A Forensic Look at Bitcoin Cryptocurrency

GIAC (GCFA) Gold Certification

Author: Michael Doran, doranmd@hotmail.com
Advisor: Richard Carbone

Accepted: October 21, 2015

Abstract

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. Since the creation of Bitcoin in 2008, cryptocurrencies have begun to make a presence in the world of ecommerce. Cryptography serves as the underlying foundation for Bitcoin, which gives it the benefits of confidentiality, integrity, non-repudiation and authentication. Having been designed and built upon the foundation of these four objectives makes Bitcoin an attractive alternative to mainstream currency and provides users with the benefits of payment freedom, security, very low fees, and fewer risks for merchants. Tools such as Internet Evidence Finder have the capability to recover some Bitcoin artifacts. However, because the cryptocurrency technology is relatively new, very little research has been dedicated to what other forensic artifacts are left on a user's system as a result of Bitcoin, what those artifacts mean and how to recover them in order to build a successful case involving Bitcoin. This research seeks to ascertain what forensic artifacts are recoverable from a user's system with Bitcoin wallet applications installed and actively used. Furthermore, 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.

1. Introduction

Since the creation of the Internet in 1969, there have been notable technological advances involving the Internet that not only drastically affect each aspect of a person's life, but also forever changes the way that a society functions (Strickland, 2007). Most of the modern day technological break-through such as e-mail and e-commerce as well as luxuries that individuals enjoy on a daily basis such as water, electric, and automobiles are directly or indirectly dependent upon the Internet (Naughton, 2010). Bitcoin cryptocurrency is one such technological break-through relying heavily on the Internet.

Due to the fact that Bitcoin cryptocurrency is such a relatively new technology, very little research has been dedicated to what specific forensic artifacts are left on a user's system as a result of Bitcoin, what those artifacts mean and how to recover them in order to investigate Bitcoin usage. This research seeks to provide a history of this cryptocurrency and through the use of a test environment, ascertain what specific artifacts are recoverable from a user's system with respect to Bitcoin installed and actively used wallet applications.

2. Bitcoin Historical Background

In 1958, President Dwight D. Eisenhower saw the deficiency in the technological development in the United States. Because of it, he created the Advanced Research Projects Agency (ARPA) as a way to put the United States ahead of other countries in the technological race, specifically in the area of computer science (Leiner, 2013). However, it was not until November of 1969, when the first host-to-host message was sent from Leonard Kleinrock's laboratory to the Stanford Research Institute over the ARPANET, the foundation of the modern day Internet was established (Strickland, 2007).

As the Internet developed from the foundation of ARPANET, so too did the technology breakthroughs, programs and benefits of the Internet. One such breakthrough was online banking, which began as an experiment in the early 1980s and finally made its debut on October 6, 1995 when Presidential Savings Bank first offered customers an online alternative to the traditional banking experience (Doyle, 2000). Online banking offered consumers four critical benefits over the brick and mortar banking experience:

convenience, no lines, availability and innovation (Smith, 2013). But despite those benefits, there was a downside to the banking industry. According to Satoshi Nakamoto, the creator of Bitcoin, the cost effects associated with the mediation of fraudulent transactions, combined with the rising costs of mediation, increases consumer transaction costs and ultimately limits the minimum transaction size (Nakamoto, 2008). Bitcoin was designed on an open source cryptographic protocol platform which enables each transaction between the users to be "computationally impractical" to reverse and would protect sellers from fraud (Nakamoto, 2008).

One of the unique qualities about Bitcoin is that Satoshi Nakamoto built it on a peer-to-peer format, which essentially means no central authority manages it. A P2P, or peer-to-peer network, consists of two or more computers that are connected and share resources without the use of a separate server (Cope, 2002). Thus in the case of Bitcoin, the P2P network is built in such a way that each user is broadcasting the transactions of other users and eliminates the need for a financial institution as a third party (Bitcoin Foundation, 2009). Because of this P2P network design, coupled with the way Bitcoin creates, operates, and distributes Bitcoins it is less susceptible to illegal money transfers, and manipulation with malware and botnets (FBI, 2012).

Initially, the network arrangement may seem troublesome. After all, when investigating a financial crime involving a bank, an investigator can obtain evidentiary artifacts by subpoenaing bank records, digital surveillance and for the most part, follow the flow of money when moved or spent. With the design of Bitcoin based on a P2P network format, the collection of evidentiary artifacts is limited because all of the transactions are stored on the Bitcoin network. However, because Bitcoin is pseudonymous and not anonymous, Bitcoins do not just disappear. Rather, each transaction is public knowledge and is visible to anyone using the Bitcoin network (Steadman, 2013).

Each transaction involving Bitcoin is identifiable within the user's Bitcoin "wallet" by a specific address characterized by a 34 alphanumeric character string. This character string is specific to a particular user's wallet and denotes specific transactions between various users (Shaw, 2013). In addition to the user's Bitcoin "wallet," the file entitled "debug.log" provides information regarding the communication to the Bitcoin P2P network as well as providing timestamps. Files entitled “db.log,” “peers.dat,” “blocks,” “chainstate,” and “database” in addition to nine more files, could potentially offer a wealth of evidence to a forensic examiner trying to build a case (Saliba, 2013).

An effective digital investigation requires a series of steps take place in order build a solid case. Those steps, according to the Digital Forensics Research Workshop (DFRWS) are Identification, Preparation, Approach Strategy, Preservation, Collection, Examination and Analysis (Reith, Carr and Gunsch, 2002). Each step has an important role in the grand scheme of the digital investigation. Depending on the particular expert, one step may be more important than the next. However, there is no denying the fact that a case is successfully prosecuted based on two key facts: the evidence recovered at the scene and the evidence extracted from the analysis of each piece of digital media. These evidentiary artifacts, whether a timestamp, an electronic document or e-mail provides a digital case with the solid foundation it needs in order to hold up in the eyes of the court. Based on this concept, to build a case involving Bitcoin it is imperative for the digital forensic community to become educated about Bitcoin. Specifically, forensic examiners should have a firm grasp of the various forensic tools and techniques used to analyze Bitcoin as well as what each evidentiary artifact recovered can ultimately provide to the overall scope of the case.

In the digital forensic community, there is a wealth of research documenting specific programs, operating and file systems, boot records, and the various evidentiary artifacts extracted and what they mean. Digital computer forensics is an ever-evolving field of study as technology and new products surface daily. In order to stay abreast of the changes, forensic examiners can either take training courses specifically devoted to those new items or they can read books or research “white papers” written by fellow experts in the field who have done extensive research and wish to report their findings back to the community. By exploring the inner workings of Bitcoin, how it functions as a cryptocurrency and the forensic artifacts that are available through a forensic analysis of a suspect’s machine, anyone charged with investigating, analyzing, prosecuting or defending a case involving Bitcoin could benefit from this information.

3. Bitcoin and its Role as a Cryptocurrency

Trust is paramount in the world of consumer finance, as the banking institution is the setting for financial transactions. In fact, a financial institution's reputation directly correlates to a consumer's overall opinion about its past behaviors. The bank's previous performance creates future expectations and a sense of security with a consumer, which in turn determines the degree of trust a consumer places in that particular bank (Edelman, 2013). With no trust between the consumer and the bank, the consumer is reluctant to conduct any business and limit their interactions with the bank. Banks have become an integral part of every economy since humans minted the first currencies.

Consumers have since become dependent upon banks for everyday transactions and avenues to save money (Beattie, 2011). Many banks have added or increased fees for online bill pay, online account transfers, transactions, coin deposits, and dozens of other services that used to be relatively cheap, or even free (Watson, 2011).

Due to increased fees, many consumers have found themselves utilizing other methods to circumvent the banking and financial industry. One popular alternative that consumers have begun to use is refillable debit cards, which resemble credit cards. However, they do not have an association with an actual bank account. Consumers buy the cards, deposit cash into them, and use them in much the same way that they would a credit card. Another option is the use of credit unions that have a similar model to banks, but where much of their profit goes back to members in the form of various benefits and cost reductions (Watson, 2011).

Even though consumers have begun to use refillable debit cards and credit unions in an effort to avoid contact with banks and the financial industry, those options still carry with them many of the same fees and aggravation commonly associated with banks (Watson, 2011). It was not until 2009 when the first cryptocurrency, Bitcoin, was created and provided consumers with a "virtual" form of exchangeable currency not subject to the various fees and aggravations associated with the financial industry. Gavin Andresen, the technical lead at Bitcoin, told Forbes.com that "cryptocurrency is an attempt to bring back a decentralized currency of the people, one that is not subject to inflationary moves by a central bank" (Janssen, 2009, Para. 3).

Cryptocurrency, by definition is a type of digital currency based on cryptography, or the process of converting plaintext into ciphertext, thus making readable text non-decipherable (Rouse, 2009). The use of cryptography in the transfer of data has four main objectives:

1) **Confidentiality** - the information cannot be understood by anyone for whom it was unintended to be (Rouse, 2009).

2) **Integrity** – ensuring the information sent remains unaltered (Rouse, 2009).

3) **Non-repudiation** - the sender of the information cannot deny that they sent the information at a later date and time (Rouse, 2009).

4) **Authentication** - the sender and receiver have the ability to confirm each other's identity and the origin and destination of the information (Rouse, 2009).

Realizing that the trust between consumers and the financial industry was rapidly decreasing due to the increased costs of mediations and basic transactions, Satoshi Nakamoto sought to provide a secure method of payment for consumers that would embody the four objectives of cryptography and enable them to feel more secure (Nakamoto, 2008). This new electronic payment system, called Bitcoin, would have transactions based on the Secure Hash Algorithm 256 (SHA256) cryptographic proof and built on the P2P network framework.

4. Bitcoin wallets and transactions

In order for a consumer to begin interacting and conducting transactions utilizing Bitcoin, he or she must first download and setup a Bitcoin wallet. A Bitcoin wallet can show the total balance of all Bitcoins it controls and let a user pay a specified amount to a specific person, just like a physical wallet (Bitcoin Foundation, 2009). Once the wallet is installed and configured, an address is generated which is similar to an e-mail or physical address, in that it provides other users a numerical location to send Bitcoins to. In addition, the wallet contains a user's private key, which allows for the spending of the Bitcoins, which are located in the block chain. The block chain is a shared public ledger or record on which the entire Bitcoin network relies. The block chain provides documentation for each of the confirmed transactions as well as providing Bitcoin wallets a way to calculate their spendable balance and a way for new Bitcoin transactions to be verified (Bitcoin Foundation, 2009).

With the Bitcoin wallet setup, a user needs to have Bitcoins in order to conduct transactions. To date, there are four methods to acquire Bitcoins: as payment for goods or services, purchase of coins through a Bitcoin exchange, exchanging them with another user or earn the coins through competitive mining (Bitcoin Foundation, 2009). The easiest method to obtain Bitcoins is to purchase them from an online vendor such as Cex.io. The current market value of one Bitcoin, according to Cex.io is $240.00 U.S., so if an individual does not mind investing that kind of money for one Bitcoin then direct purchase is by far the easiest method. The second and certainly most interesting method to obtain Bitcoins are to mine them from an online server. The term "mining" is another term for the use of computational power to process transactions for a cryptocurrency blockchain in order to receive a reward of cryptocurrency for the effort (Heid, 2013).

There are several different options available that the user can take advantage of in order to mine for Bitcoins: solo, pooled or stratum. Solo mining involves the user making use of the computational power of their own CPU or GPU to process transactions for the cryptocurrency as opposed to pooling resources with other miners (Heid, 2013). The advantage of solo mining is that the miner would receive a full payout for a completed blockchain; however, the disadvantage to solo mining is that an increasing difficulty rate makes the chances of repeatedly completing a block with a valid share submission minimal (Heid, 2013).

A "pool" is software hosted on a web server, usually on a dedicated server. Miners create accounts on the pool server and then add authentication credentials to the configuration files of their mining client software on their respective mining equipment (Heid, 2013). With Bitcoin mining software, such as Bitminter, a user's computer solves complex mathematical equations (Shaw, 2013). Because solving these complex equations is next to impossible to do with a single computer, the user needs to join a pool-mining server. This pool is a group of other Bitcoin miners that combines their computing power to make more Bitcoins (Shaw, 2013). In the pool, the individual miner receives smaller and easier equations to solve and the combined work of all the miners will solve the bigger equations. Each miner then receives payment in the form of Bitcoins according to how much work each has contributed to the productivity of the pool (Shaw, 2013). For miners with multiple mining rigs, some mining pools support the use of the "Stratum" protocol. It is used to synchronize the computational effort of multiple mining rigs to reduce the chances of duplicate share submission, thereby maximizing efficiency of the miners combined resources (Heid, 2013).

If a user is successful in obtaining Bitcoins through purchase, trade or by mining, the user's Bitcoins remain in their worker account until they are transferred to their individual Bitcoin wallet. When a user wishes to conduct a transaction, three pieces of information are required:

1. **An input** - this is the record of which Bitcoin address was used to send Bitcoins to the user (Coin Desk, 2013).
2. **An amount** - this is the amount of Bitcoins that the user is sending to another user (Coin Desk, 2013).
3. **An output** - this is the address of the recipient of the Bitcoins to be sent (Coin Desk, 2013).

In order for a person to send the Bitcoins to an intended user and complete a transaction, the person needs to have a Bitcoin address, which is automatically generated when the Bitcoin wallet software is installed and a private key generated (Coin Desk, 2013). A private key serves as a cryptographic signature that validates a user's right to send Bitcoins from a specific wallet. If a user is utilizing a software wallet, the private key is stored on the user's computer, whereas if the user makes use of a web-based wallet the private key is stored on a separate server (Bitcoin Foundation, 2009). With the addresses of the sender and the recipient, the amount and the private key, the user can then conduct a Bitcoin transaction. The user's private key signs a message with the input, amount, and output of Bitcoins before it is sent from their Bitcoin wallet out to the wider Bitcoin network where the transaction is placed on the transaction block where it is eventually verified by Bitcoin miners (Coin Desk, 2013).

Each of the transactions conducted on the Bitcoin network require a series of electronic signatures when each owner transfers the coin to the next owner. These signatures are unique to each owner and are created by digitally signing the hash of the previous transaction as well as the public key of the next owner (Coin Desk, 2013). A hash value is an algorithm that is ran on a piece of data, often an individual file, producing a long alphanumeric string to verify the integrity of files. For example, two files would be identical if the hashes generated from each file are identical (Fisher, n.d.).

The signatures will then be added to the end of the coin, which provides a payee with a visual representation of the chain of ownership (Nakamoto, 2008). Figure 1 illustrates the chain of signatures associated with a Bitcoin transaction as it progresses from one owner to the next.

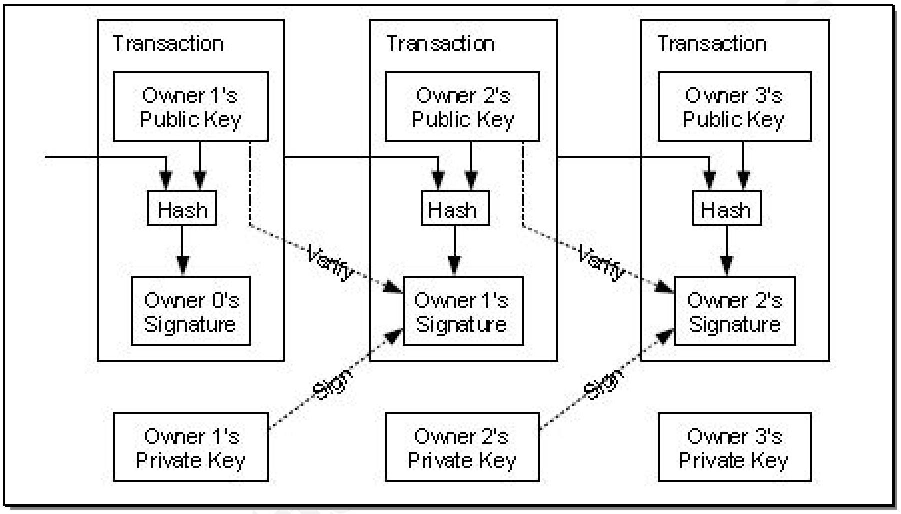


Figure 1: Chain of signatures as a transaction, or Bitcoin, progresses from one owner to the next (Nakamoto, 2008).

Because all of the information about Bitcoin is transparent, information concerning the Bitcoin money supply is readily available on the block chain for anybody to verify and use in real-time (Bitcoin Foundation, 2009). Thus, if an individual wanted to verify any of their transactions or the signatures associated with those specific transactions, they would visit a website such as www.blockexplorer.com and conduct a search based on block number, address, block hash, transaction hash or public key (Bitcoin Block Explorer, 2014). If a search was conducted on www.blockexplorer.com for the Bitcoin address of 17vPdTfLEEtFnpUZK2BUZuGBzyKbBx4iwF, a six-column ledger would appear. The ledger provides details regarding the transaction hash, the block that the transaction appeared in (including date and time), the amount, the type, who sent the

Bitcoin, who received the Bitcoin, and finally the balance available to the Bitcoin address (Bitcoin Block Explorer, 2014).

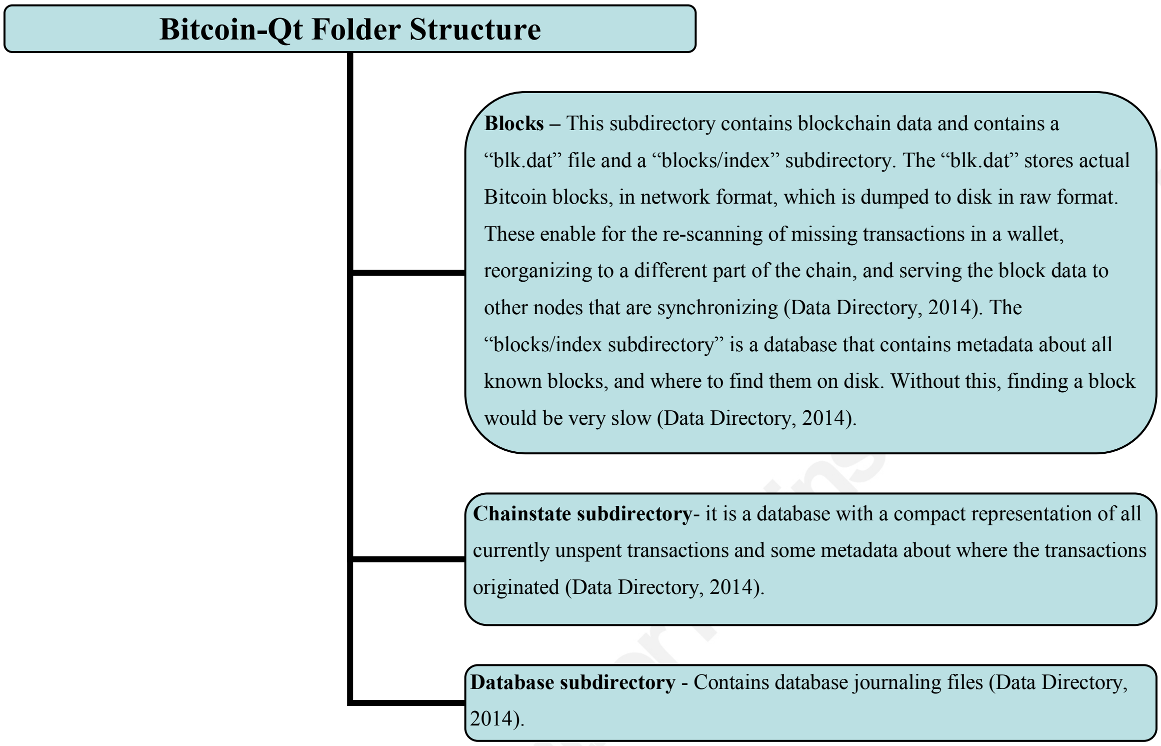
5. Bitcoin artifacts

Initially, when a user decides to become involved with Bitcoins, they first download the software, which will enable them to set up their Bitcoin wallet. This wallet, for all intents and purposes, is similar to that of a physical wallet on the Bitcoin network. It allows the user to spend the Bitcoins allocated to it as well as show the total balance of all Bitcoins it controls and let the user pay a specific amount to a specific person, just like a real wallet (Bitcoin Foundation, 2009).

Although there are numerous Bitcoin wallet software applications out on the market, the most notable is Bitcoin-Qt because it is the original Bitcoin P2P open source software created by the creator of Bitcoin. It is not only a Bitcoin wallet, but it also contains the public ledger that lists every Bitcoin transaction in the system. This is different from the standard Bitcoin wallet software such as BitMinter, which does not contain the ledger as it needs to connect to the network through another Bitcoin server (McIntyre, 2013).

When examining a hard drive image from a suspect machine that was using Bitcoin-Qt, the folder structure will consist of three folders entitled, “blocks,” “database” and “chainstate.” It will also contain five additional files: “.lock,” “db.log,” “debug.log,” “peers.dat” and “wallet.dat” (Jad, 2013).

Each one of the listed file folders and files below has its specific function and each offer specific forensic artifacts and information that can be utilized in the course of an investigation (Jad, 2013).

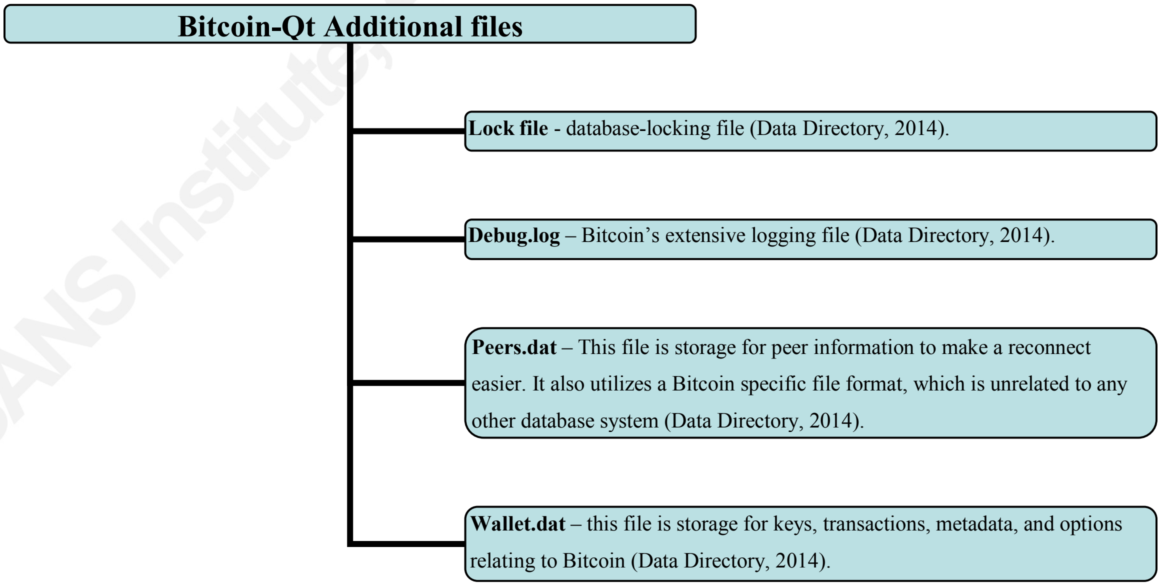


Bitcoin-Qt Folder Structure

Blocks – This subdirectory contains blockchain data and contains a "blk.dat" file and a "blocks/index" subdirectory. The "blk.dat" stores actual Bitcoin blocks, in network format, which is dumped to disk in raw format. These enable for the re-scanning of missing transactions in a wallet, reorganizing to a different part of the chain, and serving the block data to other nodes that are synchronizing (Data Directory, 2014). The "blocks/index subdirectory" is a database that contains metadata about all known blocks, and where to find them on disk. Without this, finding a block would be very slow (Data Directory, 2014).

Chainstate subdirectory- it is a database with a compact representation of all currently unspent transactions and some metadata about where the transactions originated (Data Directory, 2014).

Database subdirectory - Contains database journaling files (Data Directory, 2014).



Bitcoin-Qt Additional files

Lock file - database-locking file (Data Directory, 2014).

Debug.log – Bitcoin's extensive logging file (Data Directory, 2014).

Peers.dat – This file is storage for peer information to make a reconnect easier. It also utilizes a Bitcoin specific file format, which is unrelated to any other database system (Data Directory, 2014).

Wallet.dat – this file is storage for keys, transactions, metadata, and options relating to Bitcoin (Data Directory, 2014).

As all of the information pertaining to a user's Bitcoin account is stored in the "wallet.dat file," most users periodically make backups of their wallets and can name the file. If an investigator examines an image of a suspect's hard drive (see Figure 3) and suspects that the individual is utilizing Bitcoin-Qt, the investigator can check at offset

0×12 for the hexadecimal string "b1" which may identify the file as being a Bitcoin wallet (Jad, 2013).

In addition to the evidentiary artifacts that can be located on the user's computer, investigators can also locate artifacts by conducting an in-depth examination of the blockchain (Greenburg, 2013). Recall that the blockchain is a public record of Bitcoin transactions in chronological order and verifies the permanence of Bitcoin transactions (Bitcoin Foundation, 2009). Thus, if an investigator has the Bitcoin private key of the suspect, they can search for that particular key on the Blockchain to trace the purchases to other potential suspects. Sarah Meiklejohn, a Bitcoin-focused computer science researcher at the University of California at San Diego, conducted extensive research in to the Bitcoin blockchain and found that by looking in the blockchain an investigator can often uncover who owns a particular set of Bitcoin addresses. Utilizing the data from 344 of their own transactions, Meiklejohn and her team were able to identify the owners of more than a million Bitcoin addresses (Greenburg, 2013).

5.1. Building a case with Bitcoin artifacts

A successful case involving digital evidence depends on the content of the case as well as the knowledge, experience, expertise, thoroughness and the curiosity of the investigator in charge of the case (Casey, 2010). In addition to a well-rounded investigator, the success of a digital case rests on a foundational model that provides phases by which the investigator can progress through. The Investigation Process for Digital Forensic Science model is the foundation for a successful digital investigation. This model, released by DFRWS 2001, contains six key phases (Harrell, 2010):

1. Identification
2. Preparation
3. Collection
4. Examination
5. Analysis
6. Presentation

Building a case involving the forensic artifacts of Bitcoin is more difficult than the average case due to the technology that Nakamoto implemented to keep the transactions pseudonymous. Because of this anonymity, particular pieces of evidence are more difficult to obtain and interpret (Greenburg, 2013). However, a successful Bitcoin investigation is possible by escalating through the phases of the Investigation Process for Digital Forensic Science. Although Identification and Preservation are integral phases of the model, the focus of this research centers on the Collection, Examination and the Analysis phases as they pertain to the forensic artifacts of a Bitcoin case.

In the Collection phase, the investigator needs to search for, document, and collect any object or data that could potentially contain digital evidence (Carrier, 2006). Since Bitcoin transactions occur via a network connection, an investigator should seize any physical object that can connect to the Internet. These objects include cell phones, PDAs, laptops, tablets, desktop computers, or iPods. If during the Identification and Preservation phases it is determined that, the suspect's computer is on, it is imperative that the investigator capture the system's physical memory (RAM). Many types of evidence may be available in volatile memory relating to Bitcoin. These types of evidence include:

- Running Bitcoin processes and services
- System information
- Information about logged in users
- Registry information
- Remnants of chats, communications in social networks and Bitcoin forums
- Recent Bitcoin web browsing activities
- Recent communications via webmail systems involving Bitcoin
- Information from cloud services
- Decryption keys for encrypted volumes mounted at the time of the capture
- Running Bitcoin malware/Trojans (Gubanov, 2013)

Upon collecting the evidence, either physically or through extraction or imaging, the investigator can now begin the process of examining the data and assigning the level of importance of each individual piece. Although the Bitcoin artifacts reside on the suspect's hard drive and can be recovered using robust forensic tools such as AccessData's Forensic Toolkit or EnCase, Internet Evidence Finder permits the investigator to view just the Bitcoin artifacts (Jad, 2013).

Two different options are available that enable an investigator to recover the Bitcoin evidentiary artifacts utilizing Internet Evidence Finder. The first option is that the investigator can export the entire Bitcoin file folder from the suspect's drive and have Internet Evidence Finder analyze just that folder for Bitcoin artifacts. The second option is that the investigator can point Internet Evidence Finder at the entire image of the suspect's drive and the program will return not only the Bitcoin artifacts, but also Internet and chat history, e-mail and web searches to name a few (Jad, 2013).

In either option, the Bitcoin artifacts recovered provide a solid base for an investigator to build a case on. Because a majority of the user's activity involving Bitcoin resides within their respective Bitcoin wallets, a majority of the forensic artifacts are going to be located in the "wallet.dat" file. Internet Evidence Finder will recover the "wallet.dat" file and present the addresses from a Bitcoin wallet, as well as queries to the Bitcoin network from log files created by the Bitcoin client software in a user friendly format (Jad, 2013).

In addition to the "wallet.dat" file, the investigator can examine the chainstate subdirectory to view all currently unspent transactions (Data Directory, n.d.). These transactions, with corresponding addresses, could then be compared to the addresses recovered in the "wallet.dat" file as well as those found on the blockchain. By taking the recovered addresses, queries and information pertaining to the unspent transactions an investigator can slowly begin to piece together a case that could develop leads to not only other potential suspects or victims, but also open doors to other potential investigations.

6. Bitcoin forensic artifact examination

In an effort to provide a visual representation of the functionality of Bitcoin and the various forensic artifacts that the software application leaves on a suspect system, an experiment was designed and conducted during the period of 01/22/2014 through 02/28/2014. This experiment utilized a designated computer with a fresh installation of Windows 7 Professional, Multibit, Bitcoin-Qt, Bitminter and a basic USB ASIC Bitcoin mining rig.

A Bitcoin mining rig is typically a computer system used for mining bitcoins. The rig might be a dedicated miner built specifically for mining, or it could be a computer used to mine only on a part-time basis (Mining Rig, n.d.). An ASIC, or Application Specific Integrated Chip, is a microchip designed for a special application, such as Bitcoin mining (ASIC, 2005). After ensuring that the default settings are set with the installation of both the Multibit and Bitcoin-Qt wallet software applications and creating an account with the Bitminter mining pool, the system mined Bitcoins for approximately a month, during which time various transactions were made in order to place evidentiary artifacts inside of the Bitcoin wallets.

At the conclusion of the testing process, an image of the system's RAM and hard drive were examined with EnCase 6.19.9 and Internet Evidence Finder 6.1. The goal of the examination is to see the interaction between the Bitcoin mining software and wallet, with the operating system, registry, and RAM. By analyzing each of those areas in depth with forensic software, the forensic community will gain a working knowledge of the BitCoin forensic artifacts that are present and their importance in an investigation.

6.1. Hardware Setup

The below listed items are the specific items of hardware that were used during the experiment. The 120 GB hard drive was wiped and a fresh installation of Windows 7 was installed to ensure a clean experimental environment. The individual ASIC Mining drives were individually plugged in to the USB hub that was then plugged in to the Gateway laptop via USB connection.

- Gateway laptop ML6720 with power supply
- 120 GB Western Digital hard drive
- (4) USB ASIC Mining drives
- 7 port USB hub
- USB powered cooling fan
- 32 GB USB thumb drive

6.2. Tools

During the experiment, several tools were utilized in order to maintain a running Bitcoin mining computer as well as populate the system's file system and registry with Bitcoin evidentiary artifacts. Each of the tools utilized in the experiment had a specific purpose and were chosen based on their platform design and ease of use.

Bitminter is a Bitcoin mining pool that enables a user to mine for Bitcoins. It provides the user with a graphical user interface that enables the user to control every facet of their Bitcoin mining experience (Hansen, 2011).

Multibit is a lightweight "thin client" Bitcoin wallet for Windows, MacOS and Linux based on *bitcoinj*, which is an open source Bitcoin client library built using Java and the Bitcoin network protocol. Its main advantages include support for opening multiple wallets simultaneously, and not requiring the user to download the entire block chain (MultiBit, 2013).

Bitcoin-Qt is the Bitcoin wallet software developed by Wladimir J. van der Laan, which is based on the original source code of Satoshi Nakamoto. It is a desktop wallet system and contains the public ledger that lists every Bitcoin transaction in the system (McIntyre, 2013).

Tableau Imager 3.1.2 is a forensic imaging tool used to acquire a bit-for-bit copy of a piece of media. It supports Encase .E01, .DD, and .DMG file formats and can customize the destination path and file name conventions with the use of variables including date/time, drive serial number, and model number. It also has error recovery and reporting and conducts the calculation of MD5 and SHA-1 hash values at the conclusion of the imaging process (Software, 2014).

EnCase 6.19.7 is a forensic program designed for forensic examiners and trained investigators who are conducting full forensic examinations on any type of digital media. EnCase allows the forensic examiner to acquire data rapidly from various device types and perform an in-depth forensic analysis of the media. At the conclusion of an analysis, it provides the forensic examiner with the ability to produce comprehensive reports as well as maintain the integrity of the evidence in a format that is presentable and accepted by the courts (Software, 1997, EnCase Version 7-Overview).

Internet Evidence Finder 6.2.3 is a forensic program designed for forensic examiners and trained investigators who are conducting full forensic examinations of Windows and Mac computers. Specifically, Internet Evidence Finder recovers data from social networking sites, instant messenger chats, P2P file sharing apps, mobile backups, webmail, web browser history, pictures and videos (Magnet Forensics, 2014).

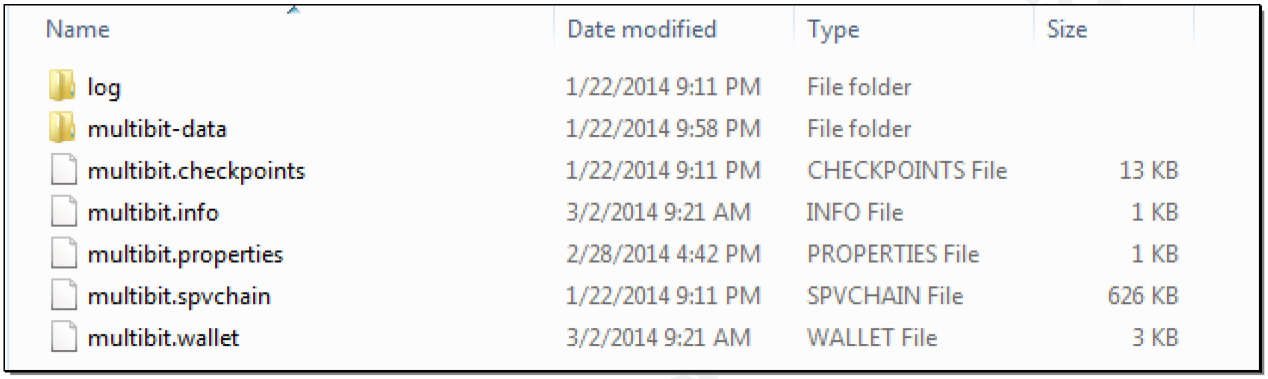
Winen.exe is a RAM acquisition tool that ships with the forensic software EnCase. It can run as a command line tool or from a configuration file. The tool collects RAM and places the collected information into an .E01 file that can be stored on an external drive (Guidance Software, 1997).

7. Testing Results

The first phase of testing was to prepare the testing environment. This phase included a clean install of the host operating system, with all drivers and updates installed. The test system was a Gateway ML6720 laptop computer running Windows 7 Professional Service Pack 1, Build 7601, 32 bit. The processor was an Intel Pentium T2310 running at 1.46 GHz. The system had 1 GB RAM and the system time zone was set to Central Standard Time and was verified through the use of an Apple iPhone utilizing Sprint's cellular network.

The second phase of testing involved configuring the test system to mine and interact with Bitcoins. The first step in this process was to install the Bitcoin wallets that would house the Bitcoin transactions, addresses, and private keys utilized during the testing. The Multibit Bitcoin wallet application was downloaded in the test system's Internet Explorer web browser and saved in the Downloads folder of the test system (Solutions, 2011, What is Multibit?). The Multibit application was located in the Downloads folder and installed by double-clicking on the "multibit-0.5.16-windows-setup.exe" file. This action installed the application with the default settings in the following location "C:\Program Files\MultiBit-0.5.16." Upon successful installation of the Multibit Bitcoin wallet, the application was opened and the Bitcoin address associated with the wallet was "1FdhjMV8s2kzfAdU6TXVS35xkCGcbxAiM6."

In addition to verifying the address of the Multibit wallet, the folder structure of the installation was documented for reference when conducting further examination with EnCase and Internet Evidence Finder. Figure 2 depicts the folder structure of the Multibit wallet application on the test system.

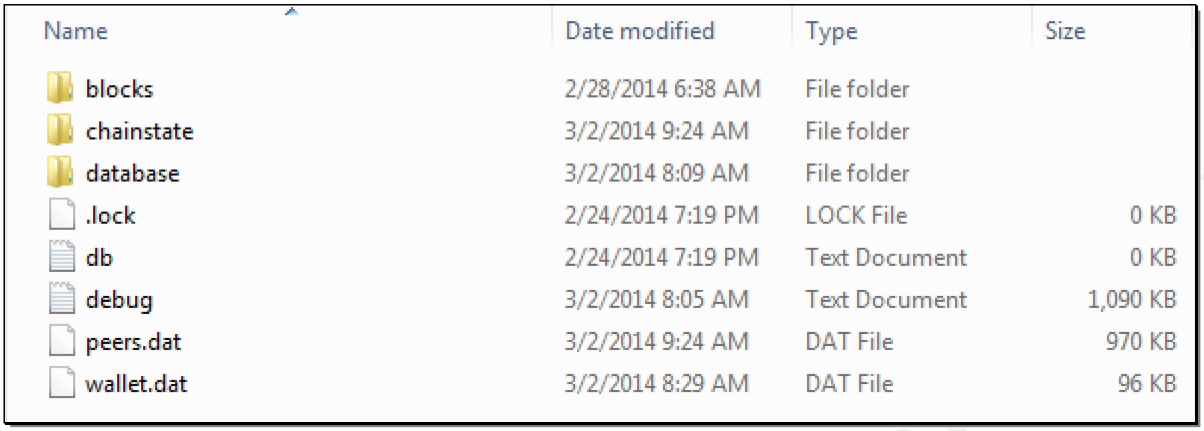


Name	Date modified	Type	Size
log	1/22/2014 9:11 PM	File folder	
multibit-data	1/22/2014 9:58 PM	File folder	
multibit.checkpoints	1/22/2014 9:11 PM	CHECKPOINTS File	13 KB
multibit.info	3/2/2014 9:21 AM	INFO File	1 KB
multibit.properties	2/28/2014 4:42 PM	PROPERTIES File	1 KB
multibit.spvchain	1/22/2014 9:11 PM	SPVCHAIN File	626 KB
multibit.wallet	3/2/2014 9:21 AM	WALLET File	3 KB

Figure 2: Screenshot of the folder structure of Multibit installed on the test system.

In order to gain an understanding of the various artifacts resulting from different Bitcoin wallets, Bitcoin-Qt was downloaded and installed via Internet Explorer to the test system as an additional wallet software application (Project, 2009). The Bitcoin-Qt application, “bitcoin-0.8.6-win32-setup.exe,” was installed with the default settings in the following location “C:\Program Files\Bitcoin-Qt-0.8.6.” After noting the Bitcoin address associated with the wallet as “14igLoRYLjmqc9H5ZSxWqBvdNT3Ro1QeUJ,” was then labeled as “Suspect” and saved within the Bitcoin-Qt wallet.

To verify the address of the Bitcoin-Qt wallet, the folder structure of the installation was documented for reference when conducting further examination with EnCase and Internet Evidence Finder. Figure 3 depicts the folder structure of the Bitcoin-Qt wallet application on the test system.



Name	Date modified	Type	Size
blocks	2/28/2014 6:38 AM	File folder	
chainstate	3/2/2014 9:24 AM	File folder	
database	3/2/2014 8:09 AM	File folder	
.lock	2/24/2014 7:19 PM	LOCK File	0 KB
db	2/24/2014 7:19 PM	Text Document	0 KB
debug	3/2/2014 8:05 AM	Text Document	1,090 KB
peers.dat	3/2/2014 9:24 AM	DAT File	970 KB
wallet.dat	3/2/2014 8:29 AM	DAT File	96 KB

Figure 3: Screenshot of the folder structure of Bitcoin-Qt installed on the test system.

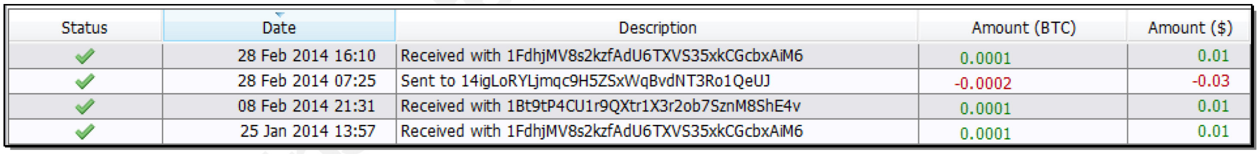
After installing and configuring both of the Bitcoin wallets, an account was created utilizing the G-Mail address of “forensicminer@gmail.com” at website “https://bitminter.com.” The account was created in order to run the software application from the test system and to store pertinent information such as Bitcoin addresses and worker identities. Upon signing on to the Bitminter mining pool for the first time, all of the default account settings were left. However, a “worker” was created and given the identifier of “1” serving as the sole worker performing mining from the test system in the Bitminter mining pool. The Bitminter application was not installed on to the test system; rather, the application was run from the website by clicking on the “Engine Start” button (Hansen, 2011).

With the Multibit and Bitcoin-Qt wallets installed and the Bitminter account created, the Bitcoin mining rig was configured. For the testing environment, the rig consisted of four ASIC Block Erupters plugged in to a seven-port USB hub. An ASIC Block Erupter is a tool utilized to mine Bitcoins that uses an Application Specific Integrated Chip and mines at 330 megahashes a second (MH/s) (Bitcoin Rigs, 2013).

All four of the ASIC miners were attached to a USB port on the hub, in addition to a USB cooling fan. The fan kept the ASIC miners cool, increasing performance and preventing damage due to the overwhelming amount of work that each miner was doing. Upon plugging the hub in for the first time, the test system did not initially recognize the ASIC miners because of the lack of the “CP210x USB to UART Bridge VCP Drivers.” The “CP210x USB to UART Bridge VCP Drivers” were downloaded via the test system's Internet Explorer web browser from the website www.silabs.com (CP210x USB to UART Bridge VCP Drivers, n.d.). Upon successful installation, the "Devices and Printers" section of the test system's Control Panel was verified in order to determine that the ASIC miners appeared on the test system as four separate entries, each with the name of "CP2102 USB to UART Bridge Controller."

Internet Explorer was used to visit the website https://bitminter.com, logging in with the username of "forensicminer@gmail.com," and clicking on the "Start Engine" button that launched the Bitminter control panel and showed the miners actively working.

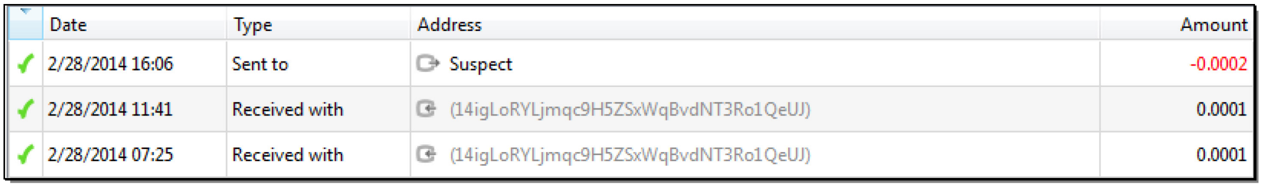
While the test system was actively mining for Bitcoins and the Bitminter account had accrued enough Bitcoins in order to conduct a transaction, three separate transactions were made from the "forensicminer" Bitminter account to the address of the Multibit wallet as well as the Bitcoin-Qt wallet. The transactions occurred on separate dates and times and the respective wallet application logged each. Figure 4 depicts the transactions conducted within the Multibit wallet on the dates of January 25, February 8, and February 28, 2014.



Status	Date	Description	Amount (BTC)	Amount ($)
✓	28 Feb 2014 16:10	Received with 1FdhjMV8s2kzfAdU6TXVS35xkCGcbxAiM6	0.0001	0.01
✓	28 Feb 2014 07:25	Sent to 14igLoRYLjmqc9H5ZSxWqBvdNT3Ro1QeUJ	-0.0002	-0.03
✓	08 Feb 2014 21:31	Received with 1Bt9tP4CU1r9QXtr1X3r2ob7SznM8ShE4v	0.0001	0.01
✓	25 Jan 2014 13:57	Received with 1FdhjMV8s2kzfAdU6TXVS35xkCGcbxAiM6	0.0001	0.01

Figure 4: Screenshot depicting the transactions conducted within the Multibit wallet on the test system.

Figure 5 depicts the transactions conducted within the Bitcoin-Qt wallet on the dates of February 28, 2014. It is important to note that the address listed as "Suspect" is actually the address of the Multibit wallet, "1FdhjMV8s2kzfAdU6TXVS35xkCGcbxAiM6."



	Date	Type	Address	Amount
✓	2/28/2014 16:06	Sent to	Suspect	-0.0002
✓	2/28/2014 11:41	Received with	(14igLoRYLjmqc9H5ZSxWqBvdNT3Ro1QeUJ)	0.0001
✓	2/28/2014 07:25	Received with	(14igLoRYLjmqc9H5ZSxWqBvdNT3Ro1QeUJ)	0.0001

Figure 5: Screenshot depicting the transactions conducted within the Bitcoin-Qt wallet on the test system.

8. Collection and analysis of evidence

8.1. RAM Capture

At the conclusion of the testing period, a 32 GB USB thumb drive was formatted as NTFS and labelled "RAM" for easy identification. The "winen.exe" program was loaded on to the thumb drive and attached to the system that assigned drive letter "F:\." The program was run by right clicking on the "winen.exe" file and selecting "Run as Administrator." A series of values in the winen.exe control panel served to tell the program the file path to save the ".E01" image file, the evidence number, examiner name, and whether or not to compress the image file.

After approximately 15 minutes, the memory acquisition completed successfully and the contents of the "RAM" thumb drive had created a new file, "Test1.E01." The thumb drive was properly ejected and stored for later analysis. The test system was shutdown properly and the hard drive was removed.

8.2. Hard Drive Imaging

The test system hard drive was connected to a Digital Intelligence UltraBay 3D Hardware Write-Blocker and a physical image of the hard drive was conducted (Coons, 2011).

When the imaging process was completed, the log file generated by Tableau Imager displayed no acquisition errors with an MD5 acquisition hash of B9CCFE1092693E9194AE617262CE3375. From this point forward, all analyses pertaining to the Bitcoin artifacts were done from the digital copy to preserve the original disk's integrity.

8.3. Forensic Analysis

The analysis began with the RAM capture file and progressed through to the system image file. The goal of the analysis was to seek out and recover any evidentiary artifacts pertaining to the Multibit and Bitcoin-Qt wallets. The analysis of the RAM capture was conducted utilizing EnCase 6.19.7 and included keyword searches pertaining to various key Bitcoin terms and artifacts. The analysis of the test image file was completed utilizing EnCase as well as Internet Evidence Finder 6.1 and included searches for various key Bitcoin artifacts, analysis of log files and Internet activity.

8.4. RAM Forensics

The “Test.E01” image file was imported into EnCase, and a new case entitled “Test System Examination” was created. The following search terms were entered in to the Keyword function of EnCase:

- Multibit
- Bitcoin
- 1FdhjMV8s2kzfAdU6TXVS35xkCGcbxAiM6
- 14igLoRYLjmqc9H5ZSxWqBvdNT3Ro1QeUJ
- Bitcoin-Qt
- Bitminter
- forensicminer

Examination of the search results revealed multiple locations in “Program Files,” “User files” and the registry where the Multibit and Bitcoin-Qt application files were stored. One of the locations indicated was “C:\Users\Suspect\AppData\Roaming.” Further examination of the search results revealed the transactions that had been conducted during the course of the testing phase. There were no specific dates and times associated with either transaction. However, the two addresses associated with the Multibit and Bitcoin-Qt addresses were in clear text.

8.5. Hard Drive Forensics

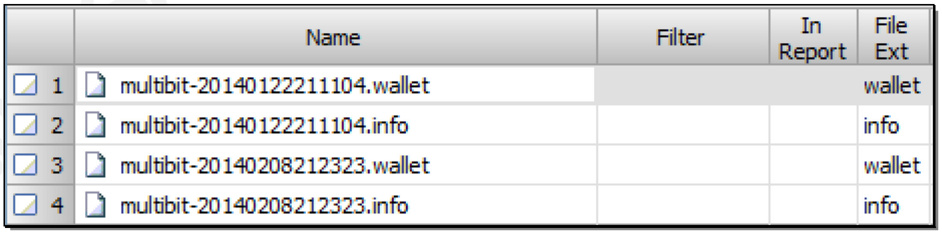
A new examination case entitled “Bitcoin Test System” was created and the disk “Test System Image.E01” file was loaded as the evidence. The examination strategy consisted of conducting an analysis of the Multibit and Bitcoin-Qt files and the analysis of the Internet activity utilizing Internet Evidence Finder.

Multibit. The root directory, “C:\,” contained the bulk majority of the files and folders used by the system and the user. Based on the results obtained from the analysis of the RAM capture, the Multibit application was found to be located in: “C:\Users\Suspect\AppData\Roaming\Multibit.”

Examination of the files in detail resulted in the following information:

- The presence of the Multibit wallet, which had the default name of "multibit.wallet." This particular file is the main wallet file that contains the user's private keys and transactions (Solutions, 2011).
- The presence of a rolling backup of the "multibit.wallet" file. This file was located in the subfolder of "rolling-backup" and was entitled "multibit-20140222190122.wallet." The series of numbers following the name of the wallet served as the time stamp when the backup was created. In this case, the timestamp of the backup was 02/22/2014 at 19:01:22 hrs (7:01:22 PM). The backup files are created by the respective user and the primary purpose of them is to recover from any sudden loss of power that prevents a clean wallet save (Solutions, 2011).
- Two backups of the wallet file. One of the backups stores the data for encrypted wallets and the other for unencrypted wallets. These files are in the format "YYYYMMDDHHMMSS.wallet" and "YYYYMMDDHHMMSS.info." The Multibit wallet is backed up to these directories each time that the user opens a wallet, adds or changes the password, adds a receiving address or imports private keys (Solutions, 2011).

There were also two separate entries on two separate dates for unencrypted rolling backups within the Suspect's Multibit wallet located in the subfolder of "wallet-unenc-backup." Figure 6 illustrates the backup files as they appear in EnCase.



	Name	Filter	In Report	File Ext
☐ 1	multibit-20140122211104.wallet			wallet
☐ 2	multibit-20140122211104.info			info
☐ 3	multibit-20140208212323.wallet			wallet
☐ 4	multibit-20140208212323.info			info

Figure 6: Screenshot depicting the two separate dates for the unencrypted rolling backups of the Suspect's Multibit wallet.

Each of those entries had timestamps attached to them providing evidence of when Multibit had generated the backups:

- multibit-20140122211104.wallet (01/22/2014 at 21:11:04 hrs)
- multibit-20140122211104.info (01/22/2014 at 21:11:04 hrs)
- multibit-20140208212323.wallet (02/08/2014 at 21:23:23 hrs)
- multibit-20140208212323.info (02/08/2014 at 21:23:23 hrs)

Examination of each of the ".wallet" files revealed unreadable data; however, examination of the two ".info" files revealed information pertaining to the wallet version, where the wallet backup was stored, and the specific addresses associated with the wallet file.

Examination of each of the remaining files within the Multibit file folder revealed the following:

- **multibit.properties** – this file is the MultiBit configuration file that contains the location and name of the wallet, the username and the configurations set forth by the user upon installation (Solutions, 2011).
- **multibit.checkpoints** – the MultiBit checkpoints file enables the Multibit program from downloading the entire blockchain (Solutions, 2011).
- **multibit.info** – in addition to the multibit.properties file, this is another location that stores the name of the wallet (Solutions, 2011).

Table 1 illustrates the Multibit artifacts recovered during the hard drive analysis and their locations:

Table 1. Multibit 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-20140222190122.wallet (Rolling Backup)	C:\Users\XXXX \AppData\Roaming\Multibit
multibit-20140122211104.wallet	C:\Users\XXXX\AppData\Roaming\Multibit\wallet-unenc-backup
multibit-20140122211104.info	C:\Users\XXXX\AppData\Roaming\Multibit\wallet-unenc-backup

Evidentiary Artifact	Location of Artifact
multibit-20140208212323.wallet	C:\Users\XXXX\AppData\Roaming\Multibit\wallet-unenc-backup
multibit-20140208212323.info	C:\Users\XXXX\AppData\Roaming\Multibit\wallet-unenc-backup
multibit.properties	C:\Users\XXXX \AppData\Roaming\Multibit
Multibit.checkpoints	C:\Users\XXXX \AppData\Roaming\Multibit
Multibit.info	C:\Users\XXXX \AppData\Roaming\Multibit

Bitcoin-Qt. Examination of the Bitcoin-Qt wallet application began by navigating to the location of the Bitcoin-Qt wallet installation obtained from the analysis of the RAM capture, "C:\Users\Suspect\AppData\Roaming\Bitcoin." Examination of the contents of the file folder, revealed the presence of two subfolders "blocks" and "chainstate." Within the "blocks" subfolder, there was an additional subfolder entitled "index." The "blocks" and "index" subdirectory contain metadata about all known blocks, and provides the location of them on the user's disk (Data Directory, 2014).

Specifically, the "blocks" subfolder contained 271 individual files. Of those files, there were 240 files with the file extension of ".dat." Of those 240 files, there were 120 files numbered in sequence starting at "blk00000.dat" and ending with "blk00119.dat." Those files store actual Bitcoin blocks in network format, and are only needed for re-scanning missing transactions in a wallet, reorganizing to a different part of the chain, and serving the block data to other nodes that are synchronizing (Data Directory, 2014). The remaining 120 files had names that were also numbered in sequence; however, they started at "rev00000.dat" and ended with "rev00119.dat." The "rev.dat" files contain "undo data." The user is able to see blocks as patches to the chain state and see the undo data as reverse patches. These files are necessary for rolling back the chainstate, which is necessary in the case of reorganizations when one chain becomes longer than the one currently being worked on (Data Directory, 2014).

Examination of the other files located within the Bitcoin-Qt file folder in detail revealed the following information:

- The presence of the “wallet.dat” file which contains the user’s private keys and transactions (Solutions, 2011). Further examination of this file revealed large amounts of unreadable Base64 text.
- The presence of the “peers.dat” file which stores peer information to make a reconnect easier. Further examination of this file revealed large amounts of unreadable Base64 text.
- The presence of the “db.log” file which also stores peer information to make a reconnect easier. Further examination of this file revealed it was an empty file.
- The presence of the “Lock” file which is the Bitcoin database-locking file. Examination of this file revealed it an empty file.
- The presence of the “debug.log” file that is the extensive logging file of Bitcoin-Qt. Further examination of this file revealed a large amount of logging data that included dates and times as well as Bitcoin transaction addresses. The entire log file was exported to the desktop of the forensic workstation and given the file name of “Test System Bitcoin Log.” Initial examination of the log revealed a standard log file in readable format containing dates, times, blocks and IP addresses. A search of the log file utilizing the test system’s IP address of 108.XXX.XX.XX resulted in several hits within the log file.

Further examination of each log file entry revealed that each was from the blockchain and contained a date and time stamp, message version, the specific blocks within the block chain, as well as the IP address of the test system and the peer network. The following illustrates the breakdown of one of the log entries from the blockchain:

- Date/Time: 03/02/2014 at 18:23:39 hrs (6:23:39 PM)
- Message Version: Satoshi: 0.8.6 version 7001 (Version of Bitcoin-Qt installed on test system)
- Blocks: 257627
- US: 108.XXX.XX.XX (IP address of the test system)
- Them= 131.XXX.XX.XX (IP address of the connected peer) A query of the peer IP address through www.iplocation.com, revealed it to be located in Ontario, Canada.

The above log file entry is a result of a series of messages transmitted and received by the peers of the Bitcoin network. When connecting to the Bitcoin network, everyone broadcasts an “addr” message containing his or her own IP address every 24 hours (Network, 2013). Nodes relay these messages to the peers and they are stored if the address is new. Through this system, everyone has a reasonably clear picture of which IPs are connected to the network at that particular moment (Network, 2013). The peers will request the full transaction with a “getdata” message that is a request for a single block or transaction. If the peers consider the transaction valid after receiving it, they will in turn broadcast the transaction to all of their peers with an “inv” message (Network, 2013).

Table 2 illustrates the Bitcoin-Qt artifacts recovered during the hard drive analysis and their locations:

Table 2. Bitcoin-Qt artifacts recovered during the hard drive analysis.

Evidentiary Artifact	Location
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

8.6. Internet Evidence Finder Forensics

The “Test System.E01” image file was loaded into Internet Evidence Finder 6.2.3 and “Internet Explorer” and “Bitcoin” were selected as the evidentiary artifacts that the program would seek out. At the conclusion of the processing, a section under the “IEF Refined Results” labeled “Peer to Peer” was populated with two entries for “Bitcoin Addresses.” Further examination of those results revealed two addresses, “1FdhjMV8s2kzfAdU6TXVS35xkCGcbxAiM6” and “14igLoRYLjmqc9H5ZSxWqBvdNT3Ro1QeUJ.” In viewing the source of the evidence, it was determined that the above listed addresses originated from the “wallet.dat” file, located at “C:\Users\Suspect\AppData\Roaming\Bitcoin.”

After right clicking on each of the addresses within Internet Evidence Finder and selecting “Query Bitcoin Block Chain,” an Internet Explorer window opened and information pertaining to each of the addresses such as the Public Key and the Public Key hash, as well as the sent and received transactions with each of the addresses was visible on the website “www.blockexplorer.com.” The following query of the Bitcoin address “1FdhjMV8s2kzfAdU6TXVS35xkCGcbxAiM6” revealed the following:

- First seen: Block 282447, 01/25/2014 at 20:10:00 hrs. (This is the first block that the address was used in)
- Received transactions: 2
- Received BTC: 0.0002
- Sent transactions: 1
- Sent BTC: 0.0001
- Hash160 (This hash value is the hash of the public key): “a082bc485913a5d5fffa79e824daa02bebac36a1”
- Public key: “02738b96756e7c101f44098665d64dd41e3a6f9b08b7130db71161be77bf978451”

The following query of the Bitcoin address “14igLoRYLjmqc9H5ZSxWqBvdNT3Ro1QeUJ” revealed the following:

- First seen: Block 288294, 02/28/2014 at 13:39:12 hrs. (This is the first block that that the address was used in)
- Received transactions: 2
- Received BTC: 0.0002
- Sent transactions: 2
- Sent BTC: 0.0002
- Hash160: 28ca45b6c41a17c31c551632c6f9412d705c46df
- Public key: 03d2e19dcabe7e5557e204ba6865355f82062f67794ccb1f450778f05954a215a0

Further examination of the findings from Internet Evidence Finder revealed no evidentiary artifacts from the Multibit wallet or Bitminter mining applications.

9. Conclusion

Bitcoin cryptocurrency is a relatively new technology and very little research has been dedicated to what specific forensic artifacts are left on a user's system as a result of Bitcoin, what those artifacts mean and how to recover them in order to build a successful case involving Bitcoin. This research sought to provide a history of Bitcoin cryptocurrency and through the use of a test environment, ascertain what specific Bitcoin artifacts are recoverable from a user's system with Bitcoin wallet and mining applications installed and actively used. The examination of the data collected after the testing phase provided evidence validating the installation of the Multibit and Bitcoin-Qt wallet applications on the test machine, as well as confirms the creation of Bitcoin transactions generated by the wallet applications. In addition, the analysis provided evidentiary artifacts relating to the Bitminter mining software and the interaction of each Bitcoin application with the operating system, registry, and RAM. The analysis of the RAM was a success in that it returned a multitude of results that matched the Bitcoin wallet addresses, transactions and Bitcoin applications on the test system.

Future work on this subject should include the testing of the other Bitcoin wallet applications such as Bitcoin Core, Hive, Armory, and Electrum. This future work should also include how those applications interact with other operating systems, such as older versions of Windows and the Linux platforms. These should also be extensive software development in to a Bitcoin based forensic artifact extraction tool. This tool would be similar in nature to "winen.exe" and would enable the forensic examiner to load the program on a forensically sterile USB thumb drive, insert it in to the suspect machine, and extract just the Bitcoin related evidence. Because this study did not address how the Bitcoin wallet and mining applications altered the registry, further research on the specific changes the Bitcoin applications and transactions make to the registry is necessary. This study stands as part of the initial discussion on the subject of Bitcoin forensics, not a definitive answer to the questions posed in this body of research.

10. References

ASIC (application-specific integrated circuit). (2005, September 1). Retrieved February 21, 2014, from WhatIs.com: http://whatis.techtarget.com/definition/ASIC-application-specific-integrated-circuit

Beattie, A. (2011, October 25). *The Evolution of Banking.* Retrieved January 30, 2014, from Investopedia: http://www.investopedia.com/articles/07/banking.asp

Bitcoin Block Explorer. (2014, January 9). Retrieved February 4, 2014, from BlockExplorer: http://blockexplorer.com/

Bitcoin Foundation. (2009). *How does Bitcoin work?* Retrieved February 3, 2014, from Bitcoin.org: https://bitcoin.org/en/how-it-works

Bitcoin Rigs. (2013). *ASICMiner Block Erupter – USB Bitcoin Miner*. Retrieved February 21, 2014, from Bitcoin Rigs: http://bitcoinrigs.org/product/asicminer-block-erupter-usb-bitcoin-miner/

Carrier, B. (2006). *A Hypothesis-Based Approach to Digital Forensic Investigations.* Retrieved February 16, 2014, from Cerias.Purdue.edu: https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2006-06.pdf

Casey, E. (2010). *Handbook of Digital Forensics and Investigation.* Burlington, MA: Elsevier Academic Press.

Coin Desk. (2013, November 26). *How do bitcoin transactions work?* Retrieved February 4, 2014, from CoinDesk: http://www.coindesk.com/information/how-do-bitcoin-transactions-work/

Coons, P. (2011, August 4). *Forensic Imaging-3 Different Methods.* Retrieved February 23, 2014, from eDiscovery: http://www.d4discovery.com/2011/08/3-methods-of-forensic-imaging/

Cope, J. (2002, April 8). *QuickStudy: Peer-to-Peer Network.* Retrieved February 5, 2014, from ComputerWorld.com: http://www.computerworld.com/s/article/69883/Peer_to_Peer_Network

CP210x USB to UART Bridge VCP Drivers. (n.d.). Retrieved February 22, 2014, from Silicon Labs: http://www.silabs.com/products/mcu/Pages/USBtoUARTBridgeVCPDrivers.aspx

Data Directory. (2014, March 12). Retrieved February 11, 2014, from Bitcoin.it: https://en.bitcoin.it/wiki/Data_directory

Doyle, M. (2000). *When Did Online Banking Begin?* Retrieved January 21, 2014, from eHow Money: http://www.ehow.com/facts_5035719_did-online-banking-begin.html

Dree12. (2013, November 28). *List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses.* Retrieved January 5, 2014, from Bitcoin Forum: https://bitcointalk.org/index.php?topic=83794.0

Edelman. (2013, January 1). *2013 Global Results.* Retrieved February 2, 2014, from Edelman: http://www.edelman.com/trust-downloads/global-results-2/

FBI. (2012, April 24). *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity.* Retrieved January 5, 2014, from www.wired.com: http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf

Fisher, T. (n.d.). *Cryptographic Hash Function.* Retrieved February 5, 2014, from About.com: http://pcsupport.about.com/od/termsc/g/cryptographic-hash-function.htm

Greenburg, A. (2013, September 5). *Follow The Bitcoins: How We Got Busted Buying Drugs On Silk Road's Black Market.* Retrieved February 8, 2014, from Forbes: http://www.forbes.com/sites/andygreenberg/2013/09/05/follow-the-bitcoins-how-we-got-busted-buying-drugs-on-silk-roads-black-market/

Guidance Software. (1997). *Memory Acquisition Tools*. Retrieved February 23, 2014, from Memory Analysis: http://www.e5hforensics.com/memoryanalysis.com/acquisition_tools.htm

Hansen, G. H. (2011). *Bitminter-Bitcoin minting made easy*. Retrieved February 20, 2014, from Bitminter: https://bitminter.com/

Harrell, C. (2010, October 19). *Overall DF Investigation Process.* Retrieved February 16, 2014, from Journey Into Incident Repsonse: http://journeyintoir.blogspot.com/2010/10/overall-df-investigation-process.html

Heid, A. (2013, July 18). *Analysis of the Cryptocurrency Marketplace*. Retrieved February 15, 2014, from Hack Miami: http://www.hackmiami.org/whitepapers/HackMiami-Analysis_of_the_Cryptocurrency_Marketplace.pdf

Jad. (2013, November 12). *Bitcoin Forensics Part II: The Secret Web Strikes Back.* Retrieved February 11, 2014, from Magnet Forensics: http://www.magnetforensics.com/bitcoin-forensics-part-ii-the-secret-web-strikes-back/

Janssen, C. (2009, March 4). *Cryptocurrency.* Retrieved February 2, 2014, from Techopedia: http://www.techopedia.com/definition/27531/cryptocurrency

Leiner, B. (2013). *Brief History of the Internet.* Retrieved January 21, 2014, from Internet Society: http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet

Magnet Forensics. (2014). *IEF Standard - Internet Evidence Finder*. Retrieved February 20, 2014, from Magnet Forensics: http://www.magnetforensics.com/software/internet-evidence-finder/ief-standard/?__hssc=&__hstc&hsCtaTracking=68ea3ab7-8bf8-4676-8a66-d18b406f1bc6|d9ef2913-83f1-4a3b-911b-97debd39a477

McIntyre, D. (2013, August 24). *Coinbase vs Bitcoin-Qt vs Bitcoin Wallet Review – What Is The Difference?* Retrieved February 11, 2014, from Newfination.com: http://www.newfination.com/2013/08/24/coinbase-vs-bitcoin-qt-vs-bitcoin-wallet-review-what-is-the-difference/4412/

Mining Rig. (n.d.). Retrieved February 21, 2014, from Bitcoin.it: https://en.bitcoin.it/wiki/Mining_rig

MultiBit. (2013, March 31). Retrieved February 20, 2014, from BitCoin.it: https://en.bitcoin.it/wiki/MultiBit

Nakamoto, S. (2008, November 1). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Retrieved January 21, 2014, from Bitcoin.org: http://bitcoin.org/bitcoin.pdf

Naughton, J. (2010, June 19). *The Internet: Everything You Ever Need To Know.* Retrieved January 23, 2014, from The Guardian: http://www.theguardian.com/technology/2010/jun/20/internet-everything-need-to-know

Network. (2013, December 25). Retrieved March 7, 2014, from Bitcoin.it: https://en.bitcoin.it/wiki/Network

Peter, I. (2004). *The History of E-Mail.* Retrieved January 23, 2014, from Net History: http://www.nethistory.info/History%20of%20the%20Internet/email.html

Project, B. (2009). *Download Bitcoin-Qt*. Retrieved February 24, 2014, from Bitcoin.org: https://bitcoin.org/en/download

Roos, D. (2008, April 15). *The History of E-Commerce.* Retrieved January 23, 2014, from How Stuff Works: http://money.howstuffworks.com/history-e-commerce.htm

Rouse, M. (2009, January 1). *Cryptography.* Retrieved February 2, 2014, from Search Software Quality: http://searchsoftwarequality.techtarget.com/definition/cryptography

Saliba, J. (2013, November 12). *Bitcoin Forensics Part II: The Secret Web Strikes Back.* Retrieved January 5, 2014, from Magnet Forensics: http://www.magnetforensics.com/bitcoin-forensics-part-ii-the-secret-web-strikes-back/

Shaw, R. (2013, June 28). *What is Bitcoin?* Retrieved January 6, 2014, from Infosec Institute: http://resources.infosecinstitute.com/bitcoin/

Smith, C. (2013). *4 Advantages of Online Banking.* Retrieved January 21, 2014, from Account Now: http://www.accountnow.com/content/online-banking/4-advantages-of-online-banking-2/

Software, G. (1997). *EnCase Version 7-Overview*. Retrieved February 20, 2014, from Guidance Software: http://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx

Software, G. (2014, January 14). *Tableau Imager (TIM)*. Retrieved February 20, 2014, from Guidance Software:

http://www.guidancesoftware.com/products/Pages/tableau/products/software/tableau-imager.aspx

Solutions, B. (2011). *What is Multibit?* Retrieved February 21, 2014, from Multibit.org: https://multibit.org/

Strickland, J. (2007). *How did the Internet Start?* Retrieved January 21, 2014, from How Stuff Works: http://computer.howstuffworks.com/internet/basics/internet-start.htm

Write Blockers. (2012, July 23). Retrieved February 27, 2014, from Forensics Wiki: http://www.forensicswiki.org/wiki/Write_Blockers

Last Updated: March 13th, 2020

Upcoming SANS Forensics Training

SANS London March 2020	London, United Kingdom	Mar 16, 2020 - Mar 21, 2020	Live Event
SANS San Francisco Spring 2020	San Francisco, CA	Mar 16, 2020 - Mar 27, 2020	CyberCon
SANS Secure Singapore 2020	Singapore, Singapore	Mar 16, 2020 - Mar 28, 2020	Live Event
SANS Norfolk 2020	Norfolk, VA	Mar 16, 2020 - Mar 21, 2020	CyberCon
SANS Oslo March 2020	Oslo, Norway	Mar 23, 2020 - Mar 28, 2020	Live Event
SANS Seattle Spring 2020	Seattle, WA	Mar 23, 2020 - Mar 28, 2020	CyberCon
Mentor Session - FOR508	Sao Paulo, Brazil	Mar 25, 2020 - Mar 28, 2020	Mentor
SANS Frankfurt March 2020	Frankfurt, Germany	Mar 30, 2020 - Apr 04, 2020	Live Event
SANS vLive - FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics	FOR508 - 202003,	Mar 31, 2020 - May 07, 2020	vLive
SANS 2020	Orlando, FL	Apr 03, 2020 - Apr 10, 2020	CyberCon
SANS Bethesda 2020	Bethesda, MD	Apr 14, 2020 - Apr 19, 2020	CyberCon
SANS Minneapolis 2020	Minneapolis, MN	Apr 14, 2020 - Apr 19, 2020	CyberCon
SANS London April 2020	London, United Kingdom	Apr 20, 2020 - Apr 25, 2020	Live Event
SANS Brussels April 2020	Brussels, Belgium	Apr 20, 2020 - Apr 25, 2020	Live Event
SANS Baltimore Spring 2020	Baltimore, MD	Apr 27, 2020 - May 02, 2020	CyberCon
SANS Bucharest May 2020	Bucharest, Romania	May 04, 2020 - May 09, 2020	Live Event
SANS Security West 2020	San Diego, CA	May 06, 2020 - May 13, 2020	CyberCon
SANS Amsterdam May 2020	Amsterdam, Netherlands	May 11, 2020 - May 18, 2020	Live Event
SANS Hong Kong 2020	Hong Kong, Hong Kong	May 11, 2020 - May 16, 2020	Live Event
Community SANS Scottsdale FOR508	Scottsdale, AZ	May 11, 2020 - May 16, 2020	Community SANS
SANS San Antonio 2020	San Antonio, TX	May 17, 2020 - May 22, 2020	CyberCon
SANS Northern Virginia- Alexandria 2020	Alexandria, VA	May 17, 2020 - May 22, 2020	CyberCon
SANS Autumn Sydney 2020	Sydney, Australia	May 18, 2020 - May 23, 2020	Live Event
SANS FOR508 Madrid May 2020 (In Spanish)	Madrid, Spain	May 25, 2020 - May 30, 2020	Live Event
SANS Dublin May 2020	Dublin, Ireland	May 25, 2020 - May 30, 2020	Live Event
SANS Stockholm May 2020	Stockholm, Sweden	May 25, 2020 - May 30, 2020	Live Event
SANS Krakow May 2020	Krakow, Poland	May 25, 2020 - May 30, 2020	Live Event
SANS Atlanta Spring 2020	Atlanta, GA	May 26, 2020 - May 31, 2020	CyberCon
SANS Nashville Spring 2020	Nashville, TN	May 26, 2020 - May 31, 2020	CyberCon
SANS London June 2020	London, United Kingdom	Jun 01, 2020 - Jun 06, 2020	Live Event
SANS Chicago Spring 2020	Chicago, IL	Jun 01, 2020 - Jun 06, 2020	Live Event