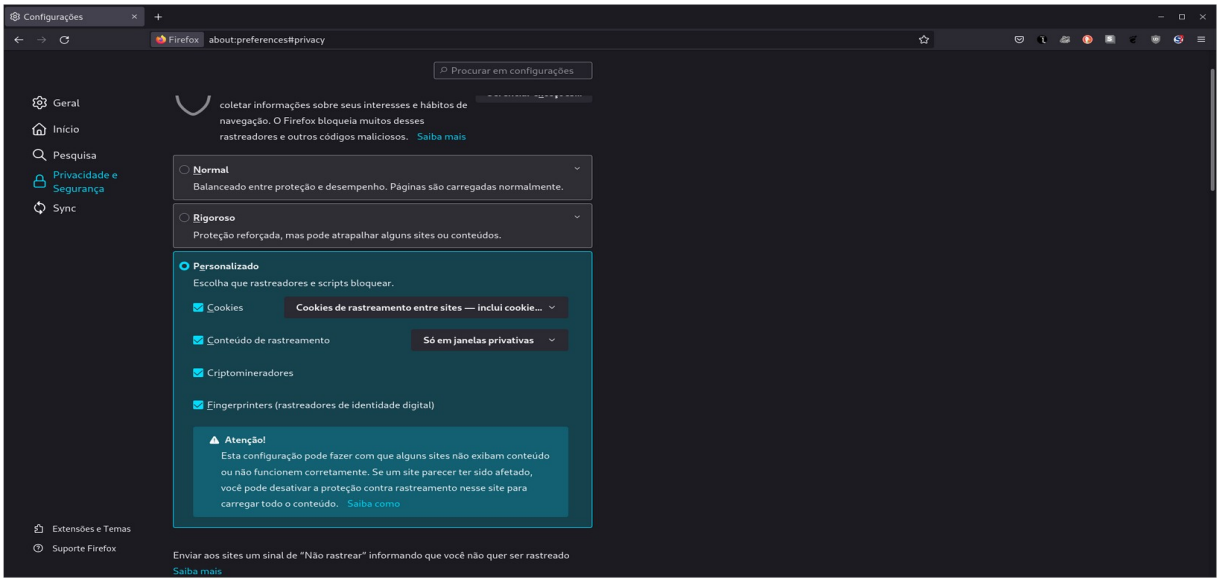


Não se esqueça de configurar seu navegador

A grande maioria esmagadora dos navegadores vem com funcionalidades de exclusão de cookie por padrão, basta ativa-las

Usando o firefox como exemplo, siga os seguintes passos:

Configurações > Privacidade e Segurança > Configure de maneira que venha atender a suas necessidades.



Considerações

Não tente em hipótese alguma se destacar na multidão, para um melhor entendimento, quando você usa um navegador com muitas extensões e personalizações, você na verdade só está se destacando na multidão pois o navegador fica de maneira diferente aos olhos dos trackers, sendo assim fica fácil identificá-lo em meio de diversos usuários que usam o navegador comum por exemplo, sendo assim use apenas os plug-ins necessários.

7.Anúncios

Os anúncios muitas vezes são necessários por quê são uma forma de lucro para os donos de sites e Big Techs, e também é um dos motivos pelo qual ainda existem muitas coisas gratuitas na internet. Porém a grande maioria desses anúncios são constrangedores e também consomem muitos recursos do dispositivo. Também tem o fato que a grande maioria das vezes os

banners de anúncio são carregados via cookies de terceiros ou seja de servidores de terceiros que podem coletar dados.

Dizendo de passagem, os anúncios se beneficiam de seu fingerprint, por exemplo vamos supor que você pesquisou sobre preços de tênis, após isso você foi ver algumas notícias em seu site de notícias preferido, porém agora só aparece anúncios de tênis para você, isso acontece devido ao seu fingerprint e aos cookies, o anunciantes geralmente compram ou coletam esse tipo de informação para efetuar vendas e mostrar anúncios mais relevantes para o usuário. Sendo assim a solução é usar Bloqueadores De Anúncios, tipo o Adblock ???…

Negativo

O Adblock não é a melhor opção pelo fato de que ele possui uma política de “Anúncios Aceitáveis”, sendo assim, existem alguns anunciantes que pagam para o Adblock não bloquear os anúncios. Então, esqueça o Adblock.

Ublock Origin

Ublock Origin é um adblocker open-source que não só não permite “Anúncios Aceitáveis” como também possui algumas opções avançadas e também bloqueio de script (Algo parecido com o NoScript).

Notícia sobre Adblockers:

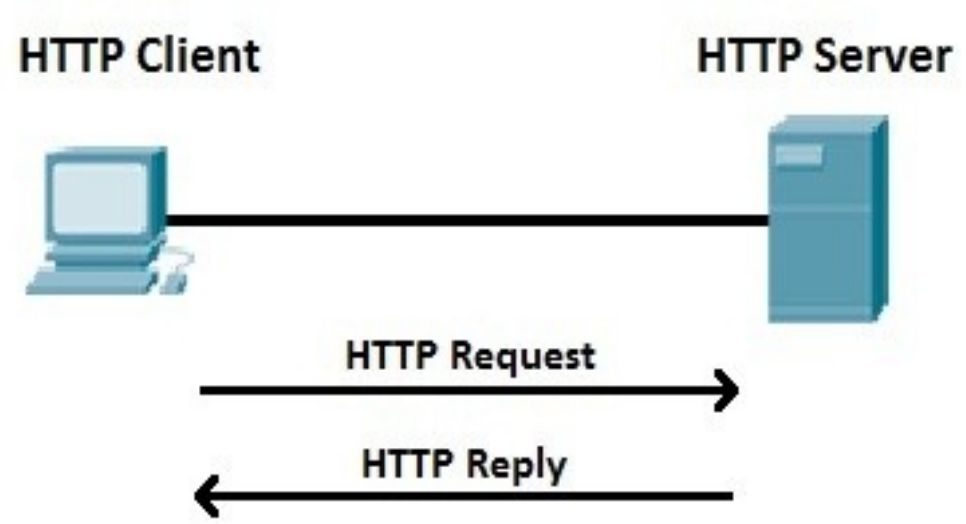
Agências de inteligência e segurança nacional dos EUA utilizam “adblockers” por causa de perigos em publicidade online: a CIA e NSA implementaram tecnologias de bloqueio de anúncios em nível de rede, utilizando informações de várias camadas, incluindo do DNS, para bloquear conteúdos publicitários. As agências receiam que anúncios maliciosos consigam coletar informações confidenciais ou hackear seus dispositivos.

Foto e Notícia tirada na Newsletter do Filipe Deschamps.

8.HTTPS

Antes de explicar oque é o HTTPS vamos entender o que é o HTTP. O HTTP é a sigla para HyperText Transfer Protocol ou protocolo de transferência de Hipertexto, é um protocolo da camada de aplicação do Modelo OSI e opera utilizando arquitetura Cliente e Servidor, no qual se baseia em requisições HTTP tais como GET, POST, PUT e etc, como já dito anteriormente é um protocolo de transferência de Hipertexto que no caso são texto, imagens, vídeos, scripts e etc, todo esse conglomerado forma um arquivo de Hipertexto no qual é transferido no payload do protocolo, agora como que ele funciona ?.

Por exemplo, vamos supor que você queira entrar no site da Desec empresa que ministra cursos e faz pentest, sendo assim eu digito no campo de busca a URL: desecsecurity.com, sendo assim o seu navegador vai enviar um requisição do tipo GET para o servidor, algo mais ou menos assim: *GET / HTTP/1.1* Após isso o servidor irá responder com os arquivos da pasta RAIZ do servidor, no qual contém o HTML, CSS e Javascript do site. Após isso seu navegador irá processar os arquivos recebidos e exibirá o site para você.



Só que tem um detalhe… a conexão estabelecida entre você e o servidor trafega em texto claro, ou seja não é criptografada e isso é um problema pois pensa comigo, vamos supor que você está fazendo uma compra no site da amazon, se a conexão não fosse criptografada os dados do cartão trafegariam em claro, dessa forma possibilitando que alguém que esteja sniffando a rede possa visualizar o conteúdo dentro do protocolo sendo assim é perigoso de mais deixar o trafego sem criptografia e é ai que entra o HTTPS.

O HTTPS se baseia no SSL/TLS, que é um protocolo separado porém atua sobre o HTTP, vamos discuti-lo agora.

O SSL sigla para Secure Sockets Layer tradução livre para “Camada de soquetes segura”, é uma padronização de industria para segurança em rede, podemos dizer que é o lado legislativo do SSL/TLS, Já o TLS sigla para Transport Layer Security tradução livre para “Segurança da camada de transporte” e é o protocolo em si, é o lado técnico podemos assim dizer, ele opera sobre 2 protocolos, que são eles o TLS record e o TLS handshake.

TLS handshake provê autenticação entre cliente e servidor, negociação do algoritmo e chaves criptográficas, a conexão acontece antes da transmissão de dados e a chave simétrica do TLS record é repassada utilizando criptografia assimétrica.

TLS record é o protocolo que opera sobre o TCP e provê confidencialidade utilizando criptografia de chave simétrica e também integridade no pacote utilizando-se de funções hash criptográficas.

De maneira resumida, o TLS handshake toma a frente criando uma conexão criptografada usando criptografia de chave assimétrica e também provê negociação do algoritmo e das chaves criptográficas, após isso o TLS record entra em jogo na hora de transmitir dados no

qual são criptografados utilizando criptografia de chave simétrica e também provê integridade de dados utilizando funções hash.

Como já dito anteriormente o SSL/TLS roda sobre os protocolos da camada de aplicação para prover mais segurança, por exemplo: FTPS, HTTPS e etc. No caso do HTTPS desde a conexão até o trafego de dados é totalmente criptografado e seguro, dessa forma você pode fazer sua compra na amazon tranquilo, sem risco de ter alguém sniffando a rede. Porém é preciso que o servidor no qual está se conectando suporte o SSL/TLS dessa forma seu navegador consegue estabelecer a conexão segura. Sendo assim, certifique-se de que o cadeado no canto superior esquerdo esteja ativado, isso simboliza de que sua conexão está usando SSL/TLS ou melhor dizendo está criptografada.

Porém possui uma solução para caso o servidor no qual está acessando não possua HTTPS, na falta de sorte, use a extensão HTTPS Everywhere. É um extensão open source que implementa o HTTPS independente do servidor ter ou não suporte ao mesmo.

9.Guia Anônima

O modo de navegação “anônima” é um modo no qual a maioria dos navegadores possuem, quando estamos nesse modo significa que o navegador não salvará o histórico de pesquisa, cookies e nem dados de formulários, porém ainda tem muita coisa em jogo no qual irei citar agora.

Vantagens:

Não armazena histórico de pesquisa
Não armazena Cookies
Não armazena dados de formularios

Em outras palavras ele oculta das outras pessoas oque você fez no navegador.

Desvantagens:

O ISP pode ver seu trafego
O admin da sua rede ou instituição pode ver seu trafego
não encripta a conexão
não oculta o IP
não impede que programas espione suas atividades

10.E-mails seguros e privados

conselho de amigo, evite ao máximo serviços de Big Techs, além de elas coletarem nossos dados e não terem o mínimo remorso disso, ela ainda vendem nossos dados para anunciantes sem nosso concentimento.

Notícias sobre:

O gmail foi flagrado dando a terceiros acesso total aos e-mails dos usuários, clique aqui para ver a notícia.

E também acompanhando todas as suas compras online, clique aqui para ver a notícia.

Facebook lê todas as suas mensagens no facebook messenger, clique aqui para ver a notícia.

Outro detalhe, apenas criptografia de ponta a ponta não basta, também é preciso ocultar os metadados, como endereço de IP, data e hora, para quem enviou e etc. E outra softwares de big techs são uma porta de coleta de dados para o estado, o programa PRISM da NSA é o responsável pela coleta de dados de várias empresas de tecnologia na internet ou seja, google, facebook, amazon e etc são uma porta de entrada para a coleta de dados estatal.

Antes de irmos as opções, vamos entender sobre segurança da informação, a segurança da informação a grosso modo se baseia em na sigla CID sigla para, C de Confidencialidade, I de Integridade, D de Disponibilidade.

Confidencialidade: Significa que apenas quem está autorizado terá acesso a tal informação

Integridade: Significa que apenas quem tem autorização pode modificar a informação.

Disponibilidade: Significa que quando precisar da informação ela deve estar disponível

Sabendo desses pilares fica fácil de saber oque que uma aplicação segura necessita ter, sendo assim uma aplicação segura deve ter um desenvolvimento continuo, dessa forma evita possíveis falhas de segurança que venham a acontecer, evita a falha de integridade já que os desenvolvedores vão manter a aplicação de forma segura e a disponibilidade também é afetada de forma positiva pois se os desenvolvedores se preocupam com a aplicação ela obrigatoriamente deve estar disponível.

Agora oque uma aplicação precisa ter para ser ideal ?, bom ela necessita ter as seguintes características:

Segurança: a aplicação deve ser seguro e seguir os 3 pilares da segurança da informação
Privacidade: Impede que terceiros vejam o conteúdo da informação
Anonimato: Proteger a identidade dos usuários.
Usabilidade: Ser fácil e intuitivo de usar.

Agora oque precisa ser observado antes de escolher uma aplicação ?:

Criptografia de Ponta-a-Ponta (E2E): Criptografia que garante a privacidade desde a hora que sai da máquina do usuário até o outro lado a conexão.

Open Source: Significa que o código fonte da aplicação na qual está usando, está disponível para ser auditado por pessoas experientes que possuem conhecimento e tempo para isso.

P2P (Peer-to-Peer): Sem um servidor intermediando as comunicações, ou seja comunicação que sai da máquina do usuário até a máquina de destino e fim de papo.

Metadados: A aplicação coleta ou armazena os metadados, se sim, deve ser evitada.

Informações de registro: quais dados são coletados para se registrar nessa aplicação.

Jurisdição: Local onde está localizado aplicação, no caso se a aplicação estiver localizada em um país da aliança de 14 olhos, deve ser evitada.

E-mails Temporários

Agora sim, vamos as opções, começaremos com os e-mails temporários, que no caso são e-mails temporários ou com tempo de vida pré-determinado, não precisam de registro porém também não possuem um anonimato absoluto já que seu endereço de IP e metadados ainda podem ser coletados, sendo assim, use uma VPN ou o TOR(Falaremos sobre mais a frente) para usa-los:

Tempmail: Gratuito, Apenas recebe e-mail. Endereço de e-mail que destrói a cada 10 minutos.

Guerrillamail: Open Source e gratuito. Envia e recebe e-mails. Exclui automaticamente e-mails recebidos em 1h. Envia arquivos de até 150 Mb (beta).

E-mails Off Shore

Agora vamos aos e-mails off shore no qual permite criação de contas e acesso pago ou uma versão grátis limitada, possuem anonimato total se acessados com uma VPN ou usando o TOR e privacidade pois as comunicações entre o servidor e você é criptografada com criptografia de ponta-a-ponta.

Tutanota: Serviço seguro de e-mails localizado na Alemanha sem investidores ou proprietários externos.

Vantagens:

1- Criptografia AES e RSA resistentes a computação quântica

2- Tanto o corpo quanto o título dos e-mails são encriptados.

3- Pode enviar mensagens criptografadas para usuários de fora, exemplo você do tutanota pode enviar uma mensagem criptografada para um usuário de Gmail.

4- Não registra endereço IP por padrão

5- Aplicativos para Desktop, Web e Mobile.

6- Open Source (Inclusive os APPs Mobile)

7- Autenticação por 2 fatores

8- Registro anônimo (só nome do e-mail e senha)

9- Sem captchas (Sem scripts externos)

Desvantagens:

1- Sede em um país dos 14 olhos, e diga-se de passagem isso é alarmante, lembra que ele não armazena o endereço IP por padrão, caso o estado requisite que ele comece a monitorar tal endereço IP, é possível que aconteça pois é regra do estado, algo semelhante aconteceu com o protonmail, inclusive por esse motivo não vou inclui-lo nesse pdf pois ele perdeu minha confiança, é algo pessoal, sendo assim ainda é recomendável usar o protonmail.

Notícia do vazamento de IP do protonmail aqui
Modelo de ameaça do protonmail aqui
Transparência do protonmail aqui
Analise forense do protonmail aqui

2- Serviço Centralizado (eles pretendem adicionar um nó na rede Tor)

CyberFear: Serviço de E-mail seguro, descentralizado e anonimo com nó na rede Onion.

Vantagens:

1- Criptografia de ponta-a-ponta incluindo e-mail e metadados

2- Registro Anônimo (Só nome de usuário e senha)

3- Proteção contra ataques de Man-in-the-middle

4- Sem registros de endereço IP

5- Sede na polônia (Sem 14 olhos)

6- Suporta pagamento anônimo, em criptomoedas

7- Opera um nó na Rede Onion (Link no final deste tópico)

8- Utiliza PGP

9- Sem Captchas (ou seja, sem script de terceiros)

10- Autenticação em 2 fatores

11- Open Source (Apenas o front-end pois se o back também fosse, teremos problemas de segurança)

Link da Rede Onion:

http://cyberfe3gvh7cvq2nhuqtaghjxebhcnqafnfvalwvq6mxrinep7m7xqd.onion/

11.Mensageiros Instantâneos

volto a dizer, evite ao máximo as Big techs além de elas venderem nossos dados sem nosso consentimentos, donos como Mark Zuckerberg se orgulham de coletar nossos dados e serem totalmente intrusivos, não vou repetir oque já disse anteriormente, sendo assim vamos direto ao assunto.

Antes de tudo vamos entender como funciona a centralização.

Centralizado: existe um servidor intermediando as comunicações, servidor esse que administrado pela empresa desenvolvedora da aplicação.

Federado: existe um servidor intermediando as comunicações, porém o servidor tem administrador próprio oque na grande maioria das vezes é serviço de empresas terceirizadas.

P2P ou Ponto-a-Ponto: De todos, o método mais descentralizado !, não possui um servidor intermediando, as comunicações acontecem diretamente de um aparelho para outro através da rede.

O que observar antes de escolher um mensageiro instantâneo ?

Criptografia de Ponta-a-Ponta (E2E): Criptografia que garante a privacidade desde a hora que sai da máquina do usuário até o outro lado a conexão.

Open Source: Significa que o código fonte da aplicação na qual está usando, está disponível para ser auditado por pessoas experientes que possuem conhecimento e tempo para isso.

Coleta de metadados e registro de IP: Procure saber se a aplicação encripta seus metadados e não registre seu IP

O que é necessário para se inscrever: informações de registro requisitadas para usar a aplicação, se pedir muitas informações, abra os olhos.

Jurisdição: Onde a aplicação está localizada, e se essa localização faz parte dos 14 olhos, como já dito anteriormente.

Dito isso, vamos as opções, começando pelas opções de celular:

Briar: Mensageiro instantâneo que tunela todo o tráfego pela rede Onion, sem falar que é fácil de usar e funciona tanto pelo wi-fi quanto bluetooth.

Vantagens:

Anonimato e Privacidade, Pelo fato de tunelar tudo pela rede Onion, sendo assim possui descentralização e criptografia de ponta-a-ponta.

P2P, significa que a comunicação acontece diretamente de um ponto a outro, sendo assim não existe um servidor intermediando.

Simples de usar, possui uma interface simples de usar.

Funciona tanto Bluetooth quanto por WI-FI, Não é limitado apenas por WI-FI, funciona também via Bluetooth.

Código fonte aberto

Desvantagens:

Consome mais bateria do que o normal pelo fato do aplicativo manter uma conexão com a rede Onion.

Só permite mensagens de texto e nada mais.

Session: é um fork do signal(Falaremos mais a frente), porém projetado para ser mais seguro e privado, as comunicações acontecem via roteamento de Cebola (algo similar a rede tor só que não é a mesma, é um protocolo novo).

Vantagens:

P2P, significa que a comunicação acontece diretamente de um ponto a outro, sendo assim não existe um servidor intermediando.

Não exige registro, sem registro, sem dados coletados, anonimato total.

Não coleta metadados, pelo fato da comunicação ser feita por uma rede de anonimato similar a rede onion, existe tanto criptografia de ponta-a-ponta, como encriptação de metadados.

Open source, Código fonte aberto.

Desvantagens:

Não possui chamada de áudio e vídeo, somente texto e áudio.

Não é Simples de usar (porém não é um bicho de 7 cabeças)

Protocolo novo, sendo assim pode conter bugs

Atox: Antox na verdade é uma versão para android, do Tox que é um mensageiro de código aberto descentralizado no qual contém também encriptação de ponta-a-ponta.

Vantagens:

Encriptação de ponta a ponta ou E2E (End-to-End Encription), ou seja toda a comunicação desde o ponto que sai de um ponto até outro é totalmente encriptado.

P2P ou ponto-a-ponto, comunicação direta de ponto a outro sem uma intervenção de um servidor.

Fácil de utilizar, possui uma interface amigável

Código aberto, ou seja o código fonte do programa é aberto.

Multiplataforma, tanto para Computador, quanto para celular.

Possui tanto um chat quanto chamada de aúdio e vídeo.

Element: Um app universal de bate-papo construído em matrix (protocolo novo).

Vantagens:

Descentralizado, mesmo que seja servidor federado existe sim uma descentralização.

Anonimato absoluto, pois não armazena IP nem metadados

Controle total dos seus dados, pois o software de servidor é executado no lado do cliente.

Desvantagens:

Protocolo novo, sendo assim pode conter bugs

Não é simples de se usar.

Signal: Um mensageiro instantâneo centralizado que possui um algoritmo de criptografia mais bem avaliado e testado por criptografos.

Vantagens:

Fácil de usar

Protocolo de criptografia considerado o mais seguro até o momento.

Desvantagens:

Centralizado

Requer número de telefone para ser usado.

Agora vamos as opções do Computador:

Antes de tudo vamos falar de um protocolo chamado XMPP que é usado amplamente na construção de mensageiros instantâneos, XMPP sigla para Extensible messaging and presense protocol tradução livre para Protocolo extensível de mensagens e presença, é um protocolo da camada de aplicação do modelo OSI padronizado pelo IETF e também é de código aberto e está em constante desenvolvimento. Utiliza de XML para transmissão de mensagens pelo simples fato do XML ser uma linguagem de marcação extensível, no próprio nome do negócio já diz isso (Extensible markup language) para mais informações veja este vídeo clicando aqui. Algumas característica que o XMPP tem são as seguintes, 1- Ele permite a detecção do status de um tal contato, por exemplo se ele está online ou off-line, e mais um detalhe, o próprio usuário pode definir o próprio status como quiser, por exemplo eu posso definir meu status como ausente mesmo estando online, 2- Possui além de mensagens de texto chamadas de voz e vídeo, 3- Pode operar sobre TLS, protocolo esse que já vimos anteriormente. Agora como o XMPP funciona, ele opera de modo descentralizado por meio de servidores federados, primeiro devemos criar uma conta em um servidor XMPP, geralmente um client XMPP tem essa opção, veremos mais adiante, após criada essa conta vamos supor que você está conversando com o seu amigo joãozinho, sendo assim você

envia uma mensagem para o joãozinho, essa mensagem vai ir pra um servidor federado do XMPP de lá a mensagem percorrerá por outros servidores até chegar no celular de joãozinho e como já dito anteriormente esse protocolo opera com TLS, dessa forma mantêm a segurança e a integridade da mensagem.

Agora para podermos acessar esse serviço de mensagens devemos ter um client, para esse exemplos iremos usar o **pidgin**, que funciona como se fosse um proxy para diversos serviços de chat, entre eles está o XMPP então usaremos ele.

Vantagens:

Descentralizado, pelo fato de você estar usando XMPP.

Open source, o código do Pidgin está disponível no site oficial deles, clicando aqui.

Desvantagens:

É um pouco difícil de usar.

Exige uma configuração correta, porém uma vez feita, não será preciso fazer mais, a não ser que queira adicionar um contato.

Caso você queira configurar o seu pidgin este vídeo vai ter ajudar, está em inglês, porém é só seguir os passos que você vai configurar o pidgin de maneira anonima e com um servidor sem política de registro de logs, clicando aqui.

Tox: Tox é um mensageiro instantâneo de código aberto, que fornece criptografia de ponta-a-ponta e serviço descentralizado, o chat também é bem potente, podendo ter não só chat de texto, como também chat de voz, vídeo e também pode-se enviar arquivos pelo chat.

Vantagens:

E2E (End-to-End Encription): o tox fornece criptografia de ponta-a-ponta usando uma biblioteca chamada NaCL que utiliza criptografia de chave simétrica tais como Salsa20 e AES.

P2P: Não possui um servidor intermediando a comunicação, sendo assim a mensagem que você quer enviar sai da sua máquina, e vai direto para o receptor.

Fácil de utilizar: Possui uma interface amigável e fácil de utilizar.

Open source: o código fonte do programa é aberto, e possui tanto versão em escrita em python ou em C ambas com interface gráfica QT.

Multiplataforma: Possui tanto aplicação para desktop quanto para mobile, como já citado anteriormente.

Chat com funcionalidades: possui tanto chat de texto como também chat de voz e vídeo e detalhe, é possui enviar arquivos pelo chat de texto.

Desventagens:

Protocolo Novo: pelo fato de ser um protocolo relativamente novo, pode conter falhas de segurança, falhas essas que podem ferir a privacidade e a segurança do usuário.

Endereço de IP não é ocultado: Pelo fato de ser P2P possui um certo grau de anonimato e descentralização, porém quando você tem um contato adicionado, ele pode ver o seu tox id e dessa forma descobrir o seu endereço de IP mesmo tunelando tudo pela rede TOR.

12. Armazenamento de arquivos em nuvem seguros

Aposto que todos aqui temos arquivos, fotos, vídeos e etc que estão armazenados em nuvem, já meio que virou uma necessidade, sendo assim possui uma solução segura para isso, volto a dizer evite ao máximo os serviços das big techs, não vou repetir a mesma ladainha aqui pois já vimos anteriormente.

O que observar antes de escolher um serviço em nuvem:

Criptografia de ponta-a-ponta, isso significa que toda a comunicação desde o momento que sai do seu computador até o destino é encriptado.

Código fonte aberto, para que alguém que tenha conhecimento e tempo possa ser auditado e melhorar a segurança e também comprovar que não existe nem um backdoor.

O que é preciso para se registrar no serviço, por exemplo, e-mail, nome, cpf e etc.

Coleta de metadados, se coleta ou não, se registra IP ou não.

Icedrive: Serviço de armazenamento em nuvem com foco em segurança, a plataforma possui Encriptação de ponta-a-ponta com algoritmo de criptografia simétrico chamado Twofish sucessor do Blowfish.

Vantagens:

Criptografia Twofish, no qual é um código de criptografia open-source e possui chave simétrica, ela emprega cifras em blocos de 128 bits, e o tamanho das chave pode variar de 128, 192 e 256 bits, também realiza 16 interações durante a criptografia, tais interações aplicam técnicas tais como, Feistel Network, S-Boxes e etc.

Encriptação do lado do cliente, dessa forma nem mesmo os desenvolvedores podem ler o que tem dentro do documento, porém essa função só esta disponível em planos pagos…..

Criptografia de ponta-a-ponta, isso significa que toda a comunicação desde o momento que sai do seu computador até o destino é encriptado.

10 Gigabytes de armazenamento no plano free

é multiplataforma pois possui tanto programa para desktop e web, quanto mobile.

Desvantagens:

Não é código-aberto, isso significa que não temos certeza de que a criptografia está implantado corretamente e principalmente se não possui backdoors.

Faz parte dos 14 olhos pois se localiza no Reino Unido.

É um serviço centralizado.

Mega.io: Embora o mega tenha passado por alguns tumultos no passado como por exemplo, na primeira versão do mega upload, ele simplesmente tenha sumiu do mapa essa nova versão pode-se dizer que está bem madura e confiável para ser usada, sendo assim vamos as vantagens.

Vantagens:

Criptografia de ponta-a-ponta, isso significa que toda a comunicação desde o momento que sai do seu computador até o destino é encriptado.

Criptografia do lado do cliente, isso significa que nem mesmo os devs podem ver os arquivos.

Multiplataforma, possui tanto programas Desktop, Web quanto para Mobile.

2FA, ou 2 factor authentication, isso significa que você pode adicionar confirmação de login em duas etapas usando o celular.

Open-source, isso significa que o código-fonte está disponível para quem tiver conhecimento e tempo para audita-lo.

20 GB de armazenamento no plano-free.

Desvantagens:

Centralizado, isso significa que possui um servidor intermediando as comunicações, porém não tem muito oque fazer, até por quê é um serviço de armazenamento em nuvem e um servidor com armazenamento é necessário.

Caso queira apenas compartilhar arquivos use essas opções

Onionshare: é um programa que disponibiliza seus arquivos em um página na rede tor….. Preciso dizer algo mais ??, é simplesmente o melhor compartilhador de arquivos, é fácil de usar e possui anonimato e segurança total durante a disponibilização de arquivos.

Vantagens:

P2P, ou ponto-a-ponto isso significa que o pacote sai do seu pc e vai direto para o pc do receptor, dessa forma mantendo um nível de descentralização máxima, sem um servidor interceptando as comunicações.

Criptografia de ponta-a-ponta, isso significa que toda a comunicação desde o momento que sai do seu computador até o destino é encriptado.

Tudo tunelado pela rede TOR, logo mais explicaremos sobre essa rede maravilhosa de anonimato na internet.

Anonimato total, ocultação de IP e metadados, trafego descentralizado com encriptação de ponta-a-ponta… mais anônimo que isso só não usando o serviço.

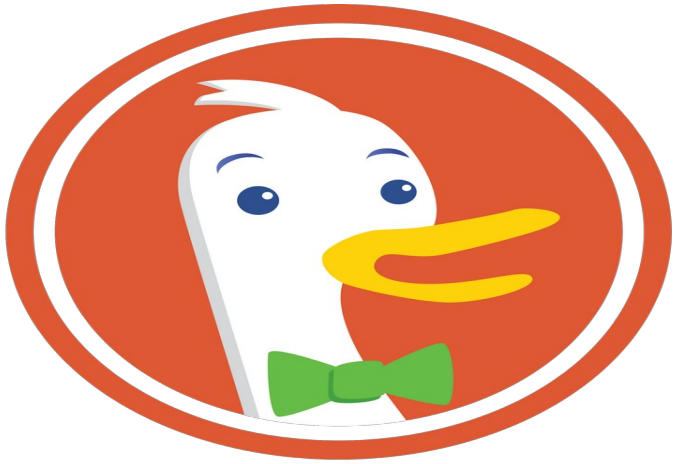
Open-source, significa que o código fonte do programa é aberto para quem tem tempo e conhecimento para auditar o código, dessa forma melhorando a segurança e a privacidade do código.

13.Buscadores de privacidade

O buscador mais popular é oque menos se preocupa com a sua privacidade e é claro que estou falando do google, é uma ferramenta eficaz e precisa porém ele só consegue isso pois ele sabe muito sobre nós, não acredita no que eu digo ??, você pode baixar os dados que o google tem armazenado sobre você (mais diga-se de passagem não são realmente todos, por exemplo, fingerprints e metadados, e sim dados brutos), clicando aqui.

Porém existe uma solução, existem buscadores focados em privacidade que não ficam tão atrás assim do google, com o tempo eles vem sendo refinados e estão cada vez melhores.

DuckDuckGo: DuckDuckGo é um buscador de código aberto com foco na privacidade do usuário.



DuckDuckGo

Startpage: Buscador que usa os mesmos resultados do google, só que sem te rastrear, ele funciona da seguinte maneira, ele meio que paga para o google não te rastrear, é um tanto quanto suspeito por quê, será que a ferramenta gera receita o suficiente para pagar o google apenas com anúncios ?, outro detalhe é que ele oculta todas as pesquisas que você faz do histórico.

Searx: é um metabuscador que usa diversas engines de pesquisa, open source com foco em privacidade.

14.Navegadores de Privacidade

Os navegadores por padrão não possuem ferramentas de privacidades já inclusos, é possível instalá las porém ainda deixam algumas coisas passar, como fingerprints, o navegador que irei apresentar já vem com o pacote todo incluso.

Tor: Open-source no qual anonimiza o usuário por meio da Rede Onion. Logo mais estudaremos a rede Onion em detalhes.

Vou deixar um parênteses aqui, tem algumas aplicações na web que proibem a rede Onion de acessar, então não precisa trocar totalmente de navegador, use o Tor para coisas importantes, e para casos convencionais utilize o firefox com as extensões já citadas.

15.Linux

Linux ao contrário do que muitos pensam, ele não é um sistema operacional, ele na verdade é o “miolo” do sistema operacional mais precisamente um KERNEL, e existem diversos sistemas operacionais que utilizam deste kernel de código aberto, é ai que entram as distribuições linux, distribuições essas que possuem propósitos diversos como o Kali Linux, distribuição focada para pentest, ou debian focado na estabilidade e no nosso caso Whonix e Tails Linux, distribuições focadas em anonimato e privacidade.

Antes de tudo vamos falar um pouco da história do linux, a história do linux remonta ao anos 60 quando existia-se um projeto ligado ao Bell Labs que na época pertencia a AT&T, esse projeto tratava-se sobre a criação de um sistema operacional de tempo compartilhado chamado Multics porém em 69 o Bell Labs saiu do projeto e foi criar o seu próprio no qual foi dado o nome de UNICS que sim é uma piada com o multics, sendo assim os dois cientistas da computação chamado Dennis Ritchie e Ken Thompson se juntaram para criar o sistema operacional e pode-se dizer que da mão desses 2 saiu da linguagem de programação C e o Unix, ou seja o C foi feito para o Unics e o Unics foi escrito em C, eles possuem essa relação simbiótica por quê o C foi criado devido a essa necessidade.

Sendo assim em 72 nasce-se o Unix (durante o desenvolvimento eles mudaram o nome para Unix), toda via na época a AT&T estava com um processo na justiça sobre uma questão relacionada a monopólio no mercado de telefonia, então eles não podiam vender o Unix por quê se eles começassem a vender o departamento de comércio ia em cima deles com o argumento de que, a AT&T tinha 60% do mercado de telefonia e ainda tá querendo entrar no mercado de sistemas operacionais…. Então a AT&T começou a distribuir o sistema de forma gratuita só que sem o suporte. Então pessoas, universidades e pesquisadores pegaram uma cópia do Unix, e dai em diante começou-se a ter os sistemas padrões Unix, por quê a AT&T enviava o código fonte e não compilado, dessa forma era possível fazer modificações no sistema. No final dos anos 70 a AT&T

foi dividida e agora ela poderia entrar no mercado de sistemas operacionais, porém ela preferiu cobrar de quem tinha pego as cópias… Não preciso nem dizer que isso deu um rolo do car%¨!# esse B.O se arrastou desde o final dos anos 70 até o fim dos anos 90 na justiça americana, no fim desse B.O foi estabelecido regras para um sistema operacional padrão Unix, regras essas que forma definidas pelo comitê POSIX que faz parte do IEEE. Durante esse B.O na justiça um hacker velho chamado Richard Stallman que trabalhava como pesquisador de IA no MIT. Ele vinha de uma tradição hacker de compartilhamento de códigos então um software de código aberto era material de estudo para ele, só que tem um porém, as empresas na época fechavam o código, não existia o open-source naquela época, e a gota d'água foi quando a Xerox doou uma impressora para o laboratório do MIT e tinha um problema, quando o papel embolava o indivíduo precisava sair da cadeira e ir lá pra ver a situação da impressora, dai o Stallman pensou "poxa eu poderia modificar o código para a impressora avisar quando o papel embolar", dai ele enviou um e-mail para a Xerox dizendo que gostaria de modificar o código fonte para um problema que estava acontecendo, e que inclusive assinaria um contrato dizendo que não iria divulgar o que tinha no código, porém sem sucesso, e foi no ano de 1983 que foi publicado o manifesto GNU que é Gnu not Unix é um acrônimo recursivo, onde a primeira letra da sigla é a própria sigla. Após isso Stallman propôs que iria desenvolver um sistema operacional padrão Unix completamente livre, e é ai que entra o Linus Torvalds que na época ganhou um intel i386 e aproveitando a grande máquina que ele tinha em mãos ele deu uma olhada no trabalho de um professor chamado Andrew Tanenbaum mais precisamente no Minix, que era um sistema operacional que usava o conceito de micro-kernel, ele era mais especifico para dar aulas, não era algo muito robusto e foi xeretando nesse sistema que o Linus chegou a conclusão de desenvolver um sistema operacional próprio, considerando o fato de que as datas são bem conflitantes em 1991, o Linus soltou a primeira versão do Kernel, só uma curiosidade sobre o nome, o kernel linux era para ser chamado de Freecx porém na universidade de Helsinki comentando com alguns amigos do Linus eles deram a ideia de ser Linux então esse foi o nome, já o lance do pinguim, é por quê pinguins é o animal que o Linus mais gosta e o nome do mascote é Tux.

OK mais…. Quais são as vantagens do Linux ?

Open-source

Seguro

Estável

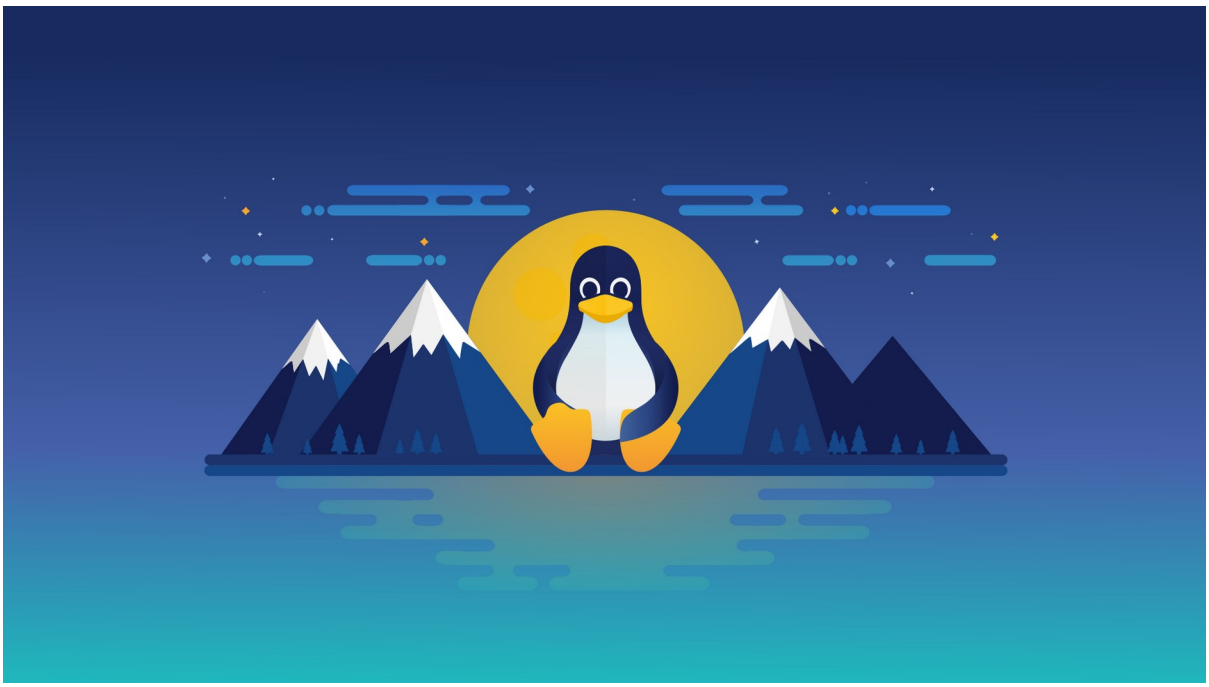
Gratuito

Amplamente utilizado em Servidores e embarcados (o mais comum SO de celular é o Android que dentro dele roda o Kernel Linux)

Comunidade muito ativa e unida

Compatibilidade com Hardwares

Leve (tão leve que algumas distros possuem o poder de ressuscitar computadores muito antigos.)

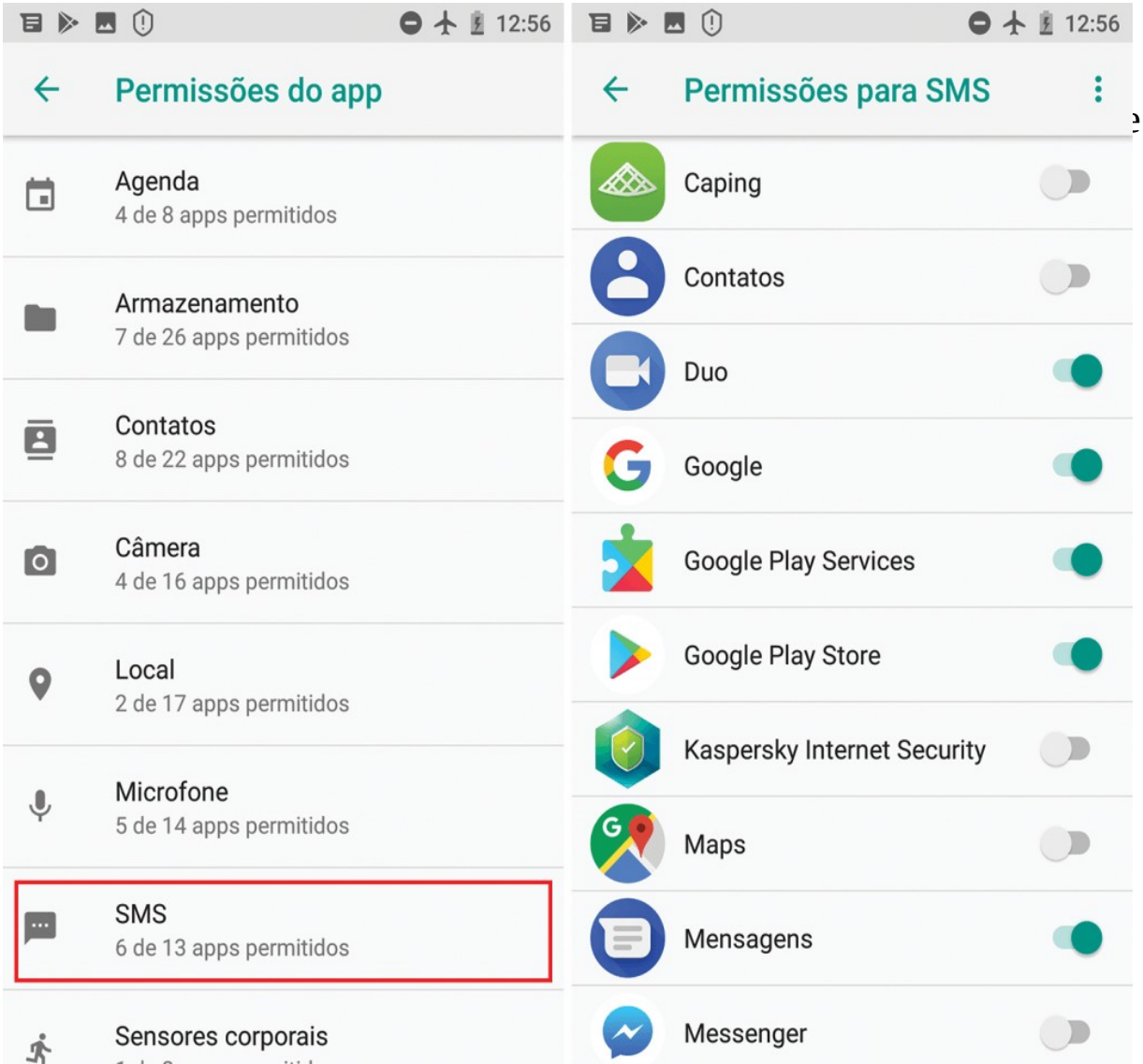


16.Privacidade em smartphones e citação a um notebook privado

Ok não vou repetir a ladainha já passada, evite Big Techs ao máximo.

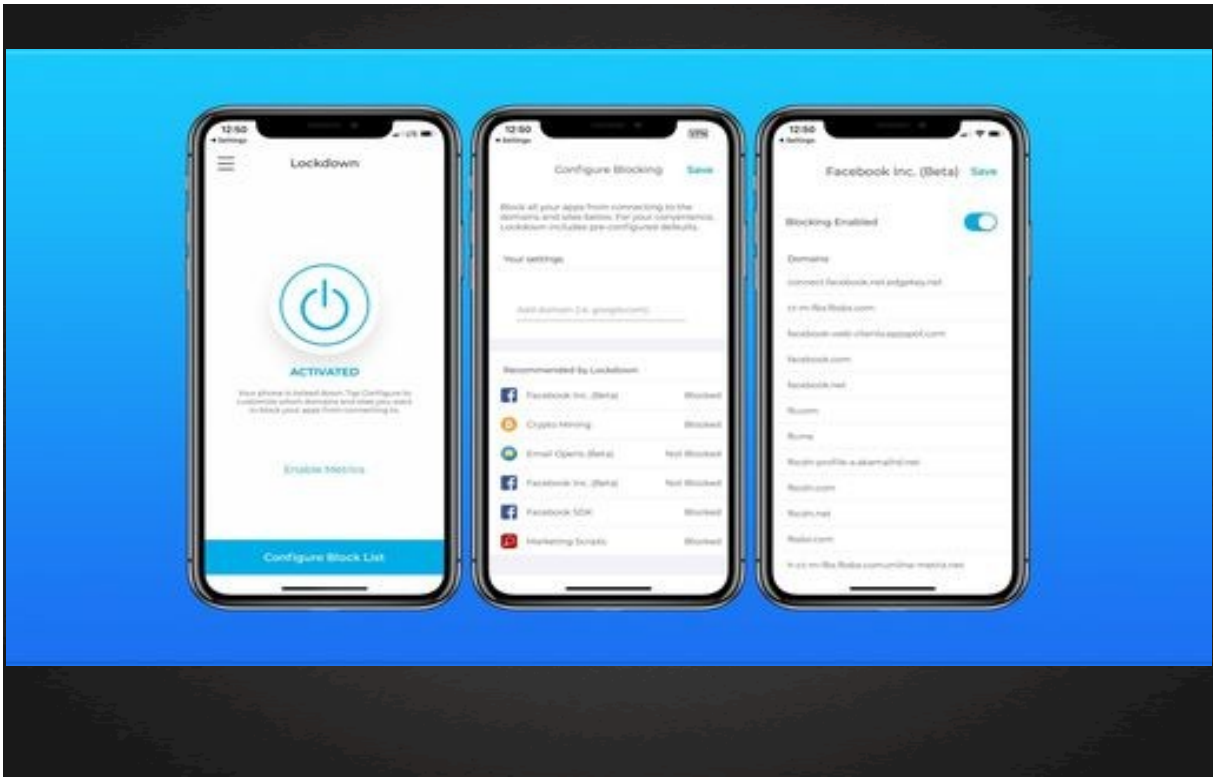
Sabendo disso vamos aos passos:

Primeiro, desative as permissões de apps, mais como assim ?, vou dar um exemplo, quando você vai nas configurações de permissões, um app de mensagem não precisa de acesso ao armazenamento (galeria e afins), localização, câmera (em alguns casos) e etc, sabendo disso filtre bem quais permissões você vai desativar, pois tem alguns apps que precisam de acesso a alguns recursos do smartphone, sendo assim navegue até a tela parecida com essa:



localização e GPS, e a verificação de WI-FI também.

Dois apps muito bons que atuam como se fosse um firewall para os outros apps são os Netguard (Android) e o Lockdown (Ios)



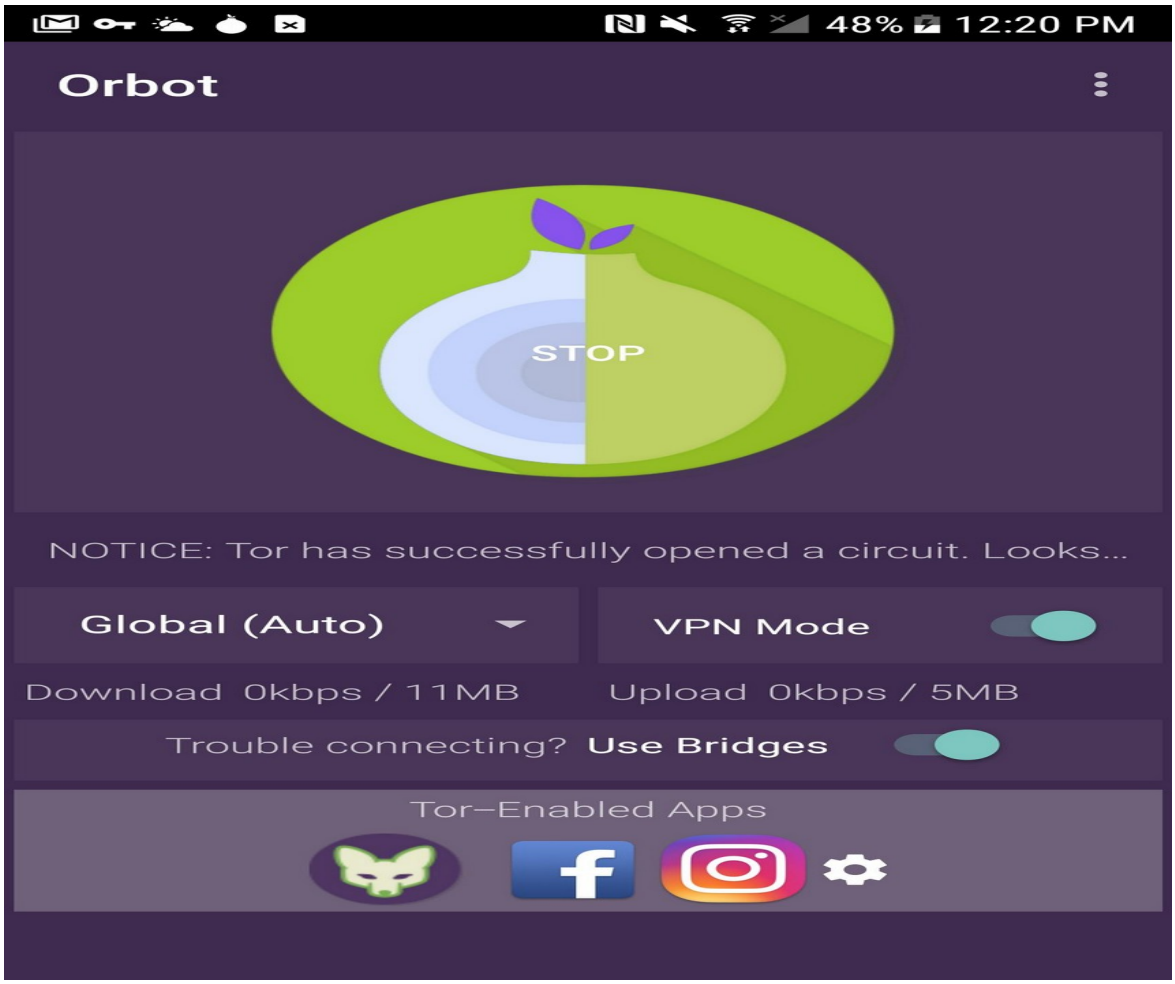
outra coisa, caso a versão do seu Android seja da 9.0 para cima, é possível configurar um DNS criptografado, neste site possui alguns DNS para colocar, vale dar uma olhada clicando aqui. Utilize PWAs e seja minimalista, ou seja não instale muitos apps, sobre os PWAs na verdade são versões de aplicativos que rodam com tecnologias da WEB, para mais detalhes veja esse vídeo clicando aqui.

Ao invés de usar o app do youtube para ver vídeos, utilize o Newpipe ele não só impede que o youtube colete seus dados como também possui vídeos sem anúncios, download e opção de assistir em segundo plano (para podcasts ou música).

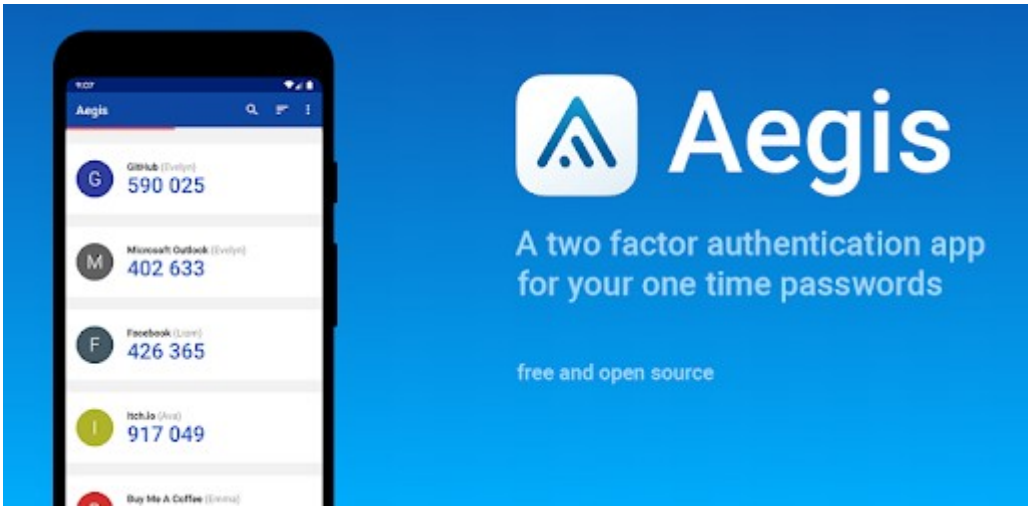
Também possui um similar ao newpipe para Desktop, no caso utilize freetupe, é um programa desktop multiplataforma que faz com que você assista ao youtube de maneira privada livre de coleta de dados.

Uma boa solução Open source e também alternativa ao google maps é o OpenStreetMap.

Caso queira rotear os pacotes pela rede Onion para aumentar o nível de privacidade, utilize Orbot.



Não preciso nem dizer que é totalmente recomendável você ativar a verificação em 2 fatores, mais para isso é preciso ter um aplicativo seguro, é obvio que você não vai usar os das big techs como google authenticator, sendo assim minhas duas recomendações são o andOTP e o Aegis.



Agora, depois de tudo que você leu até aqui, ainda precisa acessar redes sociais ou até mesmo o google, use um aplicativo chamado Webapps, ele funciona como se fosse um sandbox onde você acessa através de um navegador próprio, porém com total controle e também bloqueio de rastreadores

A partir de agora somente os paranoicos

Exclua as lojas de apps oficiais das big techs e opte por essas opções

F-droid, um repositório de aplicativos que é Open-source, quase todas as alternativas que já citamos aqui você encontrara lá.

AuroraStore, um front-end da play store caso precise de algum app que só tem na loja do google sem ser rastreado pelo mesmo.

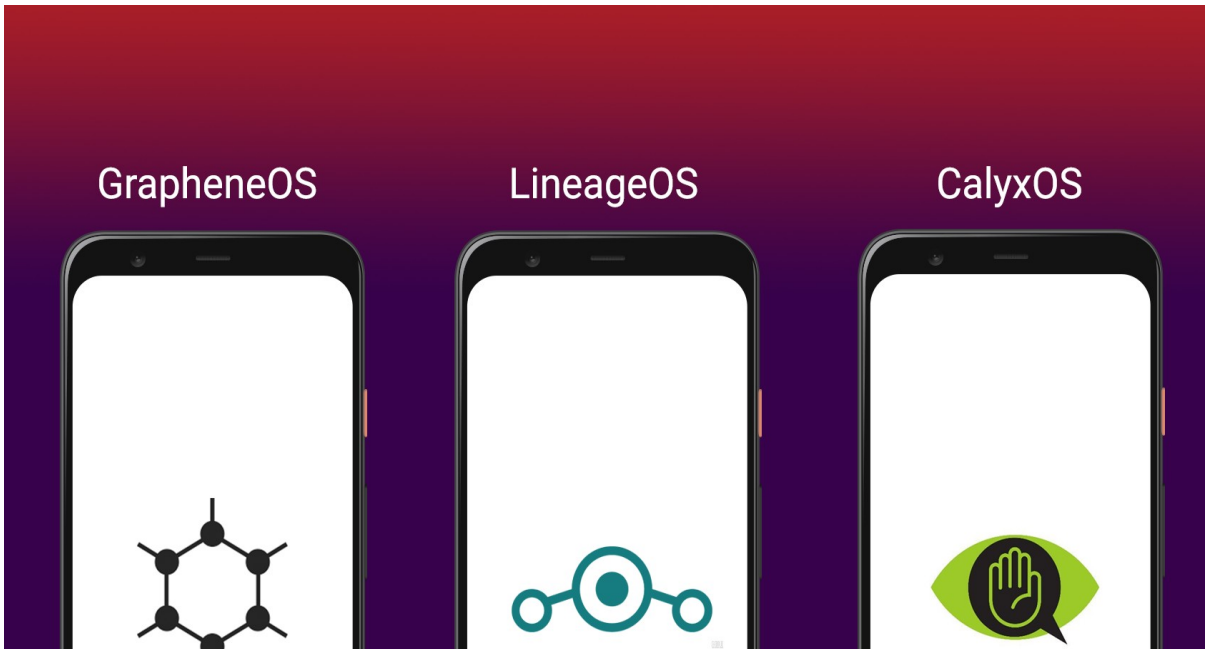
e olha, lamento informar, mas o android que vem no seu celular é lotado de rastreadores de diversas empresas, tanto do google como do facebook, netflix e etc, duvida ???, não precisa acreditar em mim, comece assistir a partir do minuto 13:56 desse vídeo que você vai entender oque eu estou falando…

é realmente lamentável e assustador.. porém tem uma solução, mude a ROM do seu aparelho, o que são ROMs ?? em outras palavras é o sistema operacional do seu aparelho, mudar de ROM significa mudar o sistema operacional do aparelho. É recomendável mudar para as seguintes ROMs

Lineage OS, Foco no controle e personalização do sistema e privacidade:

Graphene OS e Calyx OS, ambos projetados para privacidade por default porém, só são para os modelos Pixel 3 em diante.

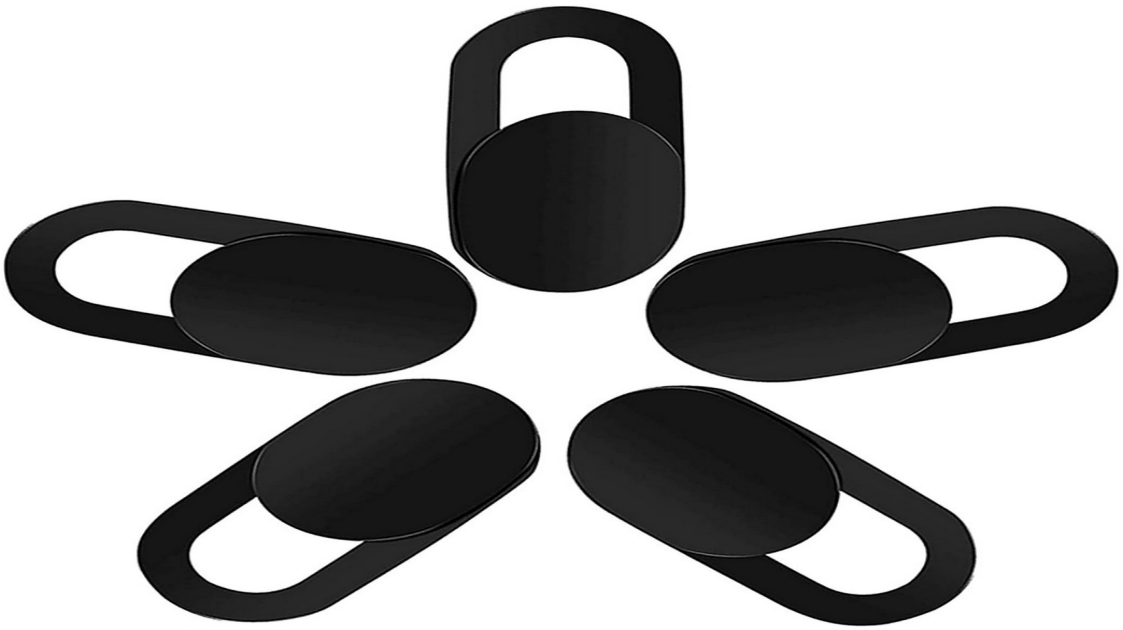
Como instalar o TWRP completo
Como instalar o LineageOS (Não instale o OpenGapps)
Como instalar GrapheneOS
Como instalar CalyxOS



A partir daqui, você liga o modo Michael Myers e sai distribuindo one-hit kill, porque só os psicopatas fazem isso…. E é claro, sou um deles….

No maior estilo Edward Snowden, retire o microfone do seu aparelho, você perde a garantia, porém tapa os ouvidos por completo de quem te rastreia.

Coloque uma fita escura ou compre tampões para as câmeras de seus aparelhos como TV, Tablet e celular, dessa forma também tampando os olhos deles.



Uma recomendação, existem celulares que já vem com linux e outras ferramentas de privacidade por built-in tais como Librem 5 da purism que não só vem com uma distro linux chamada PureOS e também vem com desativação de Gateway de WI-FI e Bluetooth, Microfone e Modem diretamente no hardware.

Vídeo a apresentação do celular

17.Transações financeiras com privacidade

As transações financeiras são um tanto quanto questionáveis e ela possui 2 problemas, o primeiro é que você precisa revelar sua identidade, a segunda é que é um serviço centralizado e é necessário diversos intermediadores. Sendo assim a solução é mudar para as criptomoedas que possuem não só um funcionamento como uma filosofia totalmente diferente do sistema padrão de transações bancárias.

Mais antes de tudo, o que é uma moeda ?. Bem, moedas são facilitadores de trocas e ela surge devido a necessidade de troca e precificação de um produto, para a precificação acontecer é necessário a confiança e a crença de que realmente é algo valioso.

Uma moeda precisa ter e ser:

- Aceita por todos
- Unidades limitadas (escasso)
- Fácil de usar
- Fungível, ou seja todas as moedas possuem o mesmo poder aquisitivo.
- Reserva de valor (de acordo com o tempo o preço aumenta)

O bitcoin é uma criptomoeda que foi criada por satoshi nakamoto, um usuário anônimo da internet, como curiosidade: ninguém sabe quem ele é até hoje, e muito menos se foi apenas ele ou um grupo de pessoas que criou o bitcoin, sabe-se que ele tinha um alto conhecimento em criptografia, pois o bitcoin gira em torno disso.

Falar de bitcoin é falar de blockchain, vamos entender o que é, podemos dizer que o blockchain é como se fosse um big data ou um banco de dados colossal que qualquer um pode alimentá-lo seguindo regras estabelecidas pelo protocolo, esse banco de dados armazena as transações que cada usuário fez, nessa transação inclui data e hora, para quem enviou e de onde veio, e detalhe é possível baixar os dados de transações de todas as transações da blockchain, ou seja não tem como ter censura pois é um armazenamento descentralizado, agora de maneira análoga vamos supor que um bloquinho de lego é uma transação quando você enviar esse bloquinho, ele ficará disponível para os computadores da rede verificarem a transação para saber se é legitima ou não, se você tem a quantia de bitcoin aceita e etc, quando confirmada esse bloquinho se junta a outros bloquinhos na blockchain no qual fica disponível para mineração, ao minerar

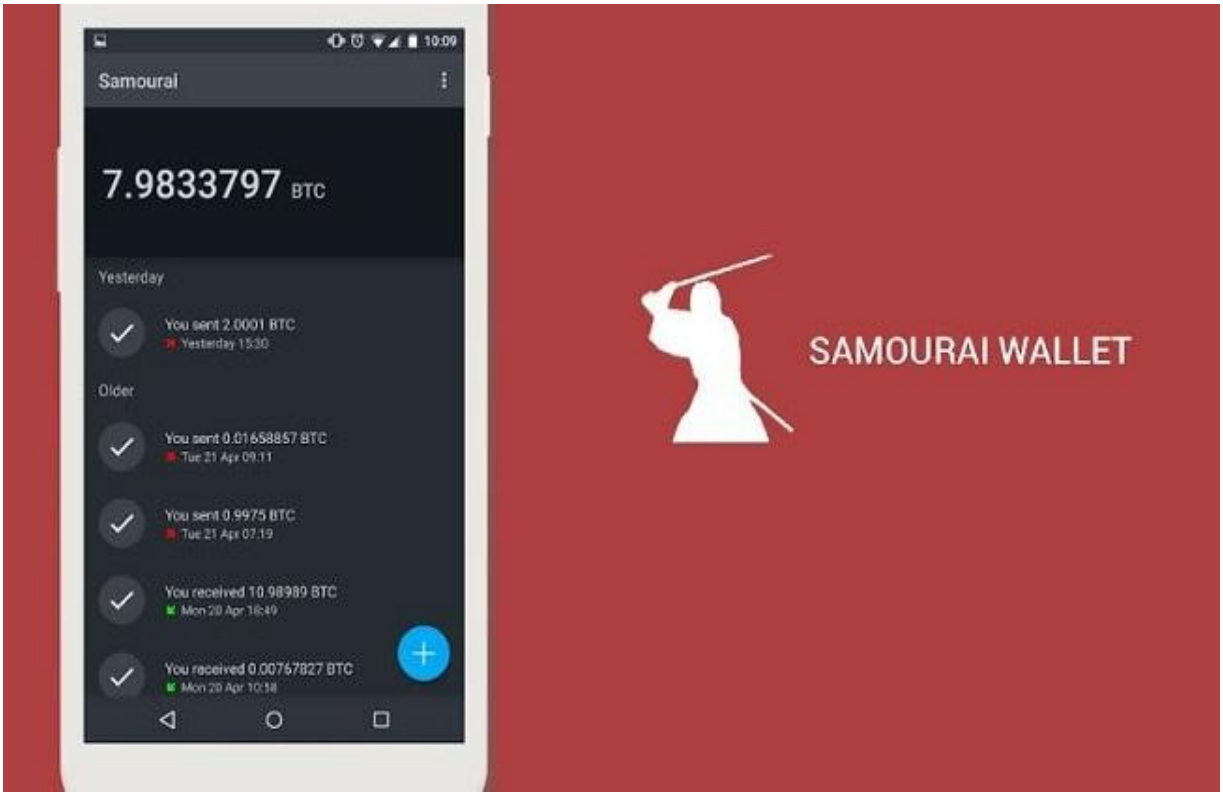
esse bloquinho ele recebe um número de identificação com base no número passado e por ai em diante, ao receber esse número de identificação significa que a transação foi confirmada e assim entra no registro da blockchain. Os mineradores fazem cálculos matemáticos complexos que exigem processamento do computador, quando o minerador termina de numerar a transação ele não só encaminha a transação para a blockchain como também recebe um valor em bitcoin como recompensa. Esse número dde identificação da a segurança da blockchain para ser imutável pois alguém malicioso para falsificar algum tipo de operação da blockchain teria que alterar todos os outros registros a partir do número de identificação no qual ele quer falsificar.

E então, entramos no Bitcoin, o Bitcoin utiliza os mesmos conceitos de moeda pois tem unidades limitadas, quando for fabricado 21 milhões de bitcoin a “fabricação” será cancelada, dessa forma deixando a moeda escassa, é relativamente fácil de usar, basta de usar a quantidade e para qual carteira precisa enviar ou simplesmente escanear um QR code. É fungível, conforme o tempo aumenta o bitcoin valoriza cada vez mais e o preço aumenta, e conforme os países aprovam o uso de bitcoins ela vai sendo aceita.

Uma boa maneira de adquirir bitcoins é pela Bisq, uma exchange descentralizada que funciona sobre a rede Tor onde seus dados são visíveis para outra parte e ficam armazenados em seu computador, negociação entre vendedor-comprador sem um servidor central.

Melhor carteira bitcoin:

Samourai, é uma carteira que utiliza payjoin uma técnica que mistura diferentes transações de bitcoin sem revelar o montante exato transacional. E também tem a vantagem de se conectar a rede bitcoin usando a rede Tor.



18.Deep Web

Em fim chegamos a tão comentada Deep web, nesse capitulo você irá ver onde vive, oque come e por onde anda a tão famosa Deep web.

A deep web é tudo aquilo que não é indexado por motores de buscas ou aquilo que não é acessível tradicionalmente durante uma navegação. Isso significa que por exemplo, vamos supor que joãozinho está comprando um bilhete para o cinema, então ele seleciona a cadeira b42, sendo assim essa cadeira será reservada e o sistema irá contabilizar que a cadeira b42 é de joãozinho, se por algum motivo eu conseguir ter acesso na versão antes disso acontecer, ou seja quando a cadeira b42 ainda estava disponível, pode

ser considerado deep web. Isso inclui painéis administrativos, bancos de dados e etc. Essa seria a tradução literal do significado porém, como ela é comumente conhecida, deep web é um sistema capaz de fornecer anonimato na internet.

A Darkweb costuma ser a parte ilegal da deep web, porém não se assuste, assim como tudo na vida tem algo ruim, na própria internet a fora, existe um lado negro e não é deep web sendo assim com a própria não iria ser diferente. Porém é uma afirmação totalmente equivocada e no mínimo tola da parte de alguém que diz que a deep web só possui coisas ilegais, a deep web é neutra pois ela fornece anonimato e isso pode ser usado tanto para o mal quanto para o bem.

A deep web possui algumas redes ocultas, dentre elas o TOR ou Onion na qual é mais conhecida, falaremos dela logo mais, porém também possui outras, tais como a freenet, i2p e etc, ambas funcionam de formas diferentes e cada uma tem sua vantagem e desvantagem.

Agora, o que você encontra na deep web ?, começando com a parte legal, porém já digo de ante mão, tudo que você encontra na surface, você encontra na deep web, o algo mais é que na verdade você pode encontrar serviços que precisem de anonimato:

sites de notícias, que provavelmente seriam censurados em seus países.

Fóruns de discussão não necessariamente ilegal

Pornografia legal

Gore

Páginas de cultos ou seitas

Plataformas de denuncias

Diretórios de links

Repositórios de softwares

Cassinos

Bibliotecas

Instituições financeiras

Venda de Criptomoedas

Venda de produtos

Enigmas

Site de perguntas e respostas

Chat de bate papo e e-mail

Streaming de áudio

Agora a parte ilegal:

Pornografia ilegal, como estupro ou pedofilia

Financiamento de organizações criminosas

Manuais para fabricação de armamentos e bombas

Manuais para cometer crimes (estupro, assassinato e etc)

Tortura ou assassinato sob encomenda (ainda assim a grande maioria é golpe)

Venda de informações bancárias e documentos falsos

Promoção e recrutamento de atividades terroristas

Venda de drogas e armas (a grande maioria é scam)

Tráfico de órgãos

Venda de informações privilegiadas

Venda de 0-day exploits e serviços de hacking

Venda de medicamento sem receita (também tem muito golpe)

Pirataria

Exposição de dados pessoais

Agora você com certeza não vai encontrar na deep web:

Segredos governamentais

Informações aprofundadas de um determinado assunto

Qualquer tipo de conteúdo sobrenatural ou fantástico

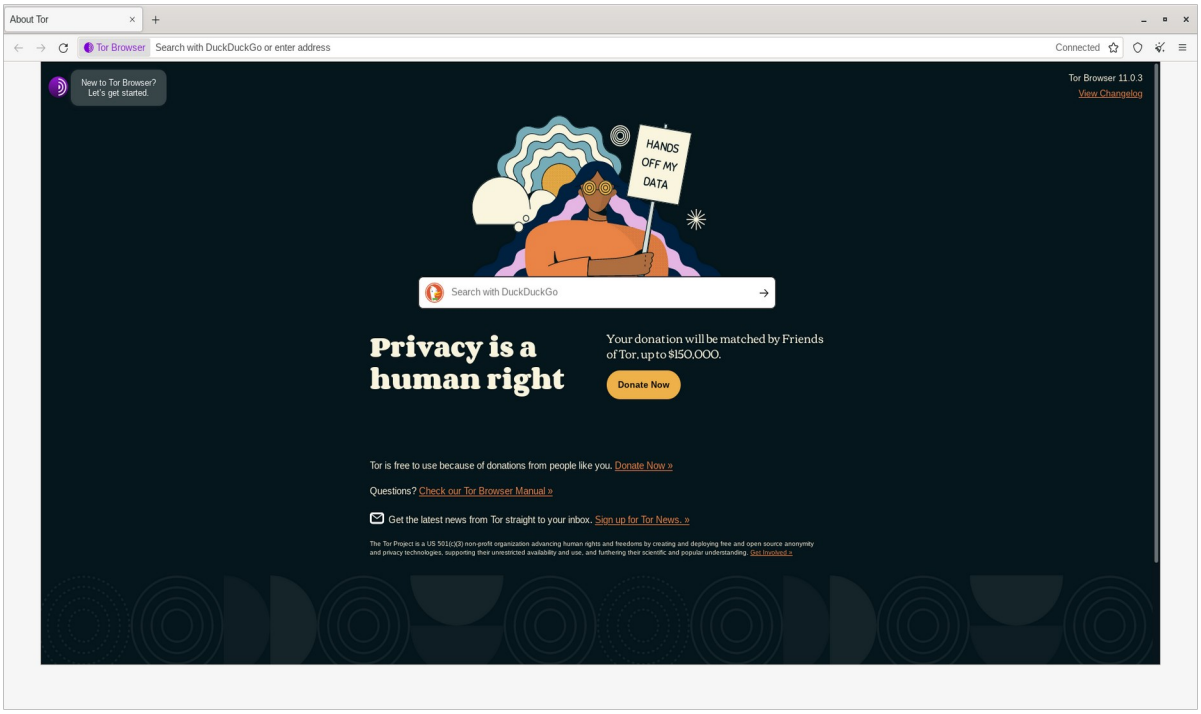
SEU PC NÃO VAI PIFAR SE VOCÊ ENTRAR NA DEEP WEB

E A PM NÃO VAI BATER NA SUA PORTA (entrar na deep web não é crime, crime depende da coisa que você for fazer lá).

E PELO AMOR DE DEUS, DEEP WEB NÃO TEM CAMADAS, NÃO EXISTE MARIANAS WEB, NEM ND DO TIPO, oque existe são camadas de criptografia para a sua proteção.

19.Rede Onion(ou Rede Tor)

A história da rede Onion nos leva para a década de noventa, quando a Office of naval research e a DARPA estavam querendo criar uma rede de anonimato na qual eles pudessem usar, essa rede recebeu o nome de “o roteamento cebola” ou *The Onion Routing*(TOR), para começo de conversa essa rede não era para ser aberta igual é hoje, porém os criadores tiveram que abrir por quê se não, ia ficar obvio que naquela rede só ia ter agentes do governo usando, sendo assim fizeram a rede e liberaram para o público, tanto que hoje em dia mais de 1 milhão de pessoas acessam o tor, também tem o fato de que o tor é código aberto, ele é escrito em C (Linguagem de programação), existem indícios de que o governo está tentando quebrar a rede através do monitoramento, porém isso é muito custoso, e em uma probabilidade muito pequena devido ao fato de ser muito bem projetada e segura.

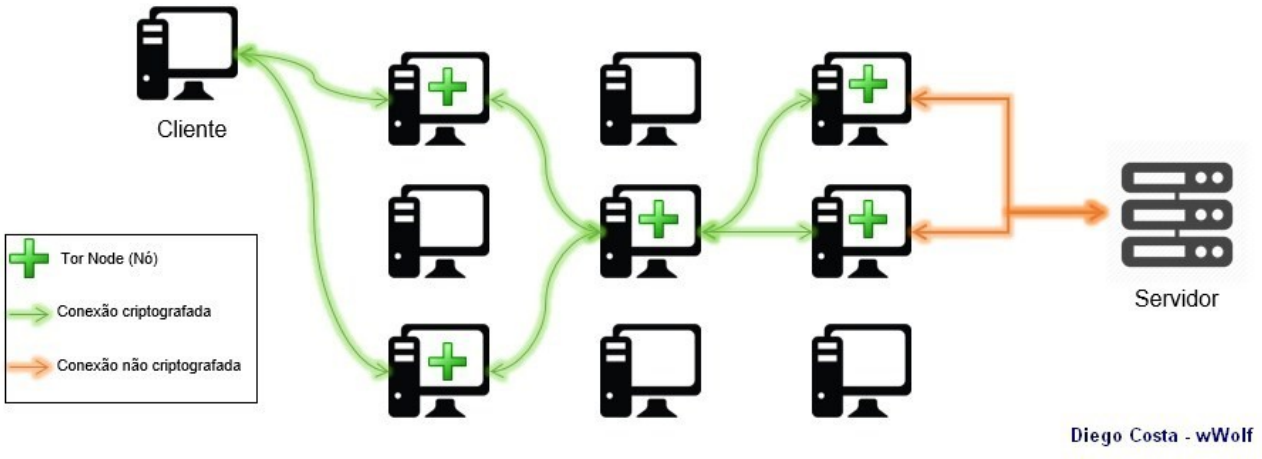


Agora como a rede Onion funciona, antes tudo a rede Onion é um protocolo (um protocolo é um programa que segue um conjunto de regras bem definidas) no qual você pode instalar em uma máquina linux para poder operar Relays da rede, o client para acessar o protocolo é o Tor Browser no qual é um fork (é meio que uma cópia, só que no mundo do open-source é permitido) do navegador Firefox com algumas modificações para privacidade, por exemplo o Tor browser não tem telemetria já o Firefox tem.

Sabendo disso o protocolo funciona da seguinte maneira, para começo o client negocia uma lista de relays e chaves criptográficas para um trajeto no qual você irá percorrer, após isso, ele salta por 3 nós de rede que são chamados de relays, a cada salto o seu endereço de ip é mudado e seus metadados da requisição são ocultados, o primeiro relay é chamado de entry guard pois ele sabe quem você é mais não sabe para onde vai, o segundo se chama middle relay, ele não sabe quem você é e também não sabe para onde vai, e o último que é chamado de exit relay sabe para onde vai mais não sabe de onde veio, ou seja o caminho percorrido para acessar é o seguinte: entry guard, middle relay e exit relay, dessa forma nem mesmo o seu ISP sabe para onde vai, ele só sabe que você está acessando a rede Tor, agora vamos supor que eu quero entrar em um site na rede Onion e envio uma requisição, essa requisição vai

receber 3 camadas de criptografia (isso sem usar o SSL/TLS por quê ai ficária 4, tem sites na deep web que tem o certificado), sendo assim quando você envia a requisição o entry guard recebe seu pacote e ele possui a chave para descriptografar a primeira camada de encriptação, sendo assim o mesmo o faz e joga para o middle relay, o middle relay possui a chave da segunda camada, sendo assim decripta e joga para o exit relay, o mesmo tem a última chave para a terceira camada, ao decriptar ele envia a requisição para o site desejado na onion ou até mesmo na web comum (sim é possível usar o Tor para acessar a web comum, reduz um pouco o anonimato e tem algumas complicações, você resolve mais captchas do que o normal ou então nem entra no site pois tem alguns sites que proíbem a requisição Tor) dessa forma mantendo o seu anonimato durante a requisição, é um pouco lento…. Porém é um preço pelo anonimato, nem sempre privacidade e anonimato vai estar atrelado a conveniência e facilidade.

Também é possível ocultar o seu acesso ao Tor do seu ISP(isso serve para se caso você more em um país onde o Tor é proibido, como a Rússia), basta configurar uma bridge, o Tor já deixa disponível 3 por padrão, porém você pode configurar a sua própria caso tenha conhecimento para isso.



sobre os links .onion (que são os links usados para acessar páginas web dentro do Tor Browser) são endereços padronizados pela ICANN que na V2 do link (atualmente já descontinuado) possui 16

Caracteres mais o .onion no final, exemplo: http://3g2upl4pq6kufc4m.onion/ , já hoje em dia usa-se o V3 no qual possui 56 caracteres mais o .onion, exemplo: http://cyberfe3gvh7cvq2nhuqtaghjxebhcnqafnfvalwvq6mxrinep7m7xqd.onion

o link V3 possui uma chave pública ed25519 mais um hash SHA1 de uma chave pública RSA1024, o principal motivo dessa migração foi para maior segurança, com o V2 a rede Tor possuía uma vulnerabilidade na qual era possível coletar e sondar endereços onion via HSDir, não vou entrar em detalhes mais técnicos aqui, porém caso tenha curiosidade esse link explica por completo as mudanças do onion V3, clique aqui

o Tor garante seu anonimato e privacidade por esses motivos:

* Esconde seu IP e localização, por quê ele efetua 3 saltos para relays aleatórios espalhados pelo mundo

* Esconde seus metadados pois ele não armazena cookies, cache e histórico de navegação.

* Evita mecanismos de rastreio, pois a cada site acessado, ele refaz o trajeto.

* Aos olhos de um observador, todos os usuários são iguais.

* Os dados transmitidos são encriptados desde o primeiro até o ultimo relay.

* Caso sua identidade não seja descoberta, os dados enviados do ultimo relay não podem ser associados a você.

Situações na qual o Tor não garante seu anonimato:

* Personalizar muito o navegador e instalar várias extensões (conceito de se misturar na multidão, caso você use algo muito diferente ou chamativo você fica destacado em meio a ela.)

* Sistema operacional comprometido com malware

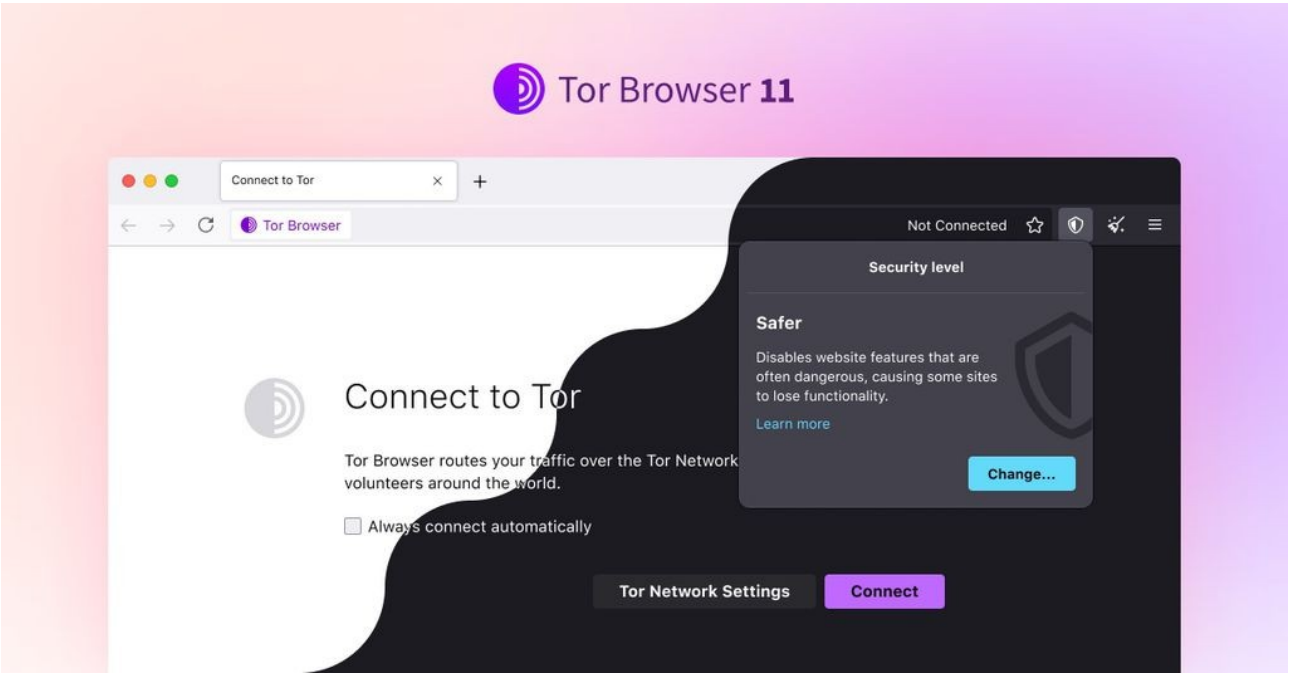
* Logar em sites, efetuar compras ou preencher formulários com informações que levem até você e usar redes sociais como facebook.

Algumas falhas do Tor Browser em si:

* O navegador Tor é um fork do firefox, sendo assim é suscetível a vulnerabilidades de segurança.

* O governo americano é o maior financiador da rede Tor e pode interferir no desenvolvimento do projeto.

Embora o governo possa intervir em alguns aspectos no Tor, eles não podem quebrá-lo pois os mesmos usam a rede.



20.Virtualização

Antes vamos entender oque é um Sistema operacional, em poucas palavras é um programa que gerencia os recursos de hardware do seu pc, pensa assim, tem você o sistema operacional e o hardware do pc, o sistema operacional fica ali no meio, recebendo seus comandos e convertendo para informações que o hardware interpreta executa.

No contexto de virtualização, um computador físico é chamado de hospedeiro.

Máquinas virtuais é um programa que reserva recursos do hardware para uso próprio e os executa em cima da máquina hospedeiro por meio de um software.

Em outras palavras caso você use linux, você não precisa comprar outro computador para usar o windows, basta você subir uma máquina virtual com o sistema operacional e pronto, você está usando o windows pelo linux.

Qual a diferença entre containers e máquina virtual ?, bem um container não precisa de um kernel operando pois o mesmo usa o kernel que a máquina já possui, por exemplo, se eu subir um container linux de uma máquina windows, ele vai usar o kernel do windows, já na virtualização, isso não acontece pois é instalado um sistema operacional sobre o hospedeiro, dessa forma utilizando um kernel separado.

Como você já deve imaginar, máquinas virtuais não criam hardware, ela utiliza do hardware disponível da máquina (é possível regular a quantidade de hardware que ela vai usar, por exemplo se você tem 8 gb de ram, pode-se regular para a máquina virtual usar apenas 2 gb, dessa forma fica 2 gb para a máquian virtual e 6gb para a máquina hospedeira), pode-se criar quantas máquinas virtuais quiser, desde que você hardware o suficiente para tal feito.

Para se criar uma máquina virtual utiliza-se de um software chamado de Hypervisor, eu recomendo o virtual box, porém não é o único, recomendamos que faça a sua própria analise.

Estrutura de uma máquina virtual:

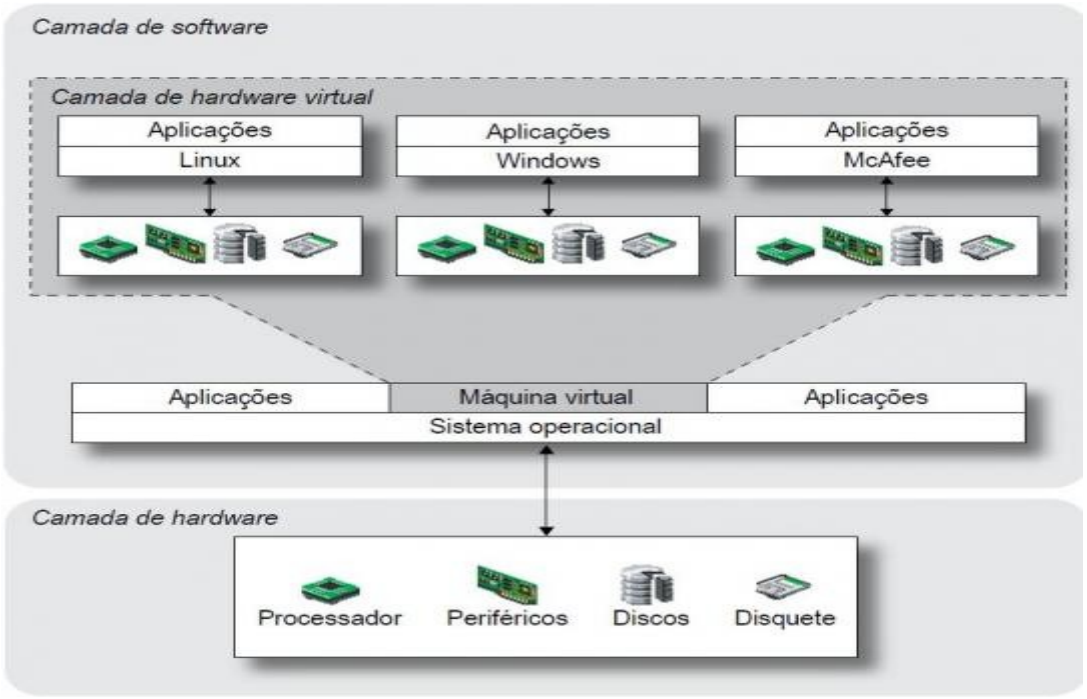
1- Infraestrutura: Hardware e máquina hospedeira

2- Sistema operacional da máquina hospedeira: Linux, windows, Mac e etc.

3- Hypervisor: VirtualBox

4- Sistema operacional virtualizado

5- Aplicações da virtualização (a máquina virtualizada possui suas própria bibliotecas e arquivos de carregamento).



Sabendo de tudo isso, deu para perceber que uma máquina virtual embora rode sobre um hospedeiro, é totalmente isolada do mesmo, dessa forma você pode fazer oque quiser dentro da máquina virtual sem se preocupar com a máquina hospedeira (existem técnicas que

by-passam a máquina virtual e fazem o pívoting para dentro da máquina hospedeira porém não é comum, então pode ficar tranquilo)

Por quê acessar a deep web por uma máquina virtual ?

* Oculta informações de hardware, por não ser algo dedicado na máquina virtual aparecerá apenas a quantidade que você reservou para a mesma.

* Caso seja infectado por malware ou algo do tipo, seu hospedeiro está protegido, pois tem um obstaculo da máquina virtual para o malware superar, para resolver isso basta excluir a vm e subir outra e pronto seu problema com malware acabou.

* Você pode criptografar (super recomendado) facilmente a imagem da máquina virtual.

21.Whonix

Whonix é uma distribuição linux baseado na Debian, na qual é especificamente projetada pra rodar na máquina virtual, o Whonix tunela todo o seu tráfego gerado pela rede Tor ou seja é um SO anonimo.

Whonix funciona em duas máquinas virtuais, Whonix-Workstation e Whonix-Gateway, o Workstation é aonde você usa o sistema operacional, e o Gateway é o responsável por redirecionar todo o tráfego pela rede Tor.
Vantagens do Whonix:

Live mode: o estado do sistema é apagado após do desligamento pois o mesmo é carregado na memória RAM, isso não só impede que malwares criem persistência (é uma técnica usada por malwares para caso o usuário desligue ou desinstale o malware, ele ainda continue no computador da vítima) como também melhora a privacidade do usuário.

Keystroke Anonymization: as teclas podem ser usadas para rastrear usuários, sabendo disso o whonix tem um software chamado kloak que muda o padrão de digitação do usuário.

Sdwdate: o relógio e a data são definidos através de um servidor da rede Onion criptografado.

Entropia aprimorada: o Whonix não confia na CPU, pensando nisso o Whonix usa programas de geradores de números aleatórios no sistema, melhorando a encriptação da rede Tor.

Autoproteção do kernel: o Whonix usa uma configuração de endurecimento de kernel dessa forma melhorando a segurança do usuário.

Site do whonix

Como instalar o Whonix na máquina virtual aqui.

22.Tails

Se você gostou do whonix, você vai amar o Tails, por quê além de tunelar todo o trafego pela rede Tor é também um sistema operacional amnésico sou seja anti-forense que é também usado por um pendrive bootavel.

Tails é uma distribuição linux segura e privada baseada na Debian, ganhou popularidade quando Edward Snowden disse que confiava no Tails na época em que ele estava pra vazar os arquivos da NSA.

O Tails diferente de um sistema operacional convencional que armazena seus programas em uma memória volátil como Hds e SSDs, o Tails é projetado para rodar em memória flash ou seja não volátil (volatilidade na computação quer dizer que um conteúdo se perde de uma memória ao ser desconectada ou desligada), Tails é um acrônimo para *The Amnesic Incognito Live System*, na prática caso você perca o pendrive com o Tails, não terá com o que se preocupar pois caso faça uma busca, apenas será encontrado arquivos de carregamento do sistema e nada mais, não haverá rastros ou qualquer arquivos que sejam associados a você.

Vantagens do Tails:

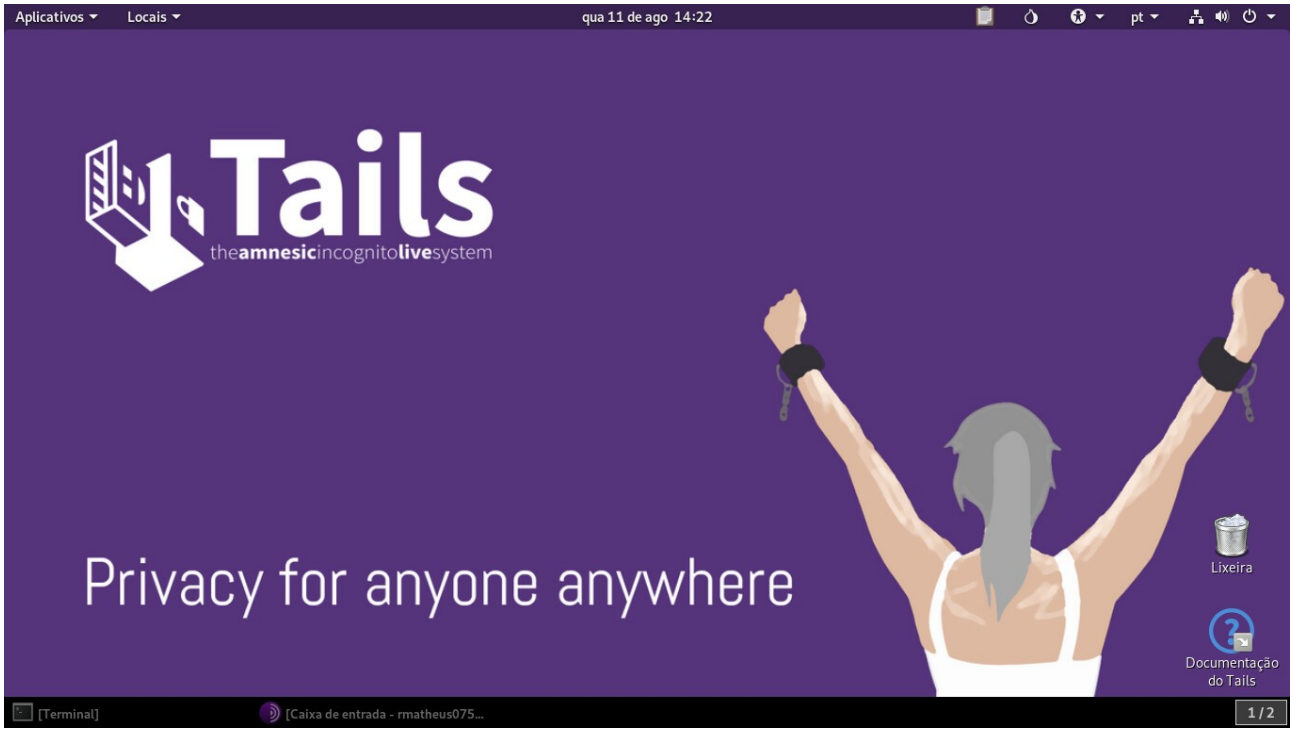
* Falsificar o endereço MAC (MAC é um tipo de endereçamento físico no qual serve para identificar o fabricante do aparelho mais um identificamento único, não vou entrar em detalhes técnicos aqui, caso tenha curiosidade clique aqui)

* Configurações de segurança tais como AppArmor (similar ao Whonix)

* É bem leve

* Mecanismos de proteção contra diversos ataques forenses
* Suporte a criptografia de dispositivo

Criando um pendrive bootavel com tails



23.Considerações finais

Então estamos chegando ao fim desse pdf, com ele você aprendeu muita coisa sobre anonimato e privacidade na web, porém tenho algumas considerações, primeiro é que não siga esse pdf como regra, eu tentei ampliar seus horizontes sobre anonimato e privacidade na web, eu tentei colocar na sua cabeça que anonimato não é tão simples, chega a ser um estilo de vida se for parar pra pensar, largar big techs e se tornar anonimo tem que fazer parte do seu dia a dia, tanto que hoje em dia algumas soluções de privacidade vem junto com usabilidade tais como Tutanota e Protonmail que são serviços de e-mails seguros e privados ou então os mensageiros instantâneos como o Briar e o signal que são quase iguais aos whatsapp só que mais anônimos e seguros e então por ai vai, porém quando se passa para o anonimato pesado, papo de irrastreável fica algo mais “menos usável” então isso serve para caso você precise de um anonimato a mais, como se você for fazer uma denúncia (na deep web tem muitos locais de denúncia) e por ai vai, porém todas as ferramentas de anonimato não substituem o bom-senso do usuário então as mesmas regras que você segue na web comum também devem ser seguidas no anonimato algo tipo não clicar em links estranhos, não baixar coisas sem conhecimento, mexer apenas em

coisas que você sabe e por ai vai. Sem falar que também tem o fato de que a deep web é bem mais segura que a própria surface diga-se de passagem você deve ter muito mais cuidado com a surface pois a chance de você ser rastreado ou pegar um malware é bem mais alta do que na deep web tirando o lance do rastreamento a deep we também possui malwares. É basicamente isso, sendo assim muito obrigado por ter lido até aqui e até mais =D.

Cursos e Materiais usados:

Sobrevivencialismo digital (curso)
Cyberdef (Canal)
PrivacyMap (Canal)
Techlore (Canal Gringo)

Privacytools (site que disponibiliza alternativas anonimas)

Caso queira contribuir para a rede TOR (além de ela fornecer um sistema de doação é possível operar Entry Guards, middle relays e exit nodes (diga-se de passagem não recomendo operar exit nodes se você não tiver conhecimento))

guia para a operação de um relay