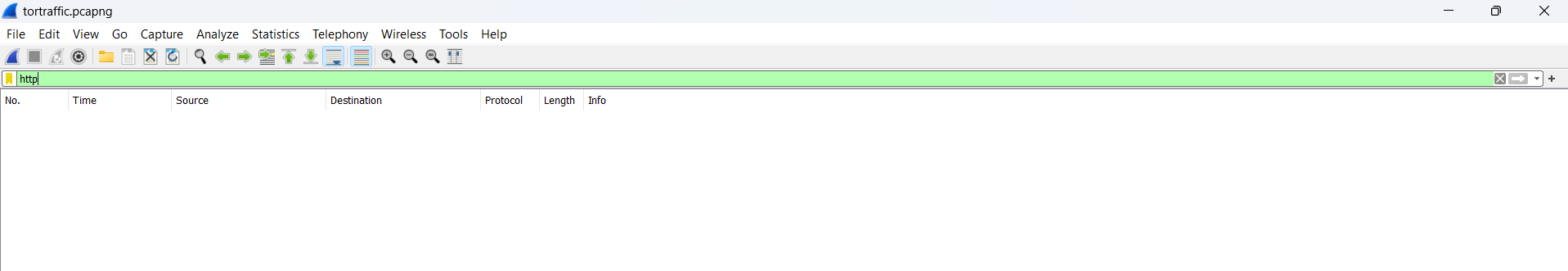
**EXPLORING THE TOR NETWORK**

The Tor Browser is a privacy-focused web browser that allows users to browse the internet anonymously. It works by routing your internet traffic through a network of volunteer-operated servers known as Tor nodes. When you use the Tor Browser, your traffic is encrypted and passed through multiple nodes (entry, relay, and exit nodes) before reaching the final destination. This process conceals your IP address and masks your online activity, making it difficult for websites, ISPs, and others to track your browsing habits. The Tor Browser is commonly used to access the regular web securely and to visit sites on the dark web, providing enhanced privacy and anonymity.

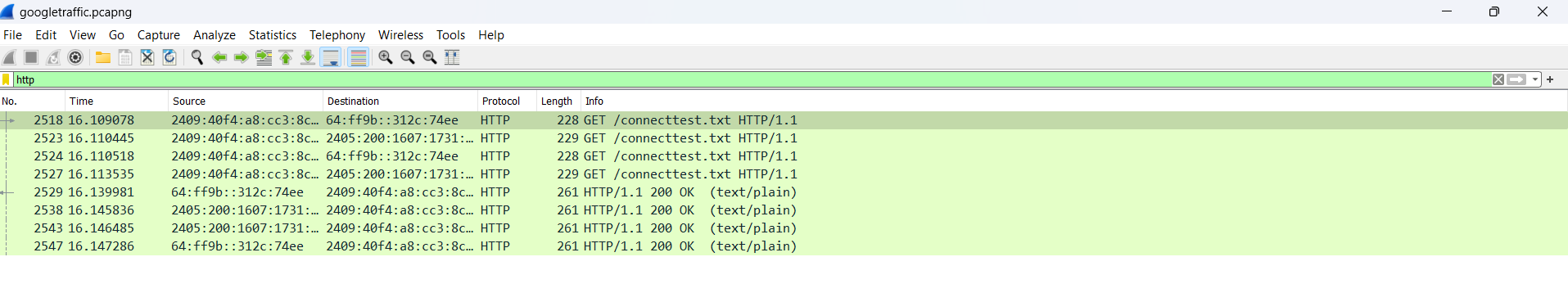
1. ANALYZE TOR TRAFFIC WITH WIRESHARK

I captured network traffic in Wireshark by running www.youtube.com in google and tor browser to check the differences

The main difference I could find in the network traffic is that there is no HTTP as the request are encrypted using TLS



While in normal browsers I could find HTTP, DNS traffic



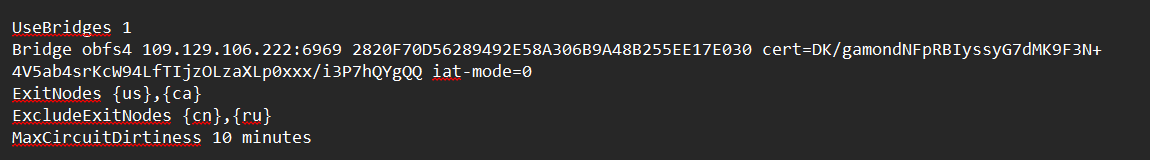
Also mainly in Tor network I could find several IP address due to several nodes where data gets transmitted but in normal traffic some IP address get data frequently.

The data in Tor network is fully encrypted while in normal browsers it may not, the tor network will have higher latency due to several hops present in between while the normal ones might have lesser.

2. USE TOR WITH A CUSTOM CONFIGURATION

I configured the torrc file by adding a bridge.

Bridges in the Tor network are special, non-public relay nodes designed to help users connect to the Tor network when access is restricted or censored. Unlike regular Tor relays, which are listed in the public Tor directory, bridges are not openly advertised, making it harder to block access to the Tor network.



Adding ExitNodes and ExcludeNodes will force Tor to use exit nodes in the U.S. and Canada and exclude nodes in China and Russia. Also MaxCircuitDirtiness controls how long Tor circuits are used before a new one is established, this setting changes circuits every 10 minutes, which can affect anonymity and performance.

Changes:

Using bridges or specific entry/exit nodes can affect the speed and latency of your browsing experience. For instance, using distant exit nodes might increase latency.

Customizing entry guards or using bridges can enhance security, especially in restrictive environments, by making it harder to identify Tor usage.

Changing exit nodes or circuit lifetimes can impact your anonymity. For example, frequent changes in circuits might reduce the chances of tracking but could also disrupt sessions.

3.EXPLORE TOR'S SECURITY FEATURES

The Tor network uses advanced security measures to protect user anonymity and communication. It encrypts traffic through multiple relays, ensuring that no single node knows both the source and destination, a method known as "onion routing." Tor also implements **perfect forward secrecy (PFS)**, generating unique session keys for each connection, ensuring past communications remain secure even if keys are compromised.

For secure communication, it's crucial to use **HTTPS** alongside Tor. While Tor anonymizes the traffic, HTTPS encrypts data between the exit node and the destination server, protecting it from interception.

To enhance security, users should follow best practices, such as avoiding plugins, being cautious with downloads, and not logging into accounts linked to their real identity. These measures help maintain privacy and security while using Tor.