|  |  |
| --- | --- |
|  | Andy Martinez’s Cybersecurity Portfolio |
|  |  |
|  | Andy Martinez |

This work was made possible by many people who have supported. I want to thank my parents and sister, who loved on me and pushed me to continue my studies. To my friends who shared in my struggles and success. I want to give special thanks to my cousin and distinguished professor of Economics at Houston Community College, Candy Meza, for serving as a great inspiration for me. My hope is for you, the reader, to enjoy this work and learn something new along the way.

Note: This is the shortened version of my cybersecurity portfolio. For the full version, check out my GitHub: *https://github.com/adjmartinez0110/CyberSec-Portfolio*

Blockchain

A Brief Introduction

When one thinks of money, they think of something they can hold in their hand, or at the very least, the balance in their bank account. However, Bitcoin is not quite like this kind of money. The currency has no physical presence, meaning a person cannot withdraw it from the blockchain and hold it in their hand. This type of currency cannot be destroyed, only lost. Through mining, new Bitcoin is generated, which involves a using a computer to solve a cryptographic puzzle to win a determined amount of Bitcoin. The issue lies in that if the winner of the puzzle-solving race fails to redeem their prize, that money is lost for good.

Following this was a discussion on wallets. Wallets are just what they sound like - a place for storage. The difference in these types of wallets is that they are not necessarily used to store the cryptocurrency but are used to store cryptographic keys. The user's private key is necessary to gain access to their funds.

Bitcoin, or cryptocurrency in general, can seems complicated but upon looking closely it has similarities to our everyday banking system. The currency is held within the blockchain (like a bank), but having a wallet is like having a debit or credit card and the private key can be thought of like a PIN number entered at the store, used for authorizing the transfer of the user's money to a merchant.

Shortly after learning about the nuances of Bitcoin, we were introduced to another blockchain technology: Ethereum.

Like Bitcoin, Ethereum has its own cryptocurrency called ether, which can also be exchanged for fiat money. Also, like Bitcoin, it is decentralized, and built upon a peer-to-peer network.

However, the differences between these two cryptocurrencies are much greater than their similarities, I felt. Ethereum functions much like a digital ecosystem rather than a simple cryptocurrency. Goods and services like applications (Dapps) are constantly being developed for it and ether is the thing that makes this new world go round, powering apps and services, and used to initiate transactions as well. Everything here runs on ether.

References

- Joshi, V. (2017, July 31). Trying to Understand Tries. Retrieved December 9, 2020, from https://medium.com/basecs/trying-to-understand-tries-3ec6bede0014

- Nakamoto, S., n.d. *Bitcoin: A Peer-to-Peer Electronic Cash System*. [online] Bitcoin.org. Available at: <https://bitcoin.org/bitcoin.pdf>.

- https://www.bitdegree.org/crypto/tutorials/cryptocurrency-wallet#:~:text=The%20software%20within%20the%20cryptocurrency,funds%20in%20the%20real%20world.

- https://ethereum.org/en/what-is-ethereum/

- https://ethereum.org/en/developers/docs/smart-contracts/

- https://blockgeeks.com/guides/smart-contracts/

- https://cointelegraph.com/ethereum-for-beginners/ethereum-wallets

- https://www.udemy.com/course/bitcoin-and-cryptocurrency-bootcamp/learn/lecture/10259778#overview

- https://medium.com/shyft-network-media/understanding-trie-databases-in-ethereum-9f03d2c3325d

Computer Forensics

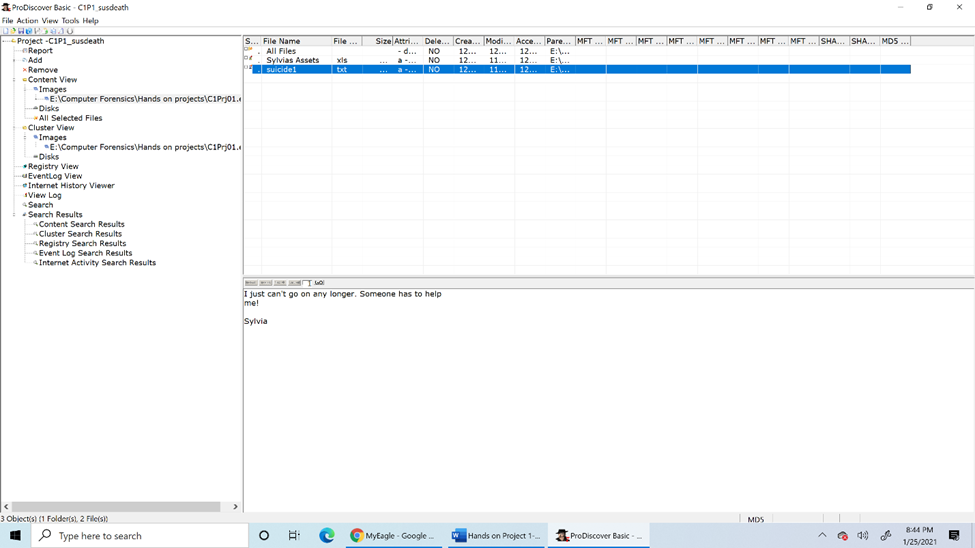
*A Brief Introduction*

Computer Forensics, also known as digital forensics, involves recovery and investigation of material found in digital devices related to cybercrime, according to EC-Council.

This example involves me using a tool called ProDiscover, which is well known in the forensics community.

Hands on Project 1-1 Suspicious death 7/29/2006

This case involves a suspicious death. I have been tasked with investigating the contents of an image of a USB Drive made by a technician. I booted up Prodiscover and created a new project. I uploaded image file C1Prj01.eve and looked through its contents.

After expanding the images tab a bit, what I found in the selected image was a mess of data. After a little more digging, I came across a file titled Sylvias Assets and another titled suicide1. I then documented these with screenshots.

Courtesy of Nelson, B. et al. 2016. Guide To Computer Forensics And Investigations. 5th ed. Boston, MA: Cengage Learning.

Report:

The data found within the USB drive indicates that the woman’s name was Sylvia and the evidence points to distress as motive for suicide but a full investigation is needed.

**References**

- https://www.eccouncil.org/what-is-digital-forensics/

- Nelson, B., Phillips, A. and Steuart, C., 2016. *Guide To Computer Forensics And Investigations*. 5th ed. Boston, MA: Cengage Learning, pp.55-59, 177-178.

- https://www.commonlounge.com/discussion/4bc16dbc2c7145ff87ad0f0d5401a242

IoT (Internet of Things)

*A Brief Introduction*

There is plenty of hype going around for Internet of Things (IoT) devices. These are what are known as smart devices, such as smart thermostats and fridges. These devices are designed to make life easier for the consumer and can be interconnected to one another. Although is it a novel idea for a person’s fridge to be able to order groceries, sadly security is hardly ever taken into consideration. These types of devices are known for having many bugs and vulnerabilities, making them an easy target for hackers to play with.

Say a customer is looking to purchase a smart TV for their home. Smart TVs have many useful features, like voice recognition and popular built-in apps and a camera. A hacker can tap into the camera by finding the device using its IP address and spy on the customer. Because of the customer’s ignorance, they would not be aware that this is taking place. The same thing could happen with other devices like baby monitors, where a bad actor could listen in on a conversation they are not supposed to hear. Researchers have been addressing these concerns for years, but progress in calling for stricter guidelines and procedures for more secure devices has been slow. Ultimately, it is up to the consumer to do their due diligence and research these devices to see what they are capable of and how to best protect their privacy and well-being.

**References**

https://techcrunch.com/2009/12/14/rockyou-hack-security-myspace-facebook-passwords/

https://www.kaggle.com/wjburns/common-password-list-rockyoutxt

https://www.cloudshark.org/captures/ba85949942a0

https://www.zdnet.com/article/coffee-machines-cuddly-toys-and-cars-the-internet-of-things-devices-which-could-put-you-at-risk-from-hackers/?&web\_view=true

https://www.cnet.com/home/smart-home/iot-attacks-hacker-kaspersky-are-getting-worse-and-no-one-is-listening/?ftag=CMG-01-10aaa1b