Anonymous Networks

- When working **online everything** you do could be **traced** back to **your machine.**
- For example, surfing the Web, sending e-mails, conducting online banking, and posting data to blog.
- **Internet Protocol (IP)** address, is the main identifier of all online users.
- To anonymize your location online, you are mainly concerned with concealing your IP address.
- There are different techniques you can employ to conceal an IP address, some of which are more secure than others.
- **Anonymous networks**, which offer the maximum protection and anonymity in today's digital age.
- In addition to being used by casual users, anonymous networks are used by military personal, law enforcement, criminals, hacking groups, terrorists, pedophiles, whistle-blowers, journalists, and of course anyone else who wants to disappear when entering the online world.

Tor Network

- Tor (formerly an acronym for "The Onion Router") is often touted as a way to browse the web anonymously.
- From human rights activists evading oppressive governments to drug dealers selling through online marketplaces, Tor is a popular way to gain significantly more anonymity than you would normally have online.
- At the same time, Tor isn't perfect, so it can provide a false sense of security if used incorrectly.

- Tor (formerly an acronym for "The Onion Router") is often touted as a way to browse the web anonymously.

- From human rights activists evading oppressive governments to drug dealers selling through online marketplaces, Tor is a popular way to gain significantly more anonymity than you would normally have online.
- At the same time, Tor isn't perfect, so it can provide a false sense of security if used incorrectly.

WHAT IS TOR BROWSER?

- Tor (formerly an acronym for "The Onion Router") is often touted as a way to browse the web anonymously.
- From human rights activists evading oppressive governments to drug dealers selling through online marketplaces, Tor is a popular way to gain significantly more anonymity than you would normally have online.
- At the same time, Tor isn't perfect, so it can provide a false sense of security if used incorrectly.

The primary uses of Tor are the following:

1. Bypassing censorship and surveillance
2. Visiting websites anonymously
3. Accessing Tor hidden services (.onion sites)

Pros:

1. If you use Tor correctly, your real IP address cannot be determined by the websites you visit.
2. You can access websites without your internet service provider being aware of your browsing history.
3. You can bypass many kinds of censorship.

Cons:

1. Tor is very slow compared to VPNs and regular web browsing, so downloading large files is usually not feasible.
2. It's possible to deanonymize your browsing by making a simple mistake.
3. Some governments and network operators can prevent Tor from functioning.

4. Although using Tor is legal in and of itself, using Tor may make your activity appear suspicious.
5. Websites may refuse to function when you're using Tor—generally to prevent anonymous spam and abuse.

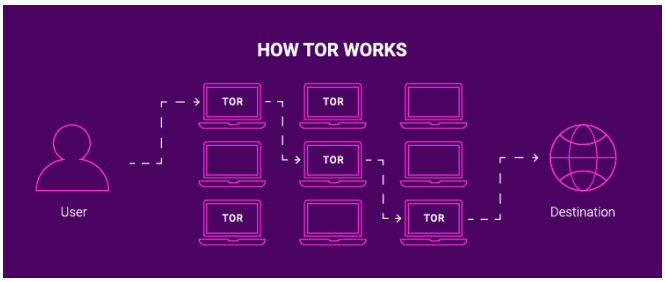
WHO DEVELOPED TOR?

- The onion routing (Tor) was developed by the United States government in the 1990s.
- It was originally designed to protect the communications of US intelligence agencies across the Internet.
- The original code for Tor was released under a free and open-source software license by the United States Naval Research Laboratory, allowing other people and organizations to contribute to the project.
- Since 2006, a nonprofit called The Tor Project has been responsible for maintaining Tor and the Tor Browser.
- Financial support comes from corporations like Google, organizations such as Human Rights Watch, and many others.

  There are two things people may mean when they say ***"Tor": the networking system and the Tor Browser.***

How Tor Works?

- To anonymize Internet usage, Tor routes traffic through multiple randomly-chosen relay servers before accessing the destination website.
- There are over 7,000 of these servers, which mostly belong to volunteers.
- The request is encrypted multiple times, so the relay servers only know the previous relay and the next relay, but not the request contents or the full circuit.
- The network request finally exits the Tor network at an exit node. From the website's perspective, you are browsing directly from the exit node.



- Tor hidden services, which will be covered below, are accessed in a slightly different way from standard websites — they use .onion domain names and are inaccessible from the regular web.
- To actually use Tor to anonymize your communications, you run the Tor Browser on your computer.
- The Tor Browser is a modified version of Mozilla Firefox that connects to the internet via the Tor network.
- In addition to the functionality necessary to use Tor, the Tor Browser also bundles a number of extensions that help users maintain their privacy.
- For example, the NoScript extension is bundled with Tor out of the box, meaning that users have to manually approve individual JavaScript files before they can run—helping to protect against fingerprinting and browser security exploits.

how safe, anonymous, and secure is it?

- The final part of the communication is unencrypted.
- Your traffic may be deanonymized using timing-based statistical techniques.
- Tor won't protect you against sophisticated fingerprinting methods.
- Even Tor has bugs that can be exploited.

Protect yourself when using Tor

1. Don’t log into your usual accounts.
2. Try not to follow any unique browsing patterns.
3. Turn the Tor Browser’s security level up to the max.
4. Use the HTTPS Everywhere extension.
5. As a general rule, never use BitTorrent over Tor.
6. Always keep Tor Browser (and any extensions) updated.

Tor hidden services

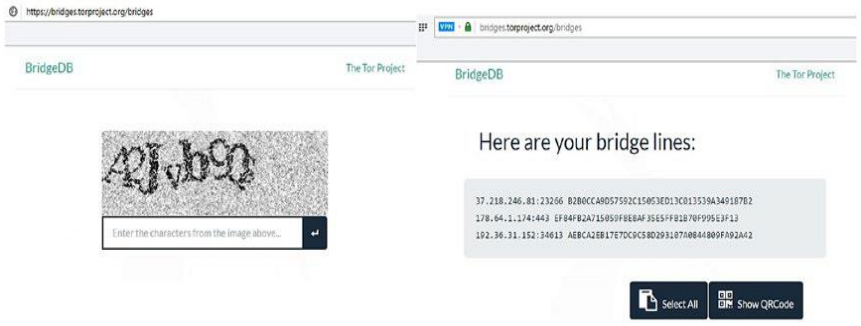
- Tor hidden services, “onion services”, or “Tor websites” are websites that are only accessible from within the Tor network.
- All hidden service domain names end in .onion and consist of a very long of seemingly-random characters.
- Collectively, Tor hidden services are sometimes referred to as the “dark web.”

Using Tor Bridges

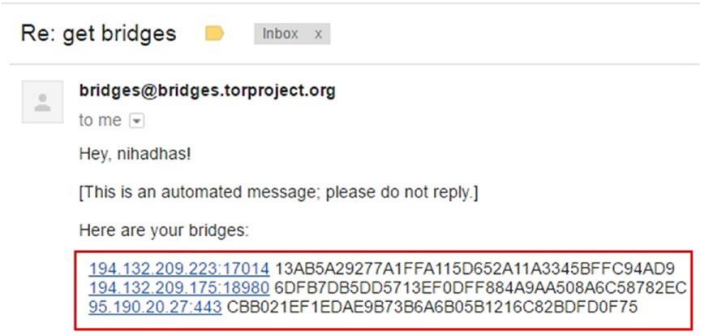
- Bridge relays (or bridges for short) are Tor relays that aren’t listed in the main Tor directory.
- Bridges are considered entry points to the Tor network.
- Since there is no complete public list of them, even if your ISP is filtering connections to all the known Tor relays, it probably won’t be able to block all the bridges.
- Please remember that this method may not fully guarantee that your ISP will not detect your Tor usage, but it will make discovering this fact difficult and will require sophisticated techniques to uncover.

To use Tor bridges, follow these steps:

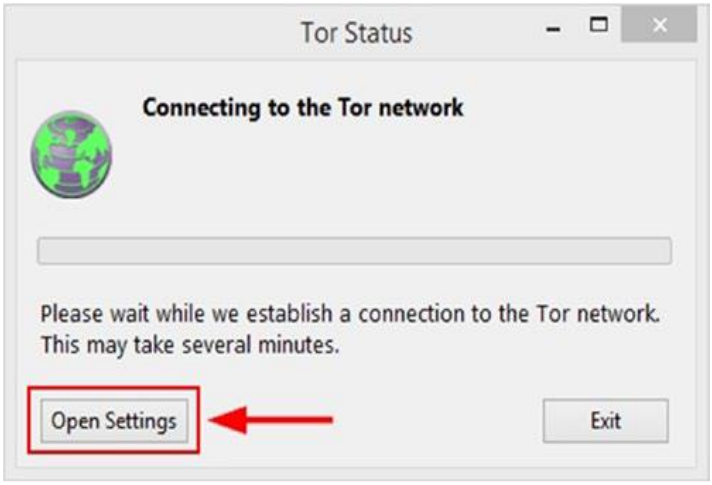
1. Go to https://bridges.torproject.org/bridges and enter the captcha to access the secure area, where you will find three bridges.



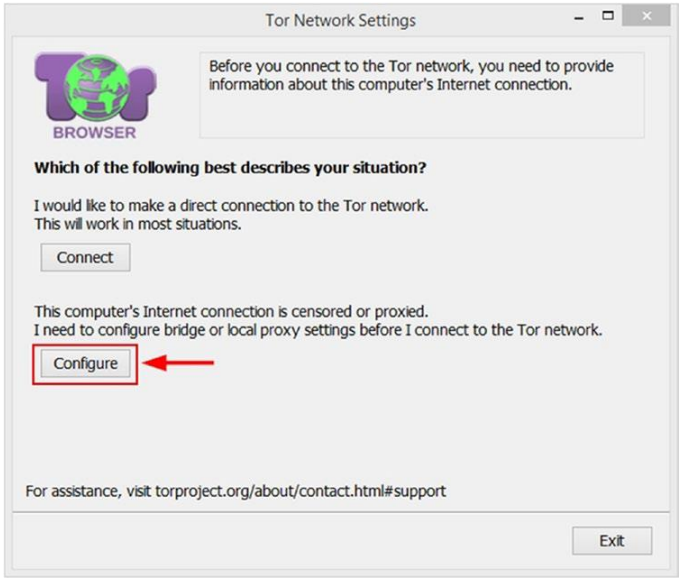
2. You can also request the bridges to arrive in your e-mail by sending an e-mail to bridges@bridges.torproject.org with the line “get bridges” by itself in the body of the mail. You’ll need to send this request from a Gmail, Riseup, or Yahoo account exclusively



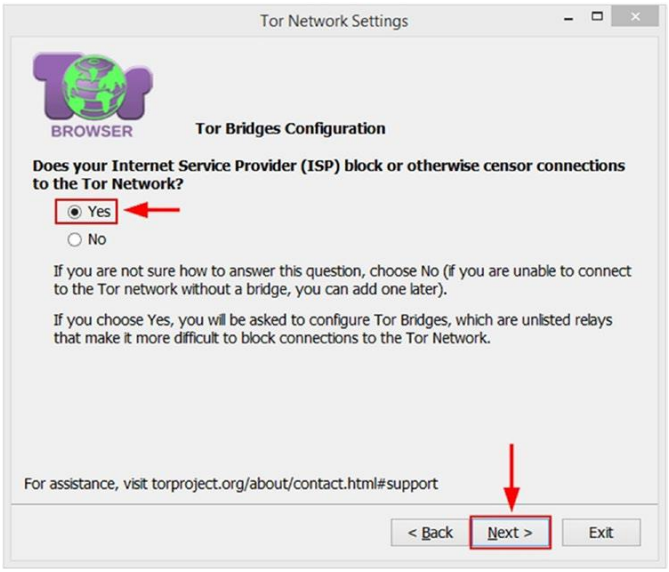
3. To enter bridges into the Tor Browser, launch Tor Browser, and before the Tor Browser connects, click the Open Settings button



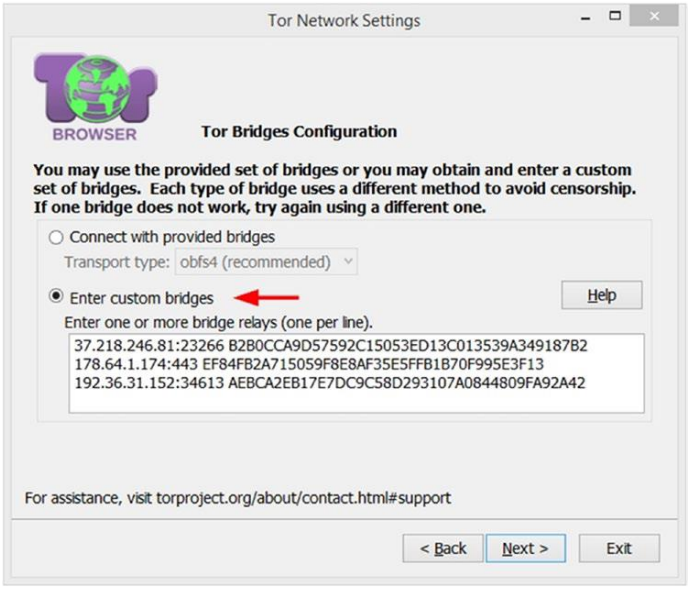
4. A Tor Network Settings window appears; click the Configure button



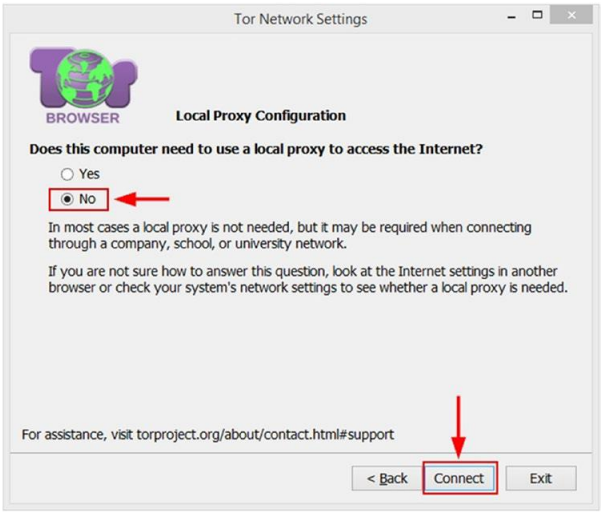
5. Tor asks you whether your ISP is blocking or otherwise censoring connections to the Tor network; select Yes (see Figure 4-7) and click Next to continue.



6. In the next wizard window, select the option "Enter custom bridges." Copy the bridges you have from step 1 or step 2 and paste them in the box; click Next to continue.



7. The next wizard asks you whether your computer sits behind a proxy server; in our case, we don't need one (which is most comment). Select No and click the Connect button to continue. If you are sitting behind a proxy server, select Yes, then enter your proxy settings, and finally click Connect.



I2P Network

- I2P is an alternative anonymity network to Tor, and it supports common Internet activities such as web browsing, e-mail web site hosting, file sharing, and real-time chat.
- Unlike Tor, whose focus is to access web sites from the normal Internet, I2P is more directed toward accessing a closed, anonymous Internet, also known as a darknet, separated from the normal Internet.
- I2P protects communications from dragnet surveillance and monitoring by different third parties (governments, ISPs, etc.).
- Anyone running I2P can run an anonymous server through a so-called eepsite, which is accessible only within I2P network using the .i2p top-level domain (similar to .Onion for Tor hidden services, as you are going to see in the next section).

How ?

To run I2P on your PC (we are using Windows for this experiment), you must have Java already installed on your machine because I2P is written using the Java programming language. You can download Java from https://www.java.com/en/download/index.jsp.

1. Download I2P from https://geti2p.net/en/download and install it like you would any ordinary Windows program.
2. Start I2P by clicking the “Start I2P (restartable)” program icon

3. The I2P service console will appear. Wait some seconds for it to connect. A browser window will also open to announce a successful connection to the I2P network.
4. After I2P starts, you need to configure your browser to access the normal Internet.
5. In our case, we will use Mozilla Firefox to configure it for I2P usage. Go to the Firefox menu, select Tools ➤ Options, go to the Advanced tab and then the Network tab, and click the Settings button.
6. In the Connection Settings window, select the option "Manual proxy configuration" and enter 127.0.0.1 in the HTTP Proxy field and 4444 in the Port field. Make sure the "No Proxy for" text box contains "localhost, 127.0.0.1." Finally, click the OK button to accept the new settings

Freenet

- This is another anonymous network. It is a fully distributed, peer-to-peer anonymous publishing network.
- We will not cover how to use this network like we did with the previous ones.
- However, you can check out http://freesocial.draketo.de for a complete tutorial on how to use this anonymous network.
- Tor, I2P, and Freenet are the most popular anonymous networks currently available.
- Tor surpasses the other two in being more widely used and more mature.
- We recommend using the Tor network for all your work that requires online anonymity.
- Later in this chapter, we will introduce Tails, which is hardened specifically to stay anonymous and to protect users' confidential and sensitive online communications.

Darknet

The term darknet also known as the deep web, deep net, or invisible web.

- All these terms are interchangeable and point to the hidden underground of an unindexed Internet
- It is hidden because regular search engines like Google and Yahoo cannot index its contents and thus it remains hidden from the general public
- The deep web refers to anything that cannot be indexed.
- For example, many government web sites have millions of documents in databases that cannot be retrieved using ordinary search engines; thus, such documents are considered part of the deep web.

How to Access the Darknet

- Web sites hosted on the darknet cannot be accessed from the regular Internet. To access these resources, you must use either the Tor or I2P network.
- A popular search engine to browse and search the darknet is Grams. It works on the Tor network only and can be found at http://grams7enufi7jmdl.onion

  These are other dark web search engines:

  1. Onion.link (http://onion.link)
  2. Tor2Web (https://hss3uro2hsxfogfq.onion.to)
  3. SurfWax (http://lookahead.surfwax.com)

Anonymous OS

- Most ordinary computer users worldwide use the Windows OS for their daily tasks, but of course there are others who prefer the macOS Google Desktop, or a Linux distribution.
- Out of the box, most OS implementations are not configured to be robust, secure, or anonymous, although you can configure them it to be more secure.
- However, by design they are not built with consideration of users who seek anonymity and security by design.
- Tails is considered the best anonymous OS currently available

- You can use Tails to communicate privately with confidence in extremely hostile environments.

Tails

- Tails stands for "the amnesic incognito live system.
- It is a Linux based operating system built to provide the maximum security and anonymity possible for its users.
- It is a portable live OS, meaning that it can be launched from within your USB stick drive without installation, and it is completely independent from the host machine's current operating system.
- Tails runs using the host machine's RAM and does not copy any files to the resident host machine's hard disk.
- Tails achieves its anonymity by forcing all network connections to go through the Tor network.
- If an application tries to connect to the Internet directly, the connection is automatically blocked Tails leaves no traces on the host machine's hard disk.
- Upon shutdown, Tails will delete all user files, unless explicitly asked not to (persistent storage
- Tails also come with several built in applications preconfigured with security in mind web browser, instant messaging client, e mail client, office suite, and image and sound editors, in addition to a plethora of cryptographic tools such as LUKS for disk encryption (Linux only), HTTPS Everywhere OpenPGP and OTR for secure IM chat.

Secure File Sharing

- Numerous providers offer file sharing online services.
- Many of which are free (although usually free accounts limit the file sizes you can upload.
- Almost all these providers store information about each online transaction that takes place through their servers.
- This is not the kind of service that security conscious people should use.

OnionShare

- OnionShare is a tool based on the Tor anonymous network dedicated to sharing files across the Internet in complete anonymity.

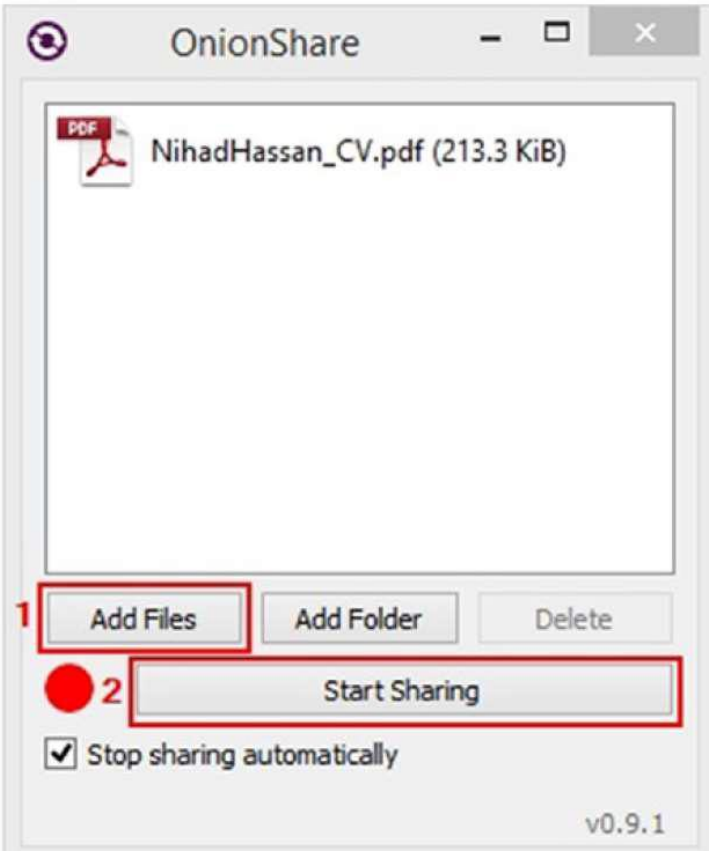
- OnionShare allows you to share files of any size anonymously using the Tor hidden network.
- It works by launching a temporary web site (similar to the Tor Onion service used in the dark web) that hosts your shared files.
- OnionShare will then produce an unguessable URL so the person you are corresponding with can access and download the shared files.
- What makes this program unique is that your shared files will not leave your computer and get uploaded to some location online instead, they will remain on your local machine, and your correspondent will download them directly using the Tor Browser.

To share a file using OnionShare , follow these
steps:

1. Download OnionShare from https ://onionshare.org/ and

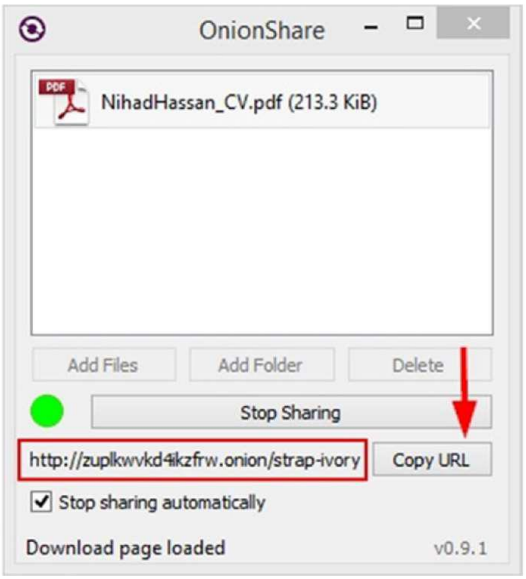
install the application like you do with any Windows program.

2. Launch OnionShare and select the files you want to share by clicking Add Files You can also add entire folders by clicking the Add Folder button instead



Adding files to OnionShare , in the same way you can add files by dragging and dropping them in the empty panel

3. Launch your Tor Browser When your Tor Browser successfully connects to the Internet, click the Start Sharing button in the OnionShare program.
4. When OnionShare successfully creates a hidden Tor service for your shared file (or files), also known as a temporary web site hosted on a Tor network, it will give you a URL to this file. The shared file (or files) will remain on your PC.



OnionShare provides a URL for your shared files, sends it to the recipient, and keeps it private

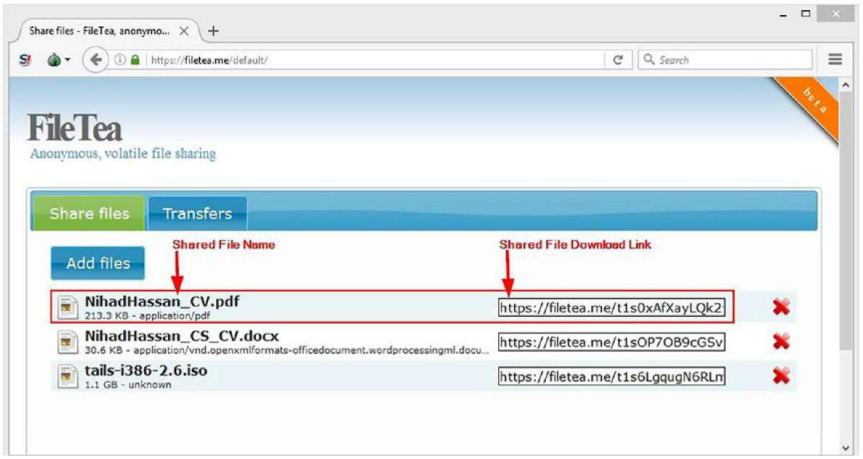
Secure File Sharing

5. Finally, all you need to do is to give the recipient the URL to that web site so he or she can download your shared file.

- Bear in mind that you must leave your Tor Browser and OnionShare programs open until the transaction ends.
- Your computer is playing the role of a hosting server for the shared file.
- When the recipient receives your file successfully, OnionShare will stop the sharing process automatically (to stop sharing automatically after recipient receives the file, you must enable the option “Stop sharing automatically” in the OnionShare program before sharing files).

FileTea

- FileTea is a new sharing provider that offers an anonymous and volatile file sharing service.
- FileTea does not store any information about its users it also does not cache the contents of files shared through its server, and it stores only limited information about each file (size, and MIME type) in the processing server's volatile memory (The IP address of the user also is not recorded anywhere.
- Sharing files is easy.
- All you need to do is go to the home page (https ://filetea me).
- click the Add files button, and select the file or files you want to share.
- FileTea will generate a link for each file copy it, and send it to the intended recipient.
- Bear in mind that your browser should remain open until the recipient receives the file FileTea will only process your file for delivery it will not upload it to its server.



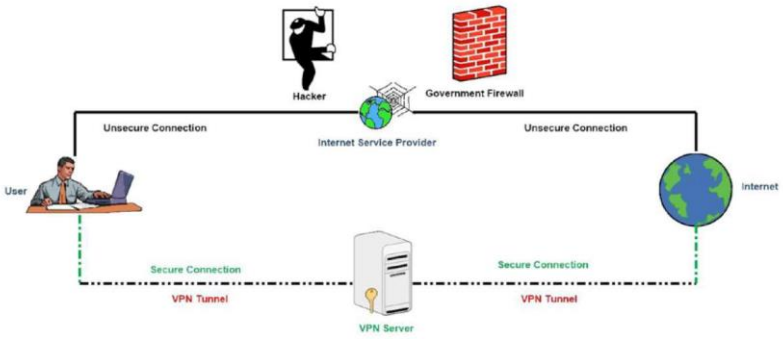
Using FileTea service to share files anonymously. We used the Tor Browser in this experiment to achieve maximum security

VPN

- A VPN works to establish a secure tunnel between two or more devices.
- Using a VPN helps users to add an extra layer of security and privacy to private and public networks such as Wi Fi connections and the Internet.
- Enterprises use VPN services regularly to secure their sensitive and business related traffic.

- However, its use by ordinary end users has become more popular of late because of the huge increase in digital communications along with the increase of cyber attacks, making more people aware of the security dangers when utilizing online services.
- When using a VPN, an organization can secure private network traffic over an unsecured network such as the Internet.
- Thus, users feel safe connecting their personal devices to the Internet, ensuring their banking details, credit card numbers, passwords, and any other sensitive data is not intercepted by an unauthorized party.
- The VPN also gives the user an anonymous IP address, making them appear as if in another location so they can avoid censorship, share files with other people anonymously, and more.

How a VPN works



Criteria to Select the Best VPN

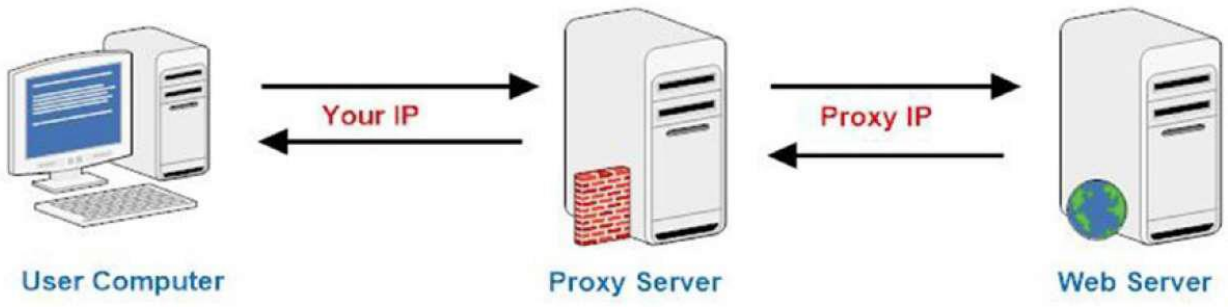
- Do not subscribe to VPN service providers that are based in one of the following countries the United States, United Kingdom, Australia, New Zealand, Canada, Denmark, France, Netherlands, Norway, Belgium, Germany, Italy, Spain, Israel, Sweden, and of course countries such as Russia, China, Iran, and all Arab states.
- The VPN provider must support the OpenVPN software this is an open source program that can be audited by anyone to make sure it is clean and does not contain backdoors.
- The VPN provider must separate Internet traffic according to the protocol used For example, it should separate web browsing from file sharing, meaning that each one has a dedicated server.

- The VPN client software must support the ability to disconnect the Internet from your computer if the VPN fails for any reason (to avoid leaking your current activities to your ISP).
- It is better to support multiple devices at the same time, so you can protect your tablet and smartphone data in addition to your laptop or PC.
- It should accept anonymous payments such as bitcoin, gift cards, debit cards, and cash, if possible without showing any IDs.
- It should not require many details to set up; a username and a password should be enough.
- It should not store any information about its users.

Proxy Server

- A proxy or proxy server is basically another computer that serves as a hub through which Internet requests are processed.
- Your computer will connect to a proxy server requesting some services like a web page, a file, or other resources available from another server The proxy server will fetch the required resources and send them to your computer.
- Today, most proxies are web proxies Their major job is to facilitate access to content on the Internet and provide anonymity by changing the real IP address of the user's computer into the IP address of the proxy server.

How a proxy server works



Connection Leak Testing

Online Anonymity Test: What Data Does Your Device Leak?

- YES. As user surf the internet, you constantly share information about your computer and internet connection with other parties. This applies to user desktop and laptop as well as user smartphone and tablet.
- Apart of this information exchange is necessary: without it, your internet connection could not be established and websites would not be properly displayed on your device.
- For example, a website might need to know whether you want to access the mobile or desktop version of a page.

How to avoid data leakage

1. **How to hide your IP address**
    - Everything you do online can be traced by your ISP and numerous other parties such as intelligence services and hackers because this information is linked to your IP address.

- So how do you keep your browser from leaking your IP address? If you use a VPN or an invisible proxy, the websites you visit, your ISP, the government and any other party that tries to monitor your behavior will see a different IP address. This means your own IP address will remain hidden – at least, in most cases.
- When you use a VPN, the actual IP address of your computer won't match the one shown in our test. Your VPN connection hides your real IP address and instead of your real IP address, the rest of the internet just registers the IP address of the VPN server. Moreover, unlike a proxy, a VPN encrypts your data traffic. This way, no one can see what you're doing online and which websites you're visiting. This improves your online security and anonymity.

2. Change your online location

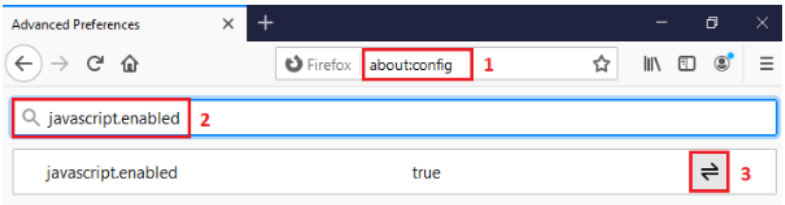
- If you want to hide your location, a VPN is used. Since the virtual location is derived from your IP address, using a VPN means you'll take on the virtual location of the VPN server.
- In other words, the location displayed to others will differ from your actual location.
- For example, if you live in the United States and use a VPN server in Germany, the location displayed could be "Berlin, Germany" instead of "New York, USA". By hiding your IP address, you'll also be able to hide your real location.
- Note: your browser has additional tactics to determine your location more precisely.

- In addition to your IP address, there are also things like Html5 geolocation which reveal information about your whereabouts.
- But for Html5 geolocation, you usually actively have to give permission.

Enable or disable JavaScript in Mozilla Firefox

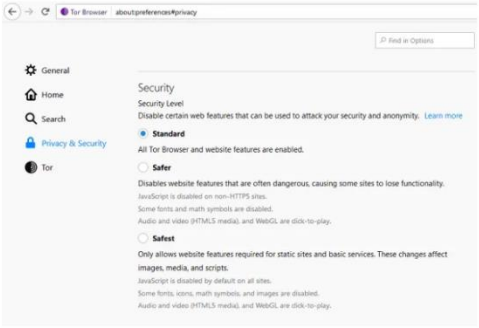
To manage JavaScript in the Firefox browser (desktop), follow these steps:

1. Open the Firefox browser and type in the following in the address bar: about:config.
2. Click on Enter. You will now get a warning from Firefox that you should be careful with changing your Firefox configuration as it can affect security. Accept this and you will see a search bar. Here you type in: javascript.enabled.
3. If JavaScript is enabled, it will read “true”. If JavaScript is disabled, it will be “false”. With the button on the right you enable or disable JavaScript.



Enable or disable JavaScript in the Tor browser

- The Tor browser is based on the Firefox browser. In Tor you can click on the three horizontal lines at the top right and then choose “Options”.
- Then choose Privacy & Security in the menu on the left and scroll down. Here you can then choose Standard, Safer or Safest. To block JavaScript on non-encrypted websites, choose Safer.
- To disable JavaScript for all websites, choose Safest. Be aware that with the latter option many sites will function sub-optimally, but this offers the greatest degree of security.



Secure Search Engine

- Almost all Internet users have used a search engine in one way or another Google is the largest search engine it has a reputation for being easy to use and able to offer the best search results relevant to the user’s search criteria
- However, Google is a privacy nightmare for its users because it records everything done online, with many of its subscribers being unaware of this fact.

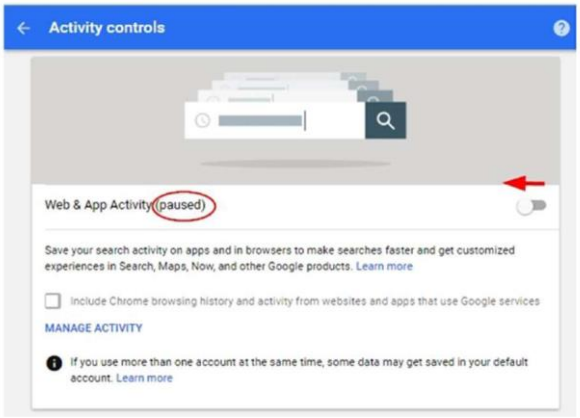
- With Google Voice Search (which allows users to search using their voice instead of typing a search keyword), Google records all your voice searches in your Google account (of course you need to be signed in to your Google account when using it).
- Google also records all your typed search keyword history the same history is kept for YouTube com searches.
- The search history can reveal a great number of details about any user, such as current health condition, sexual habits, buying habits, political opinions, geographic location, and more.
- Most users now use GPS capable devices for accessing the Internet, such as smartphones and tablets, and if a user "check ins" at some locations while signed in to a Google account, Google will record this also (this service is known as location reporting).
- A timeline of all places the user has used his or her mobile phone or tablet will be recorded and linked to the user account.
- What enables Google to perform these tracking issues in a simple and automatic way is the popular free e mail service Gmail (note that Google can track your online activity even though you are not logged into your Google account).
- Users usually sign in to check their e mail accounts and then remain signed in and use the Internet as usual.
- This allows Google to record their activities while using its services and link it back to each user account.
- The same thing happens with smartphone devices running Android OS (developed by Google) a user may remain signed in to his or her Google Play account (which is used to download/update apps and needs a Google ID to work) and use the phone as usual to send e mails or to conduct online searches, resulting in tracking and recording much of his or her online activities.

Configure Your Google Account to Stop Saving Your Activity

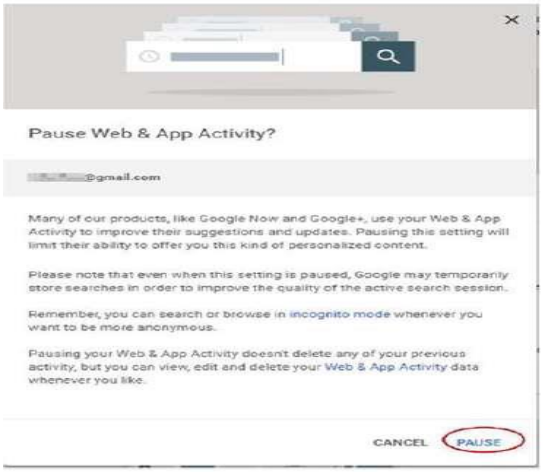
To configure Google to stop saving your private data (search history, location history, etc on any device you are using to access Google services, do the following

1. Go to https://myaccount.google.com/activitycontrols (you must be signed into your Google account first).

2. Beginning at the top with the Web App Activity section, move the slider to the left to turn off this feature. A warning message will appear click PAUSE to confirm your action. Finally, the word Paused will appear next to the section title



Turning off Web & App Activity in a Google account



Confirming you want to pause your Google account activity

Web Browser Privacy Configuration

- There are many browsers in the market.
- The market share is dominated by five of them Firefox, Chrome,Internet Explorer, Opera, and Apple Safari.
- Of course, there are some lesser known browsers such as UC Browser SRWare Iron that have proven their presence in the market lately.

- However, these browsers are either an implementation of one of the major browsers already mentioned or were developed in countries where users' privacy is not respected.
- For example, Iron is an implementation of the Chromium project Both Google Chrome and Iron share much of code and features from the same project but with different licensing agreements The UC browser was developed by a Chinese company.

Check the Browser Fingerprint

- A browser fingerprint is any information that is used to identify your machine online.
- It can be used to fully or partially identify individual users or devices even
- when cookies are turned off.
- Browser fingerprinting is used to identify individual users online and is considered, relatively, a new technique for tracking and recording the online activities of users stealthily.
- Browser fingerprinting can reveal a great amount of information about your computer.
- It works by loading a script (generally JavaScript or Flash) into your browser.
- Once it has loaded successfully, it will detect a wide array of technical information about your computer, such as screen resolution, OS type, supported fonts, browser type and version, add ons installed, and even your PC hardware components.
- Some add on providers may fool the user and collect personal identifying data about browsing habits and even personal information without his or her consent, so it is advisable to avoid installing any add on except the ones mentioned below.
- They are like HTTPS Everywhere, Privacy Badger Disconnect uBlock Origin Random Agent Spoofer

Anonymous Payment

- Anonymous payments are sometime perceived by the public to be used by criminals and terrorist groups
- A user can have many reasons to conceal his or her purchase history
- For example, some users may not feel safe to give their personal details to online merchants, others may not want to reveal what they buy (e g the purchase of sexual items could be embarrassing)

- Prepaid Gift Cards There are different types of prepaid cards Prepaid cards (the non reloadable type) are available almost everywhere, from drug stores to supermarkets.
- Prepaid cards are also available online.
- The other types of prepaid cards: Open loop prepaid card, Closed loop prepaid card, Reloadable prepaid card, Nonreloadable card Payroll card, Government benefits card, Student prepaid cards.
- Open loop prepaid card This belongs to a general credit card provider and carries its logo (e g Visa, Mastercard American Express, Discover) You can use this card anywhere you can use the ordinary card type However, this type is not anonymous because you need to supply your information to get one.
- Closed loop prepaid card This card can be used to make purchases from a single company It will carry the initiated company logo (not the credit card provider company like Visa or Mastercard and cannot be used for general purchases.
- Examples of this card are from Starbucks, telephone, fuel, stores.
- Reloadable prepaid card This is a general purpose card that consumers “load up” and spend almost anywhere This type is usually issued by popular credit card providers like Visa, Mastercard and American Express.
- Nonreloadable card This card doesn’t require any personal information to have it This type of card is widely available in major supermarkets and pharmacies, and you can buy it with cash to completely conceal your identity Major credit card providers like Visa and Mastercard issue this type of card.
- Payroll card This is usually issued by employers to their employees who do not have a bank account to receive their salary Employees can use this card to purchase items online and pay bills Obviously, this is not an anonymous card.
- Government benefits card This is issued by some government agencies to pay unemployment benefits, child support, and other government benefits
- Student prepaid cards These cards are offered by universities for their students to pay for things on campus.
- Cryptocurrency: This is a type of digital currency that is designed to work as a medium of exchange using cryptography to secure the transaction and to control the creation of additional units of currency.

- Bitcoin was the first decentralized crypto currency, appearing in 2009 and remains the dominant currency in terms of use and capitalization.
- Bitcoin Bitcoin (https ://bitcoin org) is an innovative Internet protocol created by a software developer group called Satoshi Nakamoto Bitcoin uses SHA 256.
- It is a decentralized peer to peer payment network
- Bitcoin is a digital system.
- It is not printed like ordinary currency (dollars and euros and is created by people and companies using a specialized open source software program called a bitcoin wallet.
- Bitcoin does not charge fees on transactions, and it is nonrefundable.