CHAPTER I

INTRODUCTION

A cryptocurrency is a digital asset designed to work as a medium of exchange that uses strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets. It has been argued that a cover of anonymity increases the likelihood of participation in illegal activities. Bitcoin has captured the imagination of the financial world, and, more likely, that of the criminal intent[2], who seek to use its pseudonymous nature to conceal dealings related to various illegal activities such as transacting in contraband goods and services, receiving payment for ransomware attacks, especially on the dark web.This research deals with the analysis of various bitcoin wallets and searching for its potential forensic artifacts present on various laptops and mobile devices. So, bitcoin is a digital currency created in January 2009. It was developed by the mysterious and pseudonymous developer "Satoshi Nakamoto", whose true identity has yet to be verified[2].Bitcoin, a decentralized, peer-to-peer, pseudonymous cryptocurrency and an electronic payment system, has rapidly expanded in recognition since the seminal work was distributed to an obscure cryptography mailing list on metzdowd.com[1]. Due to the fact that many people don't have a clear knowledge about bitcoin cryptocurrency and what types of artifacts can be recovered from the various bitcoin wallets, so there is a need to familiarize investigators with Bitcoin's structure and to attempt, to the greatest extent possible, to penetrate its pseudonymous nature, and some users' anonymization efforts, to link transactions with suspects in a reproducible manner that will allow for admission into court as scientific evidence in the future.

Fig 1.0:- Image of Bitcoin Cryptocurrency

Bitcoin is a type of cryptocurrency. The balance of Bitcoin tokens are kept using public and private "keys," which are long strings of numbers and letters linked through the mathematical encryption algorithm that was used to create them[1]. The public key (comparable to a bank account number) serves as the address which is published to the world and to which others may send bitcoins. The private key (comparable to an ATM PIN) is meant to be guarded secret and only used to authorize Bitcoin transmissions[3]. Bitcoin keys should not be confused with a Bitcoin wallet, which is a physical or digital device which facilitates the trading of Bitcoin and allows users to track ownership of coins. The term "wallet" is a bit misleading, as Bitcoin's decentralized nature means that it is never stored "in" a wallet, but rather decentrally on a blockchain[2].While the development of bitcoin and other comparable cryptocurrencies seems to have provided users with a unique array of benefits, these benefits have not come without corresponding risks and costs. Due to the distinctively unregulated nature of the cryptocurrency market, it has naturally been frequently used by a wide variety of criminal enterprises.These cryptocurrencies offer true anonymity in electronic transactions that trading websites such as the Silk Road, essentially a black-market Amazon or eBay, were created and became popular for criminal dealings[4]. Although the Silk Road was shut down by the FBI in 2013 for its part in facilitating the exchange of illegal goods for the cryptocurrency Bitcoin, the existence of similar websites supporting illegal business resolutely persists.With peer-to-peer transactions as the fundamental purpose of cryptocurrencies, these digital currency systems offer a different types of user activity[2].The foundations of Bitcoin, executed through cryptography, are confidentiality, integrity, non-repudiation, and authentication. Bitcoin is the first successful execution of a distributed cryptocurrency as originally described on the cypher punks mailing list.As of December 2019, one bitcoin is worth approximately ($8,545). This is significantly less than the peak value that was witnessed in December 2017 ($19, 343), but also significantly more than values reported just one year ago.

In late 2008, the financial crisis of U.S. was in full swing. In September of that year, as the world's financial infrastructure was crumbling, the domain bitcoin.org was registered. Later in 2008, a person or group using the pseudonym Satoshi Nakamoto published a white paper on bitcoin to a cryptography mailing list, explaining how the cryptocurrency would work[3].

In early 2009, Nakamoto mined the first-ever bitcoin, known as the "genesis block." Embedded in the programming of this first bitcoin was the text "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks." The text refers to a headline on that date from the British newspaper The Times, and is generally seen as proof of the date bitcoin was first mined[4]. Others also believe it pointed to the crumbling financial infrastructure of the modern world, and the need for a new way forward. The first bitcoin transaction soon followed, when a bitcoin was sent from Nakamoto to Hal Finney, a cryptography expert and enthusiast.

To this day, Satoshi Nakamoto's identity remains a mystery. Several people have claimed to be the mysterious programmer or, as often suspected, a group of programmers; numerous attempts have been made to identify the person or group, but none have been satisfactory enough to be viewed as conclusive. The only personal details that Nakamoto gave to others were claims to be living in Japan and to have been born April 5, 1975. Nakamoto encouraged other cryptographers to assist with the coding, but the creator stepped away from bitcoin in 2011 and has not been publicly seen or heard from since[5].

A blockchain is simply a block of transactions chained together in a chronological order. It is the record-keeping technology behind the Bitcoin network. Blockchain is just a chain of blocks, but not in the traditional sense of those words. When we say the words “block” and “chain” in this context, we are actually talking about digital information (the “block”) stored in a public database (the “chain”).When a block stores new data it is added to the blockchain[6]. In order for a block to be added to the blockchain, however, four things must happen:

- ✓ A transaction must occur.
- ✓ That transaction must be verified. After making that purchase, your transaction must be verified.
- ✓ That transaction must be stored in a block. After your transaction has been verified as accurate, it gets the green light. The transaction’s amount, digital signature are all stored in a block.
- ✓ That block must be given a hash. once all of a block’s transactions have been verified, it must be given a unique, identifying code called a hash. The block is also given the hash of the most recent block added to the blockchain. Once hashed, the block can be added to the blockchain.

When that new block is added to the blockchain, it becomes publicly available for anyone to view—even for us. Bitcoin is based on a distributed ledger or rsther a specific kind of distributed ledger known as blockchain.

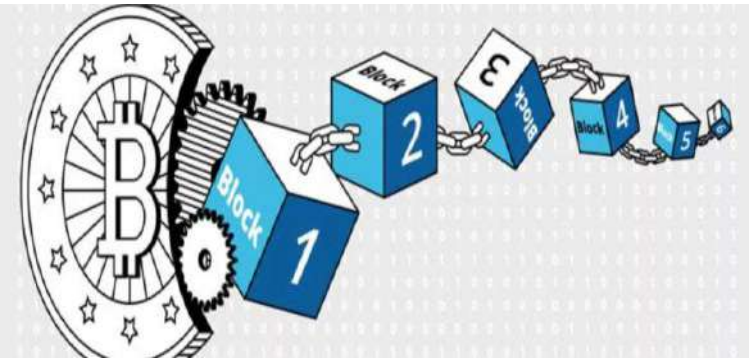

Fig 2.0:- Image of Blockchain

Bitcoin miners are geographically distributed nodes of computers whose role is to solve complex mathematical-work problems to confirm transactions and secure the blockchain. Mining is how bitcoins are 'created', and miners are awarded a periodically halving number of bitcoins, plus transaction fees, for their successes. For the first 210,000 blocks, approximately the initial four years, miners were rewarded with 50 bitcoins; during the next four years, the reward was 25 BTC. Now, the mining reward is 12.5 BTC, and that reward will be cut in half again around June of 2020. Ultimately, the limit of 21 million BTC will be mined, with the last new bitcoin expected to be created in 2140[5]. At this point, the mining reward will consist of the transaction fees.

In the beginning, when difficulty was low, miners could use laptops or desktops to mine bitcoins. As competition increased, and difficulty rose, miners created multi-graphic card rigs to harness the power of graphics processing units (GPUs). He final evolution was to Application Specific Integrated Circuits (ASICs), which continue to race to smaller and smaller chips, and greater electrical efficiency while adding more and more to their hashes/second rates[6]. ASICs are essentially mandatory for BTC mining as the cost of electricity in using any previous method outweighs the value of the expected reward.

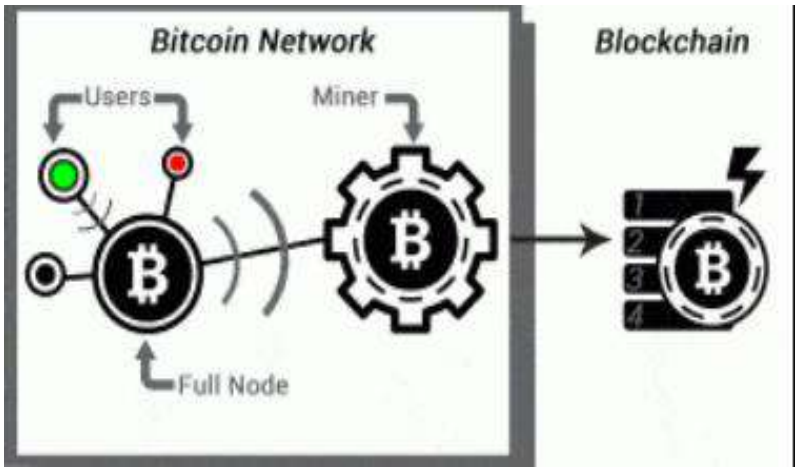

Fig 3.0:- **Image of Bitcoin Network**

Non-criminal uses of Bitcoin:- In general, there is relatively little belief that bitcoin will replace the use of traditional currencies (such as USD, EURO, etc.), rather, it will function as an alternative that supplements the global currency markets and also makes them significantly more competitive[7]. Like traditional currency, bitcoin's value is fundamentally determined by whatever people believe it is worth.

There are various ways that an individual can use bitcoin in exchange for specific goods or services.

- ✓ Air travel and hotels
- ✓ Certain applications, videos, movies, games, and electronic services (accepted in the Microsoft app store or the websites of certain artists)
- ✓ A surprisingly large number of merchants and franchises (including Subway)
- ✓ Some gift cards or other electronic gifts
- ✓ Numerous other circumstances where online payments are standard

Clearly, there are many reasons that a well-intentioned person may want to pay for certain things using bitcoin. Because the correlation between the value of bitcoin and the value of most local currencies is relatively limited, some individuals prefer to use bitcoin when the exchange value is particularly high and use traditional currencies when the exchange value is particularly low. Considering that both currency markets fluctuate over time, diversifying the range of available payment options can decrease the risk of the current holdings[5]. Additionally, even if they are not engaged in any illegal activities, individuals on both sides of a given transaction can enjoy the added layer of privacy that only cryptocurrency can offer. The future of bitcoin – and the cryptocurrency market as a whole – remains relatively unclear. Generally, it seems that there will be a wider range of cryptocurrencies to choose from and that cryptocurrencies will generally be accepted at an increased number of locations[8]. However, bitcoin's widespread use in illegal markets and its incredibly unregulated nature are both legitimate reasons for the public to be at least somewhat skeptical.

Criminal uses of Bitcoin:- Unfortunately, the characteristics of bitcoin that many people innocently enjoy – relative privacy, the removal of an intermediary, ease of international transactions, etc. are also the characteristics of bitcoin that happen to benefit criminal enterprises the most. Although it was not created with the intention of being compatible with criminality, but its increased use by criminals is something that certainly cannot be easily ignored.

Currently, there are many different ways in which bitcoin is being actively used by criminals.

- ✓ The Darknet is a portion of the internet that operates without any active hosts. Activity on the Darkent is difficult to track and difficult to accurately identify. Naturally, individuals who seek to exchange currency (cryptocurrency) for illegal services can benefit from these features.
- ✓ The Dark Web is related to the Darknet but is structurally different and typically requires specific software.
- ✓ Bitcoin is frequently used as a means for paying for drugs or other illegal goods and services (such as weapons).
- ✓ Bitcoin is also frequently used to hire individuals for malicious hacking. This includes trying to access other individual's financial information, other personal information, and trying to "take over" a specific computer.
- ✓ Terrorism and widespread criminal activity – such as the international distribution of weapons and other threats to the public – is often organized using bitcoin due to the fact that it is incredibly difficult to pin these activities on a specific individual.

Essentially, if an individual or organization seeks to engage in an illegal activity that can be entirely organized via the internet, then they will have many reasons to use cryptocurrency rather than traditional payment options[8]. On the rare occasion that a law enforcement organization is able to trace these illegal activities to a specific IP address, the burden of the prosecution is still usually not entirely satisfied. The law enforcement agency (depending on the jurisdiction

in which these activities are taking place will still need to prove this activity took place knowingly and was not a consequence of a deliberate digital misdirection[7].

Transactions:- Electronic coins, in this case bitcoins, are defined as "a chain of digital signatures," where each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. Elliptic key cryptography is used to instantiate public-key cryptography protocols because they are smaller key sizes and more efficient implementation while preserving security levels. The transfer of bitcoins ownership from one user to another is accomplished by attaching, at the end of the new transaction, a digital signature (using the owner's private key) of the hash of the previous transaction and information about the new owner's public key[9]. The digital signature can be verified with the help of the owner's public key. Transactions consist of three parts: the sender, the receiver and a digital signature (the 'witness') that verifies the sender's right to send the bitcoins. $ier a transaction is created, it is broadcast to the Bitcoin network for validation and inclusion in a block.

Multi-input transactions occur when a payment is being made by a user, but the amount of that payment exceeds the value in any given individual input address in that user's wallet, but not the user's balance. Under these circumstances, the wallet will choose a set of BTCs from the multiple input addresses and prepare the transaction, which allowed the conclusion that all these addresses belong to the same user[9]. By default, a new shadow address is generated automatically by the main Bitcoin client when the total inputs exceed the required transfer amount, and 'change' is required; therefore, if there are old output addresses with a single new address (which has never before appeared), it is reasonable to conclude that this new address is a shadow address associated with the input address. He use of shadow addresses is the only mechanism, other than its reliance on pseudonyms that Bitcoin employs to enhance user privacy.

Most individuals who own and use Bitcoin have not acquired their tokens through mining operations. Rather, they buy and sell Bitcoin and other digital currencies on any of a number of popular online markets known as Bitcoin exchanges. Bitcoin exchanges are entirely digital and, as with any virtual system, are at risk from hackers, malware and operational glitches[10]. If a thief gains access to a Bitcoin owner's computer hard drive and steals his private encryption key, he could transfer the stolen Bitcoins to another account. (Users can prevent this only if bitcoins are stored on a computer which is not connected to the internet, or else by choosing to use a paper wallet – printing out the Bitcoin private keys and addresses, and not keeping them on a computer at all.) Hackers can also target Bitcoin exchanges, gaining access to thousands of accounts and digital wallets where bitcoins are stored. One especially notorious hacking incident took place in 2014, when Mt. Gox, a Bitcoin exchange in Japan, was forced to close down after millions of dollars worth of bitcoins were stolen.

This is particularly problematic once you remember that all Bitcoin transactions are permanent and irreversible. It's like dealing with cash: Any transaction carried out with bitcoins can only be reversed if the person who has received them refunds them. There is no third party or a payment processor, as in the case of a debit or credit card hence, no source of protection or appeal if there is a problem.

CHAPTER II
LITERATURE REVIEW

Sergey Avdoshin, et al. (2018) “Bitcoin Users Deanonimization Methods”-Bitcoin is the most popular cryptocurrency on the planet[3]. It relies on strong cryptography and peer-to-peer network. Bitcoin is gaining more and more popularity in criminal society. That is why Bitcoin is often used as money laundering tool or payment method for illegal products and services. In this paper, we propose to use off-chain information as votes for address separation and to consider it together with blockchain information during the clustering model construction step.

David Neilson, et al. (2017) “Bitcoin Forensics”- Over the past eighteen months, the digital cryptocurrency. Bitcoin has experienced significant growth in terms of usage and adoption. It has also been predicted that if this growth continues then it will become an increasingly useful tool for various illegal-activities.Against this, it seems safe to assume that students and professionals of digital forensics will require an understanding of the subject. New technologies are often a major challenge to the field of digital forensics due to the technical and legal challenges they introduce[5]. This paper provides a set of tutorials for Bitcoin that allows for leaners from both backgrounds to be taught how it operates, and how it may impact on their working practice. Earlier this year they were delivered to a cohort of third year undergraduates. To the author’s knowledge, this represents the first integration of the topic into a digital forensics programme by a higher education provider.

Michael Doran (2015) “A Forensic Look at Bitcoin Cryptocurrency” - The increased use of cryptocurrencies such as Bitcoin among private users and some businesses has opened a new avenue of research in the field of digital forensics involving cryptocurrencies[5].Tools such as Internet Evidence Finder have the capability to recover some Bitcoin artifacts. This research seeks to recover any evidence of Bitcoin mining that would be present on a user’s system due to the use of such software or applications.

Satoshi Nakamoto (2009) “Bitcoin: A Peer-to-Peer Electronic Cash System” - A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending[8]. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they’ll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone. This paper defined the basic working of bitcoin cryptocurrencies and all the other things.

CHAPTER III

AIM AND OBJECTIVES

AIM:

The aim of this research is to assist and make aware the forensic cyber investigators in identifying the various crimes and frauds that take place through bitcoin cryptocurrency and also to analyse the various bitcoin wallets for potential forensic artifacts.

OBJECTIVE:

While the goal of using Bitcoin for Tor hidden services is to provide transaction and browsing anonymity, this usage typically leaks information that can be used to deanonymize hidden service users. In particular, the adversary can link users, who publicly share their Bitcoin addresses on online social networks, with hidden services, which publicly share their Bitcoin addresses on onion landing pages. This is achieved by inspecting historical transactions involving these two addresses in the Blockchain. In doing so, the adversary only relies on data that is publicly available.

CHAPTER IV

MATERIALS AND METHODOLOGY

SOFTWARES USED:

- ✓ Electrum Wallet v3.3.8
- ✓ Bitcoin Core Wallet v0.19.0.1
- ✓ Bitcoin-Qt Wallet v0.8.4
- ✓ Multibit Wallet v0.5.1
- ✓ Cellebrite UFED Physical Analyzer v3.9.8.7
- ✓ Ifun Box v3.0
- ✓ Magnet Forensics' IEF 3.8.0

The various cryptocurrency wallets which are to be examined for potential forensic artifacts are classified in the various steps:-

✓Installation of cryptocurrency wallets on various platforms(Windows, Linux, Mobile OS)

✓Wallet analysis on mobile OS (iOS Devices).

✓Network and Blockchain analysis.

✓Wallet analysis on Windows and Linux for potential forensic artifacts.

INSTALLATION OF BITCOIN WALLETS IN WINDOWS OS:-

Step1:- Download the electrum setup file from Google chrome.

Step2:- Double click the electrum icon on desktop. It will ask where we want to store our wallet file.Click on "Next" to choose the default location in C:\Program Files.

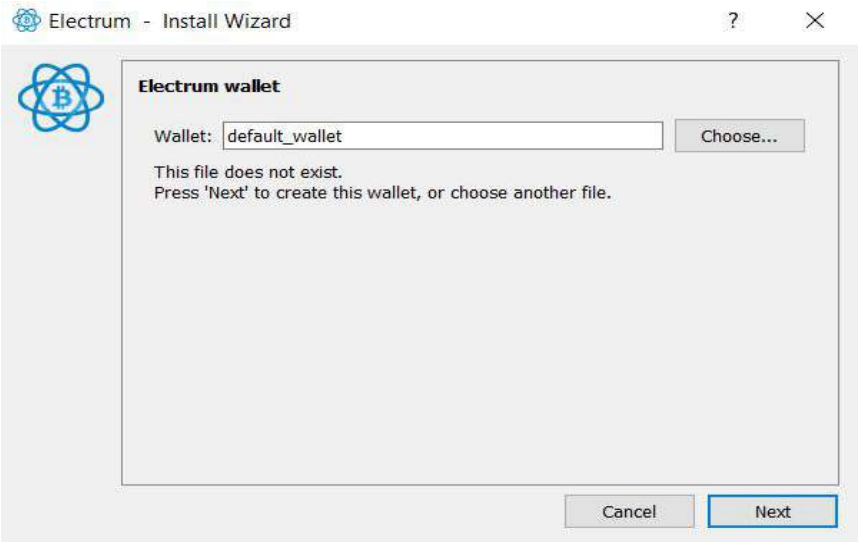

Fig 4.0:- **Select the wallet name. By default it is default_wallet**

Step3:- Electrum basically supports varioys types of Bitcoin wallets. The users using it first time should go with "Standard Wallet". Click on Next.

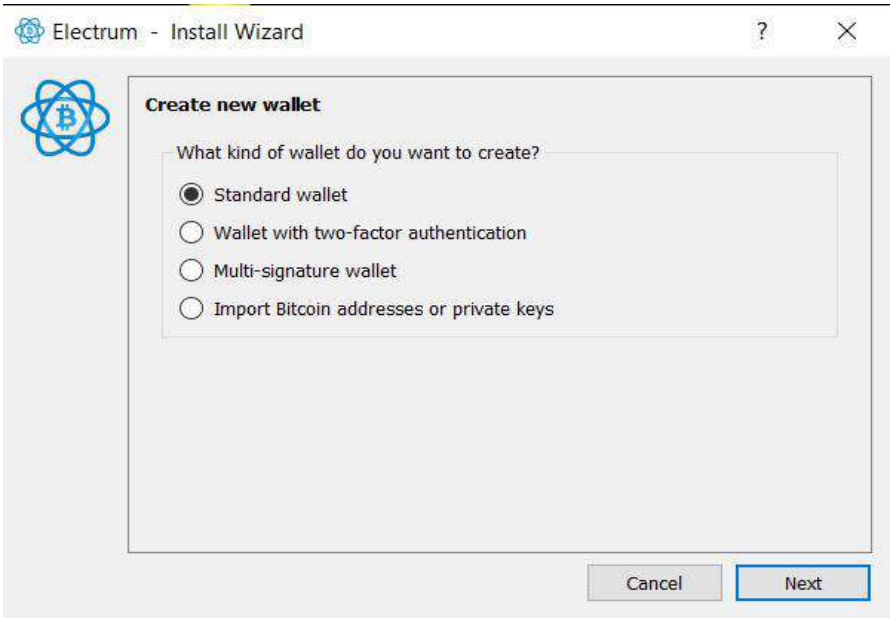

Fig 4.1:- Select the type of wallet

Step4:-Create a new wallet seed. Click next again to choose a standard "seed" type. Electrum now displays the wallet generation seed.

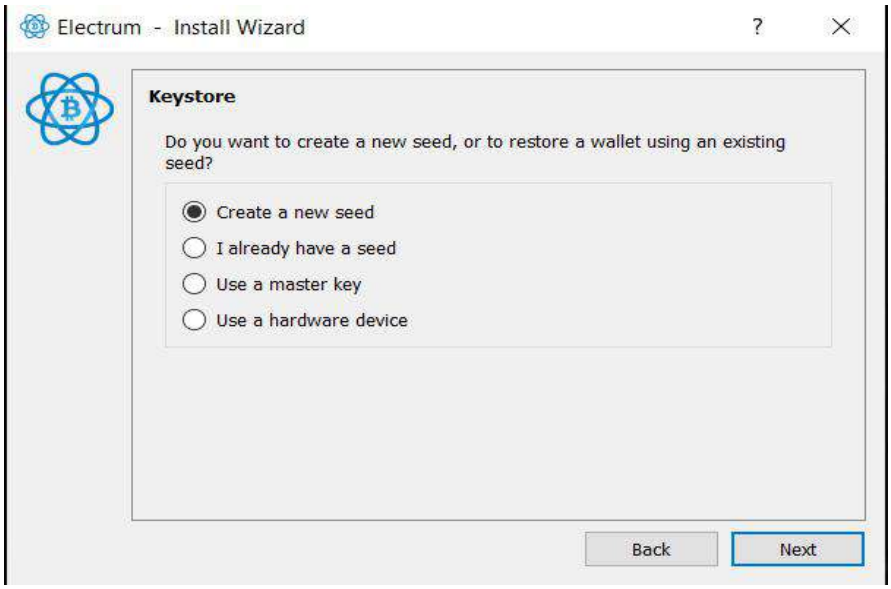

Fig 4.2:- Create a new seed for the wallet

Step5:- 12words are given as a seed.These 12 words can be used to restore the wallet if anything happens to the computer. Make sure to write that seed safely.

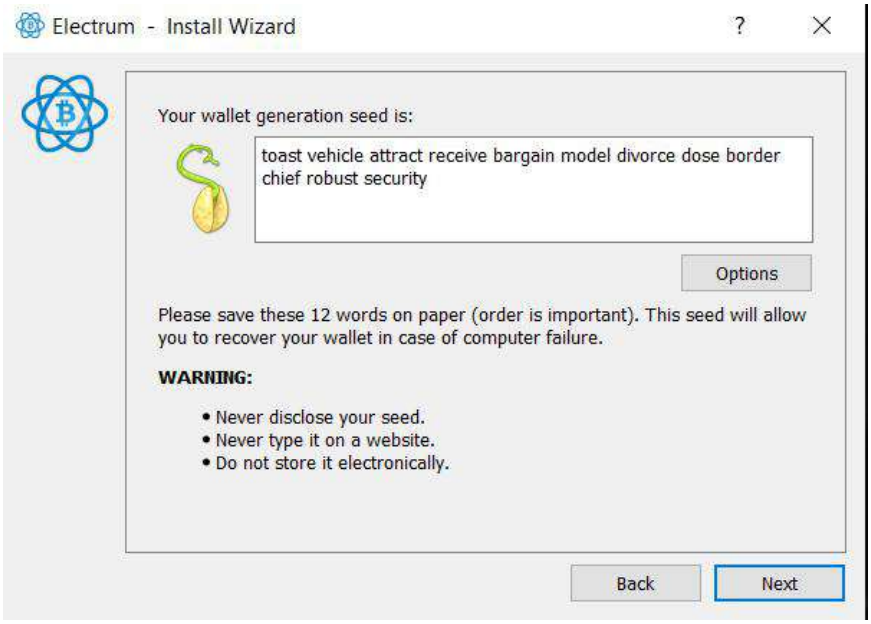

Fig4.3:- Write the wallet generation seed some other place

Step6:- Once the 12words seed is written, click on Next. It will ask to retype the seed in the following window .

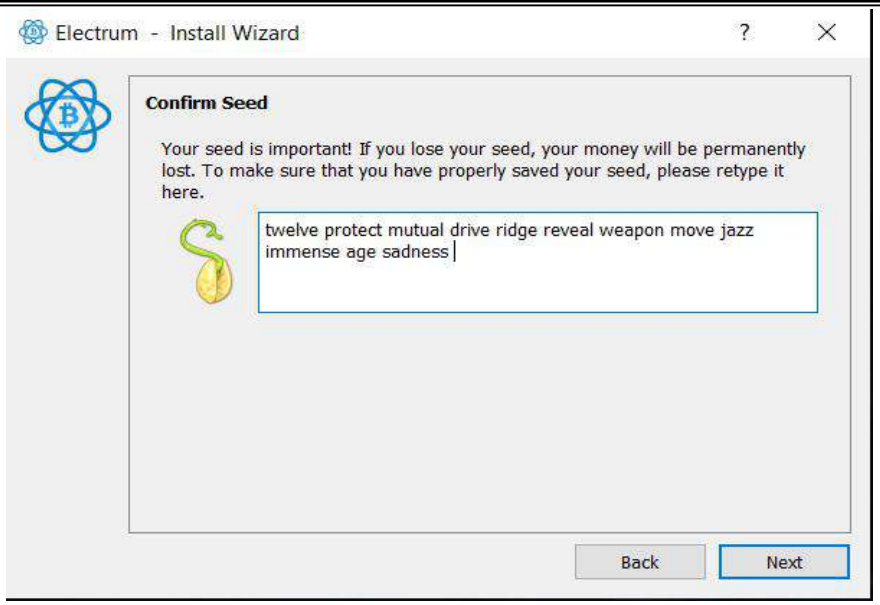

Fig 4.4:- Retype the wallet generation seed to confirm it

Step7:- Click "Next" to continue. Electrum starts generating the payment address. It will ask for keeping a password for the transactions.

Fig 4.5:- Keep a strong password for the wallet

✓ Recieving Interface Of Electrum Bitcoin Wallet.

Fig 4.6:- Recieving interface of wallet

✓ Sending Interface Of Electrum Bitcoin Wallet.

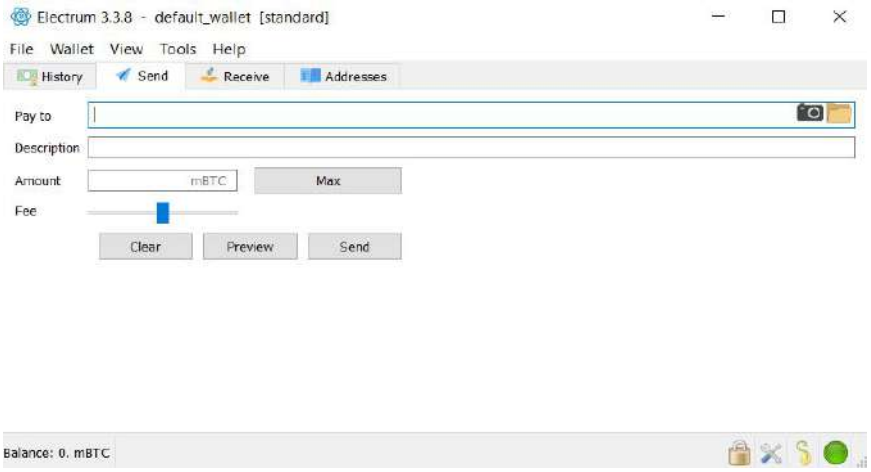

Fig 4.7:- Sending interface of wallet

INSTALLATION OF BITCOIN WALLETS IN LINUX:-

Step1:- We can start Electrum by typing “electrum” command in terminal. Upon the first launch, a setup wizard appears. Select “Auto-Connect”

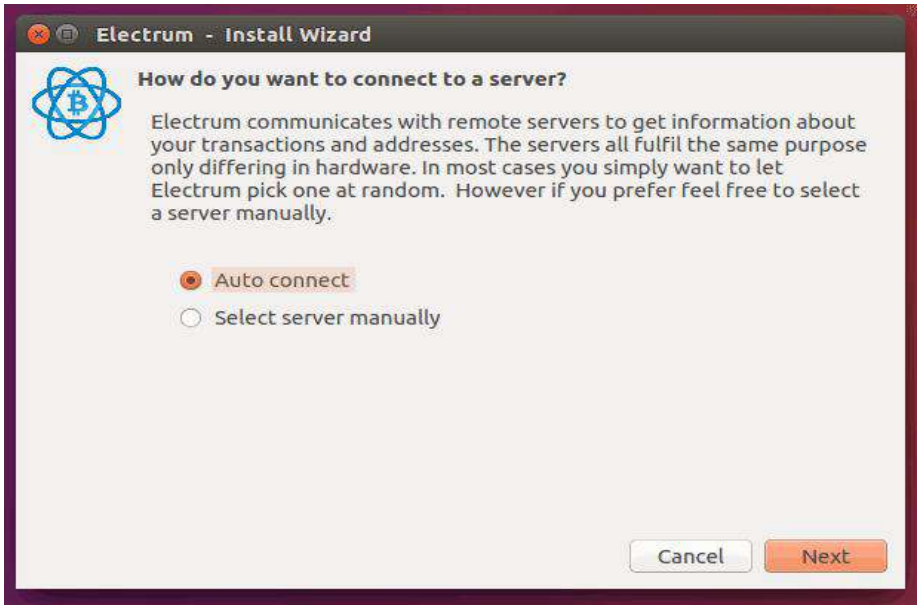

Fig 5.0:- Installation of Bitcoin Wallet in Linux

Step2:- Next it will prompt to create a default wallet. Simply click on Next button.

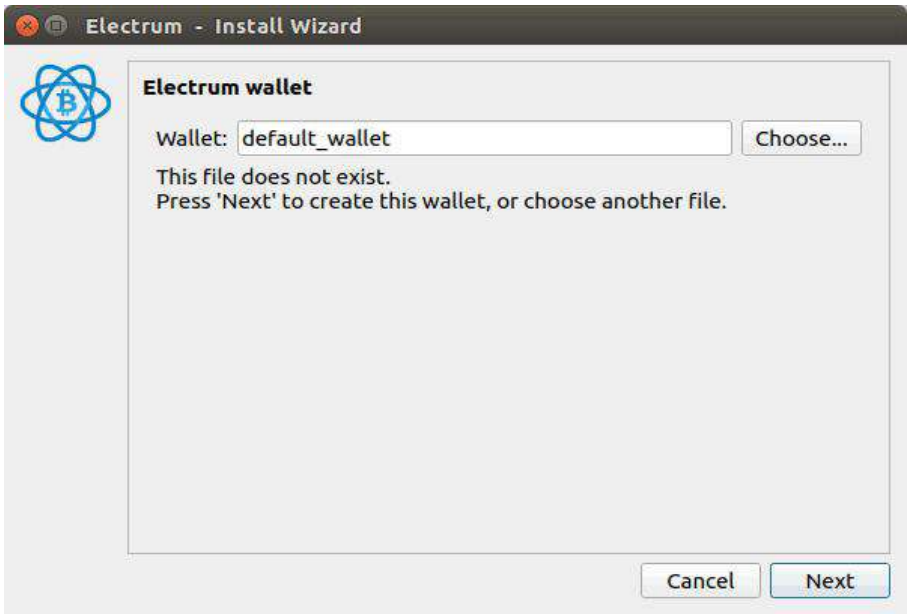

Fig 5.1:- Select the wallet name. By default it is default_wallet

Step3:- Next select the type of wallet we want. We will choose “Standard Wallet”

Fig 5.2:- Select the type of wallet

Step4:- Then select "Create a new seed" for new users.

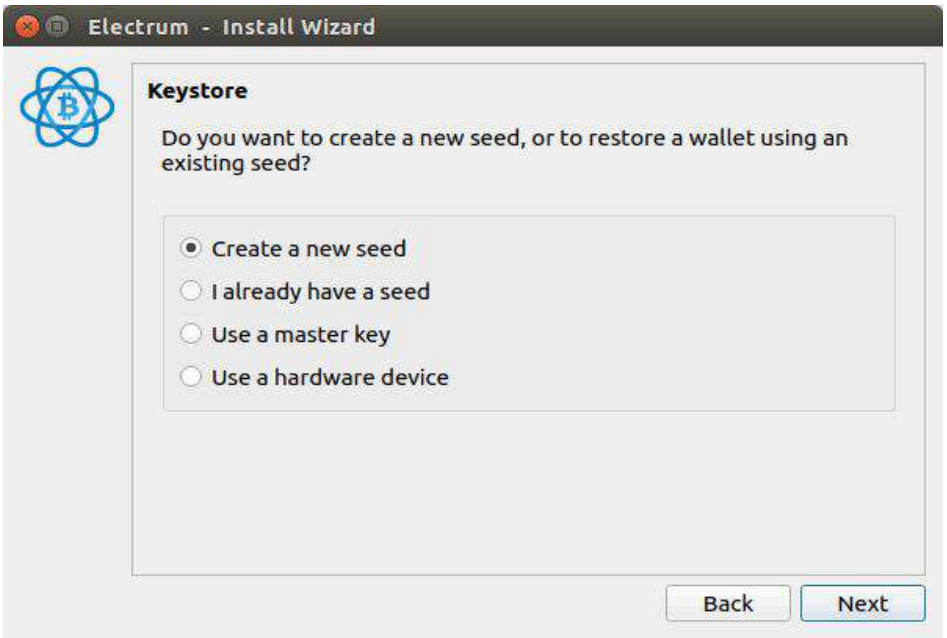

Fig 5.3:- Create a new seed for the wallet

Step5:- If we want to get bitcoins from everyone the seed type should be chosen as "Legacy".

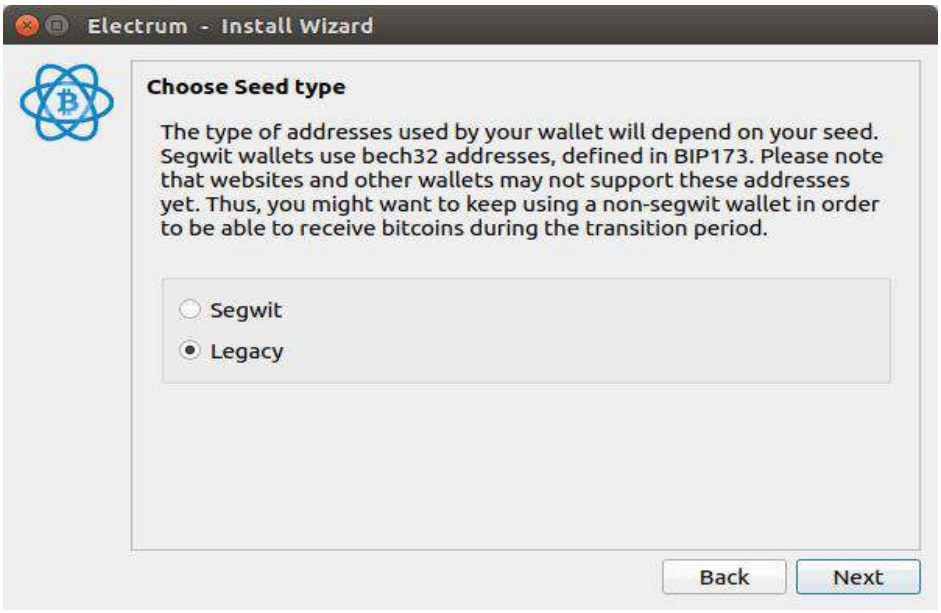

Fig 5.4:- Select "Seed Type".

Step6:- In the next step a private unique seed will there . Copy it to your system clipboard. Paste the seed in the next window.

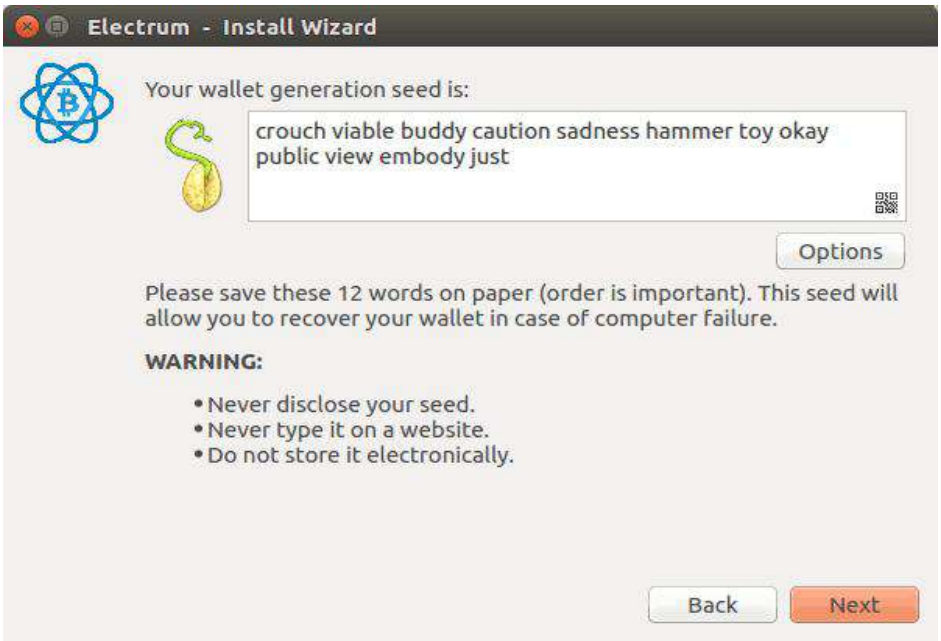

Fig 5.5:- Save the wallet generation seed some other place

Step7:- Encrypt the keys with a password.

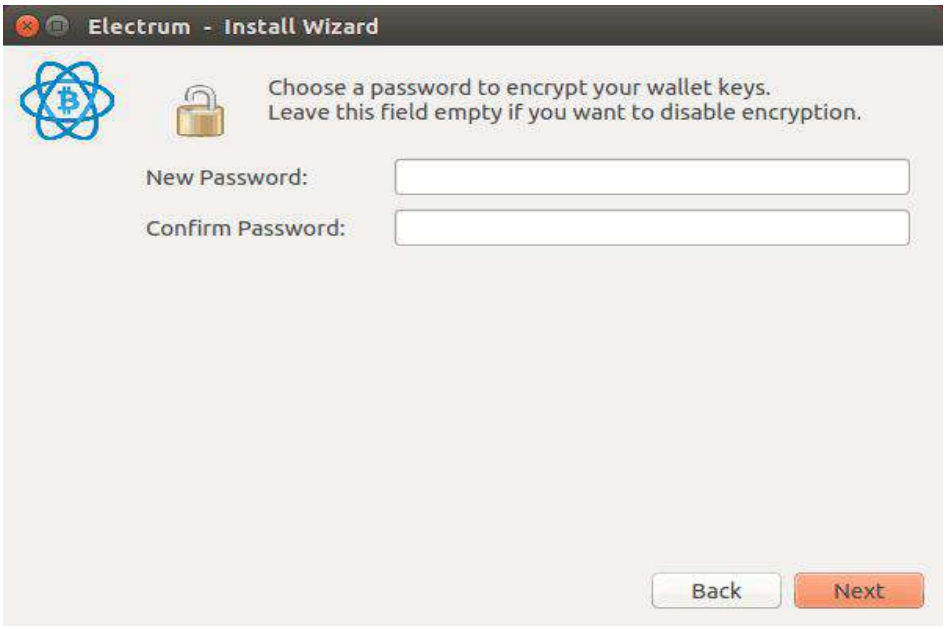

Fig 5.6:- Keep a strong password for the wallet

Bitcoin wallet analysis on iOS Devices:- To investigate the potential forensic artifacts left behind in mobile device memory by cryptocurrency wallets after controlled trading, the most popular wallet applications available for Bitcoin, Litecoin, and Darkcoin were considered for iOS devices.

The basic investigative premise was to extract the application data of each wallet from the mobile devices at four different points in the installation and trading processes:

(1) after a factory reset of the phone and prior to the installation of the wallet applications,

(2) after wallet installation and before trading,

(3) after completion of controlled trading of the currencies, and

(4) after the wallet applications had been deleted from the device.

iOS Extraction:-

The first was Cellebrite UFED Physical Analyzer (version 3.9.8.7) software. After opening the application on a desktop computer, the mobile device was plugged into one of the USB ports using the Cellebrite Tip T-110 attached to Cable A. In the application Graphic User Interface (GUI), the Advanced Logical extraction was selected and both extraction methods were performed. The extracted images were saved for later analysis.

The second method for extraction was iFunBox, an open-source app/file manager for iOS devices. Immediately after extraction in UFED Physical Analyzer for each stage, iFunBox was used to actively examine and extract application data from the still-connected iPhone. The File System folder was extracted using the iFunBox's Dump feature and saved to the encrypted hard drive. Since iFunBox is fundamentally an active file/app managing tool, analysis of the wallet applications could only be performed for Stages 2 and 3, when the wallets were still installed on the device.

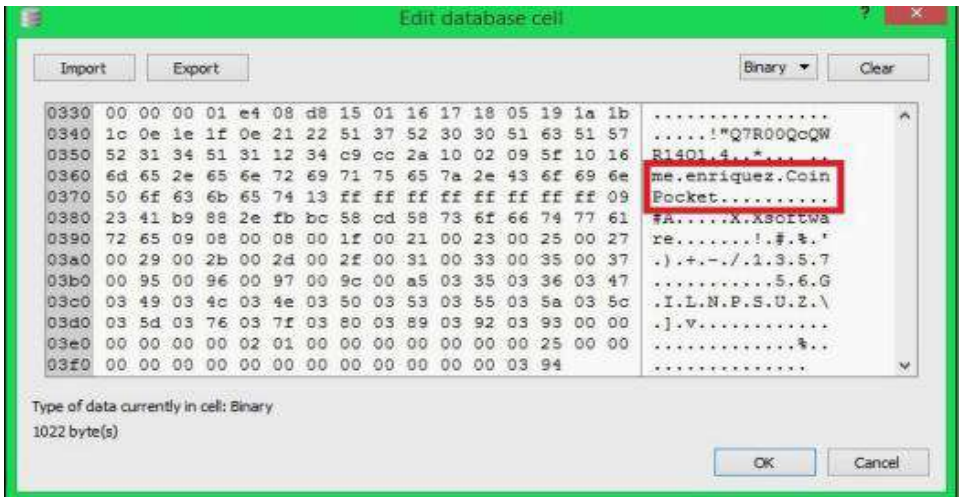

Fig6.0:- Hash values of application data of the mobile device.

iOS Stage 1: Device Set-Up

iOS Stage 2: Installation of Wallet Applications

iOS Stage 3: Trading

iOS Stage 4: Wallet Application Deletion

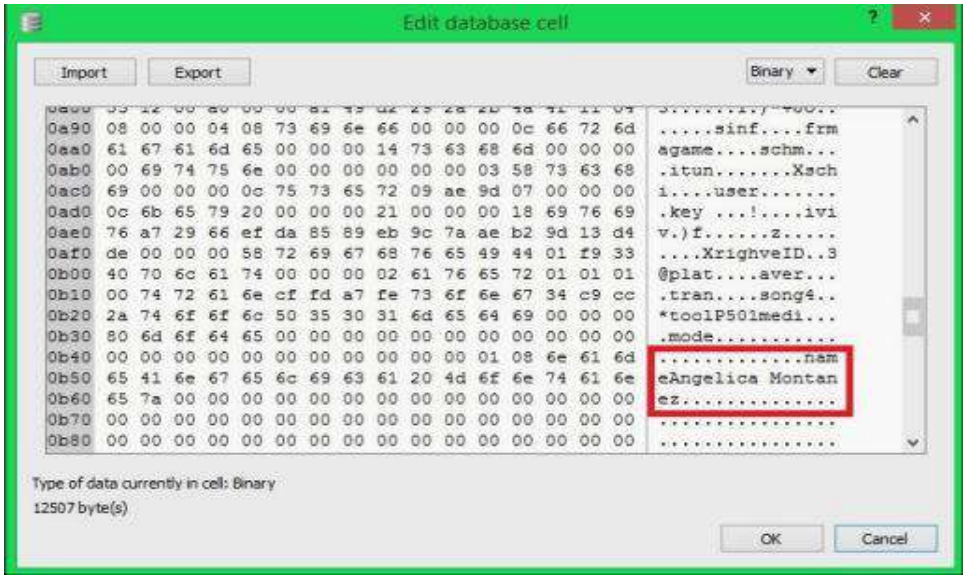

Fig 6.1:- Hash values of application data of the mobile device

iOS Analysis

To analyze the collected memory data from the iOS, UFED Physical Analyzer was used to examine the extracted .ufd files. From the encrypted hard drive, the files were opened in UFED Physical Analyzer to decode and parse the collected data. Once parsed, all extracted information listed in the left project tree pane in the GUI were examined for potential forensic artifacts. In particular, the Analyzed Data, the Data Files, Timeline, and File Systems tree items and all sub-items under each were assessed. Any extracted databases were examined both in the data view in Physical Analyzer and in the open-source tool DB Browser for SQLite. All relevant data found was dumped as a file onto the Seagate hard drive and was documented with a screen capture.

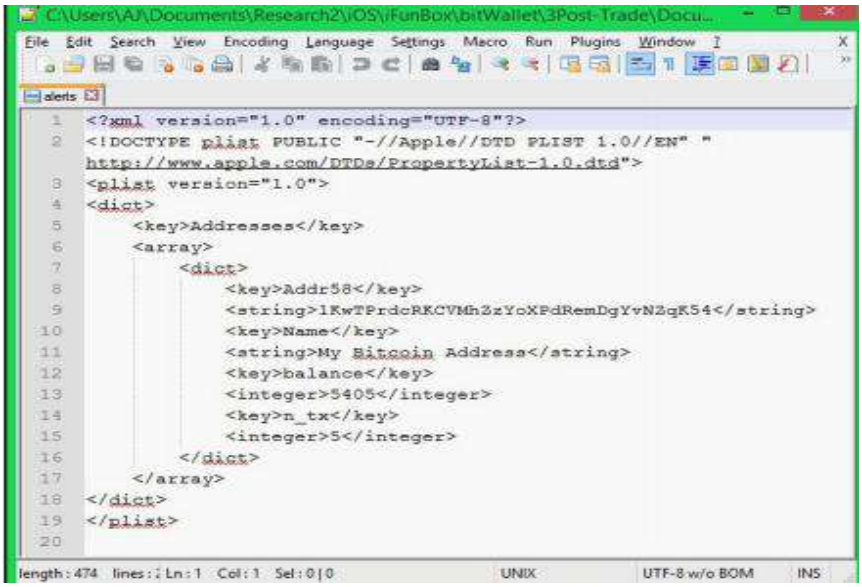

Fig 6.2:- Analysis of extracted databases for SQLite.

In the wallet application dump of bitWallet, five folders were extracted—bitWallet.app, Documents, Library, StoreKit, and tmp. In the Documents folder was an alerts.file file. When opened in Notepad++, this file was found to contain the public address string of the wallet installed on the device . In the same folder was another file: wallets.v1. This file listed not only the public address (key) of the wallet, but the private key as well .The other folders and files in the extractions of bitWallet did not hold relevant forensic data.

Traffic Analysis: The Use of Nodes to Identify a Bitcoin Participant's IP Address:-

Bitcoin traffic analysis relies on the characteristics or vulnerabilities inherent in Bitcoin's peer-to-peer network to identify the IP address of users generating transactions. The key to this mode of analysis is appreciating the role of nodes in Internet communication. Traffic analysis attacks pseudo-anonymity by "fingerprinting [Bitcoin] users based on the connections they have to other nodes on the Bitcoin p2p network. When a user connects to another node, their IP address is advertised to that node. If an attacker is connected to enough nodes, these announcements can be watched and fingerprinting can be done." Different researchers have proposed varying methodologies to exploit the nodes to identify the IP addresses of Bitcoin users

Bitcoin Peer-to-Peer Network:- Bitcoin has no central server or network infrastructure to maintain its economy. Rather, Bitcoin is composed of a network of individuals, each running software that communicates with other Bitcoin participants. More technically, the Bitcoin network is composed of peers connected to others peers over unencrypted TCP channels. Each peer attempts to maintain eight outgoing connections to other peers. These eight peers are called entry nodes.

Biryukov Traffic Analysis:- Traffic analysis exploits the role of nodes in this protocol to discover the IP address of users generating Bitcoin transactions. Biryukov's version of traffic analysis includes four steps:

- ✓ Obtain a list of peers and connect to as many servers as possible within the Bitcoin network
- ✓ Compose a target list of addresses to focus on
- ✓ Map targets to their entry nodes
- ✓ Match transactions to the targets' entry nodes

Investigations:-

Network analysis is the study of the Bitcoin peer-to-peer network. Much of the research to date has been focused on the goal of testing or improving Bitcoin user privacy, and CoinSeer was developed as a custom Bitcoin client to perform data collection for network analysis.

Methodology 1:- Peer-to-peer network analysis has met with some success in linking transactions to IP addresses, but requires a long-term, live connection to the Bitcoin network, or the results of a previous connection from software such as CoinSeer. Early research showed that opening a connection to all public peers on the network simultaneously allowed mapping of IP addresses to Bitcoin addresses based on the assumption that “the first node to inform you of a transaction is the source of it. . . [this is] more or less true, and absolutely over time" . At that point, even if 50,000 connections were required, it could be done in Python, with the bonus that this allowed an acceleration of one’s own transactions, as they could be pushed to everyone at once Currently, there are less than 7,000 nodes, suggesting that this approach is feasible. Various meta-data such as timestamp, sender IP and port, were stored in binary files and passed to the second component, the Parser, which deconstructed the files and put them into comma separated files for loading into the database He third component of CoinSeer was analysis, which allowed for data summary, transformation and visualization. Transactional analysis offers the advantage of not requiring a live connection to the Bitcoin network, and instead is retrospective in nature as it uses a collection of the blockchain, and analysis with tools such as BitIodine. Transactions can be manually reviewed on websites such as Blockchain.info or WalletExplorer.com. Integration of off-network information, such as publicly available information, and voluntary disclosures of bitcoin addresses from sources like forums and Twitter, allows even more mapping of Bitcoin addresses to identity information.

The passive, retroactive techniques used to identify users based on Bitcoin web payments leverage online tracking through both leaks and intentional dissemination to third-parties. His information would have to be compelled from the trackers and third parties for analysis. Online trackers have visibility into sensitive details of payment flows, including items' prices and identities, and this can provide sufficient information to uniquely link the transaction to the blockchain. Another form of transactional analysis is active analysis, where the investigator actively participates in the network, through deploying and tracking identified 'marked' bitcoins through transactions to discover addresses, possibly in collaboration with other users, or by operating a mixing service. BitIodine was designed as a collection of modules to parse, cluster, classify and visualize Bitcoin transactions and was successfully used to identify a likely cold storage Silk road (an infamous black market in the deep web) wallet with over 111,114 BTC, and quantify ransoms paid for CryptoLocker releases totaling 375.93 BTC .

#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$11,382,240,050	$712.76	15,969,336 BTC	$67,288,200	-1.60%	
2	Ethereum	$904,848,975	$10.54	85,831,133 ETH	$4,069,260	-1.21%	
3	Ripple	$290,446,848	$0.008121	35,765,131,899 XRP *	$2,386,420	0.26%	
4	Litecoin	$184,904,214	$3.82	48,378,029 LTC	$2,258,970	-1.05%	
5	Monero	$83,466,495	$6.27	13,311,446 XMR	$3,134,490	5.38%	
6	Ethereum Classic	$80,817,441	$0.942637	85,735,486 ETC	$603,573	2.21%	
7	Dash	$66,519,213	$9.68	6,874,532 DASH	$596,632	-0.77%	
8	Augur	$52,038,360	$4.73	11,000,000 REP *	$396,072	6.38%	
9	NEM	$37,322,550	$0.004147	8,999,999,999 XEM *	$86,817	4.40%	
10	Waves	$35,727,500	$0.357275	100,000,000 WAVES *	$133,650	-3.94%	

Fig 7.0:- Image of the graph of various cryptocurrencies

Wallet Analysis:- The Bitcoin wallet is where private keys are stored, and allows the user to conveniently conduct Bitcoin transactions. Wallets automate the mechanics of sending and receiving bitcoins and are referred to as a 'client' when they actively participate in the network.There are many different forms of wallets, all of which are designated as hot (connected to the internet) or cold (offline). Cold wallets are obviously more secure, and are used for long-term holdings, while hot wallets are for regular use. Wallets can be desktop, mobile, web, physical, hardware, or Bitcoin clients. Web-based wallets avoid the need to download the entire blockchain, but, depending on where the private keys are stored, the user may be trading convenience for security

Methodology 2 :- Complete wallet analysis of the original Bitcoin client does not require having possession of the wallet's (optional) passphrase to perform its decryption; passwords are only required to initiate transactions, as using a passphrase encrypts just the private keys . Many artefacts, regardless of wallet encryption, can be recovered using forensic tools, such as the python script BTCscan and Magnet Forensics' IEF or Axiom products . The use of Magnet Forensics' IEF or Axiom products allows an investigator to recover addresses associated with the wallet, the 'labels' or comments that the user may have added for convenience (both from the wallet.dat file), and queries on the Bitcoin network (from debug.log) which may or may not relate to local user activity . Here may also be backup wallet files, which can be named anything, but at least in the case of the common Bitcoin-Qt (now Bitcoin Core) client, offset 0x12 contains the string 'b1'.

CHAPTER V

RESULTS AND CONCLUSION

RESULT:

The chart below shows the Bitcoin-Qt wallet artifacts recovered during the hard drive analysis.

Evidentiary Artifact	Location Of Artifact
Bitcoin-Qt program	C:\Users\XXXX\AppData\Roaming\Bitcoin
“blocks” subfolder	C:\Users\XXXX\AppData\Roaming\Bitcoin
“chainstate” subfolder	C:\Users\XXXX\AppData\Roaming\Bitcoin
“index” subfolder	C:\Users\XXXX\AppData\Roaming\Bitcoin\blocks
wallet.dat	C:\Users\XXXX\AppData\Roaming\Bitcoin
debug.log	C:\Users\XXXX\AppData\Roaming\Bitcoin

TABLE 1:- Location of artifacts recovered from Bitcoin-Qt wallet

The chart below shows the Multibit wallet artifacts recovered during the hard drive analysis.

Evidentiary Artifact	Location Of Artifact
Multibit program	C:\Users\XXXX\AppData\Roaming\Multibit
Multibit wallet(multibit.wallet)	C:\Users\XXXX\AppData\Roaming\Multibit
multibit-20200222190122.wallet (Rolling backup)	C:\Users\XXXX\AppData\Roaming\Multibit
multibit-20200132111104.wallet	C:\Users\XXXX\AppData\Roaming\Multibit\wallet-unenc-backup
multibit-20200132111104.info	C:\Users\XXXX\AppData\Roaming\Multibit\wallet-unenc-backup

TABLE 2:- Location of artifacts recovered from Multibit wallet

CONCLUSION:

It is seemingly impossible to permanently get rid of this disadvantage. Even if someone were to take the most extreme stance on the topic imaginable and advocate for the total international ban of bitcoin a replacement alternative would inevitably emerge in a matter of days (or possibly even hours). Instead of banning cryptocurrencies outright, it would be much more rational to try to adapt around the existence of current systems[8]. Fortunately, it seems there are at least some things that can be done in order to decrease the use of bitcoin as a medium of illegal exchanges without destroying the cryptocurrency market as a whole.

- ✓ Increase communications between various governments in order to make it easier to detect certain patterns.
- ✓ Increase annual reporting standards from the companies that use bitcoin as a legitimate purpose (Expedia, Microsoft, Subway, etc.)
- ✓ Develop software that can effectively detect when the public ledger is exhibiting any irregularities (and subsidize or offer tax credits for these efforts if necessary)
- ✓ Shift the focus away from digital methods of payment and towards the original, tangible production of illegal goods (drugs, weapons, etc.)
- ✓ Maintain the decentralized nature of bitcoin while simultaneously creating a centralized medium for self-regulation.
- ✓ Offer benefits (such as financial rewards) to cryptocurrency users that are able to effectively identify various threats.

Unfortunately, there is no clear path forward that will immediately resolve all of the issues associated with bitcoin and other cryptocurrencies[10]. The fact that bitcoin is frequently used as the primary medium of exchange for criminal enterprises around the world certainly gives the public a legitimate reason to be concerned. But with a concentrated effort that focuses on deterring criminal activity – rather than the simple use of an alternative currency it seems that progress can certainly be made in an objectively positive direction.

CHAPTER VI

REFERENCES:

1. https://www.investopedia.com/terms/b/bitcoin.asp
2. https://bitcoin.org/bitcoin.pdf
3. https://bitcoinwhoswho.com/blog/scholarly-works/
4. https://bitcoinwhoswho.com/blog/2020/01/17/have-you-received-a-threatening-email-asking-for-bitcoin/#more-1760
5. https://www.forbes.com/sites/jasonbloomberg/2017/12/28/using-bitcoin-or-other-cryptocurrency-to-commit-crimes-law-enforcement-is-onto-you/#566275a3bdc4
6. https://blockgeeks.com/guides/what-is-cryptocurrency/
7. https://nxtforum.org/technical-development-applications/wallet-dat-file/
8. https://arxiv.org/pdf/1801.07501.pdf
9. https://scholar.google.co.in/scholar?q=bitcoin+investigation+journal&hl=en&as_sdt=0&as_vis=1&oi=scholart
10. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8058429