Bitcoin Forensics

BITCOIN FORENSICS

Haider M. al-Khateeb & Saleh Al Himali investigate Bitcoin Remnants.

/ ADVANCED

Bitcoins were introduced to the financial market as the first decentralised digital currency in January 2009. It offered an alternative currency to money since its inception and distribution. Bitcoin uses cryptographic techniques to verify funds transfer in isolation of a central bank. As the model is based on a peer-to-peer architecture, participants have the privilege of facilitating unsupervised payments. This has attracted criminals because the integrated level of anonymity in the Bitcoins network makes it an essential component to complement online black markets accessible via the Tor network. The Tor network is another peer-to-peer environment and is considered as a Privacy Enhancement Technology (PET).

While the Tor network provides many advantages to online users, it has also acted as a backbone to the darkweb where drugs, child pornography, weapons and other illegal-services are being sold. Likewise, while Bitcoin may be used to buy coffee in some of London's coffee bars or exchanges for cash in Pound Sterling using a Bitcoin ATM, it's more widely used in the darkweb. Between 2014 and 2015, several raids by law-enforcement took place on the Silk Road (a famous darkweb market) and this resulted in an immediate negative impact on the value of the Bitcoin. It is worth noting that the Silk Road (v 1.0), which was first, launched in 2011 and usually referred to, as the first modern darknet market is responsible for transactions estimated in Billions of US Dollars. Currently, and despite multiple attempts by the FBI and Europol, Silk Road 3.0 is online. Nonetheless, many outlaw groups started laundering stolen money using Xmixer, a technology to facilitate trust-less mixing of transactions. It enables users to share transactions with each other that makes the work of a digital investigator tracing the origin of a given transaction much more difficult. Moreover, multiple reports recovered evidence that terrorist groups such as the Islamic State of Iraq and Syria (ISIS) sold goods in their possessions including oil (from oil fields under their control) to fund their operations, and they have used cryptocurrencies (Bitcoin) to transfer money. The discussion so far demonstrates the essential need to have better understanding and more techniques for Bitcoin related digital investigations.

/ TRACEABILITY IN THE BITCOIN NETWORK

Earlier attempts to investigate the identification and traceability of Bitcoin related artefacts found it extremely difficult to reveal the identity of the user. However, this of course depends on multiple factors, it is inevitable to state the obvious and say that in the case of seized devices, the discovery of data remnants related to the user of a Bitcoin wallet could be utilised to recover their identity. Likewise, the behaviour of a 'non-careful' user could recover more evidence to crosscheck their activities. For instance, authorised investigation incorporating help from an Internet Service Provider (ISP) could be effective to map transactions from certain parties (e.g. the Silk Road) to users believed to be customers [1]. Further, scientific tools utilising mathematics, graph theory and statistical models have been used successfully to detect fraud in Bitcoins transactions. More work may be carried out in this area to build intelligence about the Bitcoin Block Chain (a public ledger that records all Bitcoin transactions).

/ EXCHANGING BITCOIN IS VAT FREE

While some countries have made determinations as to the legal status and purpose of bitcoins with regards to which legislation to impose, others have disregarded bitcoin transactions totally and see no need for governance or directives at this time. Bitcoins has not been authorised as a legal currency acceptable by governments because there could be tax evasion and other illegal transactions. However, it is an ongoing payments method for transactions equivalent to money, and companies like Wordpress and Wikipedia accepts Bitcoin. Her Majesty Revenue and Customs (HMRC) in UK acknowledges the existence of Bitcoin but there is no demand for taxpayers to pay Value Added Tax (VAT) on Bitcoin unless received for the provision of goods or services (Revenue and Customs Brief 9/2014: Bitcoin and Other Cryptocurrencies). The European Court of Justice has declared that purchasing Bitcoin is exempt from VAT, giving a huge boost to its potential. The New York State Department of Financial Services (NYSDFS) has put in place BitLicense for virtual currency business, which only applies to residents of New York.

/ A BITCOIN WALLET ADDRESS

It is a 26-35 case-sensitive alphanumeric string, but most of them are 33 or 34. The address in our article starts with the numerical number '1' because it was created with the Pay-to-PubkeyHash (P2PKH), otherwise addresses would start with '3' when they are generated using another method called Pay-to-Script-Hash (P2SH).

Bitcoin addresses may be generated offline, they are considered as a single-use token since new ones are generate prior to every transaction and this maintains a level of anonymity. They are used to receive payments but it is important to appreciate that the Bitcoin system, unlike emails, has no concept of a 'From' address field. However, even with emails, we are quite familiar with the challenges of verifying the actual owner of an email address.

“THE BITCOIN MODEL WORKS WELL FOR USERS WHO VALUE THEIR PRIVACY BUT CAUSES PROBLEMS FOR AUTHORITIES WHO MAY WISH TO PURSUE ILLEGAL ACTIVITIES FINANCED THROUGH BITCOIN TRANSACTIONS.”

The husband and wife team of Philip and Diana Koshy built their own version of software to join the Bitcoin network in 2014 [2]. However, it was intentionally built with a feature to download a copy of all packets transmitted in the Bitcoin network in real-time. This has helped to observe that when a client-computer sends information about only one single transaction, then it could be perceived that the user at a particular IP address is also the owner of that Bitcoin address. This approach worked because of the lack of ‘perfectly balanced’ flow of data and top-down coordination for the Bitcoin network. Furthermore, a team of researchers from the Computer Science department at the University of California, San Diego conducted an investigation to characterise longitudinal changes in the Bitcoin market. They were able to cluster addresses belonging to the same user and performing a labelling process on transactions, link them to specific institutions. Empirical interactions from their experiments helped to identify multiple services to support the labelling process, and this was based on a relatively small number of transactions [3].

/ TOP FACT

Bitcoin transactions operate on a ‘transaction known/parties unknown’ model and logs transactions on to a Block Chain, which creates a chain of ownership that is public, but the user details are not directly tied to the Bitcoin address that gets recorded and therefore keeps the user pseudo anonymous.

/ SEARCHING FOR SOFTWARE REMNANTS

Investigating remnants left by Bitcoin Wallets could help answering any of the following questions about a seized device:

- Was a Bitcoin wallet used on this system?
- Can the use of Bitcoin be associated to a local username? If yes, can a Wallet Address be associated with a specific user?
- Can we recover past events if a Bitcoin wallet was used, but uninstalled prior to the seizure of the device?

There are many Bitcoin wallets in the market place such as MultiBit HD, Armory, mSIGNA, Bitpay, Bither and Electrum. Each application is a unique project that requires separate forensic documentations to facilitate the work of a digital investigator and reduce the overall investigation time; this is the main purpose of this ongoing study. For this article however, and as a proof of concept, we will only reflect on Bither (https://bither.net/), it is a suitable Bitcoin Wallet for this demonstration since it may be installed on various recent versions of Windows, Linux, Android and iOS. This should help identifying any distinctive behaviour related to the environment (Operating System) in which the wallet is installed and used.

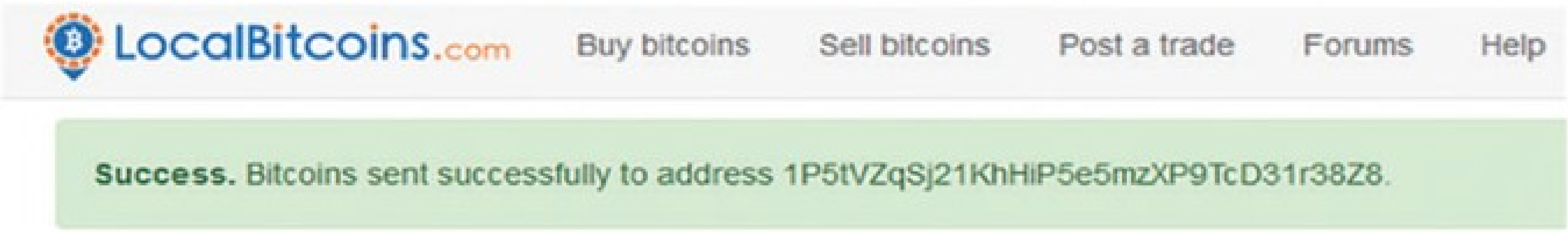
An investigation of this nature requires a solid methodology, we have adopted the Computer Forensics and Investigation Methodology which contains eight steps: verification, system description, evidence acquisition, timeline analysis, media and artefact analysis, string or byte search, data recovery, and finally concludes with reporting of results.

A suitable toolkit was defined for this cross-platform investigation, examples to what were needed include a virtual environment (VMware Workstation), OSForensic, EnCase Forensic, Process monitor, RegShot, iTunes, iPhone Analyzer, in addition to preinstalled packages in the SANS Investigation Forensic Toolkit (SIFT). Further, the mobile platforms had to be rooted in order to apply our procedure.

Multiple experiments were conducted repeatedly to cover the intended platforms, and the high-level procedure can be generalised to the following steps:

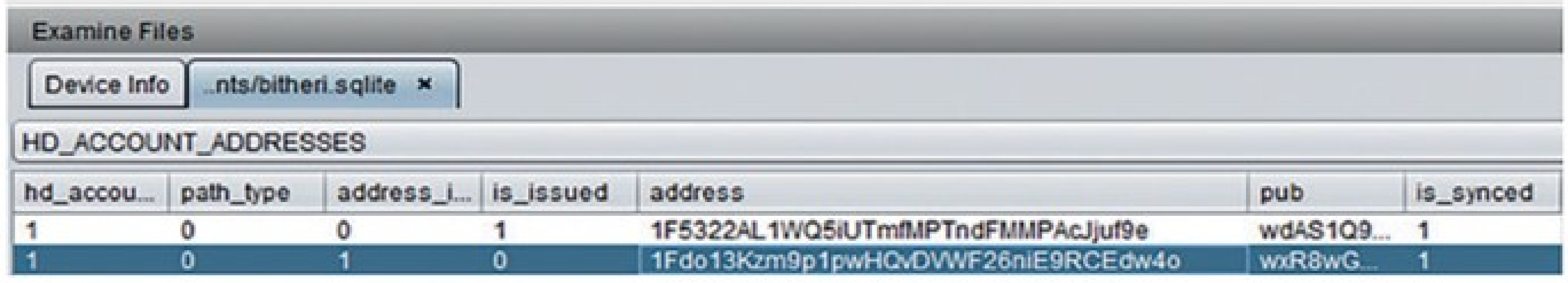
/ BITCOIN WALLETS ARE NOT ALL DIGITAL

Most Bitcoin wallets are computer-based. Some are Desktop Wallets and can be installed on Windows, Linux or OS X. Others are Mobile based or simply online (web-based), while users may be completely offline using 'Paper Wallet'. It is therefore an option to be considered when searching for Bitcoins as part of an investigation. A Bitcoin paper wallet is a document containing all the data required to generate a digital wallet, which includes the private keys and Bitcoin addresses.



Success. Bitcoins sent successfully to address 1P5tVZqSj21KhHiP5e5mzXP9TcD31r38Z8.

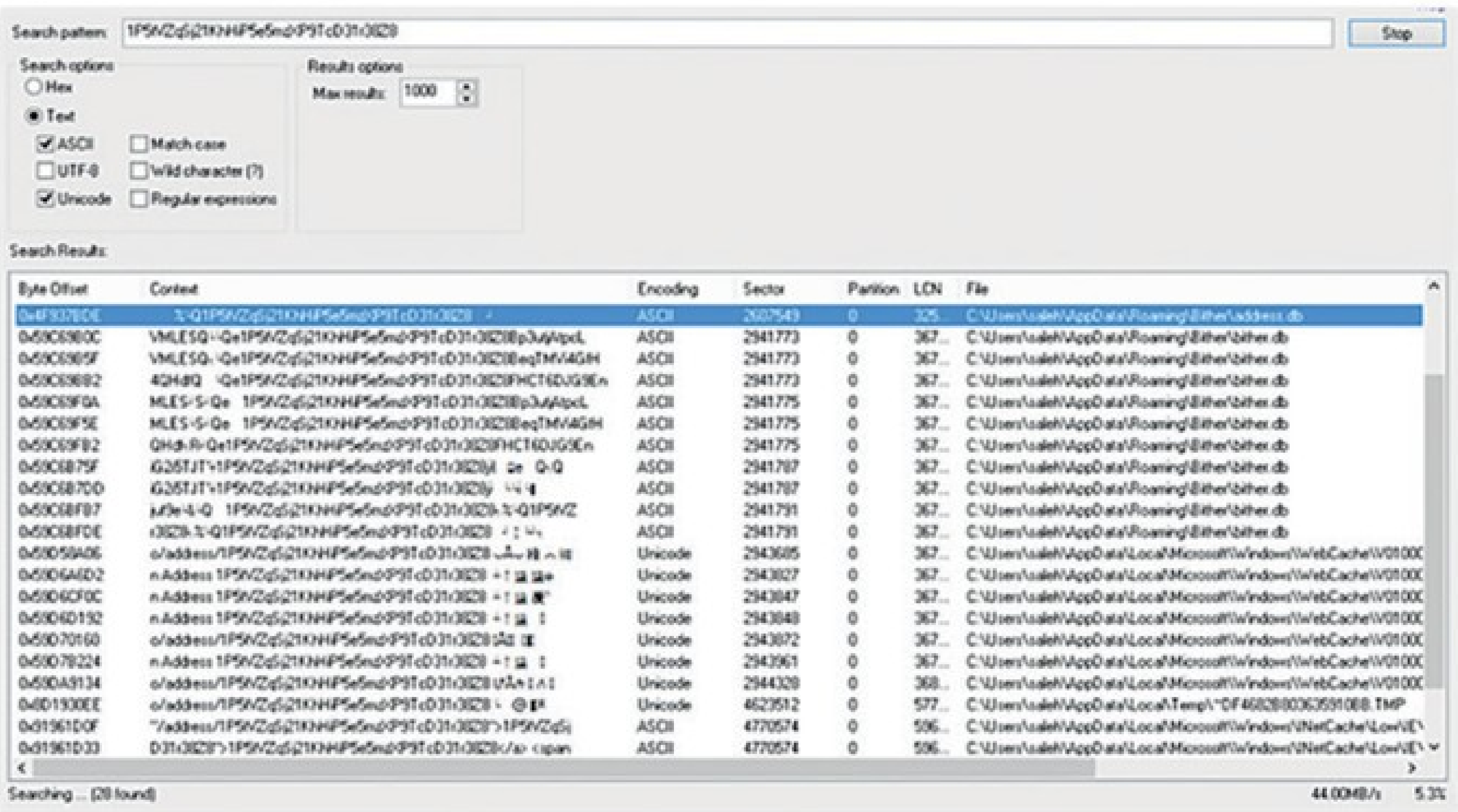
Figure 1. Transferring Bitcoin to the Bither Wallet



HD_ACCOUNT_ADDRESSES

hd_accou...	path_type	address_i...	is_issued	address	pub	is_synced
1	0	0	1	1F5322AL1WQ5iUTmfMPTndFMMPAcJjuf9e	wdAS1Q9...	1
1	0	1	0	1Fdo13Kzm9p1pwHQvDVWF26niE9RCEdw4o	wxR8wG...	1

Figure 3. Bitcoin Sender Address



Search pattern: 1P5tVZqSj21KhHiP5e5mzXP9TcD31r38Z8

Search options
○ Hex
● Text
☑ ASCII ☐ Match case
☐ UTF-8 ☐ Wild character (?)
☑ Unicode ☐ Regular expressions

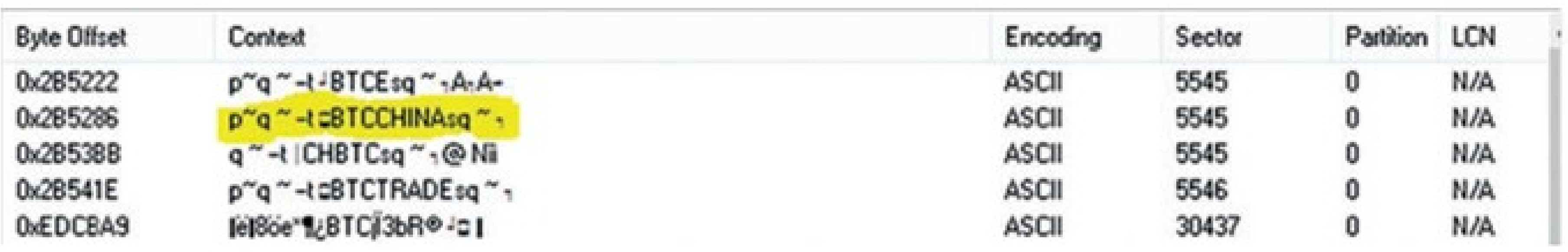
Results options
Max results: 1000

Search Results:

Byte Offset	Context	Encoding	Sector	Partition	LCN	File
0x4F937BDE	¾·Q1P5tVZqSj21KhHiP5e5mzXP9TcD31r38Z8	ASCII	2607549	0	325...	C:\Users\saleh\AppData\Roaming\Bither\address.db
0x59C6980C	VMLESQ·-Qe1P5tVZqSj21KhHiP5e5mzXP9TcD31r38Z8Bp3uAlpcL	ASCII	2941773	0	367...	C:\Users\saleh\AppData\Roaming\Bither\bither.db
0x59C6985F	VMLESQ·-Qe1P5tVZqSj21KhHiP5e5mzXP9TcD31r38Z8BeqTMV4GiH	ASCII	2941773	0	367...	C:\Users\saleh\AppData\Roaming\Bither\bither.db
0x59C69882	4QHdlQ ·Qe1P5tVZqSj21KhHiP5e5mzXP9TcD31r38Z8FHCT6DJG9En	ASCII	2941773	0	367...	C:\Users\saleh\AppData\Roaming\Bither\bither.db
0x59C69F0A	MLES·S·Qe 1P5tVZqSj21KhHiP5e5mzXP9TcD31r38Z8Bp3uAlpcL	ASCII	2941775	0	367...	C:\Users\saleh\AppData\Roaming\Bither\bither.db
0x59C69F5E	MLES·S·Qe 1P5tVZqSj21KhHiP5e5mzXP9TcD31r38Z8BeqTMV4GiH	ASCII	2941775	0	367...	C:\Users\saleh\AppData\Roaming\Bither\bither.db
0x59C69F82	QHdt·R·Qe1P5tVZqSj21KhHiP5e5mzXP9TcD31r38Z8FHCT6DJG9En	ASCII	2941775	0	367...	C:\Users\saleh\AppData\Roaming\Bither\bither.db
0x59C6875F	iG26TJT'•1P5tVZqSj21KhHiP5e5mzXP9TcD31r38Z8jM Q·Q	ASCII	2941787	0	367...	C:\Users\saleh\AppData\Roaming\Bither\bither.db
0x59C687DD	iG26TJT'•1P5tVZqSj21KhHiP5e5mzXP9TcD31r38Z8y	ASCII	2941787	0	367...	C:\Users\saleh\AppData\Roaming\Bither\bither.db
0x59C68F87	µJ9e·¼·Q 1P5tVZqSj21KhHiP5e5mzXP9TcD31r38Z8·¾·Q1P5tVZ	ASCII	2941791	0	367...	C:\Users\saleh\AppData\Roaming\Bither\bither.db
0x59C68FDE	r38Z8·¾·Q1P5tVZqSj21KhHiP5e5mzXP9TcD31r38Z8	ASCII	2941791	0	367...	C:\Users\saleh\AppData\Roaming\Bither\bither.db
0x59D59A06	o/address/1P5tVZqSj21KhHiP5e5mzXP9TcD31r38Z8	Unicode	2943605	0	367...	C:\Users\saleh\AppData\Local\Microsoft\Windows\WebCache\V0100C
0x59D6A6D2	n Address 1P5tVZqSj21KhHiP5e5mzXP9TcD31r38Z8	Unicode	2943827	0	367...	C:\Users\saleh\AppData\Local\Microsoft\Windows\WebCache\V0100C
0x59D6CF0C	n Address 1P5tVZqSj21KhHiP5e5mzXP9TcD31r38Z8	Unicode	2943847	0	367...	C:\Users\saleh\AppData\Local\Microsoft\Windows\WebCache\V0100C
0x59D6D192	n Address 1P5tVZqSj21KhHiP5e5mzXP9TcD31r38Z8	Unicode	2943848	0	367...	C:\Users\saleh\AppData\Local\Microsoft\Windows\WebCache\V0100C
0x59D70160	o/address/1P5tVZqSj21KhHiP5e5mzXP9TcD31r38Z8	Unicode	2943872	0	367...	C:\Users\saleh\AppData\Local\Microsoft\Windows\WebCache\V0100C
0x59D78224	n Address 1P5tVZqSj21KhHiP5e5mzXP9TcD31r38Z8	Unicode	2943961	0	367...	C:\Users\saleh\AppData\Local\Microsoft\Windows\WebCache\V0100C
0x59DA9134	o/address/1P5tVZqSj21KhHiP5e5mzXP9TcD31r38Z8	Unicode	2944328	0	368...	C:\Users\saleh\AppData\Local\Microsoft\Windows\WebCache\V0100C
0x8D1930EE	o/address/1P5tVZqSj21KhHiP5e5mzXP9TcD31r38Z8	Unicode	4623512	0	577...	C:\Users\saleh\AppData\Local\Temp\~DF4682B0036359108B.TMP
0x91961D0F	"/address/1P5tVZqSj21KhHiP5e5mzXP9TcD31r38Z8">1P5tVZqSj	ASCII	4770574	0	596...	C:\Users\saleh\AppData\Local\Microsoft\Windows\INetCache\Low\IE\
0x91961D33	D31r38Z8">1P5tVZqSj21KhHiP5e5mzXP9TcD31r38Z8</a> <span	ASCII	4770574	0	596...	C:\Users\saleh\AppData\Local\Microsoft\Windows\INetCache\Low\IE\

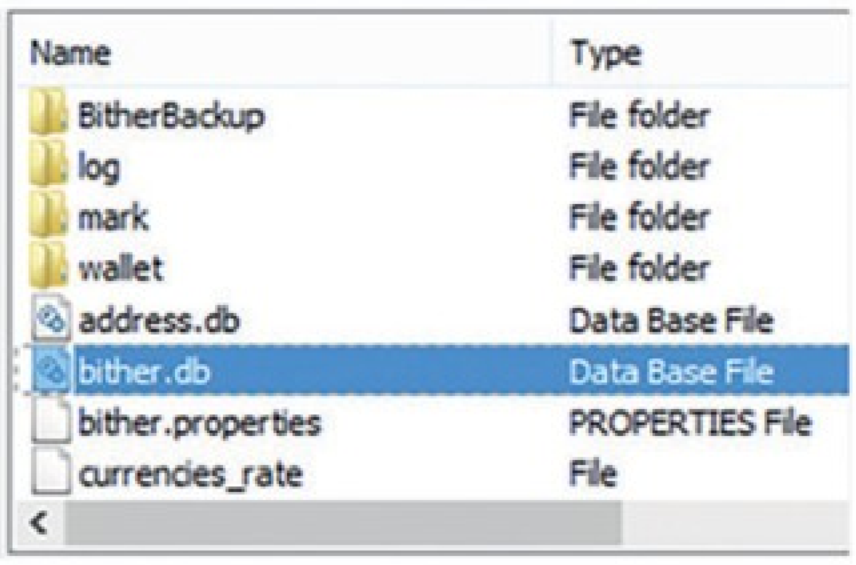
Searching ... (28 found) 44.00MB/s 5.3%

Figure 4. Wallet Address Stored In Hard Disk



Byte Offset	Context	Encoding	Sector	Partition	LCN
0x2B5222	p~q ~-t BTCEsq ~ A A-	ASCII	5545	0	N/A
0x2B5286	p~q ~-t BTCCHINAsq ~	ASCII	5545	0	N/A
0x2B538B	q ~-t CHBTCsq ~ @ Ni	ASCII	5545	0	N/A
0x2B541E	p~q ~-t BTCTRADEsq ~	ASCII	5546	0	N/A
0xEDCBA9	]e]8óe'¶¿BTC 3bR®	ASCII	30437	0	N/A

Figure 5. "BTCCHINA" is the Bitcoin Provider



Name	Type
BitherBackup	File folder
log	File folder
mark	File folder
wallet	File folder
address.db	Data Base File
bither.db	Data Base File
bither.properties	PROPERTIES File
currencies_rate	File

Figure 2. Snapshot taken from a Windows 8.1 Host Machine

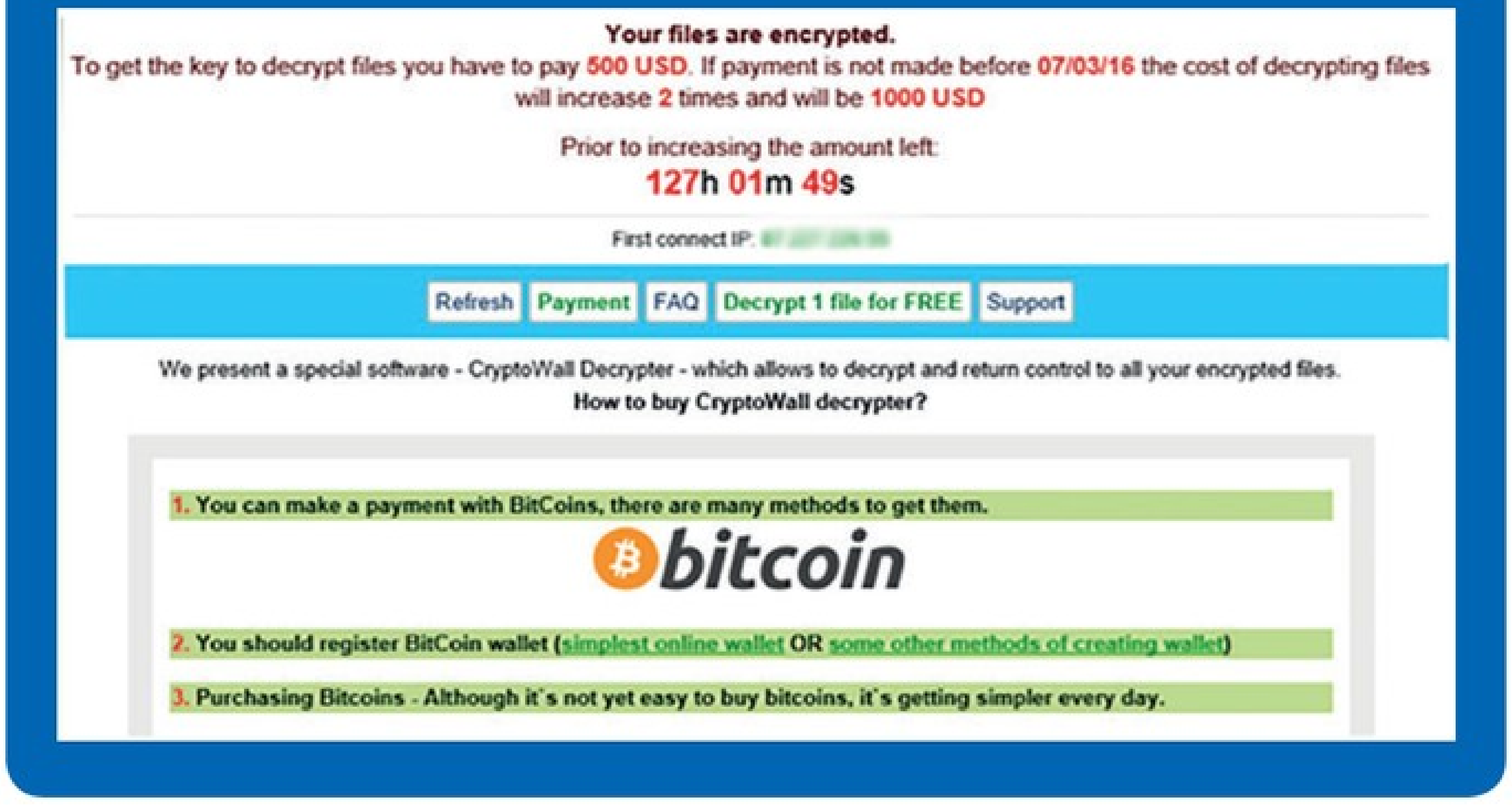
/ EXPERT TIP

Traffic analysis and transaction graph analysis can be used to facilitate the identification of Bitcoin users or services. These approaches look for patterns in addresses that lead to a single node. Current literature shows that such addresses have been clustered, labelled and thereafter linked to specific institutions.

1. A new machine/device is prepared with a fresh installation of the Operating System
2. A snapshot of the system is taken covering both volatile and non-volatile memory
3. The Bitcoin wallet is installed and a new account is registered ⇢ [AWI]
4. A snapshot of the system is taken covering both volatile and non-volatile memory
5. The Bitcoin wallet is used to send/receive a certain amount of funds (create a transaction) ⇢ [ABT]
6. A snapshot of the system is taken covering both volatile and non-volatile memory
7. The wallet is removed using standard uninstall steps available for end users ⇢ [AUW]
8. A snapshot of the system is taken covering both volatile and non-volatile memory
9. The machine/device is restarted ⇢ [ASR]
10. A snapshot of the system is taken covering both volatile and non-volatile memory

/ RANSOMWARE AND BITCOINS

Bitcoins has fuelled and escalated an increase in ransomware attacks in 2016. The picture demonstrates an example of this continuing problem, a malicious software encrypting the infected computer system with an option to release the data in return to a specific ransom paid in Bitcoins. The hard-to-trace nature of Bitcoins has made it the ideal currency for malware designers as it keeps them hidden while getting an immediate payment through the system.



Your files are encrypted.

To get the key to decrypt files you have to pay 500 USD. If payment is not made before 07/03/16 the cost of decrypting files will increase 2 times and will be 1000 USD

Prior to increasing the amount left:

127h 01m 49s

First connect IP: [redacted]

We present a special software - CryptoWall Decrypter - which allows to decrypt and return control to all your encrypted files.

How to buy CryptoWall decrypter?

1. You can make a payment with BitCoins, there are many methods to get them.

2. You should register BitCoin wallet (simplest online wallet OR some other methods of creating wallet)

3. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

> ***“EACH APPLICATION IS A UNIQUE PROJECT THAT REQUIRES SEPARATE FORENSIC DOCUMENTATIONS TO FACILITATE THE WORK OF A DIGITAL INVESTIGATOR AND REDUCE THE OVERALL INVESTIGATION TIME.”***

Analysis was then carried out on the multiple snapshots taken for each system status. Clearly, and as demonstrated by our procedure, this helps to distinguish between artefacts found After Wallet Installation (AWI); After Bitcoin Transfer (ABT); After Uninstalling the Wallet AUW; and finally, After System Reboot (ASR).

An example of the wallet addresses to which an amount of Bitcoin was transferred in our experiment is shown in Figure 1, the address is (1P5tVZqSj21KhHiP5e5mzXP9TcD31r38Z8).

/ DEMONSTRATION OF KEY FINDINGS

At the time of software installation, database files such as ‘bither.db’ and ‘address.db’ are created within the main Bither software installation directory as shown in Figure 2. These were found to be very critical since they contain wallet addresses and keys. In the case of iOS and Android, file extensions clearly indicate the use of SQLite databases. In iOS, this is located in ‘Documents/Bitheri.sqlite’ as shown in Figure 3.

That said, all other unique files are considered data remnants and can be used to evident that a wallet was installed, they should therefore be documented as part of any manual to support such investigations.

Further information was then recovered from the file system after an amount of Bitcoin was transferred. For instance, it was a straightforward task to extract current and old wallet addresses, Bitcoin service provider, exchange rates and the value of wallet’s password seed. In the case of Windows, additional Registry Keys were created. Figure 4 shows that the wallet address (1P5tVZqSj21KhHiP5e5mzXP9TcD31r38Z8) can be found in multiple database files in addition to web caches.

Other remnants include IP addresses referring to Block Chain.info and bither.net, or Bitcoin exchange services such as BTCChina as shown in Figure 5.

Another indication for the use of Bitcoin was inbound connections to Port 8333. The router and host-based firewalls will have it enabled and the network state of the host machine will show it too. ⇢

/ WHAT IS A BITCOIN BLOCK CHAIN?

Bitcoin transactions are assembled into blocks. Each block referencing its predecessor and the emerging authenticated data structure is called a Block Chain. It is a transaction database shared by all nodes participating in the Bitcoin system.

REFERENCES

1. Jacob Parks, J. C., 2013. ACFE. [Online] Available at: http://www.acfe.com/fraud-examiner.aspx?id=4294980488 [Accessed 18 April 2017].
2. Bohannon, J., 2016. Why criminals can't hide behind Bitcoin. [Online] Available at: http://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-Bitcoin [Accessed 18 April 2017].
3. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M. and Savage, S., 2013, October. A fistful of Bitcoins: characterizing payments among men with no names. In Proceedings of the 2013 conference on Internet measurement conference (pp. 127-140). ACM.

> ***“THE KEY CONCLUSION IS THAT THE WALLET IS DESIGNED TO UNINSTALL WITHOUT AFFECTING THE DATABASE FILE (.DB, .SQLITE, OR .DAT) SINCE THEY CONTAIN PRIVATE KEYS AND BITCOIN ADDRESSES NEEDED BY THE USER (OTHERWISE, THE BITCOINS WILL BE LOST FOR EVER).”***

When the uninstall procedure was attempted, not all remnants were deleted even after a system reboot. Metadata related to such files may be used to conclude whether a user attempted a system clean up. It has also been noted that Registry keys referring to installed software including Bither will remain undeleted when agents of asset management software such as LANDesk are installed on the machine. In our case, these keys were found at the following path:

```
HKEY_LOCAL_MACHINE\SOFTWARE\
LANDesk\ManagementSuite\WinClient\
SoftwareMonitoring\MonitorLog\
```

Likewise, Ubuntu, iOS and Android also kept files and folders. The key conclusion is that the Wallet is designed to uninstall without affecting the database file (.db, .sqlite, or .dat) since they contain private keys and Bitcoin addresses needed by the user (otherwise, the Bitcoins will be lost for ever). This is also convenient for the forensic investigator attempting to document these values and link them to the Block Chain. Nonetheless, deleted files were recoverable from the File Systems used on all platforms. The success here depends on the type of memory hardware and whether new data replaced the old one. Recovering deleted files from file systems and non-volatile memory is beyond the scope of this article but it is important to highlight this level of detail.

Investigating volatile memory is a gold mining process as expected; it includes all the information mentioned so far. However, memory acquisition can be challenging, as it required a rooted device in the case of mobile phones. Furthermore, memory data is lost after a system reboot except for any retrievable data remnants from a Windows crash file, pagefile; or a Linux swap file.

In this article we have shared a demonstration of our attempts towards solving the Bitcoin challenge for Digital Forensic Investigators, a suitable methodology to document relevant data remnants, and an overview with exemplars of findings related to the Bither Wallet. The value of these artefacts is significant once correlated and contextualised with the overall forensics process. /

/ AUTHOR BIOGRAPHY

Saleh Al Himali holds a BSc (Hons) in Information Technology Security and MSc (Distinction) in Information Management & Security from the University of Bedfordshire. He works as a system security specialist at the Information Technology Authority (ITA), Oman. His duties include providing consultancy services to government entities on portal protection, end-point security, and malware analysis. His current research interests include interesting in Advance Persistent Threat (APT), ransomware, big data breaches and Internet of Things security.

/ AUTHOR BIOGRAPHY

Haider M. al-Khateeb is a lecturer in the department of Computer Science and Technology, University of Bedfordshire and a Research Fellow in applicable computing and an active member of the National Centre for Cyberstalking Research (NCCR). He has a first-class BSc (Hons) in Computer Science, and PhD in Computer Security. He supervise a number of PhD students in areas such as Advanced Persistent Threats, (APT), Internet-of-Things Forensics and Social Intelligence. Haider is also a Fellow of the Higher Education Academy (FHEA).