International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IV Apr 2020- Available at www.ijraset.com

Exploration of ultimate Dark Web Anonymization, Privacy, and Security

Revanth S[1], Praveen Kumar Pandey[2]
[1, 2]Department of MCA, Jain University

Abstract: The ultimate Dark web will review the emerging research conducted to study and identify the ins and outs of the dark web. The world is facing a lot of issues day-by-day especially on the internet. Now I have a question here, do you think is working with the internet attains knowledge or it pretends to be a part of the business. Keep the business part aside, we all know that internet is a great tool for communication. Is internet is definitely giving privacy, safety and security. Does anyone have a brief idea about the dark web for all these queries we don't have any accurate solution. Through this survey, I outlined some of the major concepts and their dependencies the primary usage of the dark web and some of the survey experiences are further documented in this paper.

Keywords: Darkweb, Security, Anonymity, Privacy, Cryptocurrencies, Blockchains, Tails, Qubes, Tor network.

I. INTRODUCTION

The Internet is the world's strongest and widest power. Without the internet more than the world's 85% of the tasks will get struggled because the earth is totally dependent on network chains. Internet helps in worlds most of the leading departments like Research Centres, Hospitals, Corporate Industries, Education Institutions etc., So, with this evergreen technology, we definitely need to think about our privacy and security as a most prior concern. Hackers attack the network every 39 seconds, on average 2,244 times a day. Russian hackers are the fastest hackers in the world, according to the 2019 survey report, 3,00,000 new malware are designing every day. The average cost of data breaches will be about 150 million in 2020 [1].

The drug is the major trade that is happening globally but cybercrime is more profitable than that. According to the annual income report of the illegal drug industry reaches a profit of around 400 billion but cybercrime reaches 600 billion [1]. Now you people may have a question that darknet is used only for business and crimes? No, because it mainly helps you to anonymize from the outer world, that's why many government and private organizations are dealing with darknet. If they want to transfer any sensitive information to the intended person they will use darknet as a source. Because it hides the data from source to the destination and the possibility of finding will get reduced, even Reverse engineering will also be challenging.

Working in the Darknet is not enough, Efficient handling is more important. Many peoples are more eager to work with darknet but before going into deep you should have to be more concentrated on what you are doing.

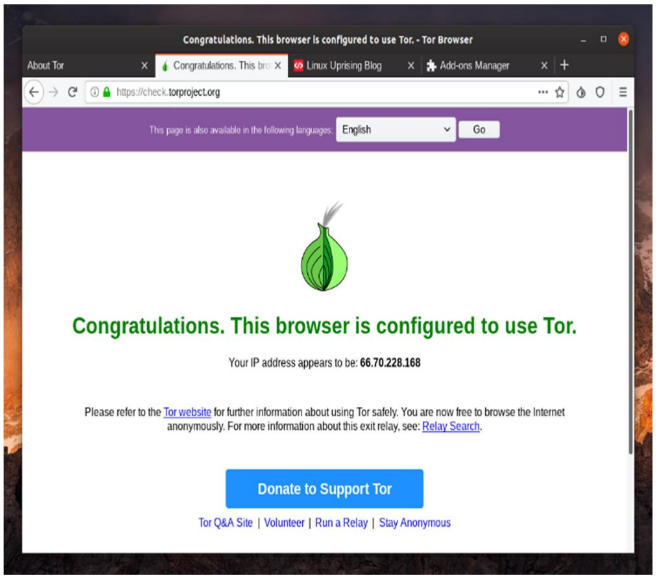
II. METHODOLOGIES TO ACCESS DARKNET

A. *Method 1: Use the Tor browser in your dedicated OS but it is simplest and not best.*

1) *What Happens When you visit a Website?:* When we are normally visiting a website such as Google.com/Facebook.com they can trace user location, browser version, operating system and much more. So, Google/Facebook has the ability to record the surfing information in terms of injecting the piece of code as a website bckground. It helps to explore user content and advertise things according to their needs. E.g. Facebook it will store all the user content and sell it to some bigger organizations we all of us know about the issue called Cambridge Analytica [2]. Some peoples might think that they don't have any social network accounts but these peoples have your information, While browsing every user can experience the sharing functionality if mistakenly any user tap those link then all your related info will be shared automatically to their database. These peoples will create a fake profiles for users without any user knowledge. So, Tor is a pretty good solution for preventing this. Tor is known as the onion router. It is a browser that enables you to work efficiently on both surface web as well as the dark web. It is basically a number of computers/servers designed to improve anonymity and privacy, and those networks of computers/servers can able to offer hidden/onion services. Tor is a normal browser with some extraordinary darknet extensions (Gives you an access to the darknet). Unlike normal browsers, it is having some advantages in terms of security that allows you to work in a non-JavaScript environment also helps to prevent unnecessary adware attacks. Onion routings are designed by the US army to protect their communications. Tor browser default search is "DuckDuckGo" is an internet search engine that gives more importance in terms of protecting searcher's privacy [3]. Tor never filters the webpages according to the user perspective it will show the same results for every end-user.

2) *Working of Tor Browser:* When the user connects to google/Facebook using Tor it bounces to three different nodes/servers before it reaches to the required website. So either google or facebook can only see the last node it can't see the original user if it tries to profile you, it's very hard because when your request is redirecting to different nodes that individual is not the only person who is visiting this website there are millions who can redirect request with the same nodes. So, it is very hard to identify who is the user trying to access. Also, data sent within the tor network is always encrypted. while leaving from the Tor it will be unencrypted [4]. When you are trying to access the Tor, your internet service providers can able to see the traffic that you are visiting. But, they can't find what content that you are visiting that's why many companies trying to do business inside the tor network it benefits you to get hide from hackers or even from any censor employees. There are certain services that are provided by the Tor network that basically we can call it has onion services. Onion services are websites that are provided inside the Tor network and the extension of those websites is referred to has onion. They will use some smart protocol to hide those servers from the outside world these servers has the ability, it doesn't track any user's identity it makes you to feel more secure. Anybody can configure their computer has the Tor node. If your request is going through that network the admin of that node can able to see the users request therefore this makes you a problem so if you are trying to use the HTTPS or HSTS features then it can be protected because it uses the request in an encrypted form [4].

3) *Installation of Tor:* Go to the website www.kali.org instead of going to any other third-party website because there is a possibility of malicious injection inside the application. Once the user enters the website, we can check for the required operating system to install the browser. After downloading the Tor browser from the website, we should have to follow certain methods in order to maintain the security. While downloading the Tor from the genuine website where the user can see the signature files which helps to prevent the integrity. The user needs to check out the hashing through the command line if it is matching then user downloaded tool is genuine if it is not then there is a possibility of a trap. GPG tools are the tool used for checking the integrity of signature files against the applications [5]. Once the installation is complete just go to the URL https://check.torproject.org there it should show the tor browser is successfully configured. And it will also give some masked public IP like this 109.70.100.19 [5]. Some people might get an error that Tor is blocked, the page will not be loaded this is because users ISP or network administrators will block this network(Block all the Tor relays). This issue can be bypassed with the help of private Tor relays(Use unpublished Relays(Bridges)) because that will never visible to public ISP. Even this is not a pretty good solution because this can also be blocked by ISP's with the help of Deep packet filtering. DPF helps to identify all the Tor traffics in an aggressive way and it tries to block. To prevent from DPF we need to obfuscate our traffic has a normal one for that we can use a technique called pluggable transports [6].



Congratulations. This browser is configured to use Tor. - Tor Browser

https://check.torproject.org

This page is also available in the following languages: English

Congratulations. This browser is configured to use Tor.

Your IP address appears to be: **66.70.228.168**

Please refer to the Tor website for further information about using Tor safely. You are now free to browse the Internet anonymously. For more information about this exit relay, see: Relay Search.

About Tor
Congratulations. This bro
Linux Uprising Blog
Add-ons Manager
Go
Donate to Support Tor
Tor Q&A Site | Volunteer | Run a Relay | Stay Anonymous

Fig. 1. Tor Browser

4) *Bypassing Tor Censorship:* This option is necessary only when the Tor browser is blocked in your country or else it is not mandatory. While setting up the Tor its necessary to configure bridges. According to my personal experience using obfs4 pluggable transport bridges are a good option [7].

5) *Examples of Obfs4 bridges*

```
obfs4 188.108.33.47:41521 DA8209F804FB568EB25589A1BEBDB922020DBDA2
cert=QJkEQcflwZ9RPXsw0HnoAxHsoFK83zJkT+M0PtD8SWm01svBSvTGFK4jTV1Rq0pkXipfaA iat-mode=0
obfs4 45.137.155.64:443 CB2CFDAB44147793B3704ADA29D57C12481584DF
cert=9nYNt2xAwE6SVY2ZaoKVUhdsZoZ3hmwLLx31kL5D8yfpQII2x1LqSJeh8uNhhlaY1qN/Cg iat-mode=0
obfs4 31.220.43.159:7778 2556D21C22A5F3E2499E4F334E7E46DDE40C5764
cert=y6d11hECcHaSdn0+sU+ha62+IvKA4PWMAqYS250rXv9NsSZDOh/aZUEa0zMLjoEb6VNpAw iat-mode=0 [8]
```

Once you get these bridges open your Tor browser and navigate to your tor network settings. Click the checkbox “Tor is censored in my country”. Add obfs4 bridges into the bridge configurations. If necessary a user can set the proxy server too and finally just click okay then restart your browser [7].

6) *Working of VPN with Tor:* VPN is the extra layer of protection to your tor network because whenever you send traffic it will send all the encrypted/unencrypted traffic in a tunnel so if someone tries to infiltrate the current tunnel, the VPN switches to the different tunnel so this remains the availability of the request with privacy [4]. Now someone may have a question, that Tor alone itself secure why do we need VPN? Using Tor is not sufficient because the request which we are sending to the tor network can able to tamper(Chances of Eavesdropping by someone) before entering into the network itself. So configuring VPN between the client and the tor network is a good option to make the user’s network in a more secure environment, this gives the additional layer of security to the user [4].

7) *Disadvantages of using Tor in normal OS:* Using the Tor in the normal browser is a quite easier way to access the darknet with less anonymity it looks simple and good, but this is not the right way to access the darknet. Because the user's normal operating systems(Windows, Mac OSX or Linux) can have the ability to collect the data of the users regularly to improve the user's experience and some other reasons too. Installed programs also have the possibility to collect user's data, these collected data can help to deanonymize and profile the particular targeted user. By using these collected programs and os information can be exploited to hack(Using code execution and buffer overflow vulnerabilities) your computer and deanonymize the user [4].

8) *Problems in the Tor Network*

a) Internet speed will dramatically drop.

b) Difficult to prevent leaks.

c) Web browser can also leak information

d) Data leave the exit node unencrypted.

B. *Method 2: Use Tails Os Which Is Great To Use The Tor Network Effectively*

1) *Tails:* Tails are the operating system which is designed for the privacy, anonymity and security we can call it has “The Amnesic incognito live system” has Linux based operating system, a live system in the sense can run the os entirely from the portable storage(USB). And you can boot that operating system as a live boot regardless of any os that you are using. The specialty of tail os uses the tor network for the entire set of programs and applications(Even if you install any third party also). By using this helps to prevent from other programs that leaks the data [9].

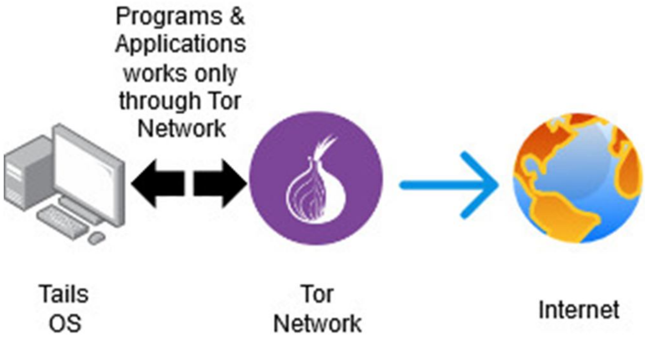
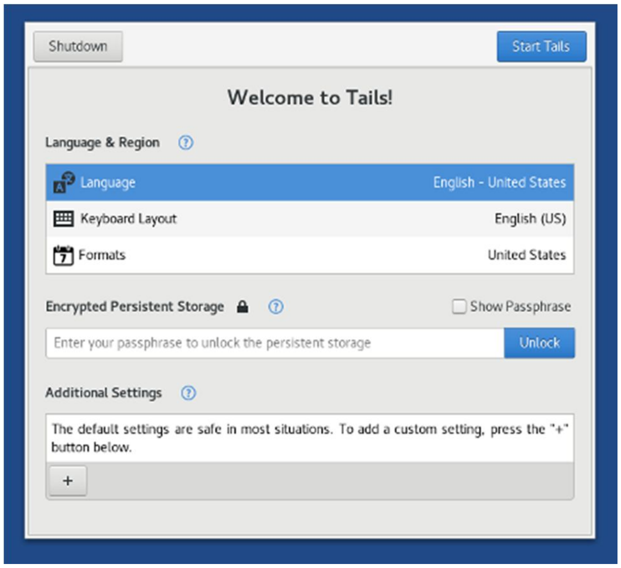


Fig. 2. Working of Tails in Tor

It never touches the storage of user computer other than the RAM, due to its volatile capability whenever we restart the systems it removes all the temporary memory which we used before therefore it leaves no traces.

2) *Installation of Tails:* There are lots of ways to install tails operating system in a machine. If a user tries to boot Tails OS as a virtual machine then it loses a lot of benefits(e.g. it uses system resources like CPU, network, storage, ram etc.,). Installing Tails as a virtual machine is a bad idea it evades users anonymity and the possibility of detection is more [9]. So, According to my research Tails should be installed as a live boot. While using the internet it helps users to be anonymized in their work. And it also gives good privacy-based protection to the users with the help of inbuilt Tor network and PGP encryption. After downloading the files from Tails website user need to check the integrity of the file using the signature which is given by Tails manufacturer. If the signature file results are matched then, the file which is downloaded by the user is genuine and they can further proceed with the installation. After the installation flash the OS into the USB/CD-ROM with the minimum of 8GB storage. Use the software called "Etcher" once the downloaded image is added into the etcher just flash it. To start a tail from the USB follow these steps:

a) Connect Tails USB
b) Start/restart the computer
c) Enter the boot menu
d) Boot from USB/External storage.



Welcome to Tails!

Language & Region

Language English - United States
Keyboard Layout English (US)
Formats United States

Encrypted Persistent Storage ☐ Show Passphrase

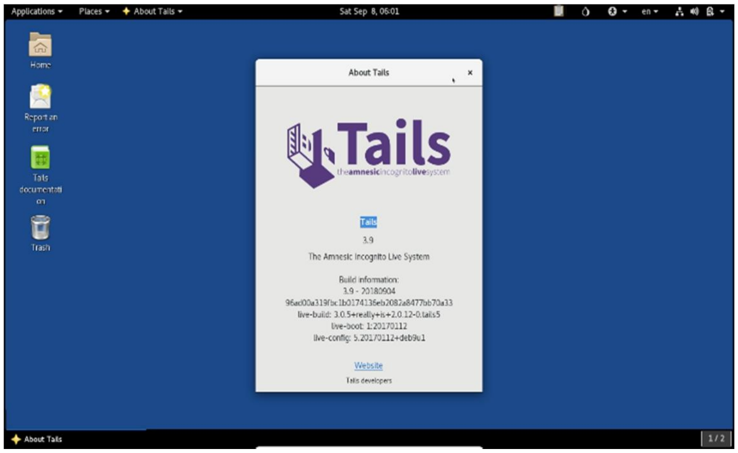
Enter your passphrase to unlock the persistent storage

Additional Settings

The default settings are safe in most situations. To add a custom setting, press the "+" button below.

Fig. 3. Tails Welcome Page

Before starting Tails it is mandatory to set -up a few additional settings to configure the tor network like Mac address spoofing and administration password to protect the system. Network settings help to configure the bridges and proxies, it determines the secrecy and efficiency of the operating system. once everything is done click add and start tails [9].



Tails
3.9
The Amnesic Incognito Live System

Build information:
3.9 - 20180904
96ad00a319fbc1b0174136eb2082a8477bb70a33
live-build: 3.0.5+really+is+2.0.12-0.tails5
live-boot: 1:20170112
live-config: 5.20170112+deb9u1

Tails developers

Fig. 4. Tails OS

3) *Disadvantages and Advantages of Tails:* Tails use RAM(Volatile) memory of the host machine. Once the Tails gets shutdown then the temporarily stored memory will get lost. And in the next fresh start user can't see any previously stored information. This will be a burden for the user to choose tails for their professional reasons. So, the company introduces a feature called "persistence" [4]. Persistence helps the user to store their data permanently and it is available for the next time. When the user restarts the Tails the stored persistent data helps the user for their future use. Persistent drives help to store data like passwords, bitcoins, personal data, browser bookmarks, additional software, network connections etc., this helps the user to access their Tails flash drives anywhere in the world's end-user systems [4].

4) *Tails Persistence*
a) Persistence allows us to store files on tails.
b) Computer storage is still left untouched.
c) Uses space left on the USB flash drive.
d) The persistent volume is encrypted with LUKS with a passphrase of your choice.
e) At boot, you'll have the choice to unlock the persistent storage.

5) *Benefits of Persistence*
a) Stores files,passwords.keys…etc.,
b) Modify settings according to the user perspective.
c) Install Programs/Plugins.

6) *Disadvantages of Persistence*
a) If it is more unique then it is easier to detect.
b) Incorrect settings and vulnerable software can compromise your anonymity.

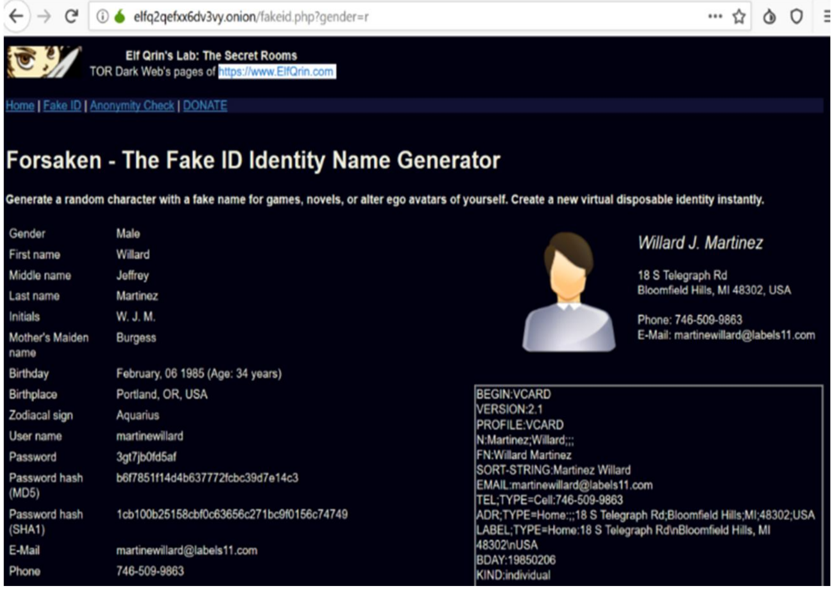
7) *Connecting to Tor using Tails:* Tails providing the inbuilt feature of Tor network. Navigate to the Tor browser and click to run the application. The user needs to choose the option called "connect" it helps the browser to enter into the tor network. If the user needs to connect any coffee shop network into their device they tried to access those network using Tor browser because using of normal browser may compromise the user's system. So connecting to Tails is a good option here, if a user is trying to connect to the Tor browser the public wifi page will never load. In order to load the page, the user needs to run any one of the unsafe browsers. It helps the user to get that coffee shop wifi login page. Once the connection is established check out this link https://check.torproject.org if it connected then close that unsafe browser and proceed with the internet anonymously and privately [10].

8) *Accessing the Darknet:* If the user needs privacy from the public internet then they should need to change the way of using the internet instead of using normal websites like google, yahoo, Gmail, Facebook, Twitter etc., because this will get users private data and they can try to use that information for something else. So preventing from these issues we need to go for onion services. Here some people will think about how to find the darknet websites? It's not so hard to find, it is actually easy just go to any of the search engines the famous one is duckduck go and type the query to find the onion websites it will give the website id with .onion or user can also find through other websites like Indexes, Forums, Subreddits etc., or user can also ask some darknet specialists to know about the websites [4].

9) *Darknet Search Engines:* According to my survey, the search engines that are more famous in darknet websites are,
a) duckduckgo.com - https://3g2upl4pq6kufc4m.onion
b) NotEvil - https://hss3uro2hsxfogfq.onion
c) Torch - https://xmh57jrzrnw6insl.onion
d) ahmia - https://msydqstlz2kzerdg.onion

Search engines are stored in the extension called. onion because all the darknet websites will use these extensions only. Here user can search for any topic they want, it gives detailed information about the content and it disables the javascript which is running in the background of the website. Darknet search engines never store user's private information (cache&cookies) it will just show the results expected by the users. So working with darknet is quite different and attractive when compared to the Clearnet [11].

10) *Fake ID generator & Email Addresses:* Email address is the major communication platform for corporate and personal users, some of the famous email service providers are Gmail, Microsoft outlook, yahoo etc. Like Clearnet even darknet also contains lots of email services for communication between the darknet users there are some darknet email services can communicate with both surface web and deep web. Using the email services is not a big deal but need to be aware of the identity. whenever people using the darknet they need to create a fake identity because I already mentioned many governments, non-government organizations and hackers may look into it. If something wrong happens they can easily identify users. Creating a masked identity is the best option. There is a website called "Forsaken" in darknet it is an onion service (http://elfq2qefxx6dv3vy.onion/fakeid.php) this gives lots of fake information to mask the user identity [4]. Like Forsaken there are lots of fake identity websites available. Users can go for their wish. There are some temporary email services which are available in the darknet. User can create a fake email id to attract the target. But using fake information is illegal users need to be genuine [4].



elfq2qefxx6dv3vy.onion/fakeid.php?gender=r

Elf Qrin's Lab: The Secret Rooms
TOR Dark Web's pages of https://www.ElfQrin.com

Home | Fake ID | Anonymity Check | DONATE

Forsaken - The Fake ID Identity Name Generator

Generate a random character with a fake name for games, novels, or alter ego avatars of yourself. Create a new virtual disposable identity instantly.

Gender	Male
First name	Willard
Middle name	Jeffrey
Last name	Martinez
Initials	W. J. M.
Mother's Maiden name	Burgess
Birthday	February, 06 1985 (Age: 34 years)
Birthplace	Portland, OR, USA
Zodiacal sign	Aquarius
User name	martinewillard
Password	3gt7jb0fd5af
Password hash (MD5)	b6f7851f14d4b637772fcbc39d7e14c3
Password hash (SHA1)	1cb100b25158cbf0c63656c271bc9f0156c74749
E-Mail	martinewillard@labels11.com
Phone	746-509-9863

Willard J. Martinez

18 S Telegraph Rd
Bloomfield Hills, MI 48302, USA

Phone: 746-509-9863
E-Mail: martinewillard@labels11.com

```
BEGIN:VCARD
VERSION:2.1
PROFILE:VCARD
N:Martinez;Willard;;;
FN:Willard Martinez
SORT-STRING:Martinez Willard
EMAIL:martinewillard@labels11.com
TEL;TYPE=Cell:746-509-9863
ADR;TYPE=Home:;;18 S Telegraph Rd;Bloomfield Hills;MI;48302;USA
LABEL;TYPE=Home:18 S Telegraph Rd\nBloomfield Hills, MI
48302\nUSA
BDAY:19850206
KIND:individual
```

Fig. 5. Forsaken ID Generator

Some of the famous email services provided by the darknet are,

a) ProtonMail – https://protonirockerxow.onion
b) Torbox – https://torbox3uiot6wchz.onion
c) Bitmessage – https://bitmailendavkbec.onion
d) Mail2Tor – https://mail2tor2zyjdctd.onion

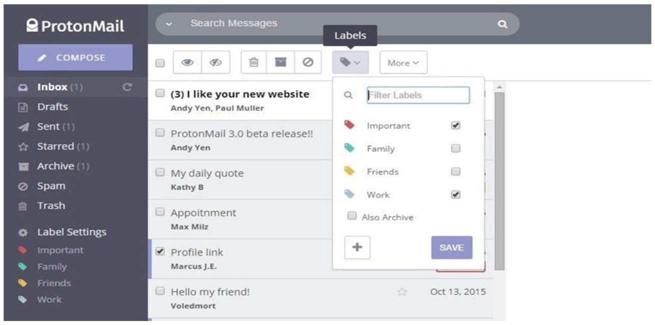
As I mentioned before, proton email service providers are best privacy-focused email providers in the darknet.

11) *Benefits of ProtonMail*

a) No Tracking
b) No Logs
c) End to End Encryption
d) No personal information required
e) Open-source
f) Enforce HTTPS
g) Available on the Clearnet and as an onion service
h) Use their own servers in Switzerland
i) Send mails to Clearnet and darknet addresses.

12) *Aware of ProtonMail*

a) Always be clear in the companies terms and conditions and privacy policies.
b) Never use your real identity.



☐ (3) I like your new website
Andy Yen, Paul Muller

☐ ProtonMail 3.0 beta release!!
Andy Yen

☐ My daily quote
Kathy B

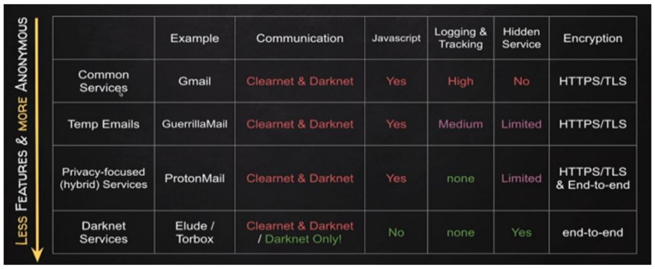
☐ Appoitnment
Max Milz

☑ Profile link
Marcus J.E.

☐ Hello my friend! Oct 13, 2015
Voledmort

Fig. 6. Proton Mail Service

Not every email services communicate with Clearnet there are certain email services that will communicate only inside the darknet. According to my survey, I mentioned the benefits of certain email services,


LESS FEATURES & MORE ANONYMOUS

	Example	Communication	Javascript	Logging & Tracking	Hidden Service	Encryption
Common Services	Gmail	Clearnet & Darknet	Yes	High	No	HTTPS/TLS
Temp Emails	GuerrillaMail	Clearnet & Darknet	Yes	Medium	Limited	HTTPS/TLS
Privacy-focused (hybrid) Services	ProtonMail	Clearnet & Darknet	Yes	none	Limited	HTTPS/TLS & End-to-end
Darknet Services	Elude / Torbox	Clearnet & Darknet / Darknet Only!	No	none	Yes	end-to-end

Fig. 7. Comparison of email services benefits

13) *File Management in Darknet:* When using the darknet we need to be more concern about the management of data. Because data should have to prevent and that should be the most prior concern for many users. Leaking of data leads to the potential loss so efficient management of data needs to take place. Whenever user sharing the file to the unknown network they need to clear their metadata of a file because that metadata contains additional information about that specific file. For example let us take an image just go to the properties of the image it contains the image type, device information, captured data etc., Instead of using google dropbox use firefox sent to share the files because google can store the data logs onto the server. If someone infiltrates that server then your sensitive information got exposed. We can encrypt our file before sharing and to decrypt we need a key so this remains our data secure while transferring over the network [4]. Also, the Tail OS providing the service to communicate inside the darknet anonymously and securely through the "Onion Share". It is a peer-to-peer service and the files are stored locally it provides the end-to-end encryption for the clients who are accessing this service and it is more private [4].

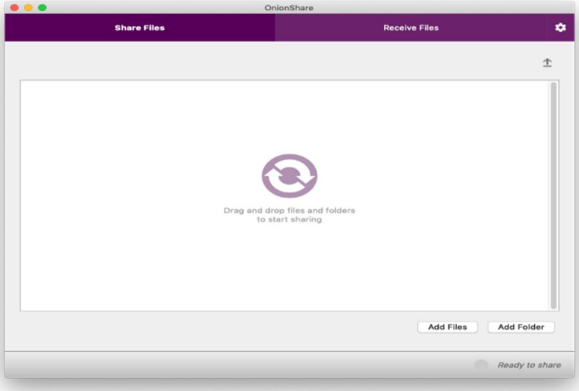


Fig. 7. Darknet's Onion share services

Once the user's data gets shared and all user work with that data is done. Deletion of shared data will not remove the data permanently. Because those removed data can be easily recovered so wipe out the data is the best option to destroy the data permanently.

C. Method 3: The User Can Go Up With Qubes If They Have A Working Environment

Suppose the user should need to work in the business environment they have lots of things to do. Doing in the single operating system is not a great deal because if someone tries to tamper that OS, then every sensitive information will get exposed. So working with the tails is not a great idea. That's why we are choosing the OS called "Qubes" it has an extraordinary functionality. Qubes using its own virtualization platform in a single operating system we can use multiple virtual environments like personal, business, workspace, network etc., So, if the user wants to do his/her personal work then he can go with personal workspace and if his/her needs to do the office work means they can go for the business workspace. So, using one workspace doesn't conflict with each other, each has its own individual functionality if a hacker tries to tamper any of the workspaces it will affect only to that particular workspace and it will never attack the remaining this ensures the privacy of the OS [12].

III. CONCLUSION

According to the study I mentioned lots of information about the darknet and how to access anonymously into it, but this information is not sufficient to go deeper if anyone has more interested into the darknet they should have to learn more about the encryption& decryption, bitcoins and cryptocurrencies. And how they are using cryptocurrency technique inside the darknet to transfer the money anonymously. There is a lot to learn about darknet it's just a part of the deep web as I already mentioned more than 80% of the internet relies in deep web, whatsoever I conveyed to you is not so easy I researched over lots of papers and tutorials to grab these much contents still I didn't disclose many because that moves beyond the study. So, the people who are thinking that working with darknet is not possible or hard then here is the solution this will gives the working knowledge for them.

REFERENCES

[1] Rob Sobers,"Cyber Security statistics for 2020" Reveived 9 Jan 2020 Available at https://www.varonis.com/blog/cybersecurity-statistics.

[2] J. Isaak and M. J. Hanna, "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection," in Computer, vol. 51, no. 8, pp. 56-59, August 2018, doi: 10.1109/MC.2018.3191268.

[3] Gabriel Weinberg,"We don't collect or share personal information", https://duckduckgo.com/privacy.

[4] Zaid Sabih," The Ultimate Dark Web, Anonymity, Privacy & Security Course",https://www.udemy.com/course/the-ultimate-dark-web-anonymity-privacy-security-course.

[5] Ian Goldberg,"Installation of the Tor Browser",https://www.torproject. Org/download/.

[6] K. Shahbar and A. N. Zincir-Heywood, "An analysis of tor pluggable Transports under adversarial conditions," 2017 IEEE Symposium Series on Computational Intelligence (SSCI), Honolulu, HI, 2017, pp. 1-7.doi: 10.1109/SSCI.2017.8280829.

[7] Y. He, L. Hu and R. Gao, "Detection of Tor Traffic Hiding Under Obfs4 Protocol Based on Two-Level Filtering," 2019 2nd International Conference on Data Intelligence and Security (ICDIS), South Padre Island, TX, USA, 2019, pp. 195-200.doi: 10.1109/ICDIS.2019.00036.

[8] The Tor Project,"Start Using your Bridges",https://bridges.torproject.or g/bridges?transport=obfs4".

[9] Tails,"Instllation of Tails the amnesic incognito live system", https://tails.boum.org/.

[10] Tails,"Connecting to Tor using Tails",https://tails.boum.org/doc/anony mous_internet/networkmanager/index.en.html".

[11] The Deep Web,"Deep web search engine lists 2020"https://www.deep websiteslinks.com/deep-web-search-engine-list.

[12] Team Qubes,"Installation and working with Qubes TorVM",https://www.qubes-os.org/doc/torvm.