Cryptocurrency Forensics

Rachael Shima, Jyoti Manchanda, Karter Rohrer, & Connor Baskin; Computer Science
Mentor: Mohammad Husain
Kellogg Honors College Capstone Project

ABSTRACT

Introduced by Satoshi Nakamoto, Bitcoin, the world's first decentralized digital cryptocurrency, catalyzed a global cryptocurrency revolution. As cryptocurrency wallet owners transfer funds worldwide anonymously, dishonest parties use the digital currency platform to hide illegally gained money. Similar to a physical wallet storing paper currency, a cryptocurrency wallet allows owners to store money digitally via use of private and public keys that interface with blockchain. Cryptocurrency wallet owners select from options including "cold storage" paper wallets that serve offline storage purposes or "hot storage" mobile wallets that ease mobile device user interface. Criminals may be unaware that it is possible for law enforcement to identify an individual behind a cryptocurrency transaction with the assistance of digital forensics examiners and network packet analysis experts.

Through the field of digital forensics, this paper aims to explore mechanisms that can expose forensic artifacts associated with cryptocurrency transactions utilizing multiple exchanges including Coinbase. This research compares data associated with cryptocurrency transactions involving three different cryptocurrencies through Windows Registry exploration via law enforcement approved forensic analysis software instruments including AccessData Forensics Toolkit. To supplement manual operating system exploitation, the researchers in this project analyzed the suspect's network via Wireshark to capture packets and automate network forensics discovery with the scripting language, Python.

OBJECTIVES

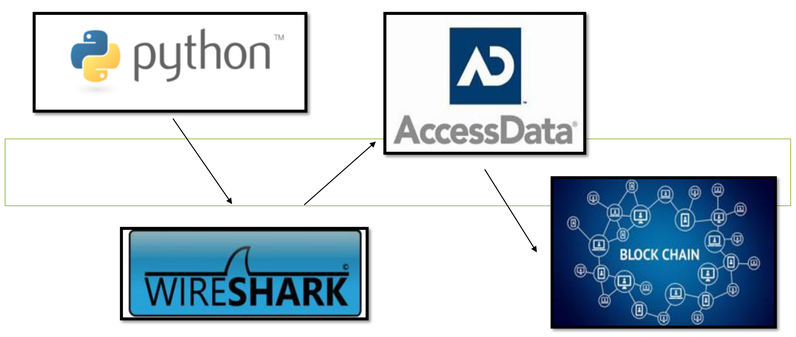
- To identify individuals who have made an illegal transaction with crypto currency with enough accuracy to obtain a warrant and/or an arrest
- To create a script that can be used to identify the artifacts necessary to obtain this arrest.

METHODS

- Utilized Wireshark to capture network packets during Cryptocurrency inter-wallet transfers and purchases
- Analyzed network packet captures and utilized data to design a custom Python script that utilizes TCPDump to scan and filter network captures for cryptocurrency activity
- Utilized AccessData Forensics Toolkit in order to find cryptocurrency artifacts in the Windows Registry

RESULTS

Following five months of extensive research, several methodologies of identifying cryptocurrency transactions have been concluded. The first methodology includes using network capture files (PCAPs) with Wireshark to analyze user activity on private networks. With the use of TCPdump, a tool installed with the Wireshark package, researchers can identify timestamps associated with a cryptocurrency transaction, which can be used to find the transaction on the block chain. Additionally, Bitcoin nodes can be identified in pcap files, which can be used to triangulate geographical locations of cryptocurrency addresses. The second method involves seizing a suspect hard drive and forensically imaging the drive using FTK Imager 3.4.2. During the analysis, researchers are able to identify everything the user typed in, from when they typed the cryptocurrency exchange URL, copying the cryptocurrency address, to hitting the send button to the recipient.



CONCLUSIONS

- Identified destination & source IP addresses
- Automated Network Forensics discovery with Python
- Identified cryptocurrency transaction timestamps in Network pcaps
- Identified cryptocurrency login sessions on Network pcaps
- Identified operating system timestamps associated with the cryptocurrency block chain
- Identified typed URLs for cryptocurrency websites
- Identified clipboard data containing cryptocurrency addresses
- Correlated discoveries directly to the block chain in multiple formats without knowing the transaction address

REFERENCES

http://damonmccoy.com/papers/ransomware_paper.pdf
https://www.wired.com/story/hansa-dutch-police-sting-operation/
https://www.forensicswiki.org/wiki/Windows_Registry

ACKNOWLEDGEMENTS

Forensics and Security Technology Club – Assisted Network Forensics Expertise

Cal Poly Pomona Polysec Lab – Varied project support

Cash

ethereum