**Advanced Security 1 – Lab 1**

**Eoin Lynch – C16310846**

**Part A**

I am using Google Chrome so I will be discussing addons that improve the security of my browser.

HTTPS Everywhere: HTTPS everywhere is an addon that changes websites that use http to https which is the more secure protocol. Users can check which version they are using by looking for the lock beside the URL in chrome.

SurfShark**:** Surfshark is a VPN service that can be used with chrome. It allows access to 63 countries and a wide variety of encryption protocols and even double VPN connections.

AntiMiner: This is an open source Chrome extension that blocks harmful websites from hijacking a user’s CPU and memory to mine cryptocurrency.

Privacy Badger: This addon blocks tracking scripts from websites. It sends Do Not Track signals to websites and if this is ignored it will block any trackers that do not follow the request.

Most browsers track what their users are doing on them apart from privacy focussed browsers such as DuckDuckGo. This is done for marketing purposes so that ad services can show you more targeted advertisements and as such increase’s revenue. It is possible to avoid being tracked. There are multiple ways of doing this including the use of VPNs which hide your internet traffic from your ISP and hide your location from websites, ad blocking software which limits the amount of ads you’re exposed to and as such limits the amount of information that can be gathered about you and anti-malware extensions that prevent scripting attacks from occurring and other malware from being installed on your computer.

**Part B**

The deep web is a section of the internet that is well known for being a hotbed of criminal activity. It is called such because it is not indexed by any search engines. However not all the deep web is filled with criminal activity. Company payroll information, medical records and other confidential information cannot be found by search engine therefore it is still deep web content; however, it is not illegal. The more illegal side of the deep web is often considered the dark web. The dark web is blocked by a variety of firewalls. For example, instead of using .com at the end of URLs most dark web websites use .onion which can only be accessed via tor browser. This means that searching up dark web websites by Google or Bing will not yield any results. To gain access to the dark web users download the TOR browser, a browser that is very secure as it uses multiple proxies to mask an IP address. A lot of users often use VPNs in conjunction with a TOR browser to further increase their security. It is estimated that over half of all websites on the dark web offer illegal goods and services. It can be used by people such as journalists and whistle-blowers to state their true opinions/ Some dangers of using the deep web include that a lot of sites hosted on it are used by scammers who will try to scam people of money that they have. It is estimated that 96%-99% of the internet is deep web which consists of things such as online banking websites and Gmail accounts. This is done for security reasons as not everyone should have access to personal information. Estimates place the size of the dark web as 0.01% of the internet which may seem small, but with the overall size of the internet estimated at 10^24 bytes or 1 million exabytes this still amounts to 100 million exabytes, or 100 trillion terabytes. Given all of this information one would assume that using browsers such as TOR would be illegal and accessing the dark web is illegal, however it is completely legal. In fact, TOR was originally create by the US Navy and is still being funded by the US government. This is done because it protects the rights of activists who are living in dictatorships.