A critical review of Bitcoins usage by cybercriminals

Jithin Jose, Krishnan Kannoorpatti
School of Engineering & IT, Charles Darwin University
Darwin NT 0909 Australia
Jithinjose009@gmail.com,
krishnan.kannoorpatti@cdu.edu.au

Bharanidharan Shanmugam , Sami Azam,
Kheng Cher Yeo
School of Engineering & IT, Charles Darwin University
Darwin NT 0909 Australia
bharanidharan.shanmugam, sami.azam,
charles.yeo@cdu.edu.au

Abstract— **Bitcoin is a new form of global digital currency based on peer-to-peer network, enabling a new payment system, and also a completely decentralised cryptocurrency. The P2P network consists of a digital file listing transactions like a ledger, a copy of which is also maintained on every computer on the network, and the transactions are also broadcasted in the public ledger of the Bitcoin network. Anonymity is the core feature that makes Bitcoin popular among people around the world. This feature is attained through the Bitcoin addresses in the public ledger, which represents the users in the Bitcoin network. Because of the illicit use of Bitcoins, the level of anonymity has reduced even though the users are still using the anonymizers like TOR to keep the anonymity stronger to connect to the Bitcoin network. In this paper, we analyse the complete process of transaction of Bitcoins and the anonymity thatlies in that process. The study also focuses on finding the forensic artefacts and the investigative way of approach towards the Bitcoin using forensic tools. The forensic tools are used to analyse the web browser activities, local drive, hard disk image, cookies, downloads and session data related to Bitcoins. The attacker can relate the transaction of the users and can control the Bitcoin blocks by even delaying the transactions. This research will focus on the methods in which the memory and even mobile devices involved in the transaction could be captured and analysed.**

Keywords- Bitcoin, Block Chain, Cybercrime, Anonymity research

I. INTRODUCTION

Bitcoin is the latest technological form of digital virtual currency which is based on cryptography and is a decentralized currency that is used in the recent generation of global money system. The pseudo-anonymous exchanging of cash over the web became common and possible by the invention of these cryptocurrencies [1,16]. Anonymity is an important factor that keeps the bitcoin more live and interesting even after years. The Bitcoins can be used without linking any kind of real world identity to it, which makes it different from the normal online currency. It's tough to tell who owns it unless linked with owner's name to the Bitcoin address. Bitcoin does not monitor clients; it monitors addresses where the cash is and keeps a public ledger for all the processed transactions [2]. Advanced coinage, for example, the dollar and the euro are controlled by governments and monetary variables which decide their quality and their operation. This virtual cryptocurrency was introduced back in the year 2008 and released the software in 2009 by Satoshi Nakamoto [16]. The basic idea of the system is peer-to-peer, where the transaction is done directly without a middle person. The transactions are confirmed by network nodes which is stored in a public ledger. This public distributed ledger is called the block chain and uses bitcoin as the unit. The mining of Bitcoins is an activity in which the coins are made as a reward for transaction handling process [3]. Here the users offer their computing energy to confirm and record the payments.

The network works without a centralized control which specifies Bitcoin as a decentralized virtual currency and often called as the first cryptocurrency. The user or clients utilizing the Bitcoin framework are required to utilize a worldwide database called the block chain [4]. It records all the transactions that have happened in the network and also keeps track of the new coins generated in the system. So the block chain can monitor who has the amount of cash at all times. New bitcoins are brought into the framework by the miners, who produce blocks that incorporate exchanges made by the customers in the network. The procedure of minting bitcoins is finished by comprehending a proof-of-work challenge that normally takes around five to ten minutes. Apart from being acquired by mining, bitcoins can be traded for other currencies, items and services. When sending bitcoins, clients can pay a discretionary exchange expense to the miners. The receiving of Bitcoins is free from any places. Till the beginning of 2015, the dealers accepting bitcoins have crossed over 100,000. Bitcoin has drawn the backing of a couple of legislators, prominently U.S. Representative Rand Paul. He is one of the famous personalities who acknowledge donations in bitcoin.

Black markets are also fully focused on the bitcoin transactions that exchanges for drug trades on deep web drug markets. Bitcoin is offered for murder-for-contract services and buying weapons, which are purportedly accessible on black market sites[5]. Because of the mysterious nature and the absence of central control on this black market business, it is difficult to know whether the administrations are genuine or simply attempting to rob the coins. Silk road is one among the several deep web black markets that have been shut down by the US Law enforcement, and in 2015, the founder of the website was sent to prison for life. Bitcoin may be used for

978-1-4673-8855-9/17/$31.00 ©2017 IEEE

money laundering which is another concern put forth by the agencies like European Banking Authority, the Federal Bureau of Investigation, etc.

In this research, we analyse the complete process of transaction of Bitcoins and the analysis of anonymity lies in the process. The study also focuses on the forensic artifacts and the investigative way of approach towards Bitcoin. Finally, the involvement of TOR network and its role in the illegal activities of this cryptocurrency and the methods followed by the criminals using TOR for illicit purposes. The purpose of this research is to analyse how virtual cryptocurrencies like Bitcoins are used in criminal activities and the reason behind the popularity of Bitcoins in these illicit activities. This is a new source of money which can be stolen and transferrable to any part of the world. This research analyses the Bitcoin network and the criminal activities associated with it. The possibility of finding evidences to track the activities done in different devices.

II. LITERATURE REVIEW

A. TRANSACTION BLOCKS

Whenever an exchange has been started in the bitcoin network, it must be checked by customers in the Bitcoin system altogether for the exchange to be completely dedicated and processed [7]. The miners accumulate the exchanges into a block once the transactions are conveyed to the Bitcoin system. The normal size of every block changes massively with a size of about 300 to 800 exchanges for each block which was by the beginning of the year 2015. But the average size was roughly from 200 to 400 only just one-year prior in Jan 2014, which shows that the size is increasing over the time. The span of these blocks ranges from around 150KB to 450KB. And in the bitcoin network, this is making an aggregate size of 33GB for the whole block chain.

B. NETWORK STRUCTURE

The Bitcoin network structure described by Satoshi Nakamoto [16] is as follows:

- Exchanges and transactions are telecasted to all system nodes.
- Exchanges are gathered and joined to shape and create a block structure.
- Always when a proof of work is discovered for a block it is relayed to all nodes in the bitcoin network.
- There is a high chance that all exchanges in a block are legitimate in the network system and bitcoins included have not as of now been spent, then the block is acknowledged.
- The acknowledged block is annexed to the transaction block chain, and its hash is presently utilized as the information for the input hash for the following block.

As such, all nodes in the network system are made mindful of new exchanges and transactions, confirmed exchanges and acknowledged blocks. Along these lines the exchange record or public ledger (block chain) is shared among all nodes in the bitcoin network system.

C. MINING PROCESS IN BITCOIN NETWORK

The data about the Bitcoin transactions or exchanges is for all time put away and stored in blocks. These blocks are assembled in a period successive sequential record or ledger called block chain, which is openly accessible to the users in the bitcoin network [7]. Every block contains an enchantment number (4 bytes), the block size (4 bytes), the block header (6 bytes), an exchange or transaction counter (from 1 to 9 bytes) and a non-vacant rundown list of exchanges [16]. The block header contains the variant of the block, the 256-bit hash of the past block header and the 256-bit hash of the Merkle base of the exchanges in the block. The procedure of making another block is called mining. And it is an asset or a resource serious calculation or computation otherwise called verification proof-of-work. This procedure of mining infers the creation (mint) of new Bitcoins that are created as a consequence of this block generation process. There is a fixed reward for the miner for each solved transaction block. The proof of work in the Bitcoin framework comprises of processing the hash SHA-256 of the block's header until the outcome is not exactly a particular target. The length of this target is 256 bits and it is solved in a manner that the normal time that it takes to find a solution for this puzzle could be around 10-15 minutes. It is specifically identified with the aggregate mining power of the network system (the more miners, the greater the difficulty). The target is upgraded each 2016 transaction blocks (around 2 weeks) for reasons of soundness (stability) and low dormancy. And the lower the target, the more the difficulty would be faced in the bitcoin network system.

Mining is an incentive based movement in light of the fact that there is a reward or prize related to it. The primary miner to get his block acknowledged by the network system gets an altered sum in addition to the aggregate of the charges of each transaction of that block. The fixed sum began to be 50 BTC and it parts each 210,000 blocks [16]. In this way, when the estimation of 210,000 blocks was gone after first time (on November 28, 2012), the prize split and at the present, it is 25 BTC. The following halve (when block 420,000 is come to) is required to happen around 2017 and the 34th split is anticipated to happen in 2140. By then, this fixed income will get to be 0 and that will be the end of the presence of new coins. At that point, the main prize will be the expenses of the exchanges [20].

III. IMPROVING ANONYMITY

To determine the anonymity issues present in the Bitcoin protocol there have been numerous endeavours to discover it. Some of these endeavours have emerged naturally inside the Bitcoin people group and are now being used. While others are proposed by research papers what's more, have yet to be actualized.

A. Mixer

An extremely normal type of clouding one's identity is to utilize a mixer or tumbler. These administrations depend on blend and mix network systems, which are utilized to cover a client's identity inside a network system. The very best example is the generally utilized TOR network system. Not at all like mix network systems which are utilized to blend or mix messages and anonymize the clients [14]. Bitcoin mix administrations mix exchanges (transactions) to anonymize the clients, every now and again charging some kind of a handling processing charge which is a fee expense for the service. The three famous mixing services investigated by Malte Moser in 2013 are: Blockchain.info, Bitcoin Fog, and BitLaundry. The key artifacts of this analysis were that Blockchain.info and Bitcoin Fog both utilized complex techniques for appropriate distribution of both exchanges and transactions [7]. And which dispose of the capacity to find any connection amongst input and output exchanges, viably anonymizing the activity in the network traffic. Then again, BitLaundry utilized direction connections amongst input and output which takes into account connections with be drawn over the mixing operations [15].

B. TOR

Tor is the most prominent low latency network system which provides anonymity. Onion routing and telescoping path-building plan are the basis of the Tor network system which is built on. A user picks the way comprising of three Tor relays at the point when he needs to connect with an Internet server while keeping his IP address in private from the server. The 3 Tor relays are Guard, Middle and Exit [8]. And these relays form a circuit and arranges symmetric key with each one of them utilizing the telescoping system. The client encrypts the message utilizing the arranged negotiated keys before conveying a message on the server. Every relay peels off its layer of encryption while the message goes along the circuit. Along these lines the message arrives finally at the last destination in its unique structure and form. And every party knows just the past and the following hop [9].

Tor tries the best to accomplish low traffic latency to give a great and better customer experience. TOR transfers don't postpone or delay approaching messages and don't use padding to keep inactivity low and system throughput high. The traffic confirmation attacks are more susceptible to Tor network and this makes Tor helpless. When a hacker can sniff both the ends of the network communication, he can affirm that a client interface with the server [9]. In the event that the initial hop of a circuit is picked randomly then the likelihood that a pernicious (malicious) node will be picked as the primary hop (and therefore will know the IP location of the client) converges to one with the number of circuits. An arrangement of three Guard nodes is there because of this, for every client. The primary hop is browsed from the arrangement of trusted Guard nodes at the point when a client makes a circuit [9].

IV. EXAMINING THE FORENSIC ARTIFACTS

Because bitcoin cryptography has become such a moderately new technology, there are no effective studies yet conducted, which are committed to understand what kind of artifacts are generated in a user's system, how those artifacts intend to perform and moreover on how the system can recuperate to conduct an investigation into the Bitcoin use. Nevertheless, the memory analysis technique will help in finding out the artifacts and to regain them. In order to execute the transaction through Bitcoin, firstly, the user must install a digital wallet. Then, the processing of currency is done through this wallet which is authenticated by the nodes and records of the block chain. According to the author [10], this case study uses memory and hard drive as forensic strategies with distinguish artifacts which are generated as a result of different Bitcoin wallets so as to be an aid for future investigations directed towards Bitcoin currency. The study also discusses the necessity of the knowledge about Bitcoin transaction networks in order to know how to fetch data from user's device.

Justification of The Importance of Bitcoin Artifacts

Bitcoin might have been not outlined to be anonymous, it might have been intended to hold a secondary degree security for its user's. As expressed by the maker himself, "The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone" [16], Bitcoin transactions data are recorded in block chain which are publically accessible. So that the Bitcoin need been portrayed as pseudo unacknowledged. Bitcoin does not demand the user's identity including their IP address and there is no central authority to monitoring those transactions. As stated by a 2013 article on the website www.Economist.com, Bitcoin has largely expanded. The rate of Bitcoin might have been worth $824.76999USD as stated by the website www.Bitcoinexchagerate.org in January 19, 2014. Bitcoin satisfies it users with certain criteria such as money as an asset, easy exchange and value. As a result of this provision, the demand of Bitcoin increased rapidly. This demand for the use of Bitcoin has attracted cyber criminals.

The criminals target over Bitcoin has sought the attention of fiscal regulators, authoritative bodies and media. The FBI published a vigilance alert to those who are using the financial schemes utilizing virtual currency [21] . There have been various instances of Bitcoin robbery. An outsider can gain entrance to the private virtual machine through the victimized person's Bitcoin address by claiming the latter's web wallet. Even though the private facts may have been stolen, every last

one of Bitcoins which form the compromised account has a chance to be exchanged. In such cases, there is no way to track the unauthorized person and retrieve the Bitcoin back to the owner [19]. The FBI assesses for the medium which certainly helps cyber criminals to use Bitcoin and furthermore create virtual currencies which they have little reason to relinquish.

This appraisal is based on variances in the Bitcoin conversion scale as of 2011, furthermore, restricted reporting weight demonstrating that Bitcoins would be taken up by some cyber criminals as the mode of payments [21]. Whether the conversion scale of Bitcoins stabilizes or not, Bitcoin gets a greater amount which is broadly acknowledged. This eventually pursues vendors, including illegal dealers who use the internet and other digital criminals to progressively utilize Bitcoins to buy illicit products. The research over Bitcoin mining malware shows that the computing power of the devices which are used for the Bitcoin mining process becomes affected. The hackers are able to access the wallet as well, therefore the banks are also not safe [17]. The reason behind the popularity of Bitcoin among criminals is that the payment procedure does not need a bank tie up.

The privacy provided by Bitcoin allowed its users to open a website anonymously. Mainly those are for the illegal substances promotion. The key factor behind this privacy is that the illegal contents are invisible to the ordinary users [21]. Such websites are called black market websites and those are visible for some privacy networks designed by Bitcoin networks. A standout amongst those well-known black market sites was the silk road marketplace, which needed an assessed offers income of $1. 2 billion USD for 1,229,465 transactions between February 6, 2011 and July 23, 2013 [21]. The main three products sold out in the black market by the silk road marketplace were weed, drugs and prescriptions. The silk road marketplace was shut down on October 1,2013 by the FBI, but they started another website with same motive named silk road 2.0 in black market. The investigation directing more over Bitcoin should expect by the forensic examiners, assuming that the virtual currency proceeds to get publicity for cyber criminals.

The increasing use of Bitcoin currency among criminals for illegal transactions demands an investigation to be conducted by the digital forensic community over the Bitcoin operation. The virtual currency provides privacy to the users as brand advertising for Bitcoin, it does not provide a complete privacy [11]. Because of the payment process, information is recorded in the block chain which is publically viewed and verified to making sure that all the transactions are done properly. And also in the case of wallet address, they give options to use more than a single address to let the wallet remain as anonymous. So the investigation about the Bitcoin artifacts is necessary to provide a backing for a criminal examination [20].

A. LIMITATIONS OF EXISTING KNOWLEDGE

There requires to be a former examination in Bitcoin network which will figure out whether the currency is virtual or not and finding out if there are any targeted users for the Bitcoin transaction. If tracking of the suspects of illicit transaction is possible, then the authorities will get the power to handle them [19]. The Bitcoin exchanges handle a large money, that is, billions of dollars of transactions. So, if they co-operate with the authorities, there is no need to shut down Bitcoin. There is a strategy to recognize the users who participate in illegal transactions. If a third party administration wants to be a part of an illegal transaction, they must register in the financial crimes enforcement network. But the gadgets information is always in the user's custody. If it is possible to get all the information about Bitcoin's illegal transactions and the users' device address, a complete study [12] over the gadgets is required to finding out whether there are any changes in wallets. The existing information about the Bitcoin wallets from its site is only the device compatibility that either mobile or system. The measurable strategies necessary with catch artifacts from a wed Bitcoin wallet, the place a user might sign-in with the username and password, might well on the way contrast from the individuals made with recuperate artifacts from a software Bitcoin wallet. This case study attempted to stand in between the recognizing of culprits and recouping the proof from their devices.

B. Intended Audience

According to the author, this case study might support the forensic examiners in an examination directed towards including the utilization of the Bitcoin with launder money, buy or sell illicit product or services, and backing the terrorist groups. This research helps to link a Bitcoin user with his or her address. The investigation about Bitcoin is very necessary because of the increasing popularity of Bitcoin and also because nowadays, Bitcoin is getting equal importance as currency which the researchers need to consider as a possibility for illicit transactions which is in the same way as the physical currencies. This research gives assistance to retrieve the digital evidence from the user's device and also to identifying the gadgets. Ultimately, this research provides support to the forensic examiners in finding out the Bitcoin artifacts from their affected devices such as mobiles and tablets.

V. METHODOLOGY

To find out the Bitcoin artifacts, it is necessary to examine the Bitcoin wallets in both the memory analysis method and the hard drive analysis method. While downloading the Bitcoin wallets to the devices, they install software which is either a web wallet that is found in the host or a mobile wallet that is found in smart phone devices. The location of the artifacts in these devices differs because of the difference in their operating systems [21,13]. Therefore, different tools and techniques are required to retrieve the artifacts from different affected devices. The purpose of this case study is to identify the evidence of illicit transaction that are in the device, extracted through Random Access Memory (RAM) analysis and hard disk analysis. RAM is the temporary storage area

used for processing the device's operations when the machine is on. Because of its volatility nature, when the power is tuned off RAM will lose the entire processing data. So, if there is any evidence expected from RAM, it should be retrieved before the power of the system goes off. RAM can be captured through two different acquisitions. These are hard-ware based and soft-ware based. Trusted tool is used for the soft-ware based acquisition [6]. When capturing RAM is completed, the string based analysis of RAM takes place because of its volatile nature. The forensic examination of hard disk includes six steps, and these are identification, preservation, collection, examination, analysis and presentation. There are several different tools available to analyse the hard disk as well as to collect the evidence from the device.

A. TARGET OPERATING SYSTEM

This analysis is done over a Windows8 Virtual Machine (VM). The forensic examiner experienced a Device Running Windows throughout the examination because of the popularity of the Microsoft Windows working frameworks. The Bitcoin wallets are supported by different Operating Systems (OS) including Windows, Mac and Linux. So, the examiner has to detect the evidence from all the OS. But it is unknown that whether there is any difference in the evidence collected over the Bitcoin transaction if the devices' OS are different. So that an extra analysis might be needed in future to explore further details.

B. BITCOIN WALLETS

After choosing the operating system, the Bitcoin wallets might have been selected to proceed the transaction process. In this case study, a web based Bitcoin wallet is examined. The transaction become easier by the use of Multi Bit wallet that are supported by both the Windows and Linux operating system [6,22]. For differentiating the two addresses during the investigation, a third Bitcoin wallet [Fig 1] was created. This analysis also examines the wallet stored in a removable hard disk. The wallet stored in the removable hard disk gives extra security than the Bitcoin wallets stored in the machine.

C. ACQUIRING BITCOINS

For acquiring Bitcoins [10] there are several ways, such as, purchasing the Bitcoin, reward them for somebody known, receiving Bitcoin as substitute to currency in sale and service or alternately acquire them through Bitcoin mining. In this case study, the website www.getcoincafe.com is used to buy, sell and use the Bitcoins. The website gives an option for new users to start free account using email address and allows exchanging original currency into Bitcoins by calculating with the current Bitcoin value. The current value of one Bitcoin as on May 26, 2016, was $455.39 USD [22]. Then the Bitcoin transferred to the account and the execution of Bitcoins transaction might initiate.

D. WINDOWS 7 PROFESSIONAL

1) Capturing RAM and creating an image

For RAM capturing, a page file device also used by the FTK lite because it contains the evidence that helps to research. The result was stored in the storage drive and it is in MD5 hash value format which compared with the previously obtained value.

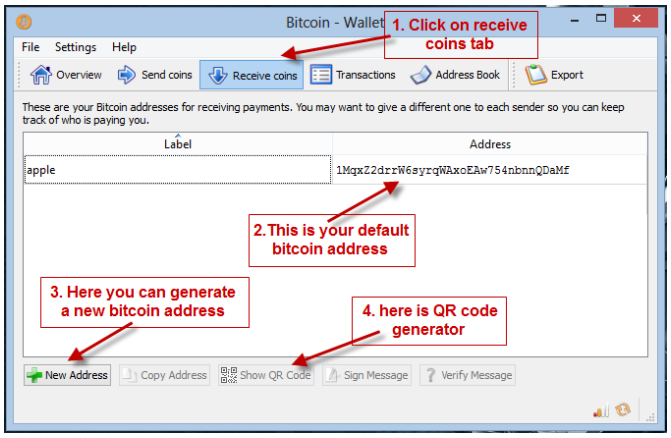

Fig 1: Bitcoin Wallet
http://bitcoinlister.com/wp-content/uploads/2014/05/Bitcoin-Address1.png

2) Creating USB Bitcoin wallet evidence

For Bitcoin transaction through the USB device, the Multi Bit wallets should have downloaded and installed in a new 8GB, SanDisk thumb drive which is also known as USB Bitcoin wallet. Also a Multi Bit folder downloaded to the USB and that folder is generated by the processing of Multi Bit transaction in Windows 7 virtual machine.

According to Jones analysis findings, through the RAM and hard drive analysis, we can retrieve some important Bitcoin artifacts. Those analysis gives information more than the Bitcoin location on a device including recuperate proof of particular transaction's amount, time, date, included parties, IP address relaying those payments, what's more transaction distinguish. There were lot of research conducted over Bitcoin artifacts to recover them by means of memory analysis, but this analysis given the essential data should search out so as with finish the objective. Using the Internet Evidence Finder(IEF), the analysis of RAM and hard disk of the affected device become successful to retrieve the Bitcoin artifacts.

3) Memeory analysis

To analysing the unstructured format of the captured RAM of the affected device, the character string searches are important using the tool FTK. During the examination, the contents of the files used for research also copied to the tool as an evidence. The forensic analysts are able to identify the thing that shows up to be an irregular string of characters

concerning the transaction information by a hit looking into a particular Bitcoin address shown possibly evidence, if the examiner have knowledge about the inner working of Bitcoin transactions. The result shows some web addresses and these are insufficient to track the IP address [23]. So further investigation takes place and gets detailed processing information with IP address, value, date, time and the Bitcoin address including hash. So it is necessary to examine the artifacts before the deletion or over writing is done in the RAM.

4) Hard Disk Drive analysis

During the hard disk analysis using FTK tool, there may find lots of files and folders in the Multi Bit folder including the wallet, log and data files. The wallet file is the actual storage area of the Bitcoin. But, if the examiner need to know about the content, he should know the password to enter into the Bitcoin wallet to transact the Bitcoin from it. Viewing the contents from the wallet file using hex format shows a random characters a random character as result. Which means the contents of the file is encrypted for the secret [6]. Then look at the file in hexadecimal format allows the examiner to show the files in the form of lowest level bytes and bits.

5) Impact of using Bitcoin wallet on a removable drive

If a Multi Bit Bitcoin wallet uses from a removable disk to proceed the Bitcoin transaction, the forensic examiner can track the evidence through the RAM analysis. The result of RAM analysis gives an opening to the hard disk analysis and through the hard disk analysis there detect an area E used by the removable disk while connected to the machine. The E drive space contain a folder gives the wallet information only, doesn't contain the transaction details [24]. But further examining over the log file gives the transaction information including the removable hard drive data. Then through the event logs investigation will get the user name and SID of the log-on account and also the serial number of the removable hard disk that connected to the machine.

VI. EXPERIMENTAL RESULTS

This section describes the experiments conducted using two tools Magnet Axiom and Belkasoft Evidence Centre. It is easy and anonymous to conduct the transactions. Support and extra functionality for recovering Bitcoin evidences was added into Internet Evidence Finder (IEF). Wallet addresses can be traced and recovered, and queries on the Bitcoin network from log files created by the client software. The figure 2 shows addresses from a bitcoin wallet. This includes labels and the activity of the address. If a person creates a wallet, a number of addresses are automatically created. Then these addresses are put in the "thread pool". Bitcoin is a tough cryptocurrency to track or investigate. But still identifying which addresses were there in a suspect's or victim's or criminal's Bitcoin wallet and then the details about the transfer of bitcoins would help you piece the puzzle back together.

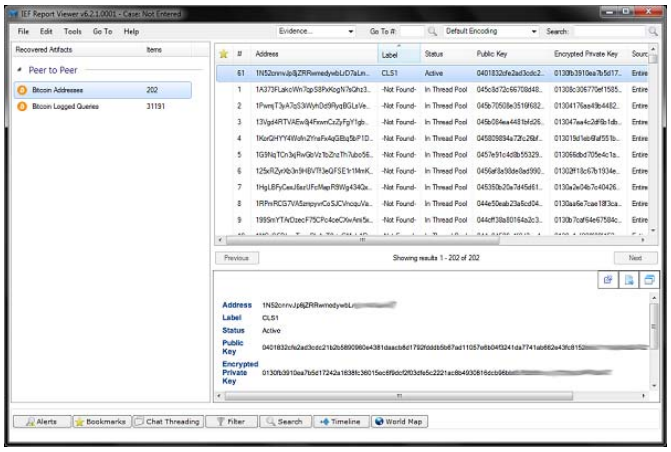

Fig 2: Details of Evidence from IEF tool

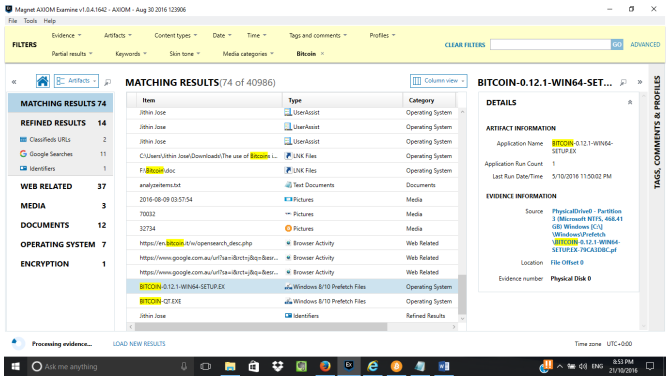

Fig 3: Laptop evidence

The above figure 3 shows the evidence acquired from the laptop analysed, shown in the Magnet Axiom Examine for the Bitcoin wallet. These are the artifacts shown about the Bitcoin offline wallet that is installed in the system. This contains the encrypted and the OS category files which are analysed to get the results.

The figure 4 shows the evidence acquired from the laptop analysed, shown in the Belkasoft evidence centre for the bitcoins. These are the web related session store artifacts found from the web browsers. In the artifacts list it shows a website link https://blockchain.info/wallet/#/login which is the website used in logging to the online bitcoin wallet to access the bitcoins in it. There are a few session details which shows that multiple login attempts are done to this website and from different web browsers at different dates and times. The dates, times and sites visited are tracked by history and cookies and the data of real evidentiary value is found in the cache.

The artifacts found are given below:

The artifacts are found from:
Internet Explorer 10 –
%root%/Users/%userprofile%/AppData/Local/Microsoft/Windows/History
Mozilla Firefox –
%root%/Users/%userprofile%/AppData/Local/Mozilla/Firefox/Profiles/*.default/Cache
Google Chrome –
%root%/Users/%userprofile%/AppData/Local/Google/Chrome/User Data/Default/Cache

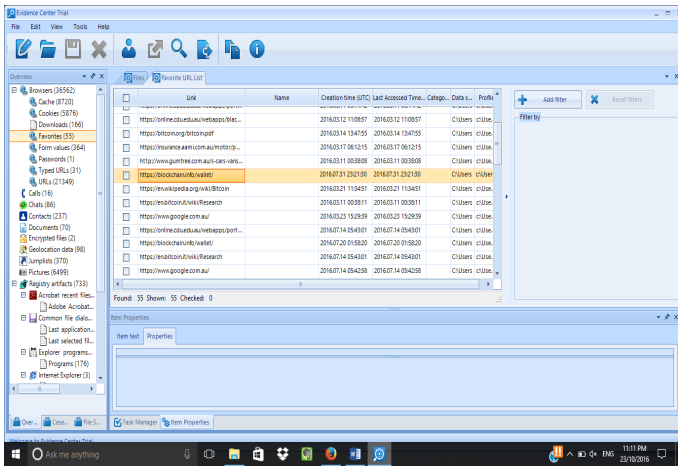

Fig 4 Laptop evidence (Belkasoft)

VII. CONCLUSION AND FUTURE WORK

The goal of this research was to analyse the bitcoin cryptocurrency from the initial stages of invention till the use of the coins in criminal activities. It gives an idea of how the network works along with the associated mining processes. It can conclude that all the illegal transactions happen through the bitcoin wallets and all the transactions are published in the public ledger. The wallet id of the illegal transactions can be matched in the public ledger, and tracing the owner of the wallet can find out the person behind the criminal activities. But still there are lots of attacks happening and possible through the Tor network which is discussed above. So, it concludes that the use of Tor network will not give complete anonymity and safety for the bitcoin users. The artifacts found from the analysis done using the forensic tools show that the evidences are lying on the suspected laptop and can be extracted. Creating an online and offline wallet and carrying out the bitcoin transactions are the better ways to generate some evidences in the machine. Normal bitcoin users do not realize that they are automatically creating the evidences for their bitcoin transactions. Even the evidences could be found from the normal queries about bitcoins and the exchange platforms on the internet using web browsers. This forensic research shows that the evidences can be extracted from a suspected machine using the forensic tools.

REFERENCES

[1] A. Biryukov and I. Pustogarov, "Bitcoin over Tor isn't a Good Idea," in *2015 IEEE Symposium on Security and Privacy*., San Jose., 37th.CA, 2015, pp. 122-134. doi:10.1109/SP.2015.15.

[2] A. Biryukov, D. Khovratovich and I. Pustogarov. (2014, Jun 3). *Deanonymisation of clients in Bitcoin P2P network (2nd ed.)* [Online]. Available: http://arxiv.org/pdf/1405.7418v2.pdf.

[3] Bitcoin Wiki. (2015). *Bitcoin*. [Online]. Available: https://en.wikipedia.org/wiki/Bitcoin#cite_note-Lavin.2C_Tim-36.

[4] C. Decker and R. Wattenhofer, "Information Propagation in the Bitcoin Network," in *Thirteenth IEEE International Conference on Peer-to-Peer Computing*., 13th. Povo Trento, 2013 ©2013 IEEE. doi:10.1109/P2P.2013.6688704.

[5] E. Z. Yang (2012, Jul). *Secure multiparty Bitcoin anonymization* [Online]. Available blog: http://blog.ezyang.com/2012/07/secure-multiparty-bitcoin-anonymization/.

[6] F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," Humboldt Univ. Berlin, Survey Rep, 2015.

[7] G. O. Karame, E. Androulaki and S. Capkun, "Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin," in *Proceedings of Conference on Computer and Communication Security*., Raleigh., NC, Oct 2012.

[8] L. D. Jones, "Examining the forensic artifacts produced by use of bitcoin currency," Utica College, Proj. Rep, May 2014.

[9] M. Möser (2013, Jul 17-18). *Anonymity of Bitcoin Transactions (1st ed.)* [Online]. Available: https://www.wi.uni-muenster.de/sites/default/files/public/department/itsecurity/mbc13/mbc13-moeser-paper.pdf.

[10] L. Morris, "Anonymity analysis of cryptocurrencies," M.S. thesis, Dept. of Comp. Sci., Rochester Inst. of Tech., NY, USA, Apr. 20 2015.

[11] B. A. Pamplin, "Virtual currencies and the implications for U.S. anti-money laundering regulations," Utica College, Proj. Rep, Aug 2014.

[12] M. K. Popuri, "Complex network analysis of crypto currencies," M.S. thesis, Dept. of Comp. Eng., Univ. of Nevada, Nevada, US., 2015.

[13] R. Pallas, "Bitcoin," M.S. thesis, Dept. of Comp. Sci., Tallinn Univ. of Tech., Tallinn, Estonia, Jun. 1 2012.

[14] S. Nakamoto (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System (1st ed.)* [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[15] E. S. Robla, "Analysis of reward strategy and transaction selection in bitcoin block generation," M.S. thesis, Dept. Elect. Eng., Univ. of Washington, Seattle, WA, 2015.

[16] L. Stuhlmiller, "Mitigating virtual money laundering: An analysis of virtual worlds and virtual currencies," Utica College, Proj. Rep, Apr 2013.

[17] C. Zhao, "Graph-based forensic investigation of bitcoin transactions," M.S. thesis, Dept. Comp. Eng., Iowa State Univ., Iowa, Ames, 2014.

[18] Forensic Focus – Articles (2016, Jan 16). *Forensics and Bitcoin | Forensic Focus* [Online] Available articles: https://articles.forensicfocus.com/2015/01/16/forensics-bitcoin/.

[19] Securing your wallet - Bitcoin. (2016). *Bitcoin.* [Online]. Available: https://bitcoin.org/en/secure-your-wallet.

[20] Buy & Sell Bitcoins | CoinCafe.com. (2016). *Coin Café.* [Online]. Available: https://coincafe.com.

[21] P. Miller, "analysis of cryptocurrency Desktop Wallet Software," Marshall Univ., Internship Rep, 2014.

[22] K. Krombholz, A. Judmayer, M. Gusenbauer and E. Weippl, "The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy," SBA Res., Vienna, Austria, Rep., 2015.