Forensic Investigation of Cryptocurrency Wallets on iOS and Android Mobile Devices

Angelica Montanez, B.S.[1]; Michael Younger, B.S.[2]; Christopher Vance, B.S.[3]; Terry Fenger, Ph.D.[1].
[1]Marshall University Forensic Science Center, 1401 Forensic Science Drive, Huntington, WV 25701
[2]Stroz Friedberg, LLC, 330 Second Avenue South, Suite 335, Minneapolis, MN 55401
[3]Syntricate, 333 South 520 West, Suite 160, Lindon, UT 84042

Abstract

Although the infamous “Silk Road”—described by some as a black-market Amazon or eBay—was shut down by the FBI in late 2013, cryptocurrencies are still being used in illegal transactions. The purpose of this research was to examine popular wallet applications for the cryptocurrencies Bitcoin, Litecoin, and Darkcoin on mobile devices for potential forensic artifacts. Using various forensic extraction tools, the data generated from controlled trading was extracted from iOS and Android devices, and analyzed for any data that could potentially link a cryptocurrency wallet, whether active or deleted, to a specific device or person.

The results of this research demonstrated that the selected extraction devices successfully harvested data indicating active cryptocurrency wallet application presence on both the iOS and Android devices, but past wallet indicators and transaction information were extracted only from the Android devices.

As their use no doubt increases in the coming years, it is important for those in law enforcement and forensics to be familiar with systems of digital currency. The results of this research may serve to aid law enforcement in connecting unlawful transactions involving cryptocurrency wallets on Android devices to implicated individual(s) and devices. Further research is still needed to discover a more reliable method for extracting cryptographic wallet data from iOS devices.

Introduction

In this research, the cryptocurrency systems of interest are Bitcoin, Litecoin, and Darkcoin. Because digital currency systems have become affiliated with illegal activities, it is necessary for them to be forensically researched. Digital forensics is predominantly concerned with user-generated data—to search for signs of user activity amid the software and memory of digital devices. While many studies have been made into the de-anonymization of a currency’s public transaction ledger, less has been done to investigate the electronic wallets that users download to hold their coins. Since an electronic wallet is, for many, the main access point into a cryptocurrency transaction network, a user’s electronic cryptocurrency wallet should be an ample store for user-generated data.

The theory driving this research is that, as a digital system, a cryptographic wallet will leave artifacts related to its presence and activity in the memory of a mobile device that can be found after forensic investigation. The work here will essentially be a discovery procedure to investigate the potential wealth of user information generated by the existence of cryptocurrency wallet software on iOS and Android mobile devices. Since an electronic wallet is, for many, the prominent access point into the cryptocurrency’s transaction network, a user’s electronic cryptocurrency wallet should be an ample store for user-generated data.

To begin, a user installs the open-source cryptocurrency client—an electronic wallet—onto his computer or mobile device to manage his account. Through a wallet, a user is able to receive, store, and send coins. Besides holding a user’s coins, this encrypted wallet stores a user’s set(s) of private and public key pairs. When a user sends coins from his wallet, his unique secret signing key (private key) is used to generate a hash composed of past and future transaction information. This first hash is the sender’s digital signature. Because each transaction includes a reference to the previous one, the sequence of transactions forms a chain.

The coin transaction is next combined with the public key of the receiver to ensure it can only be opened by the receiver. Finally, the bundle is cryptographically hashed a second time into what becomes a new block, which is broadcast to the entire network. This process of generating a block, or transaction, is pictographically summarized in Figure 1.

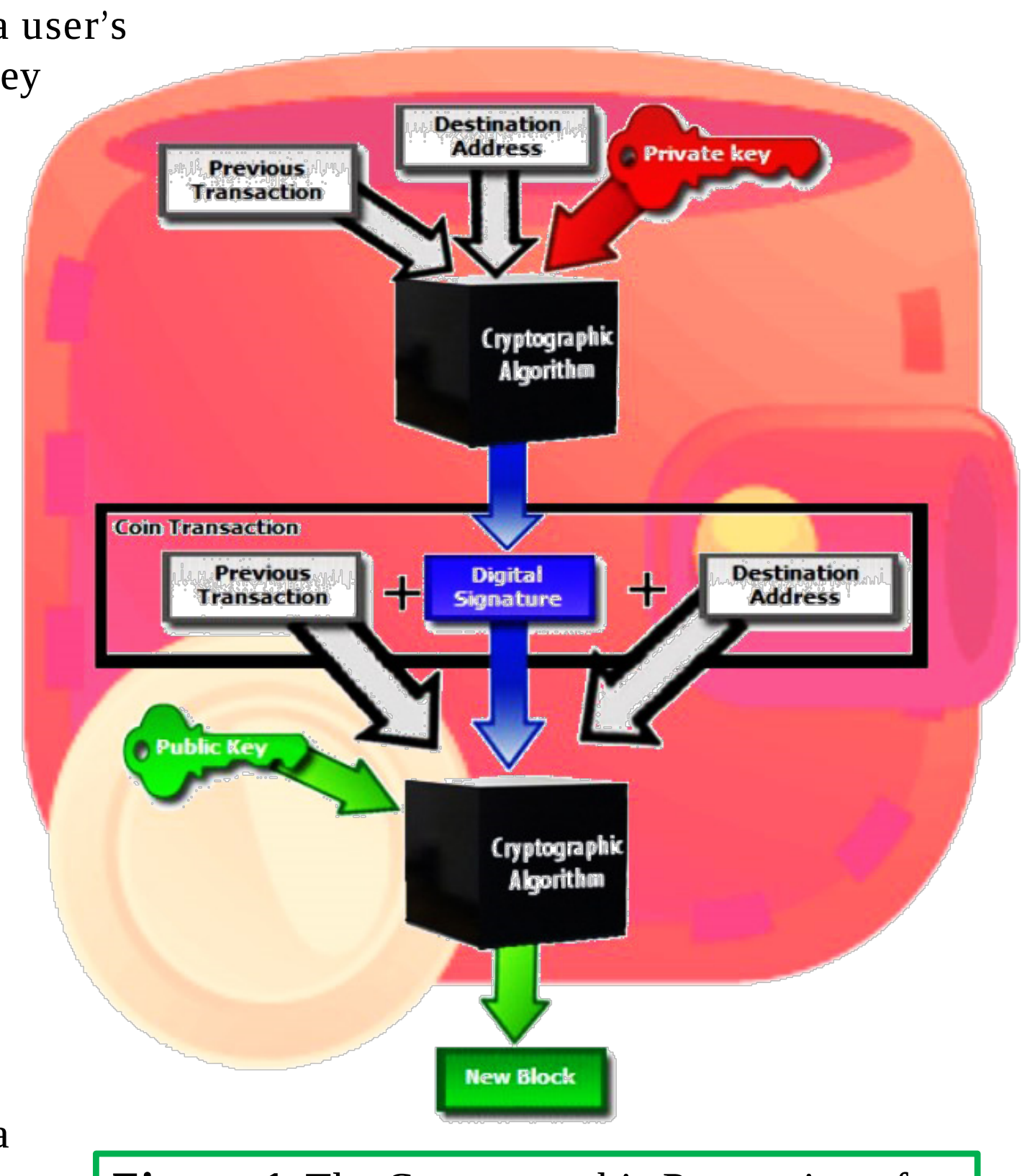


Figure 1. The Cryptographic Processing of a Bitcoin Transaction (red denotes sender components and green denotes receiver).

To ensure that a coin is legitimate in terms of ownership, a block must be verified against the public ledger. In order for the block to be confirmed, the current end of the transaction chain in the submitted coins must point to the sender as the rightful, current owner. If the validation process is successful, the block is created and then broadcast to the network so that the public ledger can be updated. Finally, the payment is permitted to pass on into the receiver’s wallet.

Materials and Methods

Stage 1: Fresh

- A physical iPhone 4S (iOS 7.1.1) and a physical Samsung Galaxy S4 (Android 4.4.2) were reset to factory settings.
- Genymotion and Oracle VM VirtualBox were used to create two Samsung Galaxy S4 virtual devices running Android 4.4.2.
- After successful resetting, the iOS device was imaged using Cellebrite Universal Forensic Extraction Device (UFED) Physical Analyzer and iFunBox.
- After successful installation, the physical Android device was imaged using Cellebrite UFED Touch Ultimate, while the virtual Android devices were imaged using the Android Debug Bridge (ADB) pull command-line tool.
- Images were saved onto a Seagate Barracuda 1 Terabyte Hard Drive.

Stage 2: Installation

- From the Apple App Store, the following wallet applications were installed onto the iOS device: bitWallet and CoinPocket.
- From the Google Play Store, the following wallet applications were installed onto the physical Android device: Bitcoin Wallet, Hive Bitcoin Wallet, Litecoin Wallet, and Darkcoin Wallet (beta).
- From the third-party Android application packet (APK) downloader apps.evozi.com, the above four Android wallet applications were downloaded and installed onto the virtual Android devices.
- After each wallet application was opened once, all devices were imaged.

Stage 3: Trading

- Trading occurred over a private wireless Internet connection.
- Trades were made between a known user running desktop wallet applications, the physical devices, the physical and virtual devices, and exclusively the virtual devices.
- Each wallet was subjected to at least two received and two sent transactions.
- Once all trades were completed, all devices were imaged.

Stage 4: Deletion

- Once all necessary trades were complete, each wallet was emptied.
- All wallet applications were uninstalled from the devices.
- After successful deletion of the wallet apps, all devices were imaged.

Analysis

- To analyze both the iOS and Android devices, the following tools were used: UFED Physical Analyzer, iFunBox (iOS only), Notepad++, and Database (DB) Browser for SQLite.

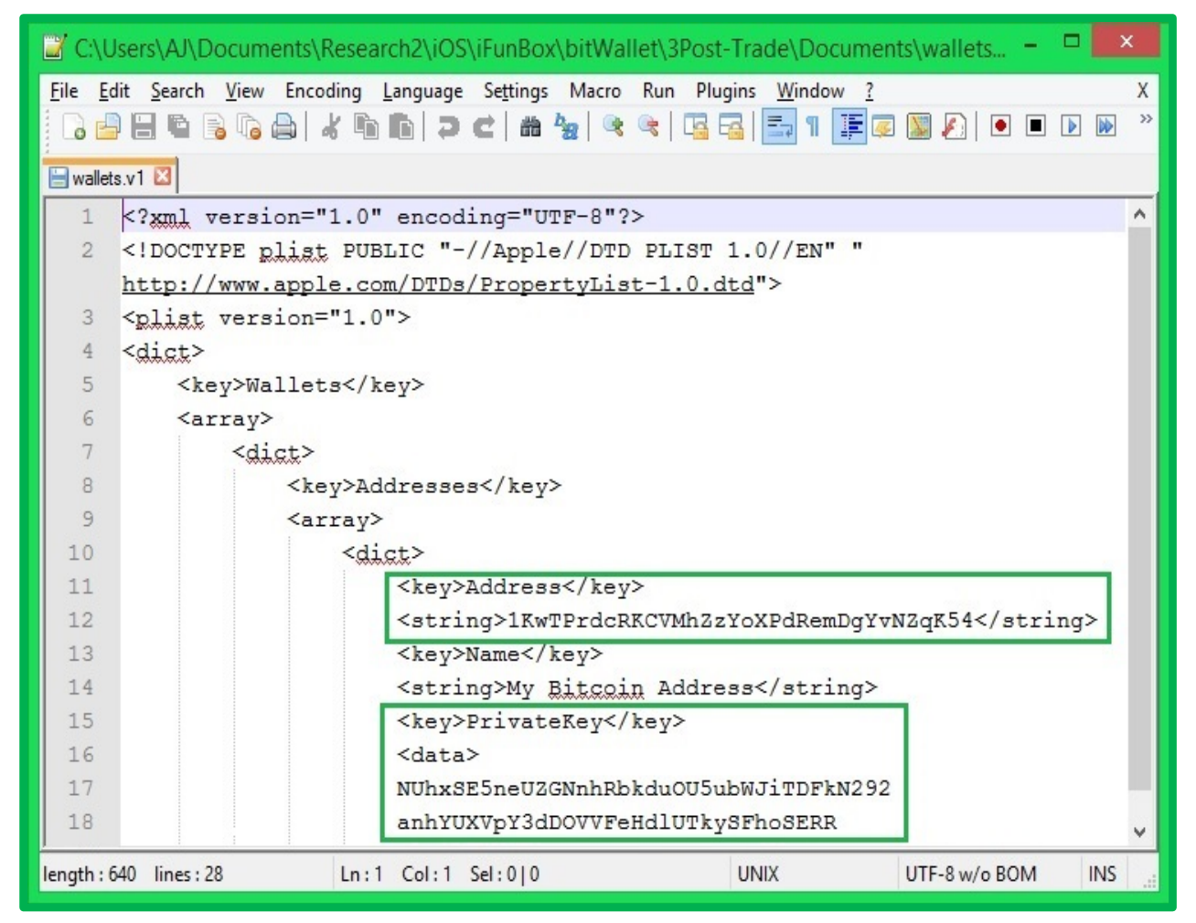
iOS Results

UFED Physical Analyzer

- All wallet application names and their app identifiers were extracted when the apps were active on the device.
- Property list, or “plist,” files for the CoinPocket application were extracted when the app was active on the device. These files contained congruent Created, Last Modified, Last Accessed date and time stamps for the app.
- Two active database files with the CoinPocket Identifier were extracted; however, neither database contained relevant data.

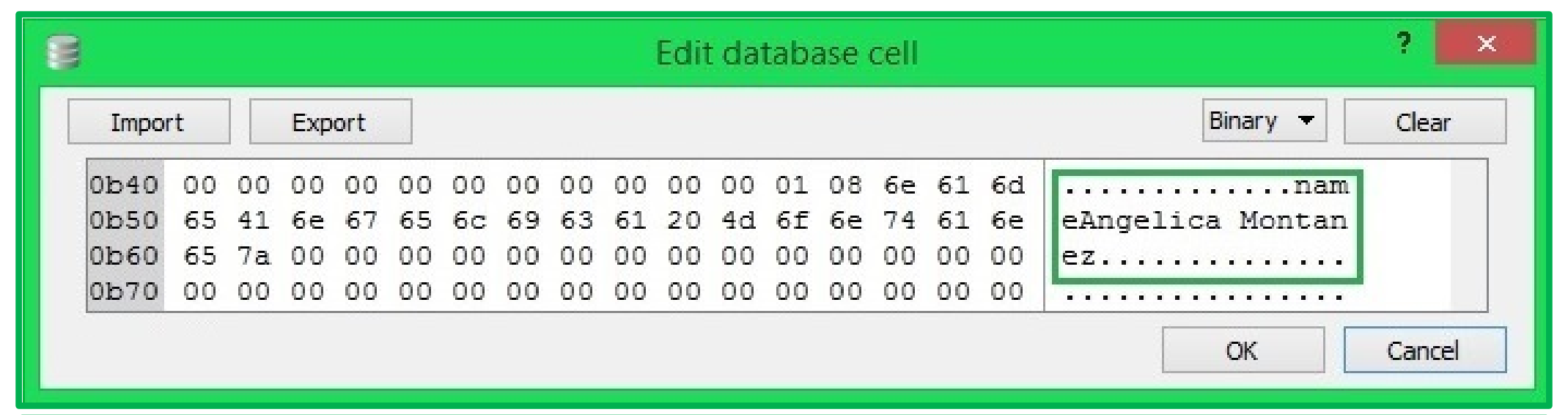
iFunBox:

- The alerts.file extracted from the active bitWallet application folder contained the wallet’s public key.
- The wallets.v1 file extracted from the active bitWallet application folder contained both the wallet’s public and private keys.
- The downloads.28.sqlitedb file extracted from the raw file system contained wallet app identifiers and the full iTunes name under which the app was downloaded in all stages after installation.


C:\Users\AJ\Documents\Research2\iOS\iFunBox\bitWallet\3Post-Trade\Documents\wallets...
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
wallets.v1
length : 640 lines : 28 Ln : 1 Col : 1 Sel : 0 | 0 UNIX UTF-8 w/o BOM INS

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "
http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>Wallets</key>
    <array>
        <dict>
            <key>Addresses</key>
            <array>
                <dict>
                    <key>Address</key>
                    <string>1KwTPrdcRKCVMhZzYoXPdRemDgYvNZqK54</string>
                    <key>Name</key>
                    <string>My Bitcoin Address</string>
                    <key>PrivateKey</key>
                    <data>
                    NUhxSE5neUZGNnhRbkduOU5ubWJiTDFkN292
                    anhYUXVpY3dDOVVFeHdlUTkySFhoSERR
```

Figure 2. Content of the wallet.v1 file extracted by iFunBox from the bitWallet folder, including the public and private keys (boxed).



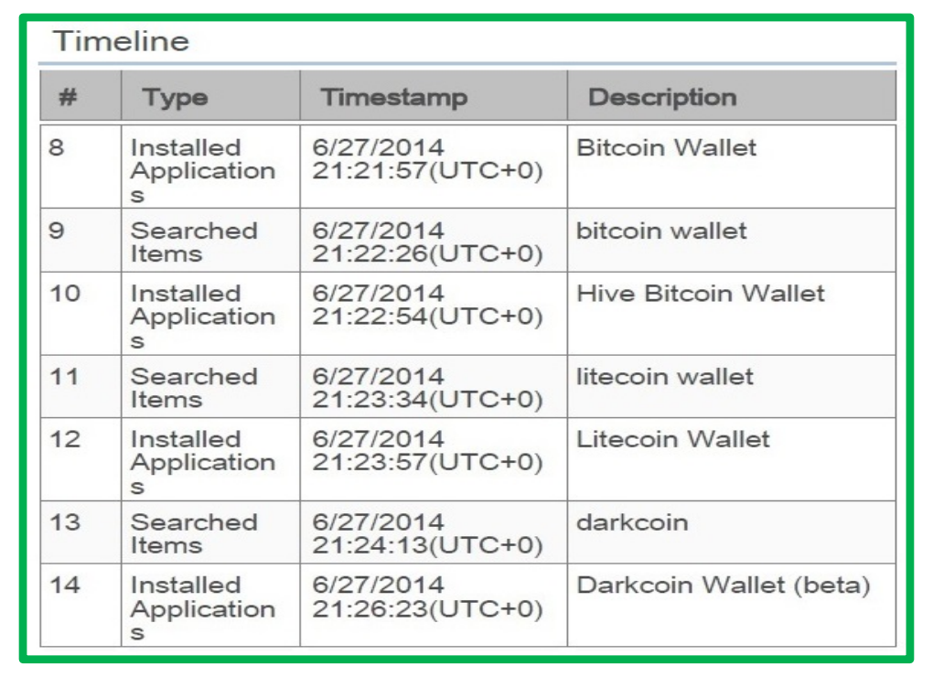
```
0b40  00 00 00 00 00 00 00 00 00 00 00 01 08 6e 61 6d  .............nam
0b50  65 41 6e 67 65 6c 69 63 61 20 4d 6f 6e 74 61 6e  eAngelica Montan
0b60  65 7a 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ez..............
0b70  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Figure 3. iTunes Name (boxed) in the Hex Value Interpreter for a data cell in the Purchase table of the extracted downloads.28.sqlitedb file.

Android Results

UFED Physical Analyzer (Physical Device):

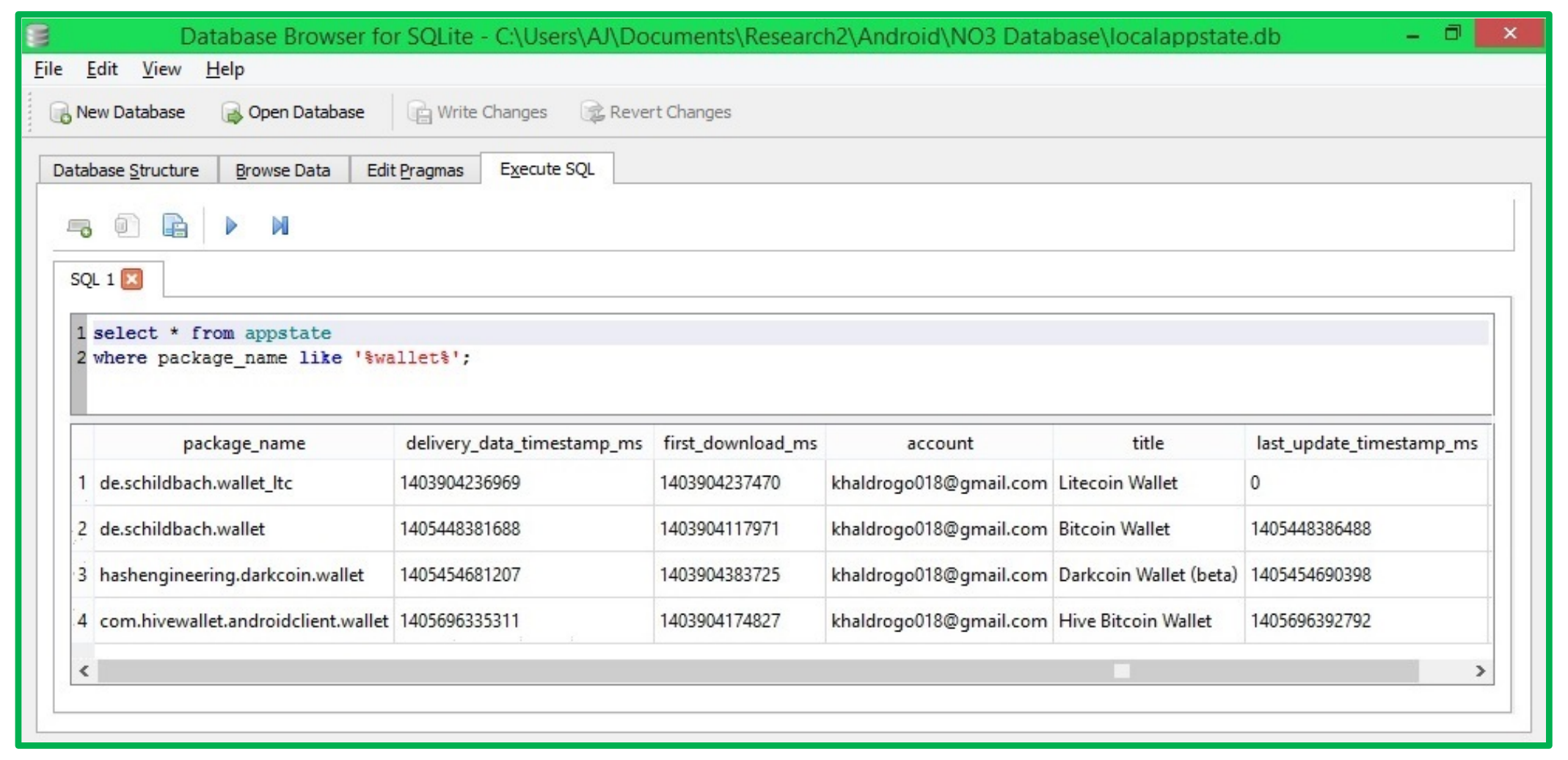
- All wallet application names and their app identifiers were extracted in all stages after installation.
- Two database files, Launcher.db and Localappstate.db, were extracted which contained tables listing the wallet app identifiers, download timestamps for the apps, the most recent app data delivery timestamps, and the user account linked to the apps’ downloads.
- A Timeline listing action events relating to the installation of the wallet apps and the search query made in the Play Store for the apps, as well as the timestamps for each action, was extracted in all stages after installation.



Timeline

#	Type	Timestamp	Description
8	Installed Application s	6/27/2014 21:21:57(UTC+0)	Bitcoin Wallet
9	Searched Items	6/27/2014 21:22:26(UTC+0)	bitcoin wallet
10	Installed Application s	6/27/2014 21:22:54(UTC+0)	Hive Bitcoin Wallet
11	Searched Items	6/27/2014 21:23:34(UTC+0)	litecoin wallet
12	Installed Application s	6/27/2014 21:23:57(UTC+0)	Litecoin Wallet
13	Searched Items	6/27/2014 21:24:13(UTC+0)	darkcoin
14	Installed Application s	6/27/2014 21:26:23(UTC+0)	Darkcoin Wallet (beta)

Figure 3. Timeline data table entries for the four cryptocurrency wallets from the UFED Touch Extraction of the Android device.



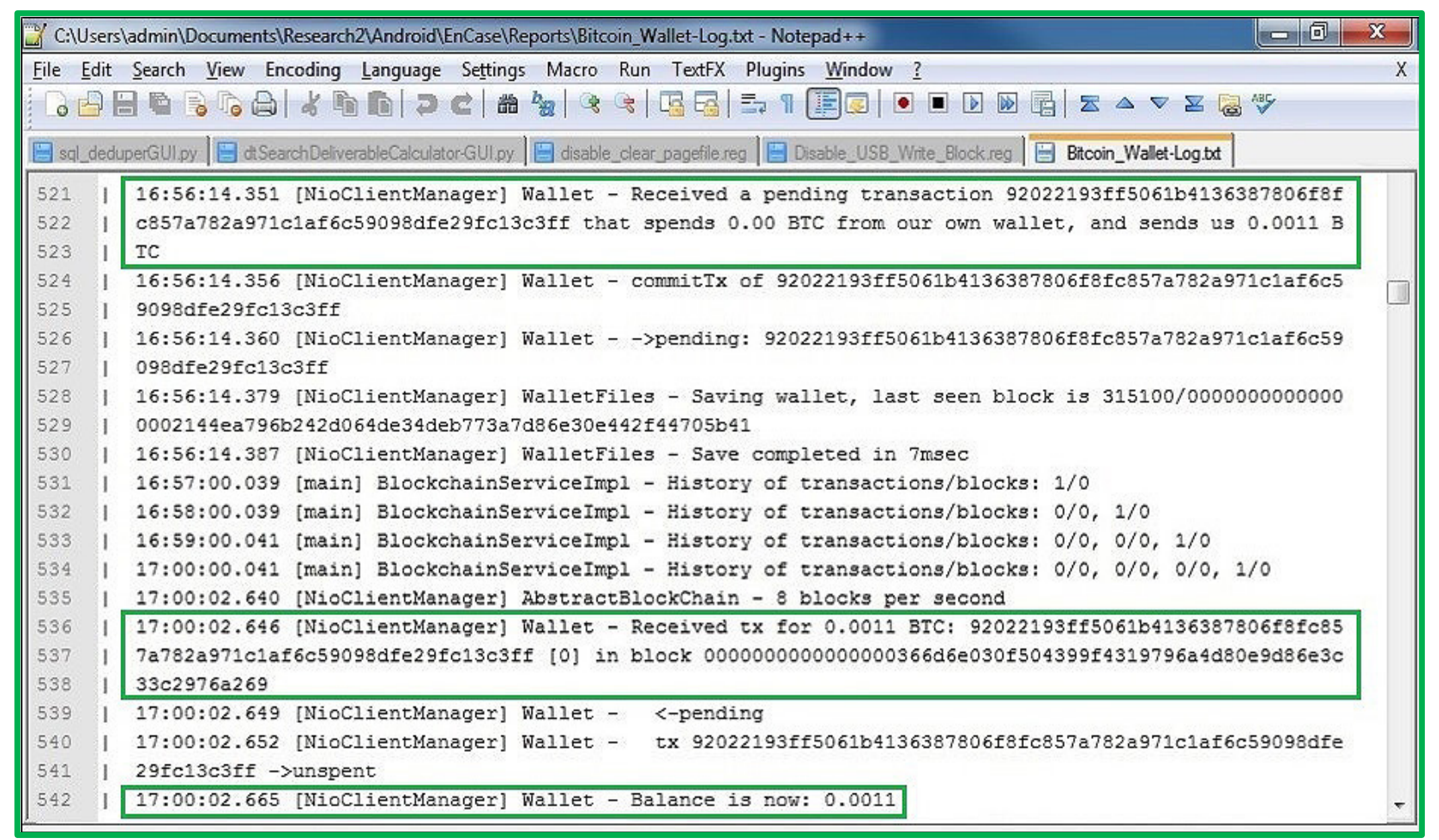
```
select * from appstate
where package_name like '%wallet%';
```

	package_name	delivery_data_timestamp_ms	first_download_ms	account	title	last_update_timestamp_ms
1	de.schildbach.wallet_ltc	1403904236969	1403904237470	khaldrogo018@gmail.com	Litecoin Wallet	0
2	de.schildbach.wallet	1405448381688	1403904117971	khaldrogo018@gmail.com	Bitcoin Wallet	1405448386488
3	hashengineering.darkcoin.wallet	1405454681207	1403904383725	khaldrogo018@gmail.com	Darkcoin Wallet (beta)	1405454690398
4	com.hivewallet.androidclient.wallet	1405696335311	1403904174827	khaldrogo018@gmail.com	Hive Bitcoin Wallet	1405696392792

Figure 4. Appstate table in DB Browser of LocalAppSate Database file from the UFED Touch Extraction of the Android device.

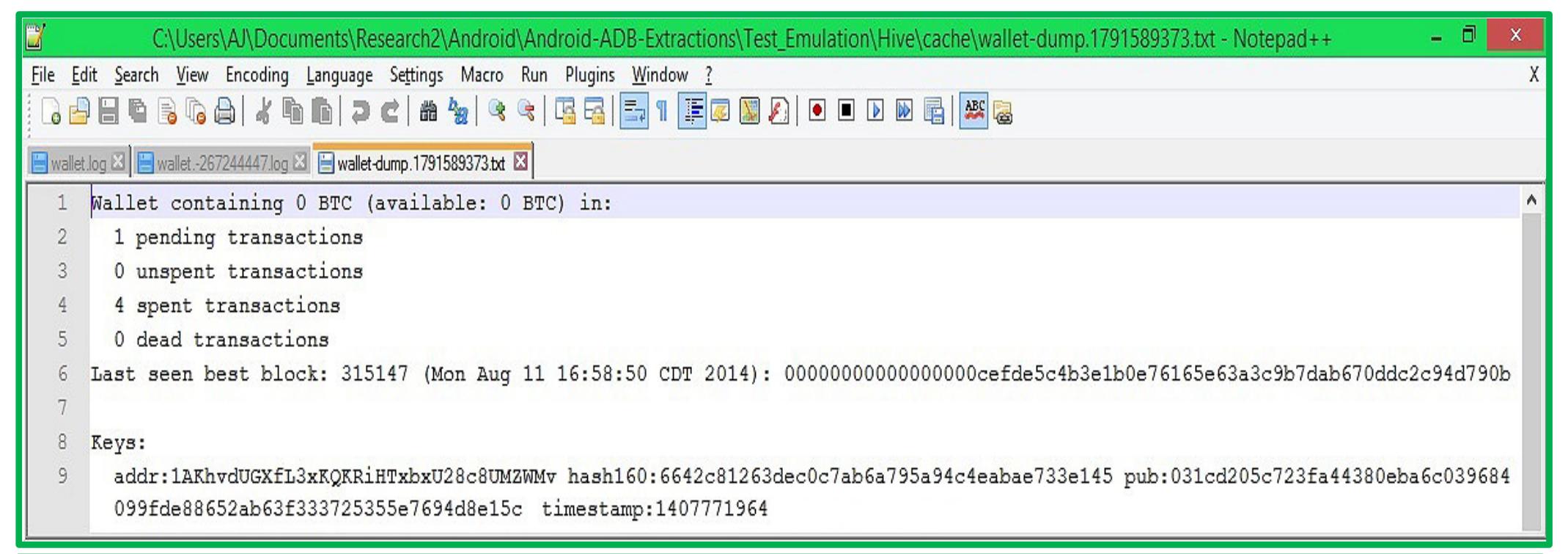
Android Debug Bridge (ADB) Tools (Virtual Device):

- A wallet.log file was extracted for each of the four wallet apps when the apps were active on the device.
- For the Hive Wallet, two additional wallet log files were extracted: Wallet.-267244447.log and Wallet-dump.1791589373.txt.
- For the Litecoin Wallet, a file was extracted that contained a privacy protection warning to the user, the private key for the wallet, and the creation timestamp of the wallet.
- From the all-application extraction, two database files of relevance were found, Downloads.db and External.db, which contained the wallet app identifiers, the source URL of the APK downloads, and the download timestamps.


C:\Users\admin\Documents\Research2\Android\EnCase\Reports\Bitcoin_Wallet-Log.txt - Notepad++
File Edit Search View Encoding Language Settings Macro Run TextFX Plugins Window ?
sql_deduperGUI.py
dtSearchDeliverableCalculator-GUI.py
disable_clear_pagefile.reg
Disable_USB_Write_Block.reg
Bitcoin_Wallet-Log.txt

```
16:56:14.351 [NioClientManager] Wallet - Received a pending transaction 92022193ff5061b4136387806f8f
c857a782a971c1af6c59098dfe29fc13c3ff that spends 0.00 BTC from our own wallet, and sends us 0.0011 B
TC
16:56:14.356 [NioClientManager] Wallet - commitTx of 92022193ff5061b4136387806f8fc857a782a971c1af6c5
9098dfe29fc13c3ff
16:56:14.360 [NioClientManager] Wallet - ->pending: 92022193ff5061b4136387806f8fc857a782a971c1af6c59
098dfe29fc13c3ff
16:56:14.379 [NioClientManager] WalletFiles - Saving wallet, last seen block is 315100/0000000000000
0002144ea796b242d064de34deb773a7d86e30e442f44705b41
16:56:14.387 [NioClientManager] WalletFiles - Save completed in 7msec
16:57:00.039 [main] BlockchainServiceImpl - History of transactions/blocks: 1/0
16:58:00.039 [main] BlockchainServiceImpl - History of transactions/blocks: 0/0, 1/0
16:59:00.041 [main] BlockchainServiceImpl - History of transactions/blocks: 0/0, 0/0, 1/0
17:00:00.041 [main] BlockchainServiceImpl - History of transactions/blocks: 0/0, 0/0, 0/0, 1/0
17:00:02.640 [NioClientManager] AbstractBlockChain - 8 blocks per second
17:00:02.646 [NioClientManager] Wallet - Received tx for 0.0011 BTC: 92022193ff5061b4136387806f8fc85
7a782a971c1af6c59098dfe29fc13c3ff [0] in block 000000000000000366d6e030f504399f4319796a4d80e9d86e3c
33c2976a269
17:00:02.649 [NioClientManager] Wallet -   <-pending
17:00:02.652 [NioClientManager] Wallet -   tx 92022193ff5061b4136387806f8fc857a782a971c1af6c59098dfe
29fc13c3ff ->unspent
17:00:02.665 [NioClientManager] Wallet - Balance is now: 0.0011
```

Figure 5. Content of the wallet.log file extracted by ADB pull from the Bitcoin Wallet folder, including valuable data on transaction activity (boxed).


C:\Users\AJ\Documents\Research2\Android\Android-ADB-Extractions\Test_Emulation\Hive\cache\wallet-dump.1791589373.txt - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
wallet.log
wallet.-267244447.log
wallet-dump.1791589373.txt

```
Wallet containing 0 BTC (available: 0 BTC) in:
  1 pending transactions
  0 unspent transactions
  4 spent transactions
  0 dead transactions
Last seen best block: 315147 (Mon Aug 11 16:58:50 CDT 2014): 0000000000000000cefde5c4b3e1b0e76165e63a3c9b7dab670ddc2c94d790b

Keys:
  addr:1AKhvdUGXfL3xKQKRiHTxbxU28c8UMZWMv hash160:6642c81263dec0c7ab6a795a94c4eabae733e145 pub:031cd205c723fa44380eba6c039684
  099fde88652ab63f333725355e7694d8e15c  timestamp:1407771964
```

Figure 6. Content of the wallet-dump.1791589373.txt file in Notepad++ constituting Hive Wallet transaction summaries.

Conclusions

iOS Mobile Device

- UFED Physical Analyzer and iFunBox are tools capable of determining active wallet application presence on a mobile iOS device.
  - These tools, however, are unable to determine wallet presence after the apps have been deleted from the mobile device and to harvest any sort of transaction information.

Android Mobile Devices

- UFED Physical Analyzer is capable of determining past and present wallet application presence on an Android device; however, it harvests no transaction information.
- ADB pull is capable of extracting a wealth of transaction information from an Android device with an active wallet application.
  - ADB pull is capable of extracting information indicating present and past wallet presence, but only if the app was downloaded as an APK file.

Future Studies

- Investigation into an effective method of extraction of past wallet indicators and any transaction information from iOS devices.
- Investigation of the ADB pull tool on a physical Samsung Galaxy S4 Android device instead of an emulator.
- Perform these tests on Android devices running newer and older Android OS versions than 4.4.2.
- Perform these tests on Android devices other than a Samsung Galaxy S4.
- Investigation into an effective method of extracting transaction information from an Android device after wallet applications have been deleted.

References

Birukov, A., Khovratovich, D., and Ivan Pustogarov. 2014. Deanonymisation of clients in Bitcoin P2P network. arXiv preprint arXiv:1405.7418. Retrieved from *http://arxiv.org/pdf/1405.7418.pdf*.

Bitcoin Developer Guide. [Internet]. Bitcoin Project. 2009 [cited 2014 October19]. Retrieved from *https://bitcoin.org/en/developer-guide#full-node*.

de la Porte, Lodewijk André. 2012. The Bitcoin transaction system. Utrecht. Netherlands.

Duffield, Evan and Kyle Hagan. 2014. Darkcoin: PeertoPeer CryptoCurrency with Anonymous Blockchain Transactions and an Improved ProofofWork System. Retrieved from *http://www.darkcoin.io/downloads/DarkcoinWhitepaper.pdf*.

How to Set Up a Wallet. [Internet]. BTC Gear. 2013 [cited 2014 July 9]. Retrieved from *http://bitcoinsimplified.org/get-started/how-to-set-up-a-wallet/*.

Intent | Android Developers. [Internet]. Android. [cited 2014 October 15]. Retrieved from *http://developer.android.com/reference/android/content/Intent.html*.

Litecoin. [Internet]. Wikipedia. 2014 [cited 2014 July 02]. Retrieved from *http://en.wikipedia.org/wiki/Litecoin*.

Luther, William J. 2013. Cryptocurrencies, Network Effects, and Switching Costs. Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, forthcoming. Retrieved from *https://papers.ssrn.com/sol3/papers.cfm*.

Main Page. [Internet]. Litecoin Wiki. 2011 [cited 2014 July 02]. Retrieved from *https://litecoin.info/*.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., and Stefan Savage. 2013. A fistful of bitcoins: characterizing payments among men with no names. Proceedings of the 2013 conference on Internet measurement conference (pp. 127-140). ACM.

Nakamoto, Satoshi. 2008. Bitcoin: A peer-to-peer electronic cash system. Retrieved from *https://bitcoin.org/bitcoin.pdf*.

Sprankel, Simon. 2013. Technical Basis of Digital Currencies. Retrieved from *http://www.coderblog.de/wp-content/uploads/technical-basis-of-digital-currencies.pdf*.

Virtual Currency: Bitcoin and Beyond, Part 1. [Internet]. Virtual Currency: Bitcoin and Beyond, Part 1. 2014 [cited 2014 July 10]. CIO Journal. Retrieved from *http://deloitte.wsj.com/cio/2014/06/24/understanding-virtual-currency-bitcoin-and-beyond-part-1/?mod=wsjcio_hp_deloitte*.

What Is Darkcoin? [Internet]. Darkcoin. 2014 [cited 2014 June 30]. Retrieved from *http://www.darkcoin.io/intro.html*.

Acknowledgments

The author thanks Michael Younger and Breandan Gleason from Stroz Friedberg LLC, Terry Fenger, PhD, from the Department of Forensic Science at Marshall University, and Christopher Vance from Access Data, Inc. for their insight, guidance, and mentorship during this research project.