Cryptocurrency Artifact Analysis

Preston Miller, B.A.[1], Lance Nudd, J.D.[2], Chris Vance, B.S.[1], Terry Fenger, Ph.D.[1]
[1]Marshall University Forensic Science Center, 1401 Forensic Science Dr, Huntington, WV 25701
[2]Stroz Friedberg, 32 Avenue of Americas, New York, NY 10013

Abstract

Virtual currencies, such as Bitcoin, have recently dominated news headlines. The term virtual currency has been around since 2012. However, virtual currencies as we know them have existed before then. Most virtual currencies can be used to buy goods anonymously, which has made them popular among privacy concerned individuals. Bitcoin's recent spike in popularity has caused a proliferation and dissemination of information regarding its use and advantages to mainstream audiences. Adoption of virtual currencies by the public has increased, which has introduced a novel issue in digital forensic examinations.

This summer, MultiBit, Litecoin, and Darkcoin desktop wallet software was examined for valuable artifacts on Windows 7 and Ubuntu 14.04 operating systems. This was accomplished in a three-fold fashion: Hard drive, Memory, and Network evidence. In all cases, some form of application settings, user timeline information, and transaction logs were among the type of information able to be recovered. The MultiBit wallet contained the greatest amount of user timeline information including a file created upon uninstalling the application. Overall, the three wallets shared remarkable similarity in artifacts generated.

Introduction

Bitcoin's creation is credited to the alias Satoshi Nakamoto, whose identity is still unknown. The idea behind Bitcoin was initially proposed in October 2008 as a "purely peer-to-peer version of electronic cash" that would cut out the middle man, i.e. financial institutions.

In the trust model, a trusted third party verifies that the money has not already been spent before allowing a transaction. This obstacle led to Bitcoin's greatest innovation, the blockchain. The blockchain is essentially a public ledger that is made up of blocks containing all previous transactions of the currency (Fig. 1). This blockchain prevents double spending by the verification process each transaction must undergo. This process is designed to take ten minutes to complete and is composed of these basic steps:

1. Assign the transaction to a block that is in a queue to be verified
2. Confirm coins were signed with the sender's address private key
3. Confirm coins have not already been spent by checking the blockchain
4. Repeat for all transactions in the block
5. Calculate a difficult SHA256 hash of the block plus "nonce"
6. Add the block to the blockchain

Materials & Methods

Materials used for this research project include:

1. One external hard drive
2. VM Workstation and ISO files for operating systems analyzed
3. Bitcoins, Litecoins, and Darkcoins for trading purposes
4. Access to forensic software programs

Results & Discussion

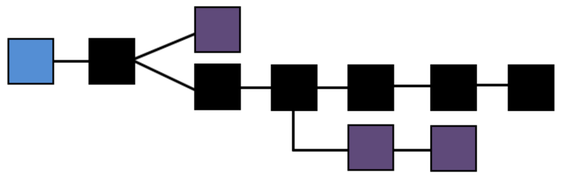

Figure 1. The blockchain is made up of blocks. Each block is made up of hundreds of transactions. The start of the chain, the Genesis block, is blue. The main chain is black and forks in the chain are purple, referred to as "orphan" blocks.

Disk Forensics

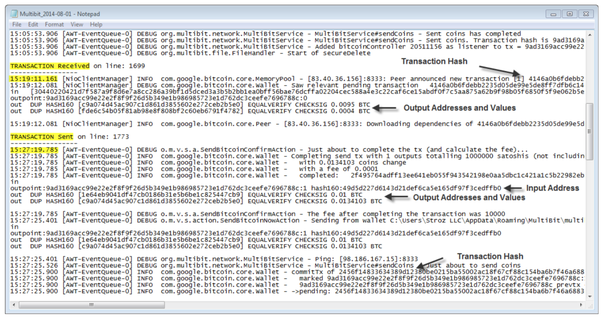

Figure 3. Transactions sent from the wallet appear after a "SendBitcoinConfirmAction" entry. Transactions to the wallet appear after a "Peer announced new transaction" entry. These transactions contain the time, transaction hash, address inputs and outputs, and amount traded. This can also be compared with the start and stop times to determine transactions in particular sessions of the application.

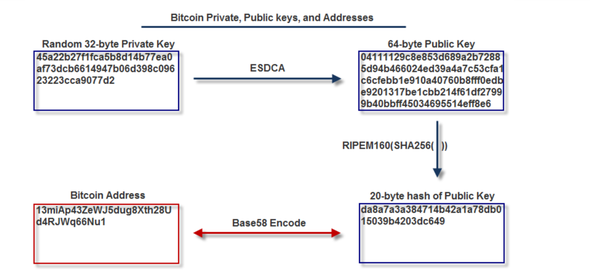

Figure 2. Demonstrates the process through which an address is generated. This process is primarily only one way. To protect the address used in this figure, the private and public key values were made up.

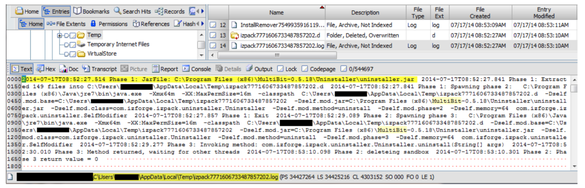

Figure 4. The izpack log appears to be generated when the user uninstalls the MultiBit program from their system.

Network Forensics

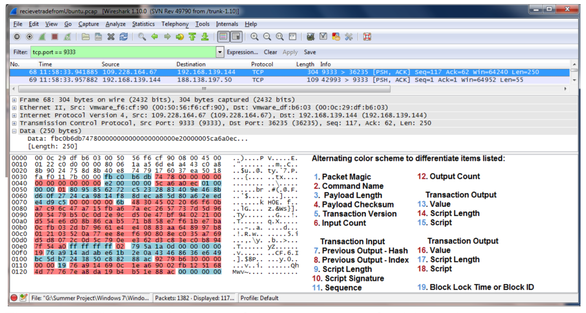

Figure 5. The breakdown of the contents of a Litecoin tx message. This process can be repeated for any cryptocurrency using the Bitcoin protocol. Please note that the length of the "Script Signature" (10) is variable and the "Output Count" (12) will determine how many "Transaction Output" fields there are. Additionally, the "Transaction Output Script" value must be processed to obtain the address in a similar fashion described in the Bitcoin section (note the Network ID for Litecoin is typically "L").

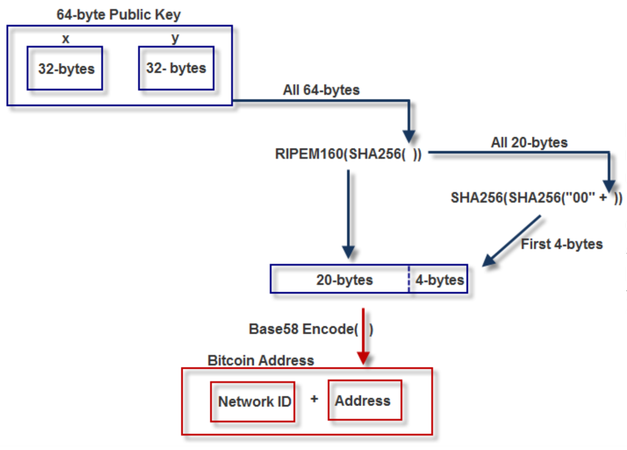

Figure 6. A more detailed version of Fig. 2 starting with the generated ESDCA public key, which is made up of its (x, y) position on the curve. The Script value from Wireshark is already the 20-byte product from the RIPEM160 and SHA256 hash of the public key. After removing the first 3-bytes and last 2-bytes from the Wireshark Script value the remaining 20-bytes must be processed. First a checksum must be calculated by sequential SHA-256 hashing of the 20-byte value with a prepended 00. The first 4 bytes of this value is appended to the original 20-bytes and base58 encoded. Then a Network ID must be prepended to arrive at the actual address. For Bitcoin, the Network ID is often 1 or 3. It is recommended that a script is created to automate this process.

inv

Byte offset	Item
0-53	Packet Structure
54-	Data
54-57	Packet Magic
58-69	Command Name (69:6e:76)
70-73	Payload Length
74-77	Payload checksum
78	Count
79-82	Type (01 - TX, 02 - Block, 03 - Uknown)
83-114	Data hash

getdata

Byte offset	Item
0-53	Packet Structure
54-	Data
54-57	Packet Magic
58-69	Command Name (67:65:74:64:61:74:61)
70-73	Payload Length
74-77	Payload checksum
78	Count
79-82	Type (01 - TX, 02 - Block, 03 - Uknown)
83-114	Data hash

tx

Byte offset	Item
0-53	Packet Structure
54-	Data
54-57	Packet Magic
58-69	Command Name (74:78)
70-73	Payload Length
74-77	Payload checksum
78-81	Transaction Version
82	Input Count
83-262*	Transaction Input *Variable length - 180 bytes in this example
263	Output Count
264-297	Transaction Output *Amount of tx output fields dependent on output count
297-301	Block lock time or Block ID

Figure 7. The packet details of the three main messages in the Bitcoin protocol are detailed. The fields within Transaction Input and Output are not shown in this figure. Note that these packet details have the same structure as Litecoin network traffic or any other cryptocurrency using the Bitcoin protocol.

Conclusions

Examiners must be aware of common artifacts and the extent of information that is obtainable from evidence. In this study, the best method for observing transactions were network captures in combination with a blockchain lookup utility. However, it is important to find remnants of those transactions on a user's computer. When examining a wallet application, it is vital to determine if there is a corresponding log file because they contain the most user activity and transaction information, outside of a network capture. The cryptocurrency wallet software examined shared remarkable similarity in the amount of information stored on the user's machine for both Windows 7 and Ubuntu 14.04. Network traffic was also similar across the cryptocurrencies studied. The process of parsing Bitcoin's network traffic, such as a tx message, was identical in Litecoin and Darkcoin. Consumers and investors have demonstrated high interest in Bitcoin and virtual currencies as a whole and examiners should be prepared to analyze cryptocurrencies effectively as the likelihood of cases involving them continues to increase.

References

Barber, Simon, et al. "Bitter to Better - How to Make Bitcoin a Better Currency." Financial Cryptography and Data Security (2012).

Duffield, Evan and Kyle Hagan. "Darkcoin: Peer-to-Peer Crypto-Currency with Anonymous Blockchain Transactions and an Improved Proof-of-Work System." (2014).

Katz, J and Y Lindell. Introduction to Modern Cryptography. CRC Press, 2007.

Litecoin Wiki. Comparison between Litecoin and Bitcoin. 22 January 2014. <https://litecoin.info/User:Iddo/Comparison_between_Litecoin_and_Bitcoin>.

Nakamoto, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. 31 October 2008. <http://nakamotoinstitute.org/bitcoin/>.

Percival, Colin. "Stronger Key Derivation Via Sequential Memory-Hard Functions.: (2009).

Perry, David. Bitcoin Mining in Plain English. 6 September 2012. <http://codinginmysleep.com/bitcoin-mining-in-plain-english/>.

Shirriff, Ken. Bitcoins the hard way: Using the raw Bitcoin protocol. < http://www.righto.com/2014/02/bitcoins- hard-way-using-raw-bitcoin.html>.

Southurst, Jon. Blockchain's SharedCoin Users Can Be Identified, Says Security Expert. 10 June 2014. <http://www.coindesk.com/blockchains-sharedcoin-users-can-identified-says-security-expert/>.

Acknowledgments

- Dr. Terry Fenger, MUFSC
- Lance Nudd, Stroz Friedberg
- Michael Younger, Stroz Friedberg
- John Shumway, Stroz Friedberg
- Dan Blank, Stroz Friedberg
- Chris Vance, MUFSC
- Dr. Pamela Staton, MUFSC
- Stroz Friedberg
- Marshall University