



ANONIMATO E  
**DEEP WEB**

0 -

# INTRODUÇÃO E APRESENTAÇÃO



ANONIMATO E  
**DEEP WEB**

# Apresentação do curso

Bem vindos!

Esse é um curso sobre **privacidade, anonimato e Deep Web**.

O que são cada uma dessas coisas?



ANONIMATO E  
**DEEP WEB**

# Apresentação do curso

**Privacidade:** é o direito à reserva de informações pessoais e da própria vida pessoal.

**Anonimato:** é a qualidade ou condição do que é anônimo, isto é, sem nome.



ANONIMATO E  
**DEEP WEB**

# Apresentação do curso

**Privacidade:** é o direito à reserva de informações pessoais e da própria vida pessoal.

*Em nosso contexto, privacidade diz respeito a realizar ações na internet de forma a não revelar detalhes dessas ações à terceiros.*

**Anonimato:** é a qualidade ou condição do que é anônimo, isto é, sem nome.

*E anonimato diz respeito a realizar ações na internet sem revelar que nós somos os responsáveis por realiza-las.*



ANONIMATO E  
**DEEP WEB**

# Apresentação do curso

Por exemplo:

*Eu fecho a porta quando vou ao banheiro, pois quero privacidade.*

*Eu oculto meu nome ao denunciar atividades criminosas, pois quero anonimato.*



ANONIMATO E  
**DEEP WEB**

# Apresentação do curso

“Somente criminosos têm algo a esconder”



ANONIMATO E  
**DEEP WEB**

# Apresentação do curso

“Somente criminosos têm algo a esconder.”

**MITO**



ANONIMATO E  
**DEEP WEB**

# Apresentação do curso

“Somente criminosos têm algo a esconder.”

**MITO**

No mundo em que vivemos, organizações, atacantes e o governo têm interesse no que fazemos na internet. E a escolha do que essas entidades podem ou não possuir deve ser nossa!





ANONIMATO E  
**DEEP WEB**

# Apresentação do curso

“Somente criminosos têm algo a esconder.”

**MITO**

No mundo em que vivemos, organizações, atacantes e o governo têm interesse no que fazemos na internet. E a escolha do que essas entidades podem ou não possuir deve ser nossa!

O objetivo principal é a privacidade. Porém, as vezes, não conseguimos “fechar a porta do banheiro”. Então, é interessante que, ao menos, não saibam que somos nós “a usar o dito banheiro”. É aí que entra o anonimato.



ANONIMATO E  
**DEEP WEB**

# Apresentação do curso

E a Deep Web?

A Deep Web pode ser definida como o conjunto de sistemas que fazem parte da rede mundial de computadores e que fornecem anonimato e descentralização ao usuário.

Além de objeto de muita curiosidade, ela está intimamente relacionada com anonimato e privacidade, e pode ser uma ferramenta útil para pessoas que precisam desses fatores.



ANONIMATO E  
**DEEP WEB**

# Apresentação do curso

O que veremos neste curso?

**Módulo 1 – Privacidade:** conheceremos, em vídeos curtos (cerca de 4 minutos), ferramentas de privacidade.

**Módulo 2 – Redes ocultas:** aprenderemos, na teoria, como a Deep Web funciona.

**Módulo 3 – Anonimato:** veremos diversas formas de usar o Tor para se obter anonimato em vários níveis.

**Módulo 4 – A porta de entrada:** conheceremos seis redes da Deep Web.

Bons estudos!

# 1 - PRIVACIDADE

# O que queremos proteger?



ANONIMATO E  
**DEEP WEB**

# O que queremos proteger?

Antes de prosseguirmos, cabe a questão: o que exatamente queremos ocultar na Internet?



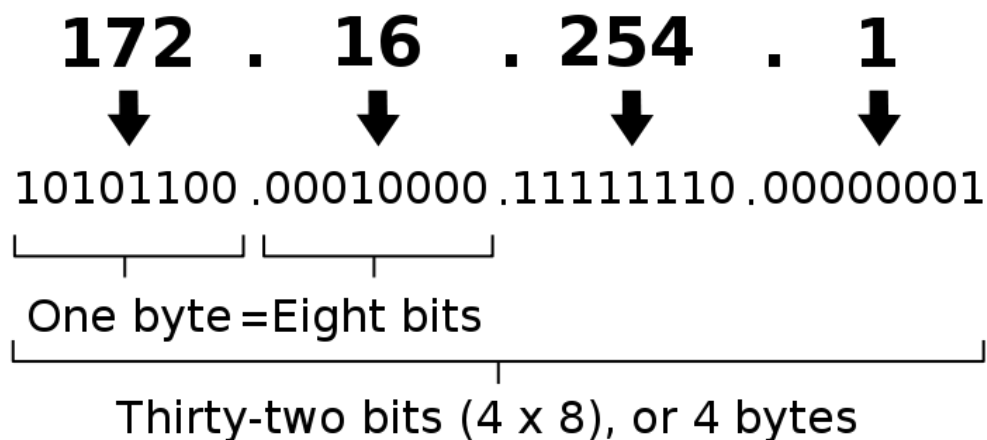
ANONIMATO E  
**DEEP WEB**

# O que queremos proteger?

## O endereço de IP

O endereço de IP é um número que identifica uma conexão de Internet na rede. Ele é geralmente compartilhado por todos os computadores que usam uma mesma conexão.

An IPv4 address (dotted-decimal notation)





ANONIMATO E  
**DEEP WEB**

# O que queremos proteger?

## O endereço de IP

Ele permite:

- Saber a cidade ou região na qual a conexão está.
- Saber o histórico de torrents baixados e semeados na conexão.
- Saber o provedor de internet da conexão.

Ele não permite:

- Invasões partindo do número de IP.
- Localização exata da conexão (latitude e longitude).

Pois é um protocolo público!





ANONIMATO E  
**DEEP WEB**

# O que queremos proteger?

## Os sites acessados

Quando você acessa um site, você envia e recebe informações, que passam pelo seu provedor de internet.

Com isso, seu provedor pode:

- Saber detalhes de sua atividade na internet.

Porém, seu provedor não pode:

- Obter senhas e outras informações sensíveis, que normalmente são enviadas com criptografia.



ANONIMATO E  
**DEEP WEB**

# O que queremos proteger?

## Sua atividade on-line

Quando você acessa alguns sites, são coletadas informações sobre sua atividade online, como abas abertas, contas logadas, etc.

Isso permite:

- Traçar um perfil de seus hábitos de navegação e interesses.
- Lhe exibir anúncios direcionados para sua atividade on-line.



ANONIMATO E  
**DEEP WEB**

# O que queremos proteger?

## Sua atividade on-line

Ferramentas de busca, como o Google, mantêm registros de tudo que você pesquisa.

Isso permite:

- Traçar um perfil de seus hábitos de navegação e interesses.
- Lhe exibir anúncios direcionados para sua atividade on-line.

# VPNs e Proxys



ANONIMATO E  
**DEEP WEB**

# VPNs e Proxys

A VPN fornece um canal seguro de comunicação entre duas partes, encriptando e desencriptando o tráfego de rede:



**Você**

Tráfego não encriptado



**Provedor  
de Internet**

Tráfego não encriptado



**Internet**



ANONIMATO E  
**DEEP WEB**

# VPNs e Proxys

A VPN fornece um canal seguro de comunicação entre duas partes, encriptando e desencriptando o tráfego de rede:





ANONIMATO E  
**DEEP WEB**

# VPNs e Proxys

Nesse processo, a VPN também atua como um proxy, pois altera o endereço de IP que o site recebe.



**Você**



IP Real

Tráfego encriptado



**Provedor  
de Internet**



IP Real

Tráfego  
encriptado



**Servidor de  
VPN**



IP do Servidor

Tráfego  
não  
encriptado



**Internet**



ANONIMATO E  
**DEEP WEB**

# VPNs e Proxys

O que uma VPN fornece:

Privacidade em relação aos pacotes enviados. O que antes era legível, agora torna-se criptografado quando sai do seu computador e passa pelo ISP.

Os pacotes só se tornam legíveis depois do servidor VPN e, desse ponto em diante, não mais é possível relacioná-los ao computador de origem.

O que uma VPN não fornece:

Anonimato absoluto. O servidor de VPN ainda pode saber seu endereço real de IP, pois é centralizado.





ANONIMATO E  
**DEEP WEB**

# VPNs e Proxys

O que uma VPN fornece:

Privacidade em relação aos pacotes enviados. O que antes era legível, agora torna-se criptografado quando sai do seu computador e passa pelo ISP.

Os pacotes só se tornam legíveis depois do servidor VPN e, desse ponto em diante, não mais é possível relacioná-los ao computador de origem.

O que uma VPN não fornece:

Anonimato absoluto. O servidor de VPN ainda pode saber seu endereço real de IP, pois é centralizado.

O que algumas VPNs comerciais fornecem:

Garantia de que seus dados não são armazenados em nenhum lugar.

Recomendação de VPN open-source: SoftEther VPN Gate.

# Bloqueando trackers



ANONIMATO E  
**DEEP WEB**

# VPNs e Proxys

Trackers são recursos presentes em sites que registram sua atividade on-line: abas abertas, contas logadas, etc.

Como evitar que essas informações sejam coletadas?



## Privacy Badger

Oferecido por: [www.eff.org](https://www.eff.org)

★★★★★ 1.507 | [Social e comunicação](#) |  930.242 usuários



ANONIMATO E  
**DEEP WEB**

# VPNs e Proxys

O Privacy Badger identifica, bloqueia e lhe avisa sobre eventuais trackers que sejam identificados.



Privacy Badger

versão 2019.7.1



O Privacy Badger detectou um potencial **rastreador** neste site. O controle deslizante permite que você controle como o Privacy Badger lida com ele. Você não precisa ajustar o controle a menos que algo esteja quebrado.



googleads.g.doubleclick.net



Desabilitar o Privacy Badger para este site

O Privacy Badger quebrou este site? Deixe-nos saber!

Doar para EFF

# Bloqueando anúncios indesejados

Ninguém gosta de anúncios. Ao passo que muitas vezes  
anúncios servem para manter um site funcionando, diversos  
sites exibem anúncios abusivos ou enganosos ao usuário. Veja:



Fotos tiradas no momento certo que só podem ser feitas uma vez

UNOFF.NET



Ele abandonou sua mulher por causa de uma foto, olhe mais de perto e entenda!

UNOFF.NET



As cirurgias insólitas mais populares do mundo!

PICKTURE.COM



Top 22 tatuagens lindas que se completam para casais

PICKTURE.COM



A reação incrível de animais vendo a neve



Esses atores foram demitidos em plena gravação



ANONIMATO E  
**DEEP WEB**

# VPNs e Proxys

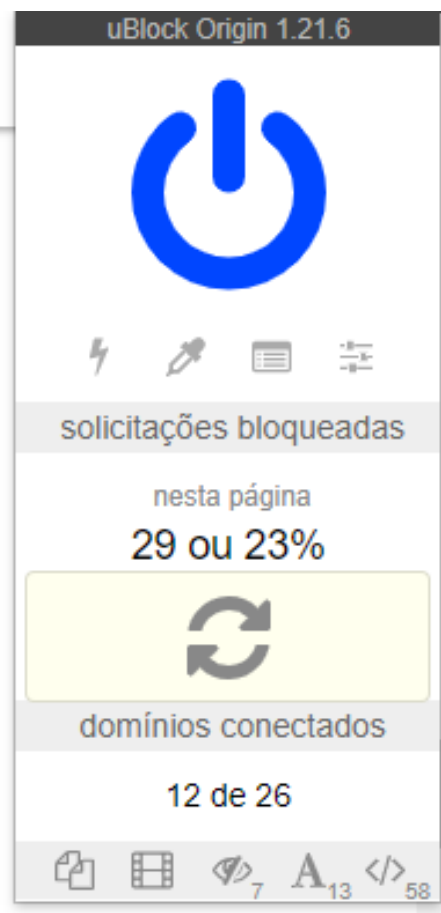
Como evitar que esses anúncios sejam exibidos?



uBlock Origin

Oferecido por: Raymond Hill (gorhill)

★★★★★ 21.372 | [Produtividade](#) | 10.000.000+ usuários







ANONIMATO E  
**DEEP WEB**

# VPNs e Proxys

O que mais o uBlock Origin é capaz de fazer?

**Bloquear fontes remotas** evita que fontes sejam baixadas para o computador. Esse procedimento pode implicar em problemas de segurança.

**Bloquear grandes elementos de mídia** evita que imagens e vídeos muito grandes sejam automaticamente baixados, economizando franquia de internet.

**Bloquear o Javascript** evita a execução do Javascript em um determinado site. Isso pode ter vantagens, mas não é indicado para iniciantes, pois pode comprometer o funcionamento do site.

# Privacidade e rede sociais



ANONIMATO E  
**DEEP WEB**

# Privacidade e redes sociais

Existem duas abordagens envolvendo privacidade e rede sociais.

**A primeira diz respeito à comportamentos ativos:** o que você posta na rede.

Com essas informações:

- Um atacante pode usar informações postadas em redes sociais contra você em ataques de engenharia social.
- A sua vida pode ser facilmente exposta em ataques de *doxxing*.
- Um atacante pode tentar localizar você com base em seus posts de localização.



ANONIMATO E  
**DEEP WEB**

# Privacidade e redes sociais

Como apresentar um comportamento ativo nas redes sociais voltado para privacidade?

- Não informe relacionamentos (namoro, casamento, parentes) nas redes sociais.
- Deixe suas postagens e fotos como “somente amigos”.
- Desative a localização nas postagens.
- Evite confirmar presença em eventos.
- Quando fizer login em redes públicas que exijam autenticação via Facebook, faça-o na forma privada.
- Deixe sua lista de amigos privada.
- Filtre quem você aceita como amigo em redes sociais.
- Pense nas consequências de qualquer informação que você publicar.



ANONIMATO E  
**DEEP WEB**

# Privacidade e redes sociais

**A segunda diz respeito a comportamentos passivos:** o que a rede faz enquanto você a usa.

Com essas informações:

- A rede social obtém um perfil sobre seus hábitos de navegação.
- A rede social pode exibir anúncios direcionados ao seu perfil de consumo.



ANONIMATO E  
**DEEP WEB**

# Privacidade e redes sociais

**A segunda diz respeito a comportamentos passivos:** o que a rede faz enquanto você a usa.

A única forma de impedir que essas informações sejam coletadas é bloquear trackers desde o momento em que você começa a usar a rede social pela primeira vez, já que o armazenamento é cumulativo.



ANONIMATO E  
**DEEP WEB**

# Privacidade e redes sociais

Podemos, também, obter um registro de tudo que uma dada rede social sabe sobre nós. Faça isso nos links a seguir:

Facebook: [https://www.facebook.com/settings?tab=your facebook information](https://www.facebook.com/settings?tab=your_facebook_information)

Twitter: [https://twitter.com/settings/your twitter data](https://twitter.com/settings/your_twitter_data)

Google: <https://takeout.google.com/settings/takeout?pli=1>

# Mecanismos de busca alternativos





ANONIMATO E  
**DEEP WEB**

# Privacidade e redes sociais

Ao efetuar uma busca no Google, os dados pesquisados são registrados e usados para compor seu perfil de interesses, que será, posteriormente, utilizado para lhe exibir anúncios direcionados.

Existem serviços de busca que não fazem isso. Essa seção apresentará algumas delas:

- Duck Duck Go: <https://duckduckgo.com>
- StartPage: <https://www.startpage.com>



ANONIMATO E  
**DEEP WEB**

# Privacidade e redes sociais

## Duck Duck Go

Possui uma política de busca transparente, mas armazena históricos de forma não agregada (que não podem ser diretamente ligados a você).

Exibe termos buscados no histórico.



ANONIMATO E  
**DEEP WEB**

# Privacidade e redes sociais

## StartPage

Não armazena nenhum tipo de dado, e não exibe termos buscados no histórico.

O StartPage elimina metadados de uma solicitação de busca e as envia para o Google, de forma a fazer uma busca privada.



# E-mails descartáveis



ANONIMATO E  
**DEEP WEB**

# Privacidade e redes sociais

Ao nos cadastrar em um serviço duvidoso, frequentemente desejamos usar endereços de e-mail que possam ser facilmente descartados se necessário.

Essa seção lhe apresentará algumas alternativas do tipo.



ANONIMATO E  
**DEEP WEB**

# Privacidade e redes sociais

## Opção 1: e-mail totalmente descartável

Algumas opções existentes:

GuerrillaMail: <https://www.guerrillamail.com/pt/>

TempMail: <https://temp-mail.org/pt/>

Mohamal: <https://www.mohmal.com/en/inbox>

Esses e-mails duram entre 1 e 24 horas, e servem como e-mails descartáveis. Não podem ser usados para nada que os requeira no futuro.




ANONIMATO E  
**DEEP WEB**

# Privacidade e redes sociais

## Opção 1: e-mail *off shore*

Uma boa opção é o Cock.li: <https://cock.li>

Permite a criação de uma conta de e-mail permanente que não necessita de demais dados pessoais.

E-Mail Address	<input type="text" value="emailtestededescartavel"/>	@	<input type="text" value="airmail.cc"/>
Password	<input type="password" value="....."/>		
Confirm Password	<input type="password" value="....."/>		
	<input type="text" value="mf97n"/>		
<input type="checkbox"/> Receive updates about cock.li via e-mail			
<input checked="" type="checkbox"/> I agree to Cock.li's <a href="#">Terms of Service</a> and <a href="#">Privacy Policy</a>			
<input type="button" value="Agree and Register"/>			

# HTTPs em todo lugar





ANONIMATO E  
**DEEP WEB**

# Privacidade e redes sociais

Os protocolos HTTP e HTTPS são usados para troca de pacotes de informação na internet.

No protocolo HTTP, tais pacotes trafegam em texto limpo, ao passo que, no protocolo HTTPS, os pacotes trafegam com criptografia.

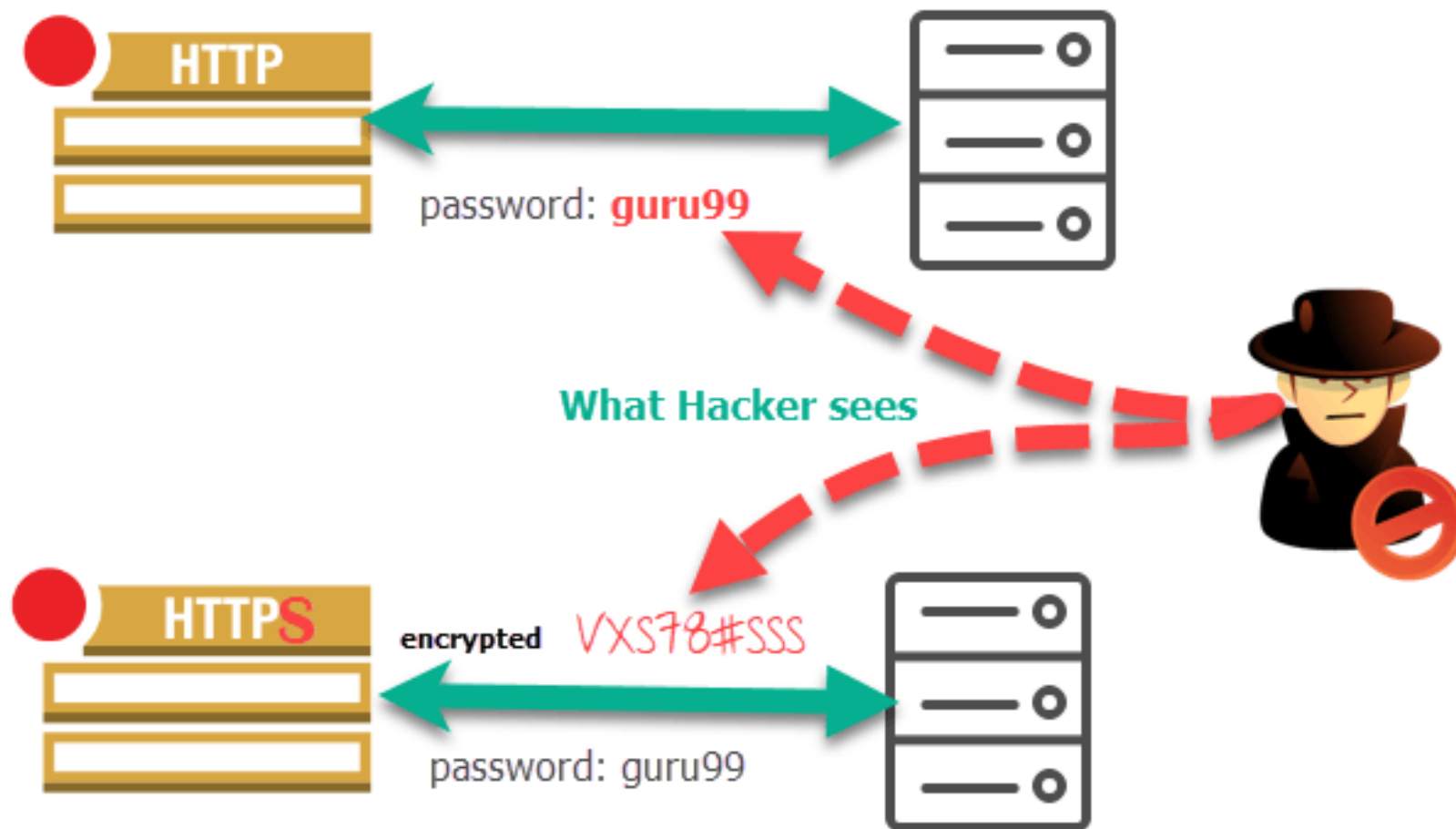
Atualmente, o uso de HTTPS para enviar dados sensíveis, como senhas, é uma diretriz.

Porém, o uso de HTTP nas demais situações permitem que um usuário na mesma rede espione o que você faz.



ANONIMATO E  
**DEEP WEB**

# Privacidade e redes sociais





ANONIMATO E  
**DEEP WEB**

# Privacidade e redes sociais

Como solucionar?



## HTTPS Everywhere

Oferecido por: [www.eff.org](http://www.eff.org)

★★★★★ 4.132 | [Social e comunicação](#) |  2.077.057 usuários

# Cookies



ANONIMATO E  
**DEEP WEB**

# Privacidade e redes sociais

Cookies são pequenos arquivos de texto que armazenam informações a respeito de sua relação com um site específico, tais como:

- Preferências de configuração do site (tema, cores).
- Histórico de acessos e número de visualizações.
- Logins e senhas salvas.

Com cookies, um site pode:

- Construir um perfil do usuário com base em suas preferências.
- Manter registro do número e horário dos acessos realizados.
- Customizar o site para atender às preferências do usuário.



ANONIMATO E  
**DEEP WEB**

# Privacidade e redes sociais

Muitos consideram cookies uma invasão de privacidade. Como se livrar deles?



## Cookie AutoDelete

Oferecido por: Kenny Do

★★★★★ 199

| [Produtividade](#)

|  98.576 usuários

A extensão remove cookies imediatamente após o usuário sair de um site.

# Guia anônima



ANONIMATO E  
**DEEP WEB**

# Privacidade e redes sociais

O modo anônimo de um navegador normalmente pode ser acessado pelo atalho  
CTRL + SHIFT + N.







ANONIMATO E  
**DEEP WEB**

# Privacidade e redes sociais

O modo anônimo serve para:

- Não armazenar cookies ou histórico da sessão.
- Ocultar o que você faz de outras pessoas que tenham acesso ao seu navegador.

O modo anônimo não serve para:

- Encriptar sua conexão.
- Ocultar seu endereço de IP.
- Ocultar o que você faz do seu provedor de internet.
- Evitar que programas instalados na máquina verifiquem o que você faz.



ANONIMATO E  
**DEEP WEB**

# Privacidade em transações comerciais

A maioria dos métodos de pagamento on-line convencionais são dominais: débito em conta, cartão de crédito, PayPal, PicPay e assim por diante. Eles estão associados ao seu nome.





Existe uma forma de se fazer pagamentos on-line (e até presencialmente) sem que o pagamento seja atrelado ao seu nome.

**As criptomoedas.**



Existe uma forma de se fazer pagamentos on-line (e até presencialmente) sem que o pagamento seja atrelado ao seu nome.

### **As criptomoedas.**

O termo “criptomoeda” engloba todo um conjunto de tecnologias que gerenciam uma moeda virtual.

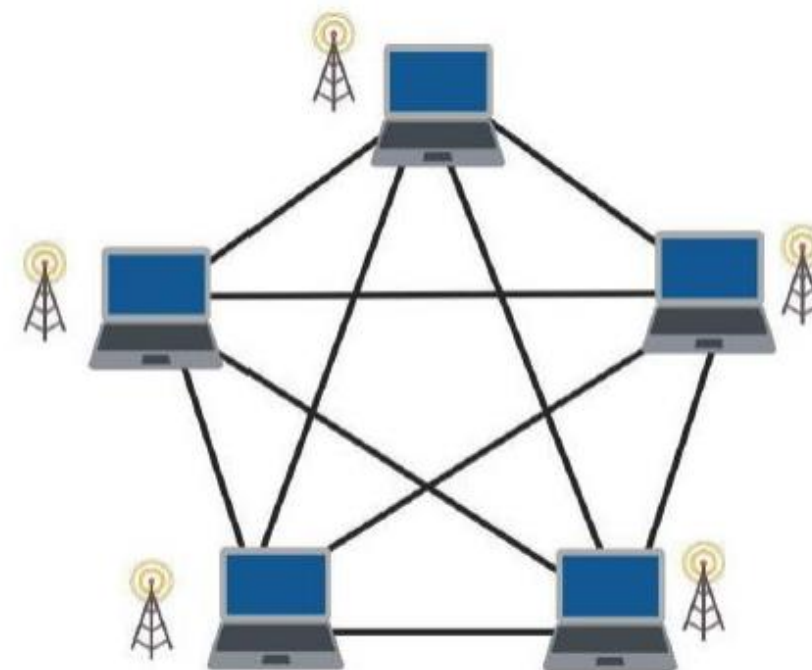
Nesse vídeo, estudaremos essa tecnologia com dois exemplos: o Bitcoin e o Monero.

O que um item precisa para ser usado como moeda?

- Ser aceito por todos.
- Possuir relativa raridade.
- Possuir praticidade: deve ser de fácil manuseio.
- Lastro: garantia de um valor implícito.

Porque a Bitcoin e o Monero servem como moeda?

- Possuem raridade determinada por um algoritmo que não depende de nenhuma pessoa ou instituição para funcionar, dependendo apenas da comunidade como um todo.
- Isso torna essas moedas confiáveis e permitem que surja um lastro.
- Adicionalmente, essas moedas são relativamente práticas, o que facilita seu uso.



## Como as criptomoedas surgiram?

Em 2009, um programador japonês – ou uma equipe de programadores – denominado Satoshi Nakamoto apresentou o Bitcoin. Tratava-se de um complexo sistema descentralizado no qual os usuários poderiam adquirir e enviar unidades da moeda para outros usuários.

A invenção de Nakamoto era controlada unicamente através de software, o qual seria responsável por liberar um total de 21 milhões de Bitcoins, ao longo de aproximadamente vinte anos. A cada dez minutos, as moedas seriam distribuídas através de um processo semelhante a uma loteria, na qual mineradores deveriam “jogar” sucessivamente e o que tivesse o computador mais rápido seria recompensado.



## Como as criptomoedas surgiram?

Nos anos seguintes ao lançamento do sistema, o interesse dos usuários foi aumentando, fazendo com que mais e mais usuários se interessassem em minerar a moeda, o que culminou para o surgimento de casas de câmbio, que permitiriam que qualquer pessoa pudesse adquirir Bitcoins a partir de dinheiro oficial.

Gradualmente, vendedores também começaram a aceitar Bitcoins, fazendo com que o valor de cada Bitcoin aumentasse expressivamente. Poucos anos depois, Nakamoto havia construído uma nova moeda, capaz de ser utilizada em transações, minerada, vendida ou comprada.

Como as criptomoedas surgiram?

Desde então, o Bitcoin passou a ser  
aceito e utilizado como moeda,  
chegando a cotação de 19 mil dólares.



Como as criptomoedas funcionam?

Infográfico na página 15:

<https://ia800803.us.archive.org/16/items/ManualDoInicianteEmCriptomoedasFbricaDeNoobs/Manual%20do%20Iniciante%20em%20Criptomoedas%20-%20Fábrica%20de%20Noobs.pdf>

Como a Bitcoin pode ajudar na privacidade?

- As transações em Bitcoin não são nominais.
- Não é necessário informar dados pessoais ao criar uma carteira Bitcoin.

Entretanto:

- Ainda é preciso informar dados pessoais para comprar bitcoins, a menos que você as compre de alguém de forma informal.
- Seu endereço de IP, endereço da carteira, saldo e quantia envolvida na transação são públicos.

Como o Monero pode ajudar na privacidade?

- O remetente e a quantia envolvidos na transação não são públicos.
- O endereço de IP do remetente não é público.
- O seu saldo não é público.

Porém:

- A menos que você compre de forma informal, você ainda precisará informar dados pessoais para comprar Monero.

Como começar a usar criptomoedas?

Esse assunto é extremamente extenso, e foge ao escopo deste curso. Porém, você pode aprender a fazer isso de forma gratuita em

<https://ia800803.us.archive.org/16/items/ManualDoInicianteEmCriptomoedasFbricaDeNoobs/Manual%20do%20Iniciante%20em%20Criptomoedas%20-%20Fábrica%20de%20Noobs.pdf> e

[https://www.youtube.com/watch?v=\\_O6VhWBOoCs&list=PLlevgZoV2cAinmuDTgwB3ZnTwY1hqTm\\_b](https://www.youtube.com/watch?v=_O6VhWBOoCs&list=PLlevgZoV2cAinmuDTgwB3ZnTwY1hqTm_b)

# 2

# REDES OCULTAS

# O que é a Deep Web?



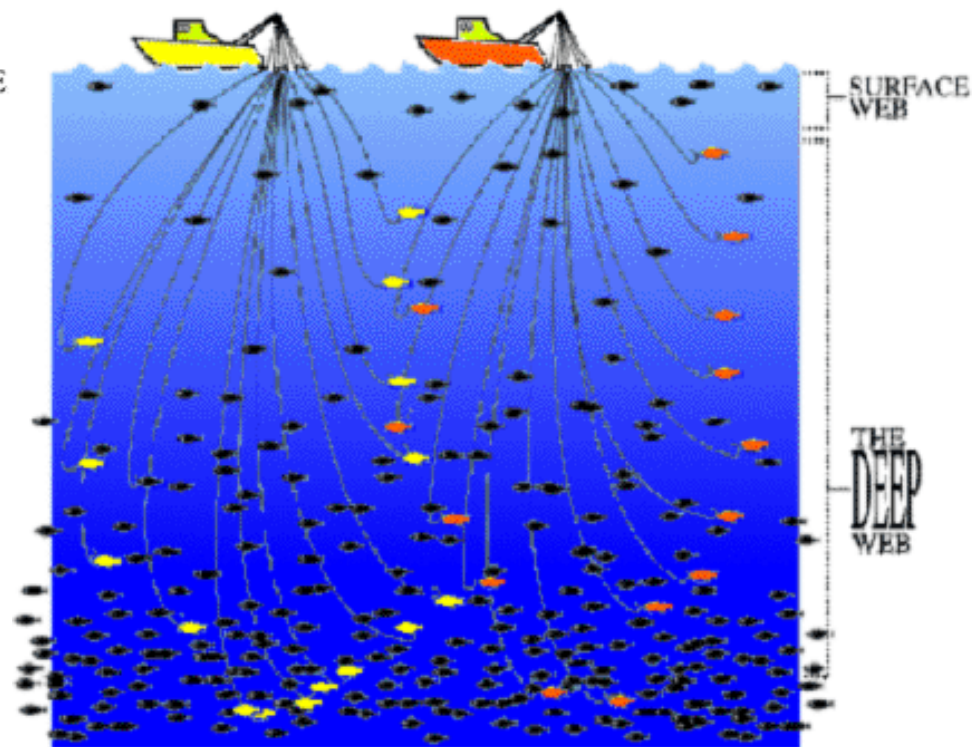
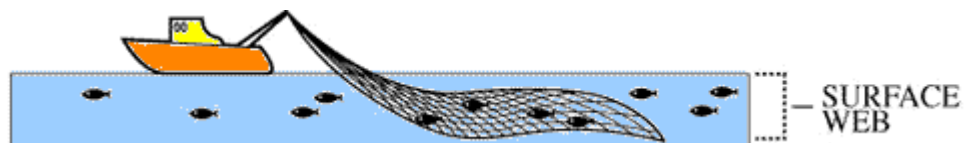


ANONIMATO E  
**DEEP WEB**

# O que é Deep Web?

Existem duas definições.

**Definição de Bergman:** toda a parte da internet que não é acessível diretamente por mecanismos de busca.





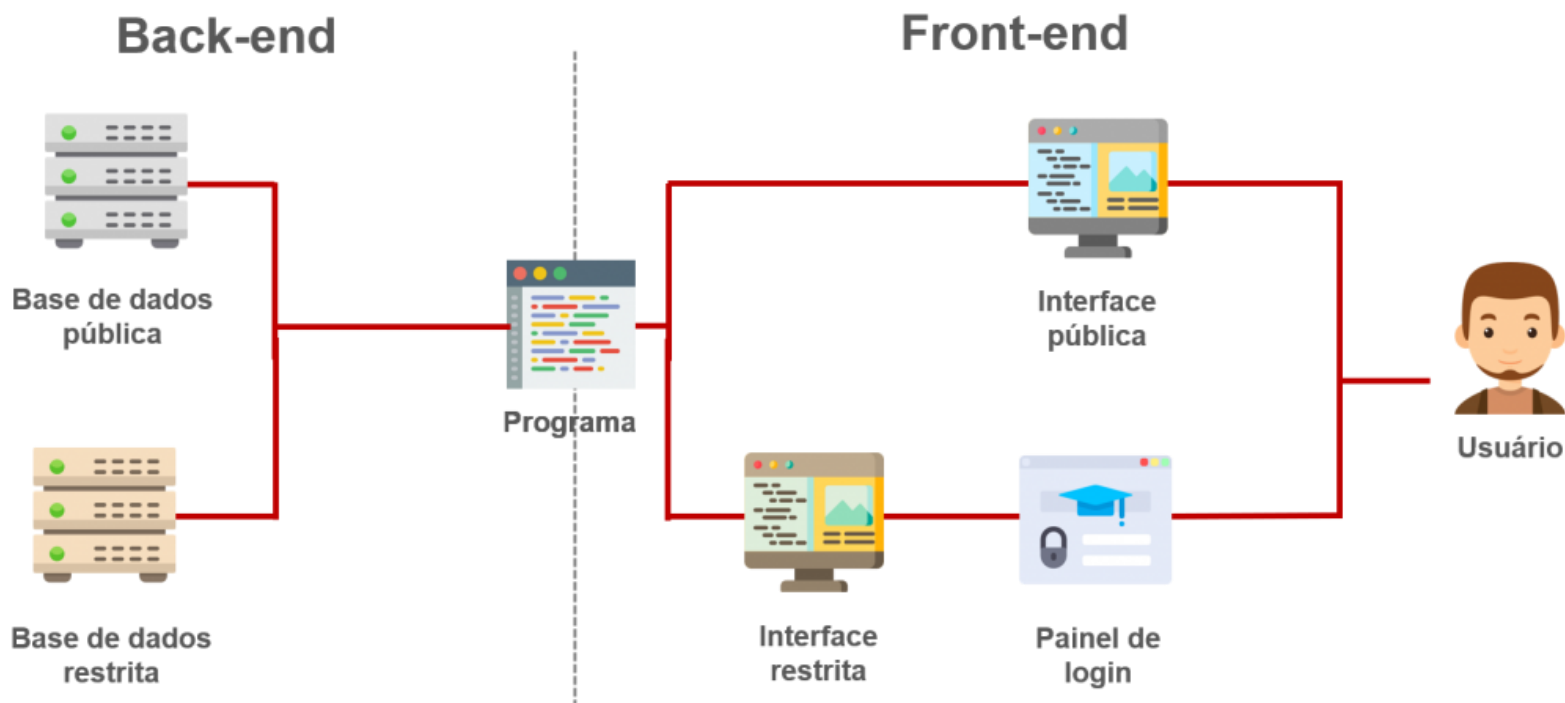
ANONIMATO E  
**DEEP WEB**

# O que é Deep Web?

Existem duas definições.

**Definição de Bergman:** toda a parte da internet que não é acessível diretamente por mecanismos de busca.

Essa definição inclui o back-end de qualquer tipo de serviço.





ANONIMATO E  
**DEEP WEB**

# O que é Deep Web?

Existem duas definições.

**Definição de Bergman: toda a parte da internet que não é acessível diretamente por mecanismos de busca.**

**E cadê a Deep Web que eu conheço?**

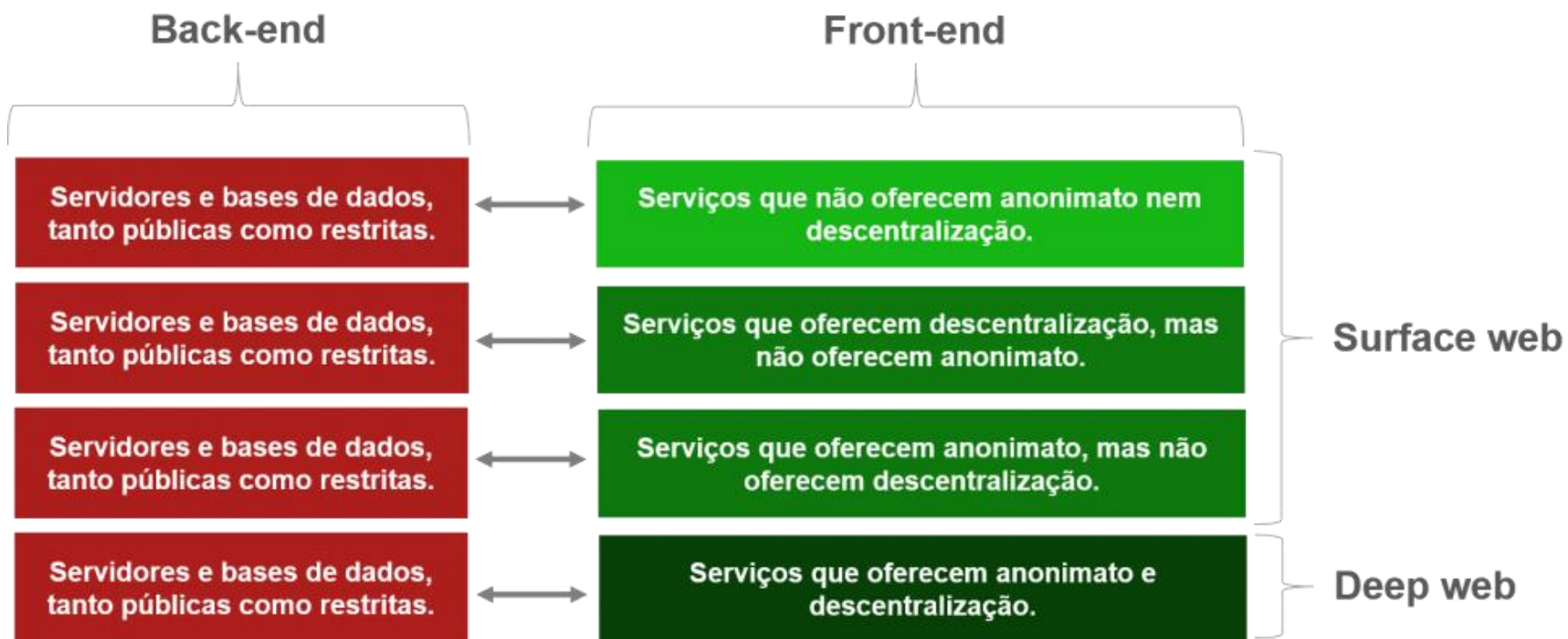


ANONIMATO E  
**DEEP WEB**

# O que é Deep Web?

Existem duas definições.

**Nova definição: todo sistema conectado à internet que forneça anonimato e descentralização.**





ANONIMATO E  
**DEEP WEB**

# O que encontro e o que não encontro na Deep Web?



ANONIMATO E  
**DEEP WEB**

# O que (não) encontro na Deep Web?

Precisamos lembrar da definição:

**Nova definição: todo sistema conectado à internet que forneça anonimato e descentralização.**

**O anonimato diz respeito a ninguém ser capaz de saber que você é o responsável por postar um dado conteúdo.**

**A descentralização diz respeito a ninguém ser capaz de tirar um conteúdo que você postou do ar.**



ANONIMATO E  
**DEEP WEB**

# O que (não) encontro na Deep Web?

Precisamos lembrar da definição:

**Nova definição: todo sistema conectado à internet que forneça anonimato e descentralização.**

**O anonimato diz respeito a ninguém ser capaz de saber que você é o responsável por postar um dado conteúdo.**  
É geralmente obtido através do uso de uma VPN descentralizada.

**A descentralização diz respeito a ninguém ser capaz de tirar um conteúdo que você postou do ar.**  
É obtida através do próprio anonimato, ou armazenando-se o site em pedaços espalhados por diversos computadores.



ANONIMATO E  
**DEEP WEB**

# O que (não) encontro na Deep Web?

Precisamos lembrar da definição:

**Nova definição: todo sistema conectado à internet que forneça anonimato e descentralização.**

Portanto, você encontra em sua maioria **conteúdos legais e ilegais que precisem de anonimato e descentralização.**

Você também encontra **conteúdos que não precisam de um ou nenhum desses dois fatores**, assim como na Surface Web.





ANONIMATO E  
**DEEP WEB**

# O que (não)encontro na Deep Web?

- Pornografia ilegal, normalmente infantil ou de estupro.
- Venda de drogas;
- Venda de armas;
- Tráfico de órgãos;
- Manuais para fabricação de drogas, bombas, armas e modificações em armas;
- Manuais para cometer crimes, como estupros e assassinatos;
- Tortura e assassinato sob encomenda;
- Venda de informações bancárias de terceiros;
- Venda de dinheiro falsificado;
- Tentativa de golpes;
- Venda de caixas misteriosas com conteúdo ilegal;
- Venda de informações privilegiadas sobre governos ou corporações;
- Vazamento de informações privilegiadas;
- Venda de *exploits 0-day*;
- Fóruns e *boards* sobre práticas ilegais, onde criminosos interagem;
- Venda de medicamentos sem receita;
- Pirataria;
- Venda de documentos falsos, como passaportes e habilitação;
- Venda de produtos sem restrições alfandegárias;
- Sites que permitem financiar organizações criminosas;
- Exposição de dados pessoais;
- Serviços que fazem o intermédio de transações ilegais;
- Promoção e recrutamento de atividades terroristas;



ANONIMATO E  
**DEEP WEB**

# O que (não)encontro na Deep Web?

- Sites de notícias, que provavelmente seriam censurados em seus países;
- Fóruns e *boards* de discussão sobre práticas não necessariamente ilegais, como hacking;
- Fóruns e *boards* de discussão sobre assuntos legais;
- “Confessionários”, nos quais usuários postam anonimamente;
- Páginas de cultos ou seitas;
- Plataformas para denunciante;
- Espelhos de sites da Surface Web;
- Pornografia legal ou fetiches consensuais;
- Venda de caixas misteriosas sem conteúdo ilegal;
- Sites que agregam imagens de violência gráfica;
- Diretórios de links;
- Enigmas;
- Páginas de teste ou em branco;
- Repositórios de software;
- Bibliotecas;
- Artigos científicos;
- Livros e materiais censurados em determinados países;
- Instituições financeiras;
- *Faucets* de criptomoedas;
- Cassinos;
- Venda de criptomoedas;



ANONIMATO E  
**DEEP WEB**

# O que (não) encontro na Deep Web?

Precisamos lembrar da definição:

**Nova definição: todo sistema conectado à internet que forneça anonimato e descentralização.**

E o que você não encontra?



ANONIMATO E  
**DEEP WEB**

# O que (não) encontro na Deep Web?

**Qualquer tipo de conteúdo de cunho paranormal ou fantástico**, como a cura do câncer, a localização de Atlântida, provas da existência de vida extraterrestre e relacionados não tem maior probabilidade de serem encontrados na Deep Web do que de serem encontrados em qualquer outro lugar. Afinal, não há evidências de que essas informações possam ser encontradas em qualquer tipo de lugar.

**Informações aprofundadas sobre um determinado assunto** provavelmente serão encontradas em pesquisas acadêmicas disponíveis na Surface Web, e não na Deep Web. Não há nenhum motivo pelo qual esse tipo de conteúdo necessitaria de anonimato e descentralização.

**Informações governamentais ou corporativas** (como bases de dados contendo informações pessoais) não são hospedados em redes anônimas e descentralizadas, mas sim em bases de dados restritas. Você só vai encontrar essas informações na Deep Web se alguém invadir tais bases de dados e as disponibilizar na Deep Web.



ANONIMATO E  
**DEEP WEB**

# O que (não) encontro na Deep Web?

**A Deep Web não é um oráculo.** Se você quer encontrar algum tipo de conteúdo legal, é muito mais provável que o encontre na Surface Web, por meio da boa e velha pesquisa no Google.

**As histórias de terror envolvendo a Deep Web**, como bonecas sexuais humanas, *shadow web red rooms*, lutas de gladiadores até a morte, centopeia humana e outras equivalentes são falsas. As três primeiras são contos que se originaram em fóruns de histórias de terror na Surface Web e se tornaram lendas urbanas. A última é apenas o tema de três filmes de ficção.



ANONIMATO E  
**DEEP WEB**

# Como a Deep Web é dividida?

E quem garante que não há conteúdo sobrenatural na Deep Web?

A resposta é mais um conceito filosófico do que prático. Certamente, existem coisas que não conhecemos: existem casas na sua vizinhança nas quais você nunca entrou e existem planetas no universo que não conhecemos.





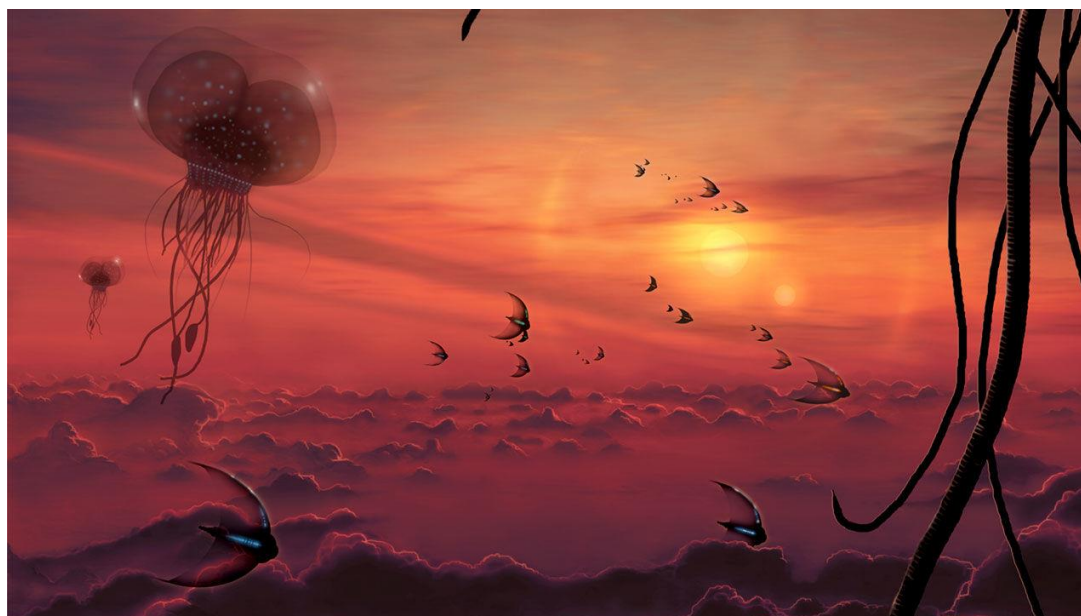


ANONIMATO E  
**DEEP WEB**

# Como a Deep Web é dividida?

E quem garante que não há conteúdo sobrenatural na Deep Web?

É possível que esses lugares que não conhecemos contenham algo fora do normal? Sim, sempre é possível. Seu vizinho pode ter um corpo escondido na garagem, ou um planeta desconhecido pode abrigar vida. Porém, é estatisticamente mais provável que seu vizinho e esse planeta sejam mais ou menos semelhantes aos outros que nós já conhecemos.





ANONIMATO E  
**DEEP WEB**

# Como a Deep Web é dividida?

E quem garante que não há conteúdo sobrenatural na Deep Web?

Além disso, o desconhecido muito, muito provavelmente não viola nenhuma lei natural. Seu vizinho definitivamente não tem um dragão na garagem, e esse planeta definitivamente não abriga uma população composta somente por clones do Felipe Melo.





# Como a Deep Web é dividida?



ANONIMATO E  
**DEEP WEB**

# Como a Deep Web é dividida?

Precisamos lembrar da definição:

**Nova definição: todo sistema conectado à internet que forneça anonimato e descentralização.**



ANONIMATO E  
**DEEP WEB**

# Como a Deep Web é dividida?

Precisamos lembrar da definição:

**Nova definição: todo sistema conectado à internet que forneça anonimato e descentralização.**

Nada mais coerente do que dividirmos a Deep Web em **sistemas**, chamados, a partir de agora, de **redes**.



ANONIMATO E  
**DEEP WEB**

# Como a Deep Web é dividida?

Existem diversas redes que fornecem anonimato e descentralização e, portanto, que compõe a Deep Web.

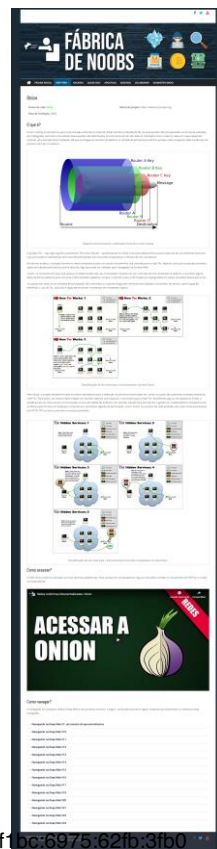
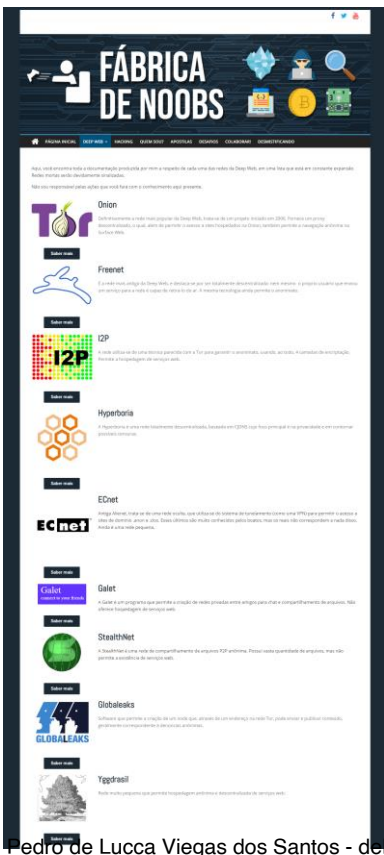




ANONIMATO E  
**DEEP WEB**

# Como a Deep Web é dividida?

Meu trabalho é documentar cada uma dessas redes, bem como suas formas de acesso e conteúdo presente nelas. Você pode obter mais informações sobre isso em <http://www.fabricadenooobs.com.br/deep-web/redes-documentadas/>.





ANONIMATO E  
**DEEP WEB**

# Como a Deep Web é dividida?

Essas redes muitas vezes têm objetivos e características distintas:

**Hospedagem de sites:** Tor, I2P, Hyperborya, Zeronet, Freenet, Ecnet, Yggdrasil, Globaleaks

**Chat:** Tox, Galet, Ricochet

**Arquivos:** Stealthnet, Demonsaw, PerfectDark, Tribler, Retroshare

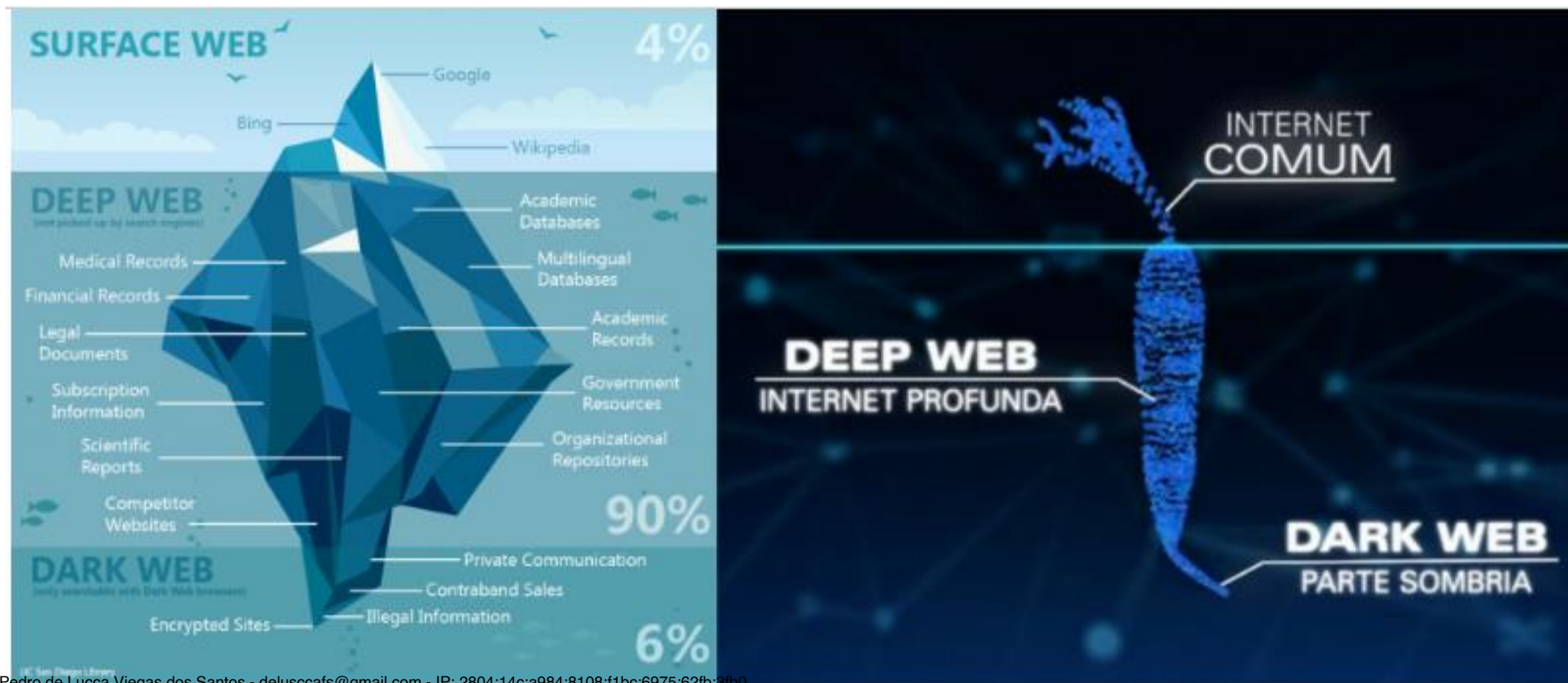
Neste curso, aprenderemos a usar algumas delas. Você pode descobrir sobre as outras gratuitamente em meu site.



ANONIMATO E  
**DEEP WEB**

# Como a Deep Web é dividida?

E onde estão as camadas?





ANONIMATO E  
**DEEP WEB**

# Como a Deep Web é dividida?

Existem três conceitos errados envolvidos na classificação em camadas:

- (1) Quanto mais profundo é um conteúdo, mais ilegal ou macabro ele é.
- (2) Quanto mais profundo é um conteúdo, mais difícil ele é de ser acessado.
- (3) Quanto mais profundo é um conteúdo, maior a quantidade de informações que podem ser encontradas lá.





ANONIMATO E  
**DEEP WEB**

# Como a Deep Web é dividida?

Existem três conceitos errados envolvidos na classificação em camadas:

(1) Quanto mais profundo é um conteúdo, mais ilegal ou macabro ele é.

A noção (1) é a mais razoável dessas três, mas ainda apresenta problemas. Qual exatamente seria o critério para classificar um conteúdo como mais ilegal que outro? E para classificar um conteúdo como mais macabro que outro, já que o que eu considero macabro pode não ser macabro para você? Além disso, a Deep Web é repleta de sites totalmente legais e inocentes, ao passo que já encontrei muita coisa ilegal e doentia (como pornografia infantil ou estímulo ao assassinato) na Surface Web. Essa classificação implicaria em misturar todos os sites, além de envolver um critério relativo.



ANONIMATO E  
**DEEP WEB**

# Como a Deep Web é dividida?

Existem três conceitos errados envolvidos na classificação em camadas:

(2) Quanto mais profundo é um conteúdo, mais difícil ele é de ser acessado.

A noção (2) é errada por que dificuldade é um conceito extremamente relativo, em especial quando tentamos comparar as dificuldades em se executar uma sequência de passos no computador. Qual exatamente seria nosso critério? Número de passos? Tempo que eu levo para executar? Tempo que você leva para executar? Quantidade de linhas de código envolvidas? Assim, por mais que essa noção permitiria separar as redes, ela envolveria um critério totalmente relativo e impreciso.



ANONIMATO E  
**DEEP WEB**

# Como a Deep Web é dividida?

Existem três conceitos errados envolvidos na classificação em camadas:

(3) Quanto mais profundo é um conteúdo, maior a quantidade de informações que podem ser encontradas lá.

Por fim, a noção (3) é a mais errada de todas. A melhor fonte de informação, em toda a Internet, é, sem sombra de dúvidas, o próprio Google e a Surface Web. É incrível a quantidade de informações que você pode encontrar por aqui, com poucos cliques. A menos que você procure por serviços ilegais, nenhuma rede da Deep Web vai lhe fornecer tanta informação quanto a que você pode, com os procedimentos corretos, encontrar no Google. Se fôssemos considerar essa noção, a Surface Web deveria ir ao fundo do Iceberg – ou da gloriosa cenoura – e as redes experimentais e projetos mortos, muito pouco conhecidos e que contêm algumas dúzias de sites, deveriam estar no topo.



ANONIMATO E  
**DEEP WEB**

# Como a Deep Web é dividida?

Assim, não faz sentido classificarmos o conteúdo da Deep Web em profundidade, tampouco faz sentido classificarmos as redes em numerais ordinais, pois isso implica uma noção de profundidade, e **não há critério absoluto para fazer essa classificação.**



ANONIMATO E  
**DEEP WEB**

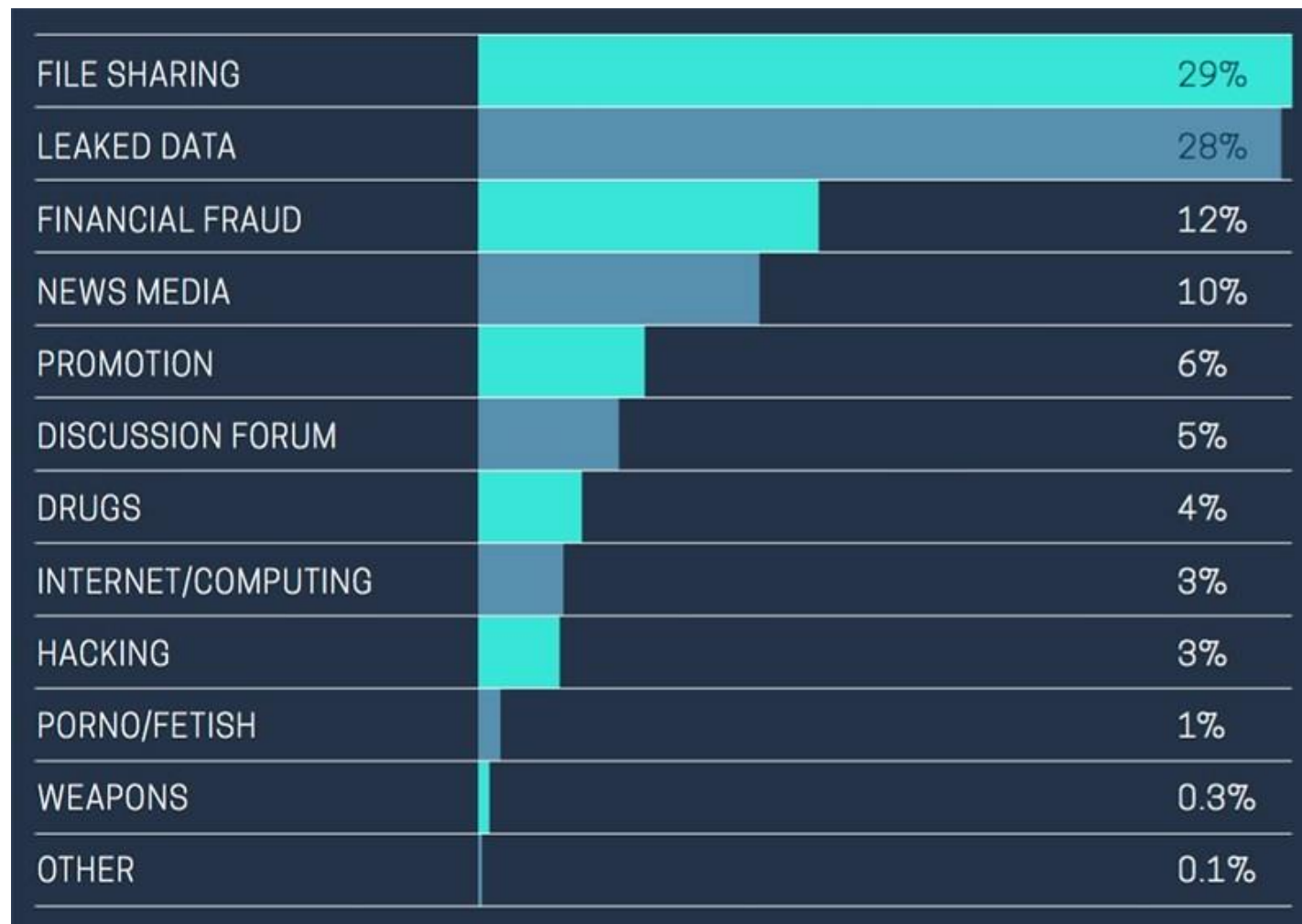
# Como a Deep Web é dividida?

O conceito da Dark Web é alvo de muito debate: os que consideram a definição antiga definem a Dark Web como toda a parte não indexada que fornece anonimato.

Muitos atualmente – que sequer conhecem as duas definições – usam o termo para se referir à toda atividade ilegal realizada na internet, ou apenas na Deep Web.

Se corretamente definido, não há problema nenhum em usar tal conceito.

Porém, preferimos não adotá-lo uma vez que não existem separações técnicas que permitam distinguir entre o que é Dark Web e o que não é.





ANONIMATO E  
**DEEP WEB**

# Como a Deep Web é dividida?

Se você pesquisar pela definição de Mariana's Web encontrará:

- A parte mais profunda da internet
- Utilizada para guardar segredos governamentais, corporativos e mundiais.
- “Campo de batalha” de hackers
- Computação quântica
- Endereços de  $10^{137}$  caracteres

Segredos governamentais e corporativos simplesmente não são armazenados diretamente na internet, mas sim em bases de dados off-line, que possuem medidas de segurança específicas para serem acessadas por pessoas autorizadas dentro do governo ou da empresa em questão.

Não há nenhum motivo razoável para se armazenar tais conteúdos em uma rede anônima e descentralizada: isso só facilitaria que pessoas não autorizadas os acessassem.

Existem diversas formas de se garantir a segurança dessas bases de dados, mas elas não envolvem computação quântica (a computação quântica é um campo ainda em desenvolvimento) ou endereços com  $10^{137}$  caracteres (um endereço deste tamanho ocuparia mais espaço do que o que há em todos os discos rígidos do mundo juntos).

Com um bom conhecimento de computação é possível implementar um sistema suficientemente seguro para armazenar todo tipo de informação.

3

**ANONIMATO**

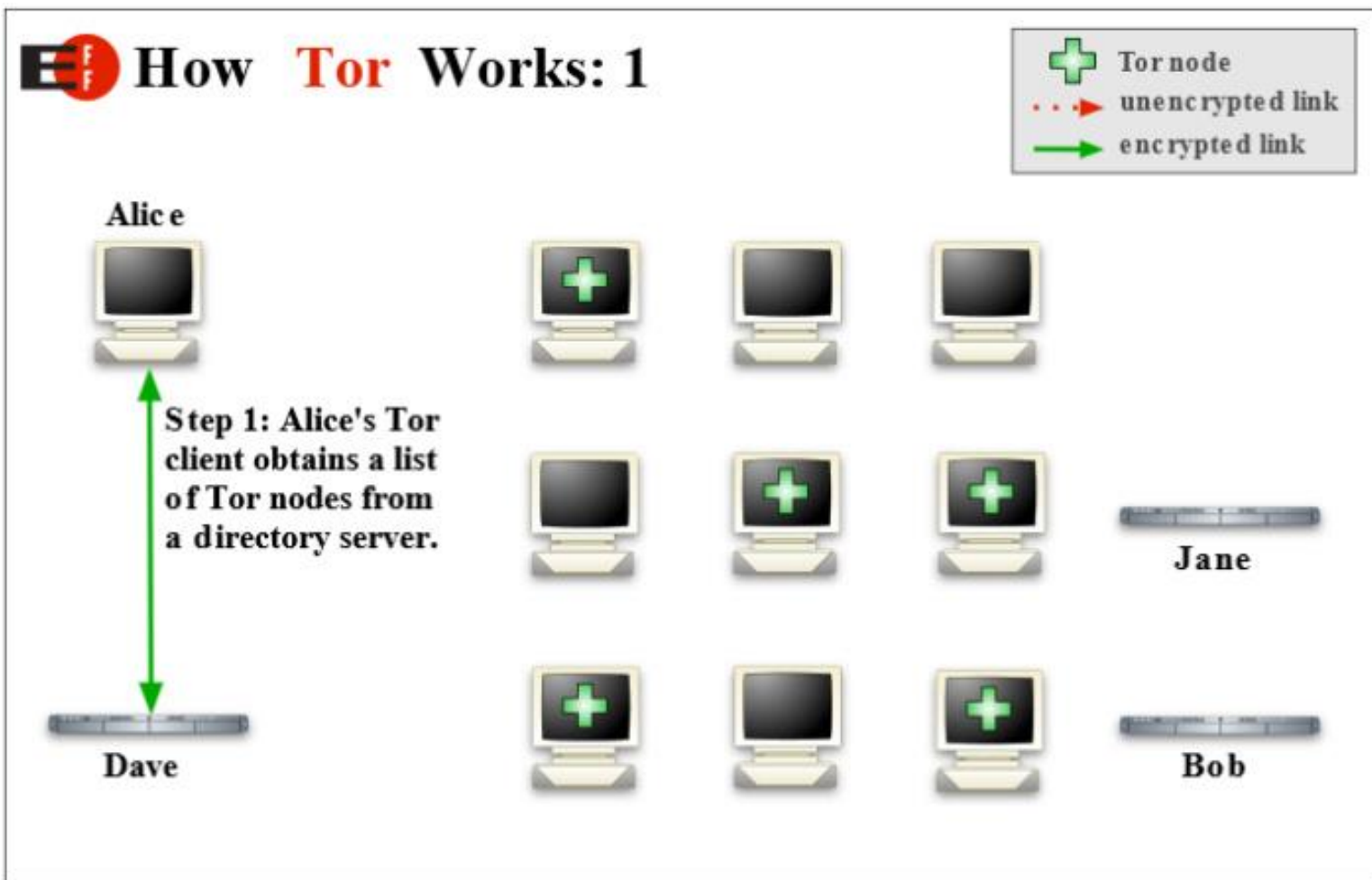
# Usando o Tor para navegação na Surface Web





ANONIMATO E  
**DEEP WEB**

# Segurança na Deep Web

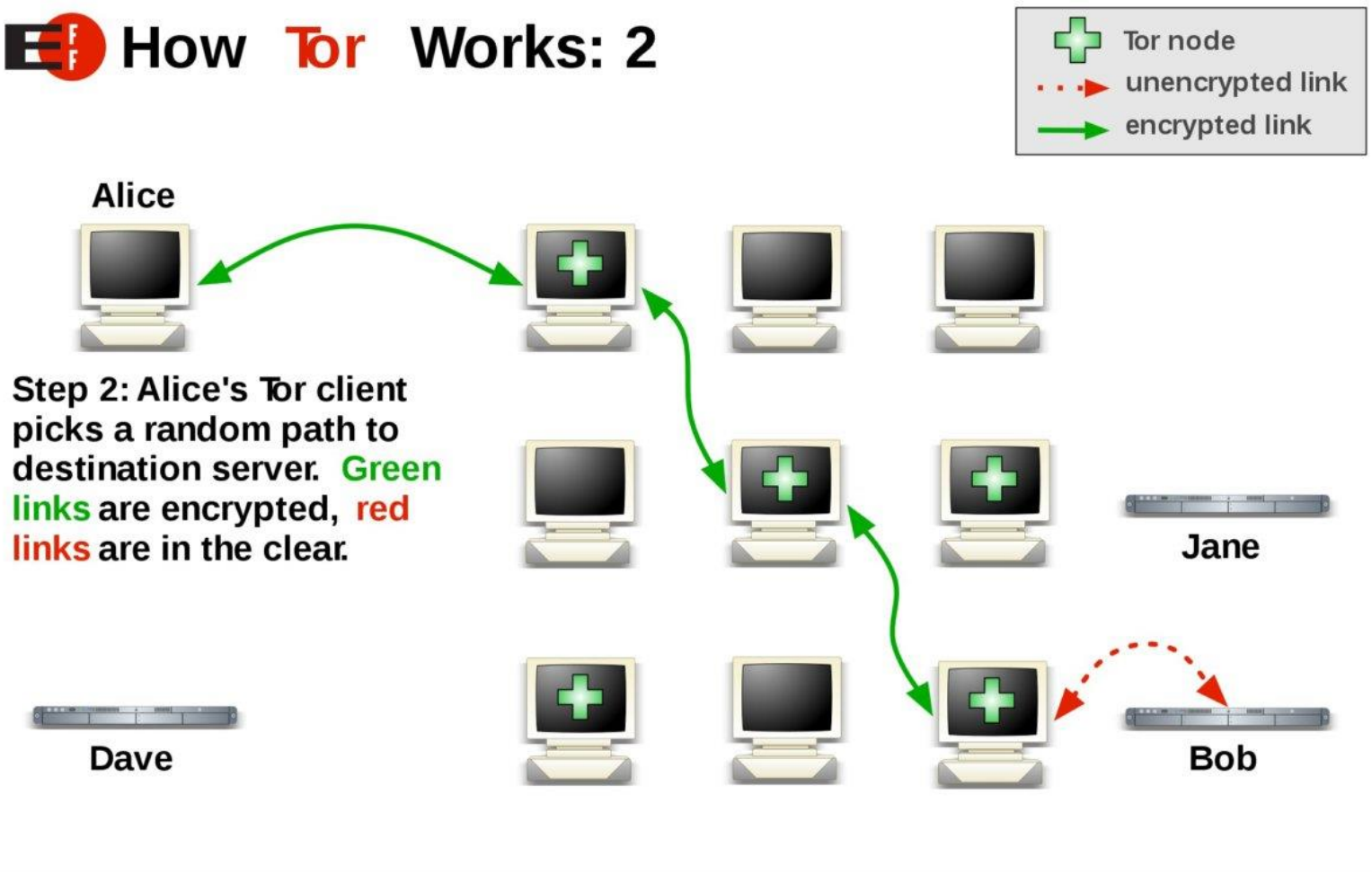




ANONIMATO E  
**DEEP WEB**

# Segurança na Deep Web

## How Tor Works: 2

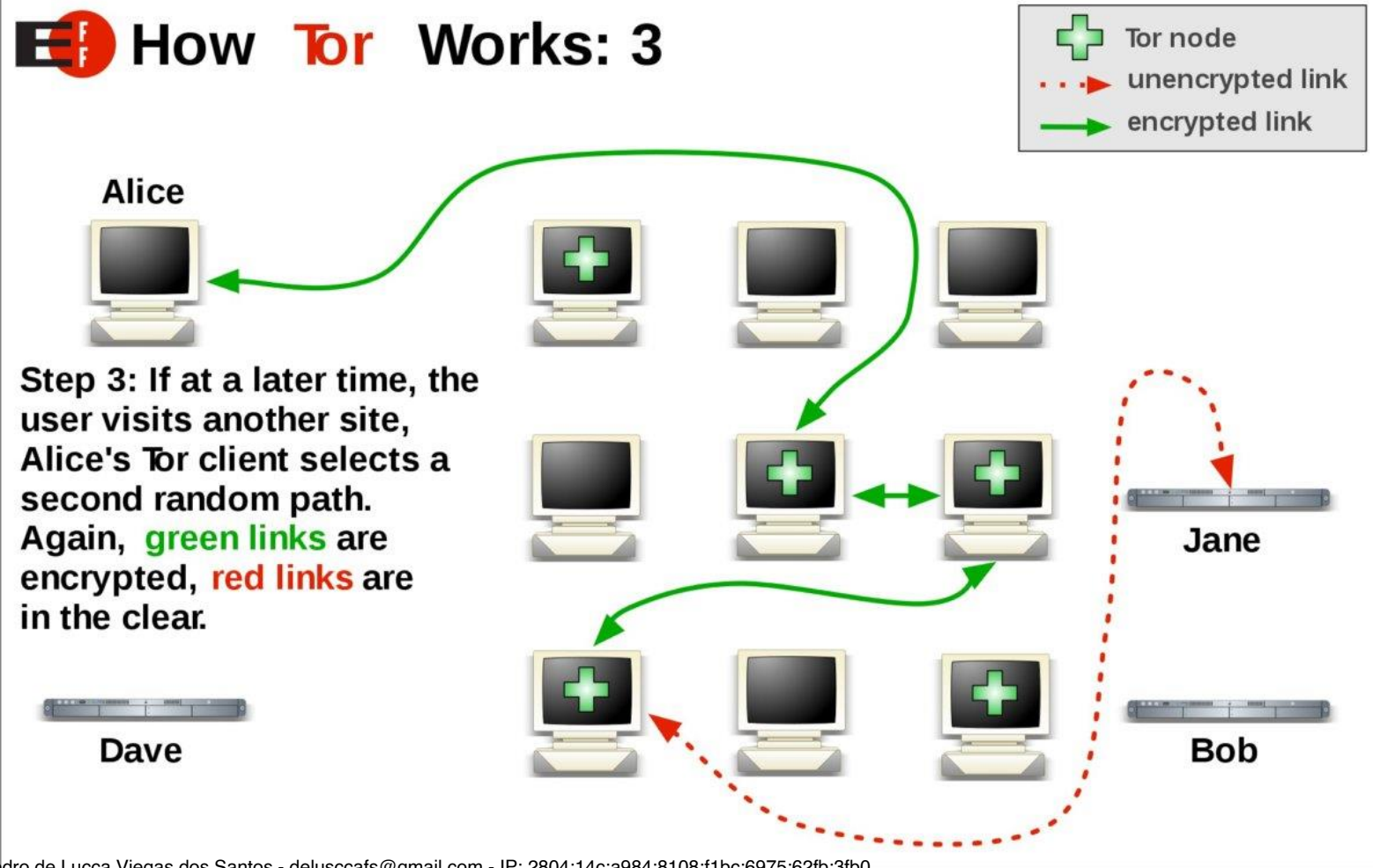




ANONIMATO E  
**DEEP WEB**

# Segurança na Deep Web

## How Tor Works: 3





ANONIMATO E  
**DEEP WEB**

# Segurança na Deep Web

## O que o Tor fornece

Navegação anônima na internet,  
por meio de uma VPN  
descentralizada.

Não permite trackers.

Não armazena histórico ou cookies.

## O que o Tor não fornece

Anonimato para todos os  
programas que rodam na máquina.

Ausência de rastros da execução do  
Tor na máquina.

Bom senso do usuário ao navegar.

# Máquinas Virtuais



ANONIMATO E  
**DEEP WEB**

# Segurança na Deep Web

**Uma máquina virtual é um sistema operacional que roda em um hardware emulado dentro de outro sistema operacional nativo.**

Assim, pode-se simular vários computadores dentro de um mesmo computador, através do uso de um virtualizador.

VMWare Player:

<https://www.vmware.com/br/products/workstation-player.html>

VirtualBox: <https://www.virtualbox.org>

# Usando o Whonix



ANONIMATO E  
**DEEP WEB**

# Segurança na Deep Web

## O que o Whonix fornece

Navegação anônima na internet, por meio de uma VPN descentralizada.

Não permite trackers.

Não armazena histórico ou cookies.

Anonimato para todos os programas que rodam na máquina.

## O que o Whonix não fornece

Ausência de rastros da execução do Whonix na máquina.

Bom senso do usuário ao navegar.



# Usando o Tails



ANONIMATO E  
**DEEP WEB**

# Segurança na Deep Web

## O que o Tails fornece

Navegação anônima na internet, por meio de uma VPN descentralizada.

Não permite trackers.

Não armazena histórico ou cookies.

Anonimato para todos os programas que rodam na máquina.

Ausência de rastros da execução do Whonix na máquina.

## O que o Tails não fornece

Bom senso do usuário ao navegar.

# Hábitos para manter o anonimato



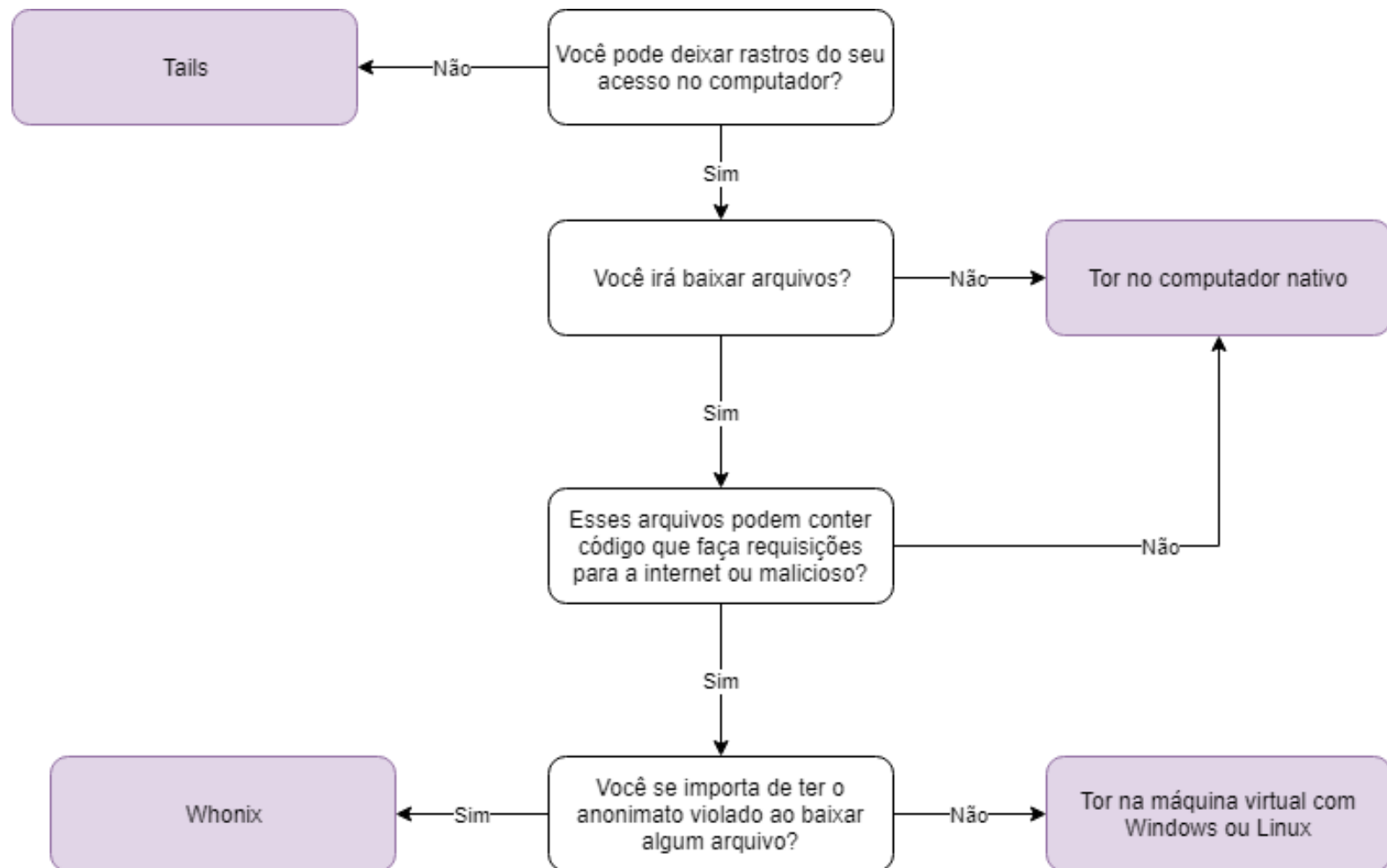
1) Decida qual das formas de anonimato é melhor para você, e se comporte conforme as limitações da forma escolhida.

	Tor no computador nativo	Máquina virtual com Windows/Linux + Tor	Whonix	Tails
IP camuflado na conexão	SIM	SIM	SIM	SIM
Ambiente isolado	NÃO	SIM	SIM	SIM
IP camuflado globalmente	NÃO	NÃO	SIM	SIM
Vestígios eliminados	NÃO	NÃO	NÃO	SIM



ANONIMATO E  
**DEEP WEB**

# Segurança na Deep Web





ANONIMATO E  
**DEEP WEB**

# Segurança na Deep Web

## **2) Jamais vincule seu acesso anônimo com informações relacionadas a você.**

Essa diretriz pode ser traduzida em “nada entra ou sai do acesso anônimo”.

Ou seja, jamais use, ao fazer um acesso anônimo, contas que estejam vinculadas a você (como redes sociais ou e-mail).

E jamais use, fora do acesso anônimo, contas que você usou no acesso anônimo.

Se precisar de uma conta, crie-a durante o acesso anônimo em provedores que não exigem dados, ou com todos os dados falsos.

**Jamais informe dados pessoais verdadeiros no acesso anônimo.**



ANONIMATO E  
**DEEP WEB**

# Segurança na Deep Web

## 3) Para o Tails:

Destrua a unidade utilizada após o acesso: triture-a, coloque fogo, etc.



ANONIMATO E  
**DEEP WEB**

# Segurança na Deep Web

## 4) Para o Whonix:

O Whonix permite usar qualquer sistema operacional como Workstation. Porém, evite usar outros navegadores além do Tor para acessos anônimos, uma vez que esses navegadores não são projetados para o anonimato.

Jamais mantenha arquivos que possam te identificar na Workstation. Se suspeitar de comprometimento, faça uma nova Workstation.





ANONIMATO E  
**DEEP WEB**

# Segurança na Deep Web

## 5) Para Tor em máquinas virtuais:

Alguns tipos de malwares ainda conseguem escapar do ambiente controlado, apesar disso ser raro. Portanto, mantenha-se cauteloso.

Lembre-se sempre que, a partir da execução de um arquivo, podem haver conexões não anônimas com a internet, violando seu anonimato.

Instale um monitorador de rede para analisar melhor o comportamento dos arquivos que você baixa.

Aprenda, usando as técnicas de navegação segura apresentadas em

<https://www.youtube.com/watch?v=8zVsR495F-M>, a identificar potenciais arquivos maliciosos e assim evita-los.



ANONIMATO E  
**DEEP WEB**

# Segurança na Deep Web

## 6) Para Tor no computador nativo:

Evite downloads ao máximo, a menos que você realmente saiba o que está fazendo.

Certifique-se de que não há programas espiões em sua máquina que possam comprometer o anonimato.

Não instalar extensões ou plugins no Tor.

3

# ACESSANDO A DEEP WEB

# Segurança na Deep Web



ANONIMATO E  
**DEEP WEB**

# Segurança na Deep Web

Faremos um breve exercício lógico:

**Pessoas usam a Deep Web como forma de permanecer anônimo, e têm sucesso. Inclusive criminosos.**

Portanto:



ANONIMATO E  
**DEEP WEB**

# Segurança na Deep Web

Faremos um breve exercício lógico:

**Pessoas usam a Deep Web como forma de permanecer anônimo, e têm sucesso. Inclusive criminosos.**

Portanto:

**A Deep Web fornece segurança e anonimato para os usuários.**



ANONIMATO E  
**DEEP WEB**

# Segurança na Deep Web

Faremos um breve exercício lógico:

**Pessoas usam a Deep Web como forma de permanecer anônimo, e têm sucesso. Inclusive criminosos.**

Portanto:

**A Deep Web fornece segurança e anonimato para os usuários.**

Logo:

**A Deep Web também lhe fornecerá segurança ao acessá-la.**



ANONIMATO E  
**DEEP WEB**

# Segurança na Deep Web

Faremos um breve exercício lógico:

**Pessoas usam a Deep Web como forma de permanecer anônimo, e têm sucesso. Inclusive criminosos.**

Portanto:

**A Deep Web fornece segurança e anonimato para os usuários.**

Logo:

**A Deep Web também lhe fornecerá segurança ao acessá-la.**

O que significa que:

**Você está mais seguro acessando-a do que acessando a Surface Web.**





ANONIMATO E  
**DEEP WEB**

# Segurança na Deep Web

## O momento do acesso

As duas principais características de qualquer rede da Deep Web são a descentralização e o anonimato.

Essas características valem para absolutamente qualquer pessoa que acessa determinada rede, seja ela um criminoso, um agente do FBI, ou você.

Todos os usuários de uma dada rede da Deep Web (e isso é especialmente válido para a Tor) estão protegidos e com suas identidades ocultadas no momento em que realizam o acesso. Não há como ninguém te localizar nesse momento.



ANONIMATO E  
**DEEP WEB**

# Segurança na Deep Web

## Mantendo o anonimato

- Siga as instruções da aula passada, incluindo o fluxograma para a Onion.
- Para outras redes, use seu computador nativo caso não pretenda baixar arquivos, uma máquina virtual caso pretenda baixar arquivos sem se importar com o anonimato, ou uma máquina virtual com Whonix Gateway caso se importe com o anonimato.



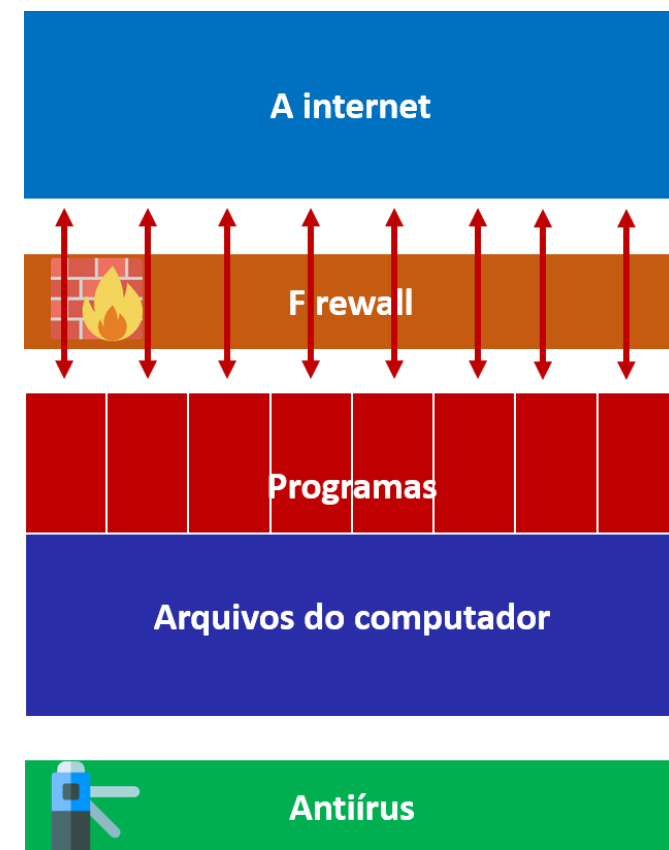
ANONIMATO E  
**DEEP WEB**

# Segurança na Deep Web

## Devo usar antivírus ou firewall?

O antivírus age como um filtro que checa os arquivos que entram na máquina, eliminando aqueles considerados maliciosos e permitindo a entrada daqueles considerados seguros. Adicionalmente, o antivírus também pode procurar por atividades suspeitas já dentro da máquina.

Os programas autorizados funcionam no computador, e se conectam com a internet para enviar e receber informações. Esse tráfego é filtrado pelo firewall, que bloqueia as conexões consideradas suspeitas e permite aquelas consideradas seguras, tanto de entrada quanto de saída.



Entrada de arquivo





ANONIMATO E  
**DEEP WEB**

# Segurança na Deep Web

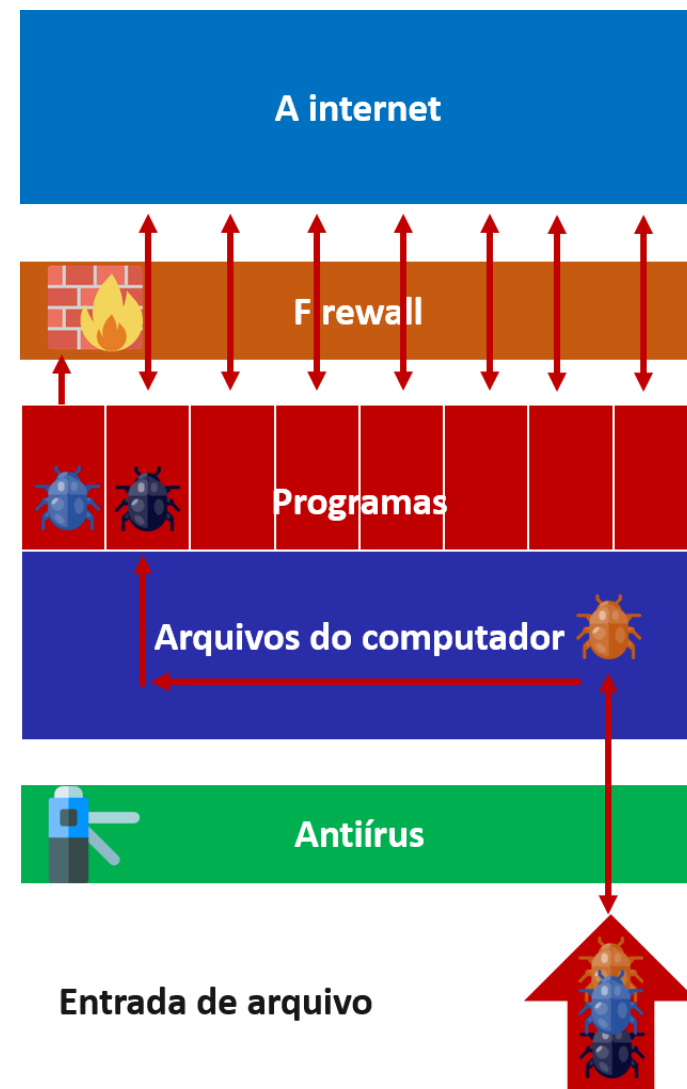
## Devo usar antivírus ou firewall?

Assim, quando um arquivo malicioso tenta entrar na máquina, o primeiro filtro é o antivírus. Muitos tem sua entrada barrada neste momento, mas outros conseguem passar essa barreira e se instalam no computador.

Quando isso acontece, existem duas opções: o programa malicioso pode agir dentro da própria máquina, danificando arquivos ou trancando-os com senha ou, ainda, se conectar à internet para transmitir informações roubadas da máquina ou para fornecer o controle da máquina a um atacante, que pode usá-la para o fim que bem desejar.

Para os que realizam a conexão, é possível que o firewall impeça o tráfego de entrada ou o de saída, evitando, assim, que haja troca de informações entre o programa malicioso e a internet.

Porém, alguns ainda conseguem passar o firewall e, com isso, além de ter acesso ao sistema de arquivos da máquina, estes ainda podem estabelecer um canal de comunicação entre a máquina e uma pessoa com más intenções fora dela.





ANONIMATO E  
**DEEP WEB**

# Segurança na Deep Web

## Devo usar antivírus ou firewall?

Existem duas formas de evitar que tais coisas aconteçam. A primeira delas é utilizando o antivírus mais poderoso que existe: o próprio usuário.

Se você dedicar algum tempo para aprender quais tipos de arquivos são mais propensos a possuírem ameaças, você será capaz de selecionar o que entra e o que não entra na sua máquina melhor do que qualquer antivírus.

Estudar [técnicas de navegação segura](#) pode lhe ajudar nisso.

Assim, use os mesmos recursos que você já está acostumado a utilizar ao navegar na Surface Web.



ANONIMATO E  
**DEEP WEB**

# Segurança na Deep Web

## Devo usar uma VPN?

Não! Uma VPN centralizada sobre o Tor pode, inclusive, quebrar o anonimato criado pelo Tor.

Uma VPN centralizada sob o Tor é inútil, e só deixará a conexão mais lenta, no máximo fornecerá pseudo anonimato para os demais processos.

Se você precisa de anonimato global, use as técnicas estudadas anteriormente com VPNs descentralizadas.



ANONIMATO E  
**DEEP WEB**

# Segurança na Deep Web

## Qual sistema operacional devo usar?

Observando as medidas já estudadas, use o sistema operacional que você já está acostumado a usar.



ANONIMATO E  
**DEEP WEB**

# Segurança na Deep Web

## **Estarei sob vigilância constante de hackers e policiais ao acessar a Deep Web?**

Todas as formas de quebra de anonimato ou de causar danos ao seu computador que estudamos também são estudadas e exploradas por hackers e agentes policiais. Por melhor que sejam, eles não são magos ou feiticeiros, capazes de fazerem o que quiserem com alguns cliques e comandos de terminal: toda ação envolve a descoberta e exploração de uma vulnerabilidade específica, e você pode impedir que essa vulnerabilidade ocorra seguindo as recomendações aqui presentes.

Além disso, as pessoas na Deep Web reconhecem que vulnerabilidades do tipo são raras e difícil de serem exploradas e, justamente por essa razão, não ficam à espreita do menor deslize para explorar essas vulnerabilidades e lhe atacar. Na maioria das vezes, expor uma vulnerabilidade por um curto período não tem maiores implicações, especialmente se você está agindo dentro da lei.





ANONIMATO E  
**DEEP WEB**

# Segurança na Deep Web

## **Estarei sob vigilância constante de hackers e policiais ao acessar a Deep Web?**

Por fim, ter seu endereço de IP revelado pode, no máximo, permitir que alguém com uma ordem judicial ou com um grande poder de chantagem chegue até você. Você não será intimado judicialmente se não cometer crimes, e precisará incomodar muita gente poderosa para que alguém se preocupe em chantagear seu provedor de internet visando conseguir seus dados. Um endereço de IP por si só não revela sua localização física, nem seus dados pessoais: apenas a região em que você está (a cidade correta ou uma cidade próxima), seu provedor de internet e seu histórico de *torrents*.



ANONIMATO E  
**DEEP WEB**

# Segurança na Deep Web

## Acessar a Deep Web é ilegal?

A maioria dos países (incluindo o Brasil) não possuem legislações que proíbam o acesso ao Tor ou a demais redes anônimas e descentralizadas.

Porém, cometer crimes na Deep Web – ou em qualquer outro lugar – é ilegal. A melhor pessoa para lhe responder o que exatamente é considerado crime não sou eu, mas sim um advogado.

Em linhas gerais, se seu objetivo é somente acessar para “conhecer”, sem participar de atividades específicas, não é ilegal.

# Navegando na Onion

# Navegando na Freenet

# Navegando na I2P

# Navegando na Ecnet

# Navegando na Zeronet

# Usando o Tox