A picture containing text, screenshot, diagram

Description automatically generated

*Table of Contents*

[***1-*** ***Introduction.*** 3](#_Toc137574716)

[***2-*** ***How to protect yourself from the dark web.*** 4](#_Toc137574717)

[**2.1-Using dark web scan.** 4](#_Toc137574718)

[**2.2- Use a password manager.** 4](#_Toc137574719)

[**2.3- Make two-factor authentication available.** 4](#_Toc137574720)

[***3-*** ***How to access the dark web securely.*** 5](#_Toc137574721)

[**3.1- Using VPN to add security.** 5](#_Toc137574722)

[***4-*** ***How to use the Dark Web securely?*** 6](#_Toc137574723)

[***5-*** ***Evidences.*** 7](#_Toc137574724)

[**5.1- The command used to generate a username and password.** 7](#_Toc137574725)

[**5.2- The username and password to access the site and type of encoding.** 9](#_Toc137574726)

[**5.3- The suspect’s username.** 12](#_Toc137574727)

[**5.4- the suspect's initial and surname names, and the address where he is now residing.** 13](#_Toc137574728)

[**5.5- The date of the first and last posts that related to drug trafficking.** 14](#_Toc137574729)

[**5.6- The GPS coordinates the delivery location and the date of the next shipment.** 15](#_Toc137574730)

[**5.7- The seaport.** 15](#_Toc137574731)

[**5.8- other potential crimes and their usernames.** 16](#_Toc137574733)

[**5.8.1- Guns.** 16](#_Toc137574734)

[**5.8.2- Human parts.** 18](#_Toc137574735)

[***6-*** ***Next course of action.*** 20](#_Toc137574736)

[***7-*** ***Conclusion***. 21](#_Toc137574737)

[***8-*** ***Individual reflection.*** 21](#_Toc137574738)

[***9-*** ***References.*** 22](#_Toc137574739)

1. ***Introduction.***

Other names for the Dark Web include the Hidden Web and the Undernet. Regular Internet users cannot access the dark web, a secret portion of the Internet. (Tereen Prasanga & Upulie Handalage, 2021). The "dark web" is a section of the internet that is unreachable through regular search engines and needs specialised software, like the TOR browser, to access. Despite having some legitimate uses, the dark web has a reputation for being a hub for illegal activities. Utilising the dark web as opposed to common websites offers far greater privacy and anonymity (What Is the Dark Web and Should You Access It?, 2023).

The dark web is mostly used to give anonymous surfing and communication to users who want to avoid being tracked by authorities, businesses, or other people who might try to keep an eye on their online behaviour. Journalists, activists, and residents of nations with severe internet control can all fall under this category. ‎‎ ‎‎ (*Elmwood Campus*, 2021).

However, the dark web is also well-known for being a market place for illegal products and services like drugs, guns, fake cash, stolen data, and even people trafficking. Since these activities are carried out via anonymous cryptocurrency, it is challenging for law authorities to identify and pursue individuals responsible. ‎‎‎ (*Elmwood Campus*, 2021).

In addition to illicit activities, the dark web is the home to several online forums where people debate contentious issues like political extremism, terrorism, murders, hacktivism, and conspiracy theories. These groups can nonetheless have a negative impact on society and spread destructive ideals even though they may not always be involved in unlawful activity. ‎‎‎‎ (Upulie Handalage & Tereen Prasanga, 2021).

Overall, it's important to be aware of the risks and exercise caution when navigating the dark web because it's a complex and frequently dangerous environment. It is advised that people avoid using the dark web unless they have a clear, valid reason to, and even then, they should take precautions to protect their online identity and abstain from unlawful activity.

‎‎‎‎‎

1. ***How to protect yourself from the dark web.***

**2.1-Using dark web scan.**

When the victim suspects that any of his personal accounts, including email, bank accounts, or other sensitive data, may have been compromised, he should think about using a free dark web scan. Your personal information will be found by the scan when it searches the dark web for listings of stolen data. The scan will quickly notify you if any of your information is discovered, even if it may not be feasible to identify all of the compromised data on the dark web. ‎‎‎‎‎‎ (*5 Ways to Protect Yourself from the Dark Web*, 2022).

**2.2- Use a password manager.**

Use a password manager and update your passwords as another method to increase the security of your personal data. It's a typical mistake to use the same password for all of your accounts, which might make it simpler for hackers to access your data. For each online account, such as one for Instagram, one for Amazon, and one for online banking, it is advised to have a different, secure password. You can never forget another password again since a password manager creates secure passwords for you. ‎‎‎‎‎‎‎ (*5 Ways to Protect Yourself from the Dark Web*, 2022).

**2.3- Make two-factor authentication available.**

It is advised to implement two-factor authentication to increase online account security against the dark web. A two-step process, often involving your password or login and a verification technique like a code delivered to your phone or a biometric scan, is required to confirm authorization while using this security feature. It is considerably harder for hackers to access your accounts when you use two-factor authentication, especially if your login information has been hacked. ‎‎‎‎‎‎‎‎ (*5 Ways to Protect Yourself from the Dark Web*, 2022).

1. ***How to access the dark web securely.***

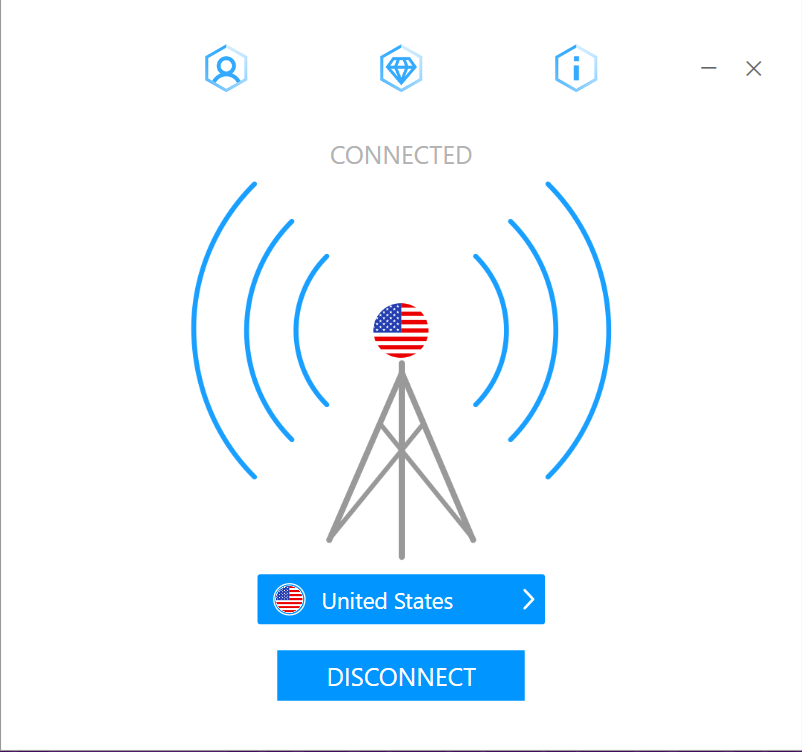


Figure (1)

**3.1- Using VPN to add security.**

Since Tor node IPs are made public, internet service providers and websites may be able to detect when Tor is being used. Even if they cannot read the encrypted internet data, websites and ISPs may be able to detect the use of Tor. This can spark rumours and attract unwelcome attention.

A user can use a VPN to encrypt and route all internet traffic to and from the device through a server in any location they choose. By using a VPN in addition to Tor, the user's security and anonymity can be further increased. ‎‎‎‎‎‎‎‎‎ (*How to Access the Dark Web Safely: Updated for 2023*, 2023).

1. ***How to use the Dark Web securely?***

A screenshot of a computer

Description automatically generated

Figure (2)

To enhance anonymity while browsing online, you might consider leveraging the security offered by the Tor Browser and its associated network. Such a move can protect against activities of potential concern by ISPs and governmental entities that may want to monitor web users. It's also a helpful tool when undertaking sensitive research such as investigating business competitors or legal opponents. That being said, note that accessing some web services when using Tor may prove difficult due to access restrictions or reduced browsing speeds. Additionally, recognize that repressive governments sometimes prohibit access rights for this browser due to its ability to enable anonymous communication and publishing behaviors which can incur legal repercussions. Nonetheless, proponents laud Tor as indispensable for upholding freedom of expression online. Ongoing research is being done to improve the anonymity capabilities of Tor. ‎ (J.M. Porup, 2019).

The Tor Browser is the most direct route to Tor and the Dark Web. It is available for free download and installation on the official website. You can use a VPN and your existing browser's private or incognito mode to hide your Tor Browser

download.The Tor Browser is currently only supported by Windows, Mac, Android, and Linux. The user can access "Tor hidden services," which are dark web websites, once connected. Addresses on the Dark Web finish in ".onion" rather than ".com" or ".org." ‎‎ (*What Is the Dark Web? How It Works & Why It’s so Dangerous*, 2022)."

1. ***Evidences.***

**5.1- The command used to generate a username and password.**

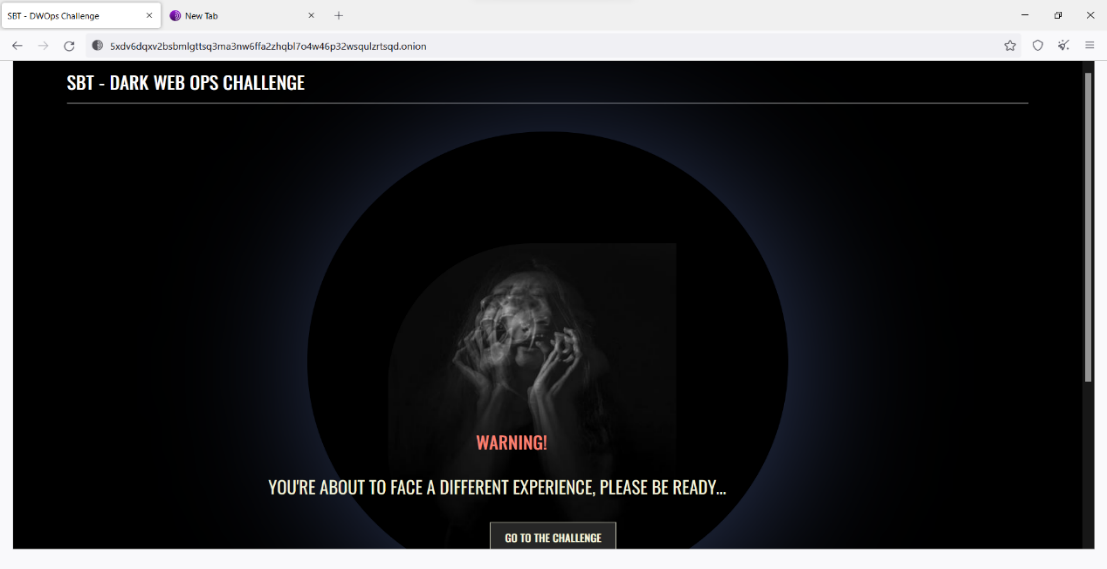


Figure (3)

The principal platform used by users to share their stories on the website has this as its main interface.‎‎‎

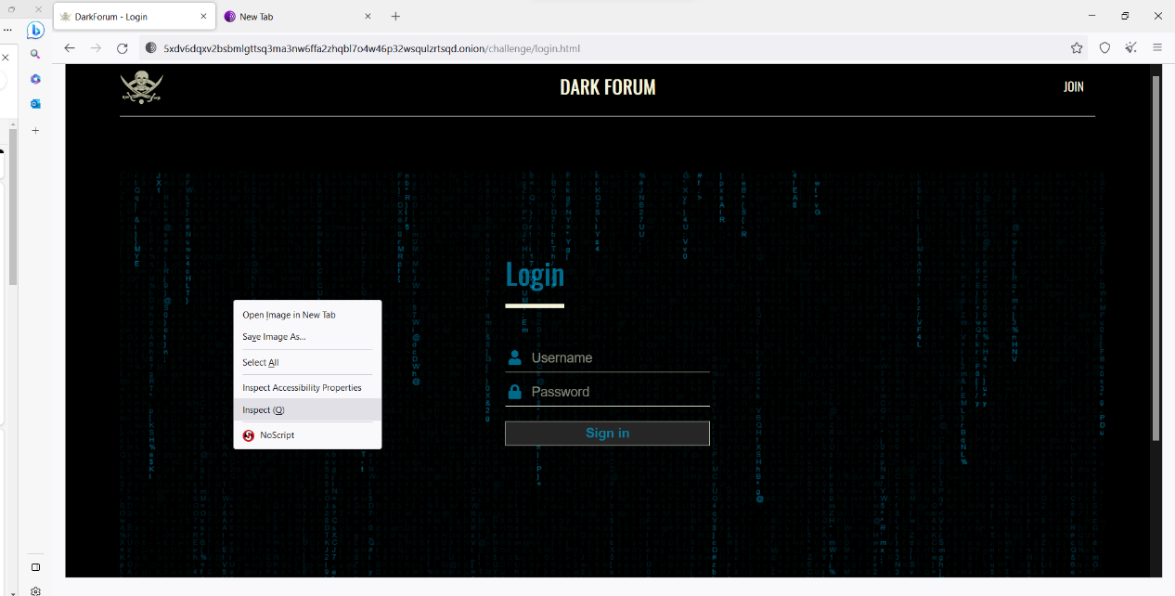


Figure (4)

A screenshot of a computer

Description automatically generated

Figure (5)

This marked the start of the username and password creation process. Then, select "Inspect" from the context menu, "Console" from the tab bar, and "generateUserCredentials()" into the text box. The Username and Password are then revealed by decrypting a message that is then shown. With those, you can access the accounts, discover additional information and supporting documentation, and look for any additional potential crimes that might have occurred. Whether or not shipments are scheduled to arrive in the near future.‎‎‎‎

**5.2- The username and password to access the site and type of encoding.**

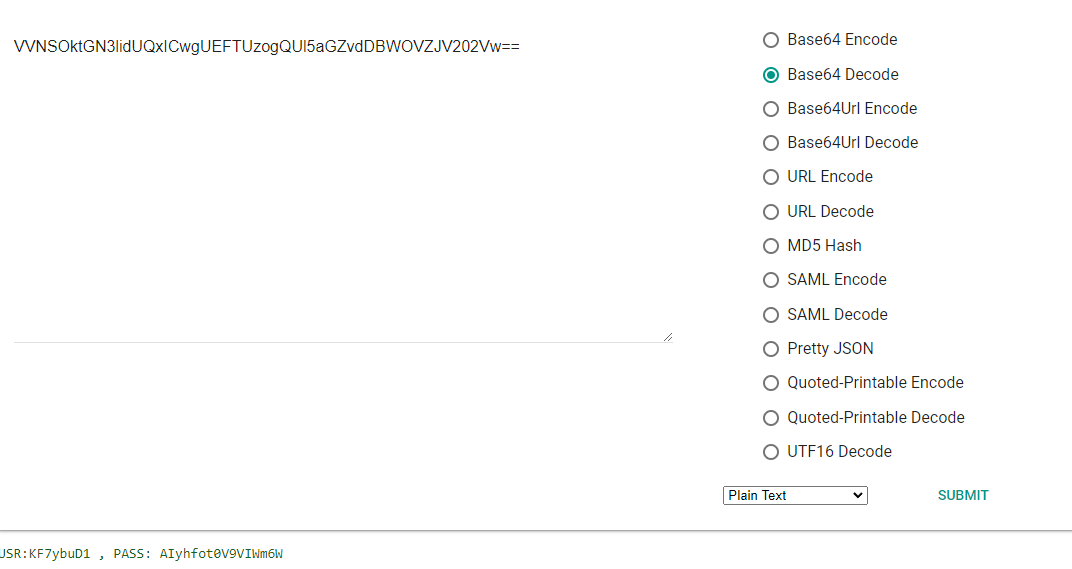


Figure (6)

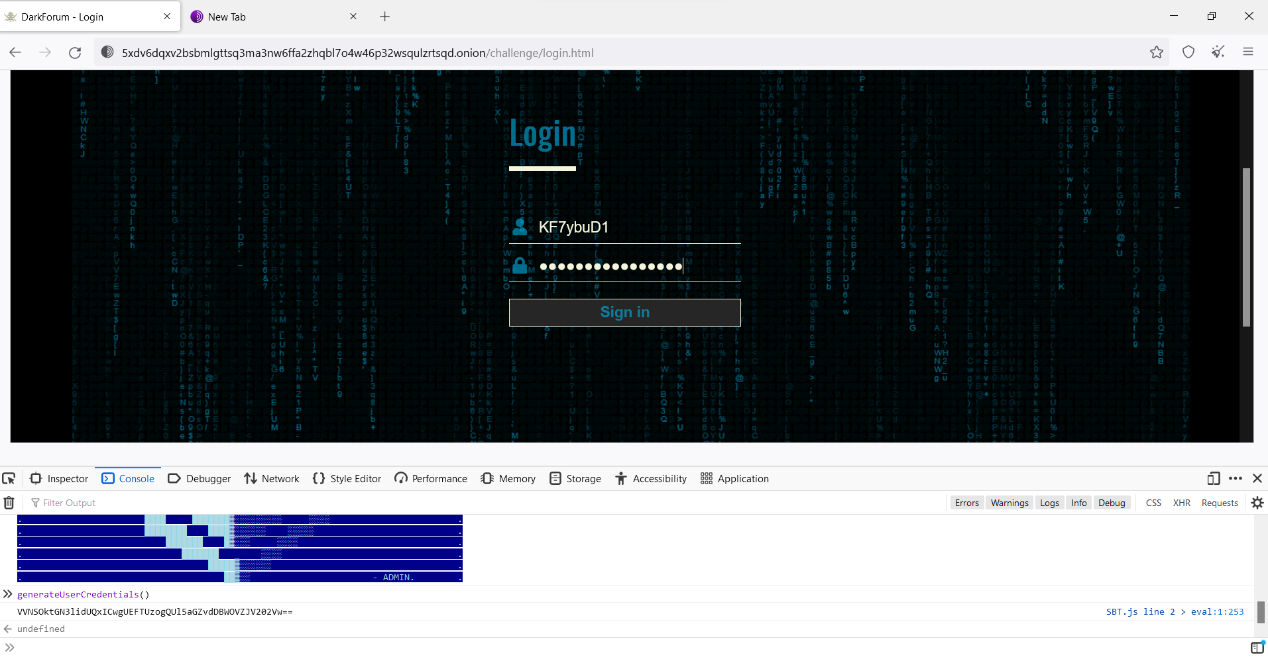


Figure (7)

The shown message will be in Base 64 (VVNSOktGN3lidUQxICwgUEFTUzogQUl5aGZ vdDBWOVZJV202Vw==). Decrypting the generated encoded message will show us the Username and the Password that can be used to access the main page.

USR: KF7ybuD1 , PASS: AIyhfot0V9VIWm6W

As shown in the above Figure (6) the tool that helps to decode the encrypted message is the (Google Admin Toolbox Encode/Decode) [click here](https://toolbox.googleapps.com/apps/encode_decode/).

A screenshot of a computer screen

Description automatically generated with low confidence

Figure (8)

This is the targeted website's Home Page interface, which is suspected of holding confidential data on drug trafficking. because it is obvious that Base 64 was used to encode the content.‎‎‎‎‎

A screenshot of a video game

Description automatically generated with medium confidence

Figure (9)

Calendar

Description automatically generated with medium confidence

Figure (10)

Graphical user interface, application

Description automatically generated

Figure (11)

Graphs 10 and 11 illustrate the procedures involved in decoding the object of Figure 9, starting with translating the bytes from Base 64 to Base Hexadecimal and then from Hexadecimal to Text using the ASCII table. The tool that aids in the decoding of the encrypted communication is the (cryptii), as seen in the aforementioned Figures (10&11) ‎‎‎‎[click here](https://cryptii.com/pipes/hex-decoder).

**5.3- The suspect’s username.**



Figure (12)

As mentioned in Figure (12) that “DarkChest984” is the username of the suspect responsible for drug trafficking.

**5.4- the suspect's initial and surname names, and the address where he is now residing.**



Figure (13)

According to the boarding pass in the graph above, the suspect's name is Kesther Rinharo. The fact that the plane is leaving from London and landing at JFK international airport in New York suggests that the suspect now resides in the United Kingdom (UK).‎‎‎‎‎‎‎‎

**5.5- The date of the first and last posts that related to drug trafficking.**

A hand holding a cigarette

Description automatically generated with low confidence

Figure (14)

A picture containing text, indoor, computer

Description automatically generated

Figure (15)

The numbers shown above (numbers 14 and 15) show that the first post about drug trafficking was made on November 26, 20XX, and the most current post about drug trafficking was made on October 26, 20XX. Additionally, it specifies that the subsequent medication shipment will reach the UK on October 31. ‎‎‎‎‎‎‎‎‎

**5.6- The GPS coordinates the delivery location and the date of the next shipment.**

Graphical user interface, application

Description automatically generated

Figure (16)

The coordinates (51°56'59.2"N 1°19'26.1"E) in the aforementioned figure (16) illustrate the location of the shipment delivery.

**5.7- The seaport.**

Graphical user interface

Description automatically generated

Figure (17)

The location of the shipment delivery is shown in the aforementioned figures (16 & 17) to be at (51°56'59.2"N 1°19'26.1"E), which suggests that it is near to the harbour shown in the earlier-posted suspect photo. Additionally, Felixstowe Port Container is the name of the seaport where the consignment will be delivered.‎‎

**5.8- other potential crimes and their usernames.**

**5.8.1- Guns.**

Graphical user interface, application

Description automatically generated

Figure (18)

Graphical user interface, application

Description automatically generated

Figure (19)

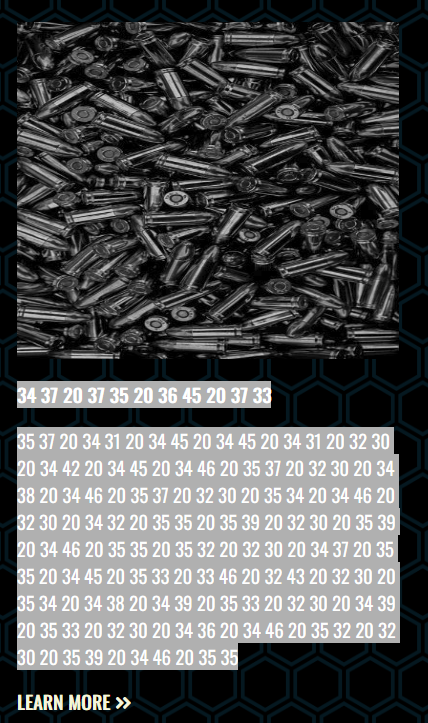


Figure (20)

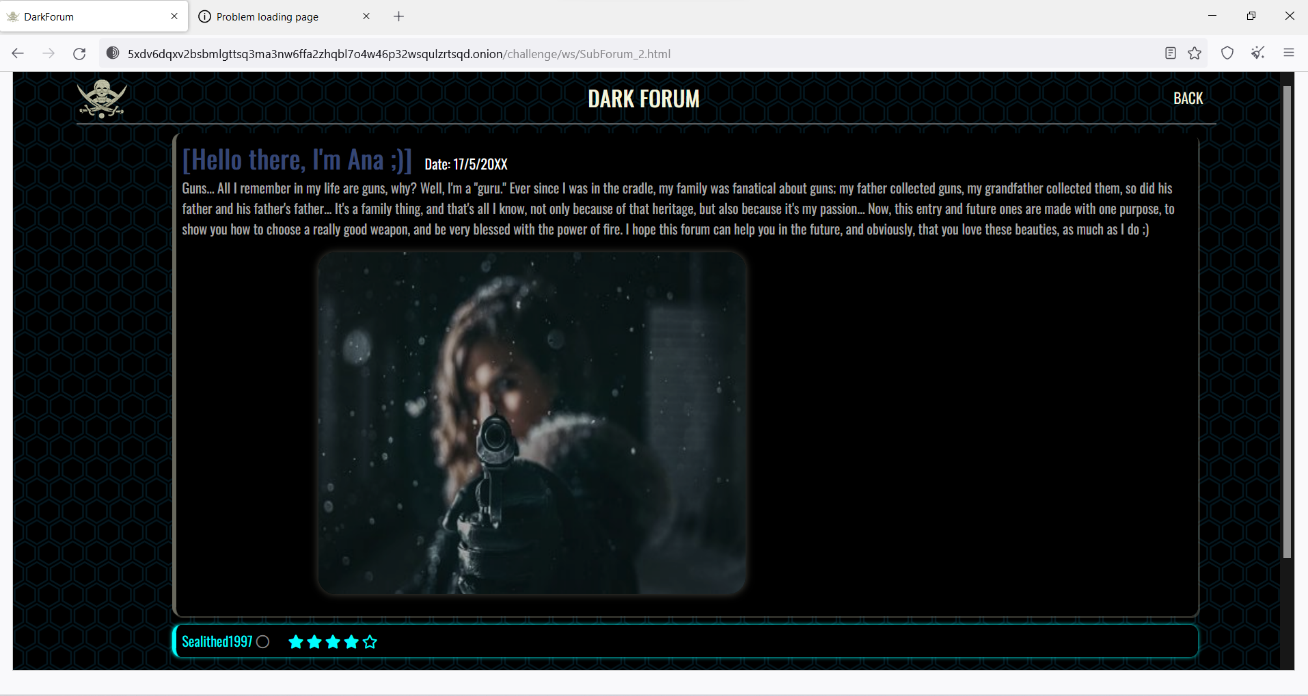


Figure (21)

One of the numerous possible crimes is the sale of guns. Graphs 19 and 18 show the steps needed to decode the figure 20 object. The bytes must first be converted from Base 64 to Base Hexadecimal, and then, using the ASCII table, from Hexadecimal to Text. The (cryptii) tool is used to help decipher the encrypted message ‎[click here](https://cryptii.com/pipes/hex-decoder), The message has been deciphered and is (Guns), as seen in the aforementioned Figures (18) and (19). WANNA KNOW HOW TO BUY YOUR GUNS? THIS IS FOR YOU), the username for this site is "Sealithed1997".‎‎‎‎‎

**5.8.2- Human parts.**

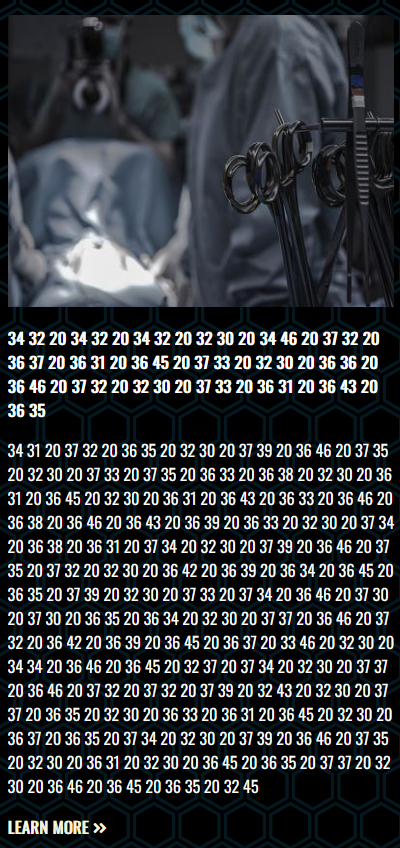


Figure (22)

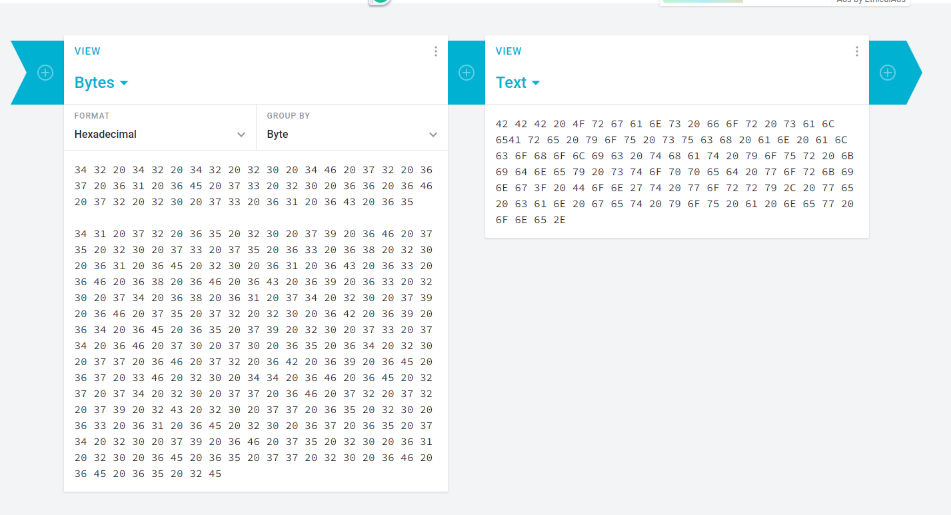


Figure (23)

A picture containing application

Description automatically generated

Figure (24)



Figure (25)

Graphs 23 and 24 show the procedures that were used to decode the object in Figure 20. Convert the bytes from Base 64 to Base Hexadecimal using the ASCII table, and then from Hexadecimal to Text. The (cryptii) gadget permits the decryption of the encrypted message ‎[click here](https://cryptii.com/pipes/hex-decoder). It demonstrates that the wording is "BBB Organs for sale," as stated.Are you such a heavy drinker that your kidneys have ceased functioning? We can get you a new one, so don't worry. The trader on this page goes by the name 3B\_0rg, and it is obvious from this message that the suspect deals in the sale of human organs.‎‎‎‎‎‎‎

1. ***Next course of action.***
2. To ensure swift justice while upholding safety measures in our society, it is vital we immediately alert law enforcement officials upon discovering any related evidence. This pertains specifically to gathering information on a suspect's user identification including their full name along with potential ties to drug trafficking activities or unlawful dealings involving firearms or human body parts sale. It is vital that all obtained findings are relayed promptly alongside supporting proof for effective investigation.
3. Preserving digital evidence is of utmost importance. It includes documents such as screenshots, decrypted messages. And other relevant files or data. Securing and backing up the evidence is essential to maintain its integrity for legal purposes and future investigations.
4. To improve our chances of capturing our suspected individual who is allegedly involved in international criminal activities while present in the United Kingdom, it would be wise to work alongside overseas law enforcement agencies as well. We recommend coordinating efforts together by communicating effectively particularly between UK and US authorities on matters concerning this case at hand. This way by sharing gathered pieces of evidence from all participating parties could yield better results during any possible joint investigations or extradition procedures required moving forward.
5. ***Conclusion***.

In conclusion, the dark web is an inaccessible area of the internet that is notorious for its illegal activities. but also acts as a haven for people looking for privacy and secrecy. When using the dark web, extreme caution must be taken. and to take precautions to safeguard oneself from such dangers. This involves protecting personal information using tools like a dark web scan, a password manager, and two-factor authentication as well as accessing the dark web safely by using a VPN and the Tor Browser. Although some people may find the dark web to be a beneficial resource, it is important to access it cautiously and with knowledge of its perils.‎‎‎‎‎‎‎‎

1. ***Individual reflection.***

I've picked up the habit of exercising greater caution and paying closer attention to everything, including what appears in images that are available to the public. In addition to that, I am now aware of how to access the dark web in a secure manner and how to shield my device from the content of the dark web.‎‎‎‎‎‎‎‎‎

This project improved my understanding of security and forensic technology concepts, particularly deep, dark, and surface webs. I conducted thorough research to understand their underlying distinctions. The project involved team members navigating uncharted terrains, accessing hidden services platforms, and collaborating with agencies worldwide. This experience helped me fine-tune skills in digital forensics operations.

**Total words count 2205.**

1. ***References.***

* *What Is the Dark Web and Should You Access It?* (2023). Investopedia. https://www.investopedia.com/terms/d/dark-web.asp
* ‌ *What Is the Dark Web? How It Works & Why It’s So Dangerous*. (2022). Aura.com. https://www.aura.com/learn/dark-web
* ‌ *Elmwood Campus*. (2021, June 29). Tulane School of Professional Advancement. <https://sopa.tulane.edu/blog/everything-you-should-know-about-dark-web>
* Upulie Handalage, & Tereen Prasanga. (2021, December 19). *Dark Web, Its Impact on the Internet and the Society: A Review*. ResearchGate; unknown. https://www.researchgate.net/publication/357163863\_Dark\_Web\_Its\_Impact\_on\_the\_Internet\_and\_the\_Society\_A\_Review
* ‌ *How to Access the Dark Web Safely: Updated for 2023*. (2023). Comparitech.com. https://www.comparitech.com/blog/vpn-privacy/access-dark-web-safely-vpn/
* J.M. Porup. (2019, October 15). *What is the Tor Browser? And how the dark web browser works*. CSO Online. https://www.csoonline.com/article/3287653/what-is-the-tor-browser-how-it-works-and-how-it-can-help-you-protect-your-identity-online.html