Deon Perera

The Tor Network

1. What is Tor?

'It is impossible to have perfect anonymity' (TOR. n.d. para.4), however, TOR provides an open-source privacy technology to improve online anonymity.

When a user is connected to the TOR network, their internet traffic is passed through at least three nodes. Moreover, internet traffic is encrypted with multiple layers of encryption. Therefore, internet activity is hidden; the ISP can observe the TOR entry node's IP address and the website server we visit sees the TOR exit node's IP address. Effectively, it is impossible to trace a Tor connection to the original user., Tor allows us to access the Tor Network which houses the dark web, and lastly, it provides untraceable communication.

At the final node, internet traffic is unencrypted and transmitted to the server. Consequently, the exit node can see internet traffic, although the risk is mitigated with HTTPS.

TOR prevents ISPs and third parties from collecting information and bypasses censorship. As a result, TOR is beneficial for journalists, whistleblowers, activists, and other entities that require unfettered and anonymous internet use. Simply stated, TOR is an unregulated environment; generally, users can publicise any material without consequence.

It is important to understand that the TOR network is used for both legal and prohibited activities, including creating open forums for extremist groups and creating illicit marketplaces.

2. Is it legal?

In Australia there is nothing intrinsically prohibited about the use of Tor.
However, the Tor network hosts a plethora of illegal activities, and accessing or participating in this material may be incriminating. Furthermore, some countries like China have blocked Tor.

3. What is a Tor Circuit?

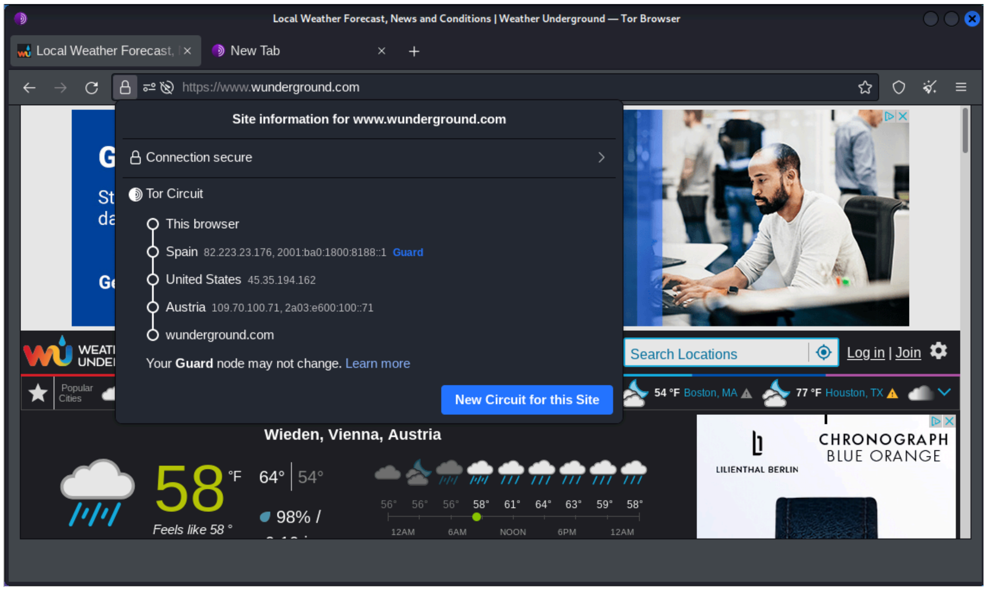
Tor's anonymity is facilitated by transmitting packets through relays located in various geographical locations. The transmission of data through the sequence of relays is characterised as a 'circuit'. As such, *Tor Circuit* refers to the sequence of relays the packets pass through.

Questions 5b and 6 have different relays located in different geographical locations. Therefore, the website server presumes that I live in the location of the exit node.

Deon Perera

Visit https://www.wunderground.com/
Using tor browser, let's demonstrate changing of location

Screen shot 1: Location: Wieden, Vienna, Australia
Screen shot 2: Location: Spain



Local Weather Forecast, News and Conditions | Weather Underground — Tor Browser

https://www.wunderground.com

Site information for www.wunderground.com

Connection secure

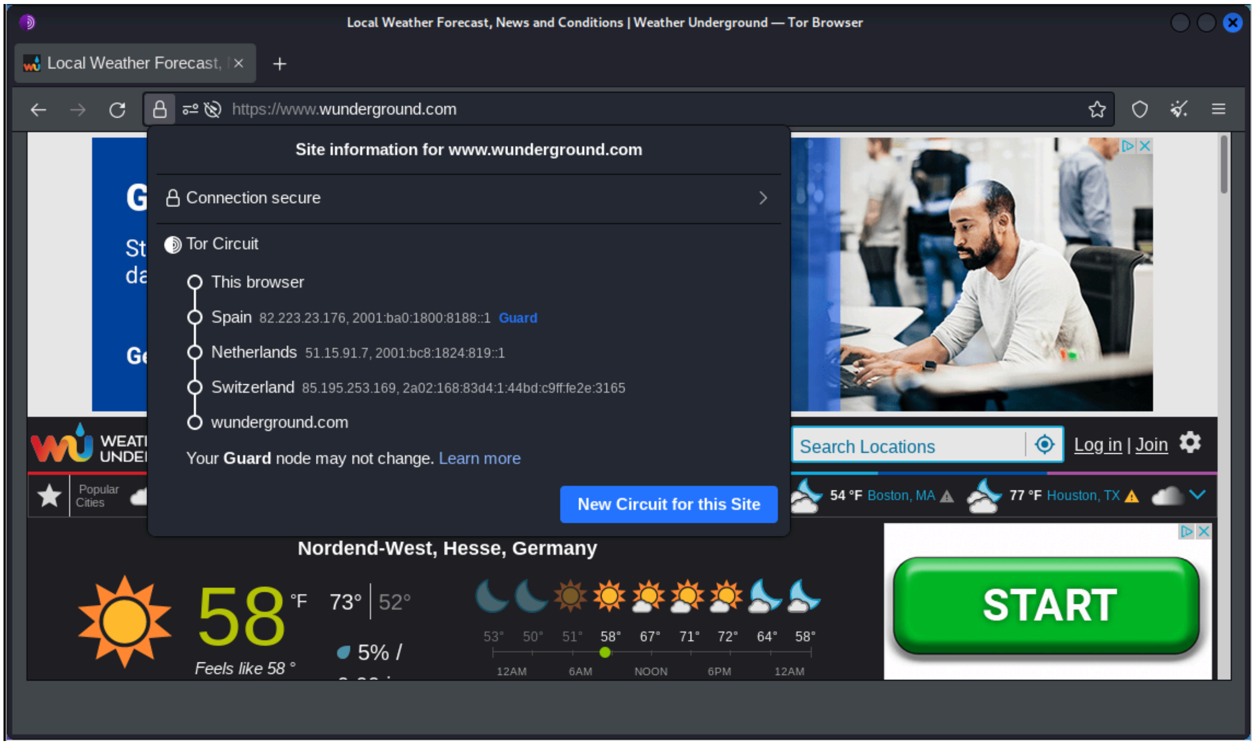
Tor Circuit

- This browser
- Spain 82.223.23.176, 2001:ba0:1800:8188::1 Guard
- United States 45.35.194.162
- Austria 109.70.100.71, 2a03:e600:100::71
- wunderground.com

Your **Guard** node may not change. Learn more

New Circuit for this Site

Wieden, Vienna, Austria



Local Weather Forecast, News and Conditions | Weather Underground — Tor Browser

https://www.wunderground.com

Site information for www.wunderground.com

Connection secure

Tor Circuit

- This browser
- Spain 82.223.23.176, 2001:ba0:1800:8188::1 Guard
- Netherlands 51.15.91.7, 2001:bc8:1824:819::1
- Switzerland 85.195.253.169, 2a02:168:83d4:1:44bd:c9ff:fe2e:3165
- wunderground.com

Your **Guard** node may not change. Learn more

New Circuit for this Site

Nordend-West, Hesse, Germany

Deon Perera

8. What does the "New Identity" option do? Is it different from the "New Tor Circuit for this site" option? What is the difference?

The New Identity feature of the Tor Browser thwarts subsequent browser activity from being linked to internet activities previously performed. The feature works by closing all tabs, deleting browsing history, clearing private information, closing downloads, and creating a new circuit.

The *New Identity* feature is different from the New Circuit feature. The *New Circuit* feature does not delete cached data, furthermore, its use is limited to a single website you have selected to use the feature on. Whereas, the *New Identity* feature creates a new circuit for all subsequent connections.

9. In the Tor browser address bar, enter https://www.facebookcorewwwi.onion/. What page is shown as a result? Is this a legitimate website? NOTE: If the site is down.

The website is the legitimate .onion address for Facebook.
The Tor browser challenges Facebook's security mechanisms and therefore Tor users are blocked from accessing Facebook's conventional domain. Simply stated, the .onion website enables Tor users to access Facebook.

10. What are ".onion" sites?

.onion domains are not registered with the domain name system and cannot be accessed by conventional browsers. The .onion sites exist inside the Tor network and therefore it is accessible through the Tor Browser.

It offers anonymity, bypasses regional censorship, and offers other privacy features of the Tor Network. Therefore, the owners of the .onion sites are anonymous and law enforcement agencies cannot ascertain their personal information or locate them.

11. What does Jacob Appelbaum mean by "privacy by design"?

'Privacy by design' is a system designed to use Tor. He describes that when someone uses the Tor Network, they bypass censorship and surveillance instigated by the state. Also, when a user visits a website, the website cannot ascertain the user's location.

He adds that the Tor Network compartmentalised security. To elaborate, Tor's security is formed by the collective consent of multiple arbitrary nodes. By this token, if one network node was compromised, user data maintains its privacy.

He posits the *security by design* system supports our democratic liberties and shields us from authoritarianism.

Deon Perera

12. What is the DARKWEB? How do you access it?

Darkweb simply refers to the websites that are not found on search engines such as Google and Bing. Inside the Darkweb is the Deepweb. It is not accessible through conventional browsers and search engines.

Deepweb refers to the website existing inside the Tor network and therefore it is accessible through the Tor Browser. The Deepweb houses unregulated websites.

13. What is the DEEPWEB used for?

The Deepweb is an anonymous and unregulated environment. It houses various websites for legal and illegal motives, such as narcotics, weapons, black market items, and benevolent motives such as forums to promote free speech, and exchange ideas.

14 Difference between Tor and a VPN

As noted, Tor facilitates security by transmitting packets, with multiple layers of encryption, through an arbitrary sequence of relays (minimum of three relays). The relays are operated by volunteers across the world. Tor emphasises anonymity, which is hiding who you are, allowing us to connect to the dark web, and making communication untraceable.

Whereas, VPN encrypts packets and routes them through a proxy server. The server is operated by the VPN provider. VPNs emphasise removing region-locked content, allowing torrenting and higher speed internet, and securing public wifi.

.

15. Does the Internet Service Provider (ISP) know that you are using Tor when using Tor?

Yes, the ISP can observe packets transmitted to the TOR network entry node. However, the packets are encrypted with multiple layers of encryption and passed through relays. As a result, the ISP is unable to ascertain substantive information about Internet behaviour.

Due to the equivocal nature of the Tor network, connections to the entry node may create suspicion by authorities. Although very unlikely, our Internet behaviour may be subject to audit by law enforcement agencies.

16. Can Network administrators block Tor?
this)

Network admins can block Tor's nodes, thereby blocking Tor altogether. Network admins can obtain the normal relay nodes through the publicly available Tor directory.

In order to circumnavigate censorship, we can use bridges. Bridges are special relays that are not publicly available. Therefore network admins find it difficult to block.

Reference

The Guardian. 2015. ‘Facebook opens up to anonymous Tor users with .onion address’. https://www.theguardian.com/technology/2014/oct/31/facebook-anonymous-tor-users-onion . Accessed May 07 2022.

Comparitech, date 2022. ‘Tor vs VPN: Which should you use and what’s the difference?’. https://www.comparitech.com/blog/vpn-privacy/tor-vs-vpn/#:~:text=A%20VPN%20encrypts%20your%20connection,of%20servers%20run%20by%20volunteers. Accessed 07 May 2022

Fortinet. Date 2019. ‘How Tor Browser Works and Where to Find Built-in Tor Bridges’. *https://www.fortinet.com/blog/threat-research/dissecting-tor-bridges-pluggable-transport.* Accessed May 07 2022

Tor, n.d. ‘New Identity. https://support.torproject.org/glossary/new-identity/#:~:text=New%20Identity%20is%20a%20Tor,Tor%20circuits%20for%20all%20connections. Accessed 07 May 2022.

Tor, n.d. ‘Most Frequently Asked Questions’. https://support.torproject.org/faq/. Accessed 7 May 2022.