|  |  |
| --- | --- |
|  | 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.



[This Photo](https://researchleap.com/cryptocurrency-framework-diagnostics-from-islamic-finance-perspective-a-new-insight-of-bitcoin-system-transaction/) by Unknown Author is licensed under [CC BY](https://creativecommons.org/licenses/by/3.0/)

Blockchain Portfolio

An end-of-term report

# Module 1

## At the start of this course, the class was split into two groups, and the members of the group worked together to tackle the various tasks presented. This very first module introduced the concept of blockchain technology and cryptocurrency. My task here involved familiarizing myself with these concepts, what they do, why they were created, and how it can affect the tech industry.

## I first directed my attention toward Satoshi Nakamoto's white paper on Bitcoin to get myself up to speed. Although this technology has been around for a while, this was all new to me.

## 

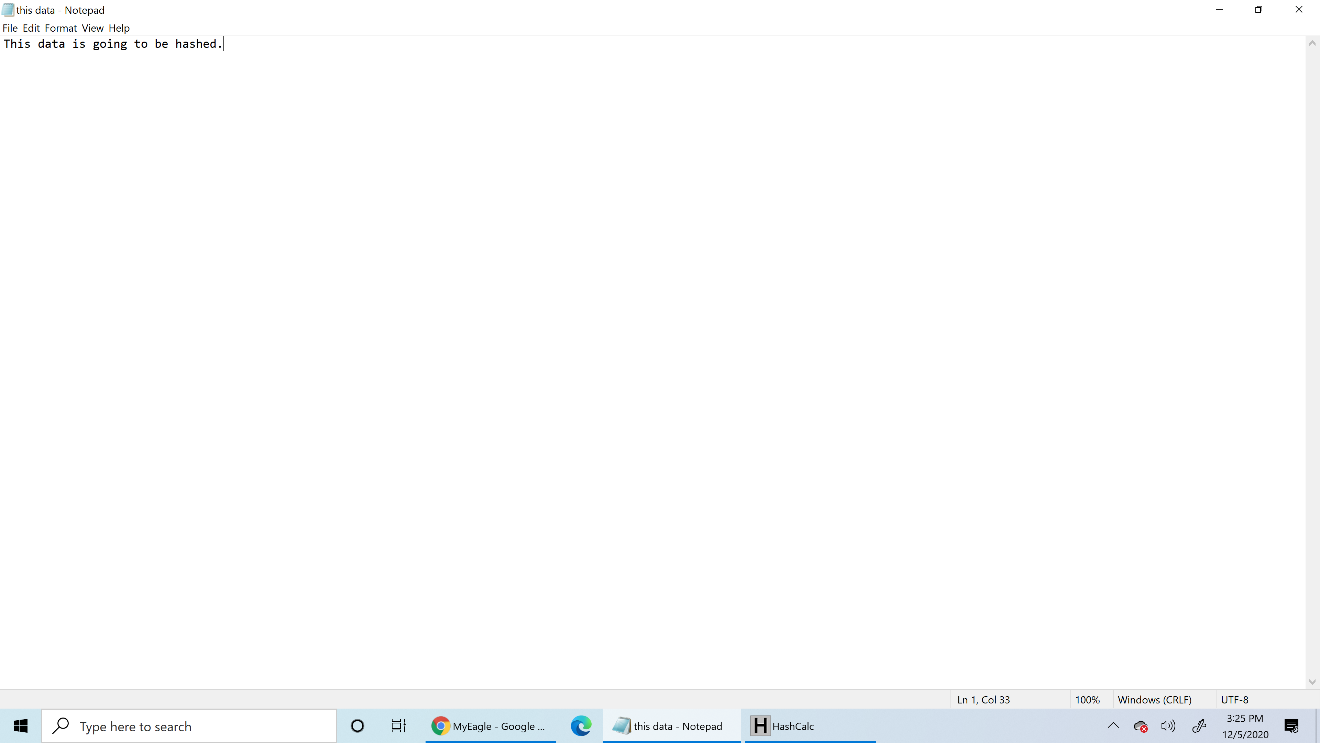
## *White paper by Nakamoto*

## Upon reading part of the paper, the task of understanding this seemed very daunting. Bitcoin (or more generally, Blockchain) was not only very technical, but also had in-depth aspects of socioeconomics and psychology, which one would hardly expect to present themselves in a computer science research paper.

## This forced me to not only look to other sources to understand each individual idea brought forth in this paper, but I had to read through the paper a few times to see how the ideas came together, to further cement the concept in my mind.

## This first assignment involved experimenting with different hashing algorithms and reporting on their characteristics. Hashing, in the simplest terms, is to get a piece of code from a complex formula (algorithm) and using that code to check to see if data has not been altered in any way. Hashing was something I was familiar with as a student coming from an information security background.

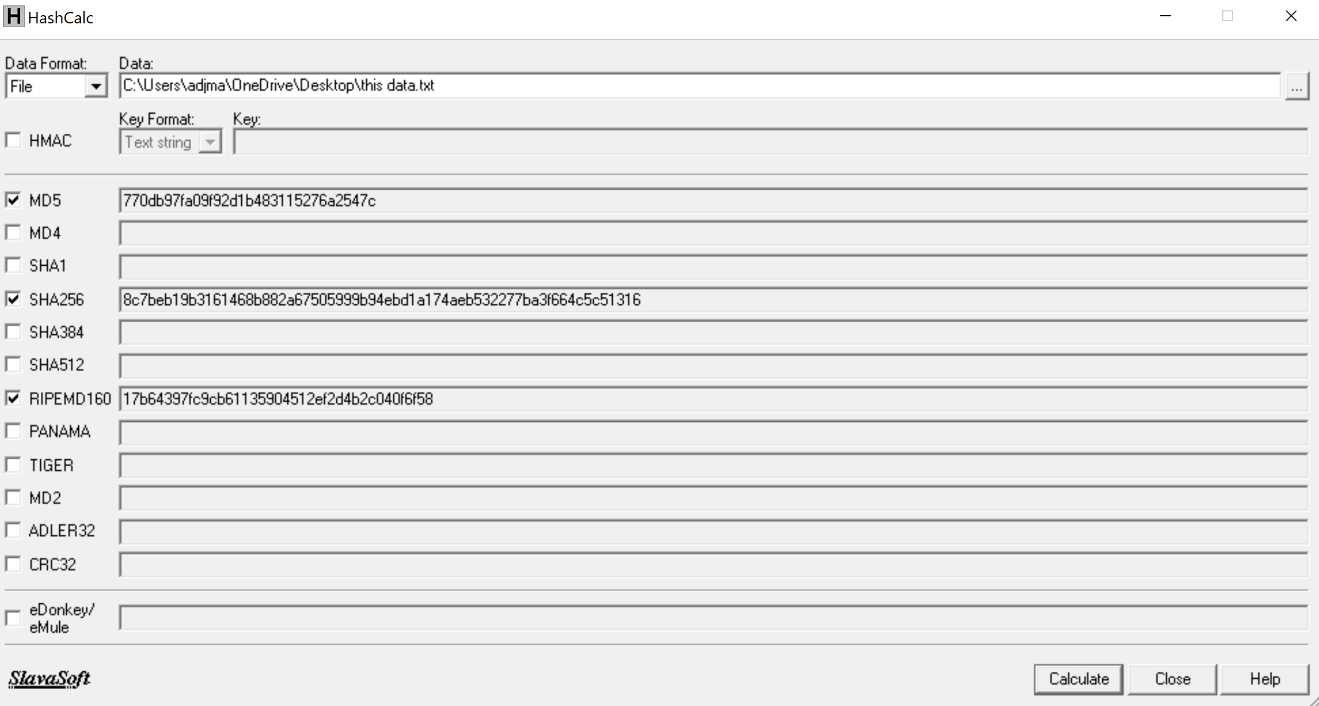
## I decided to experiment with hashing on my own using a program called HashCalc. The interface is intuitive, just browse for your text and choose a hashing algorithm to be used. The next picture I will use to demonstrate the hashing process.



*File name: this data.txt. This data is going to be hashed.*



*Layout of HashCalc, the software used for this demonstration.*



*The file has been run through the hashing algorithms.*

As seen in the picture, I chose to use MD5, SHA 256, and RIPEMD160 algorithms. Now modifying the text a little by adding an extra character and running it through once more gets this output:



*A modified this data.txt is hashed once again.*

It interesting to note how one small change in the text leads to a substantial difference in the hash. This ensures the integrity of data, and when it comes to the blockchain, ensures that the information that is altered within an established block gets rejected.

# Module 2

This portion of the course had the group delving into some of the aspects of Bitcoin.

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.

# Module 3

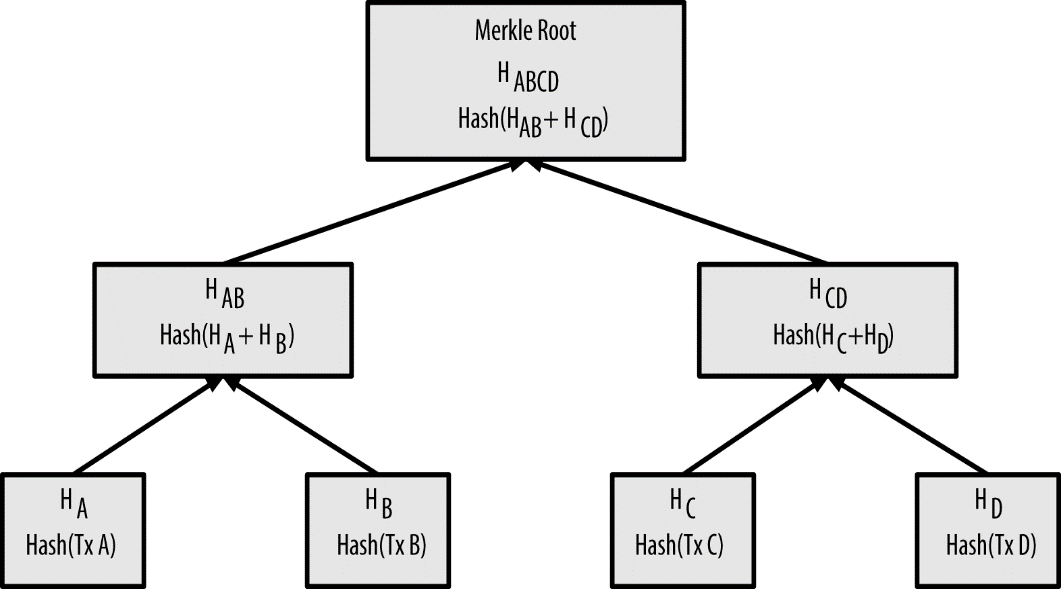
Shortly after learning about the nuances of Bitcoin, we were introduced to another blockchain technology: Ethereum.

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.

Merkle trees are data structures that carry hashes, and their main purpose when it comes to blockchain is maintaining the integrity of data. For new transactions to be added to the blockchain, previous transactions must remain unchanged, and Merkle trees provide a list of hashes taken from these previous transactions, proving that the transactions have not been modified in anyway.

Below is a picture of a Merkle tree:



[This Photo](http://bitcoin.stackexchange.com/questions/10479/what-is-the-merkle-root) by Unknown Author is licensed under [CC BY-SA](https://creativecommons.org/licenses/by-sa/3.0/)

Hashes of transactions are continuously stored and built upon, and transactions can thus be traced however far back on the tree, just like a ledger allows blockchain transactions to be traced back. Bottom hashes are made, and the hashes on top of those create hashes of those previous hashes on top of its own. Those hashes are then collected as well up until the root (top) hash is created.

# Module 4

Smart contracts, according to the definition on the Ethereum website, is a program that runs on the Ethereum blockchain. Smart contracts are fully automated pieces of code.

The analogy that continually comes up is the vending machine. The machine is programmed to dispense snacks when money is inserted. It knows what to do without any sort of human intervention (except when it malfunctions or needs to be restocked). Smart contracts can also exist as accounts, able to transfer ether and can even be used generate new contracts.

Having the smart contracts not only uphold the terms of the contract but also enforce them eliminates the need for a middleman in different types of scenarios (lawyers, stewards, etc.). It will be interesting to see how this will shake up the industry.

We now entered a discussion on Ethereum wallets. Like other crypto wallets, an Ethereum wallet is used to store a user's private key (actual ether is stored on the blockchain). Ethereum wallets are very similar to Bitcoin wallets, except that the user can deploy smart contracts to have more flexibility and freedom when managing funds. Transactions also clear much quicker for the most part.

Next, the group explored other key features of Ethereum that allows it to distinguish itself from other blockchains. First is the proof-of-stake system, which gives a lower barrier of entry for those wanting to invest in the cryptocurrency. Next is the concept of sharding, which provides a way to for users to download only a piece of the blockchain that they are interested in through horizontal partitioning (thus saving disk space within a desktop environment). Lastly, the Casper FFG protocol heavily discourages dishonesty or sabotage of the blockchain. Users must follow a set of guidelines before investing, and if they fail to do so, they potentially forfeit their funds. All this certainly makes ether more attractive to prospective investors.

# Module 5

Merkle Patricia Tries are the data structure that makes up the foundation of the Ethereum blockchain. A trie is tree-like data structure whose nodes store the letters of the alphabet, and strings/words can be retrieved by traversing down a branch path of the tree (Joshi V., 2017).

Tries include three primary trees: the receipts tree, the transactions tree, and the state tree. Transaction trees record the transactions and never updates. The receipts tree keeps records of the outcomes of transactions, and never update once written. The state tree contains a key-value pair for every Ethereum account. The key consists of an Ethereum address and the value is encoded. However, unlike the other two, this tree constantly updates as the blockchain grows.

# Conclusion

As far as investing in cryptocurrency goes, my choice would have to be Ethereum. Bitcoin has its merits (more bitcoin per block than ether), but the features Ethereum has such as the proof-of-stake mechanism and sharding, make ether the safer choice, which is what matters to me personally.

I came in knowing next to nothing about this subject. Now that this course is over, I still cannot say I know a whole lot about it, but the beauty of learning is that it never stops. Perhaps I can revisit this subject soon. And what I do know would make great dinner party conversation.

# 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



[This Photo](https://www.iphonemod.net/chaos-computer-club-claims-it-can-reproduce-fingerprints-from-peoples-public-photos.html) by Unknown Author is licensed under [CC BY-NC](https://creativecommons.org/licenses/by-nc/3.0/)

Computer Forensics Portfolio

*An end-of-term report*

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 course had me barely scratch the surface of what can be done with the different tools and methods available but here I will showcase a few examples.

This first few examples involve 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.

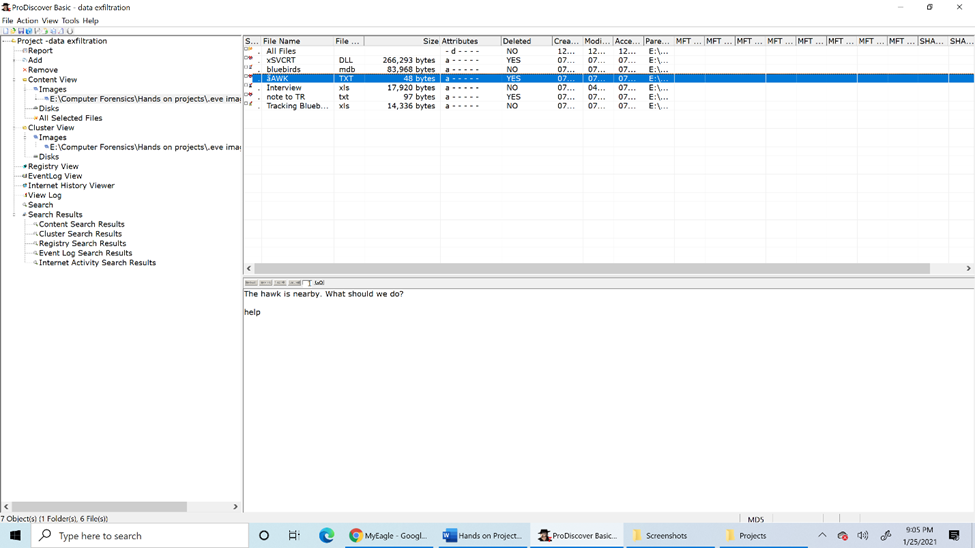
Courtesy of Nelson, B. et al. 2016. Guide To Computer Forensics And Investigations. 5th ed. Boston, MA: Cengage Learning.

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.

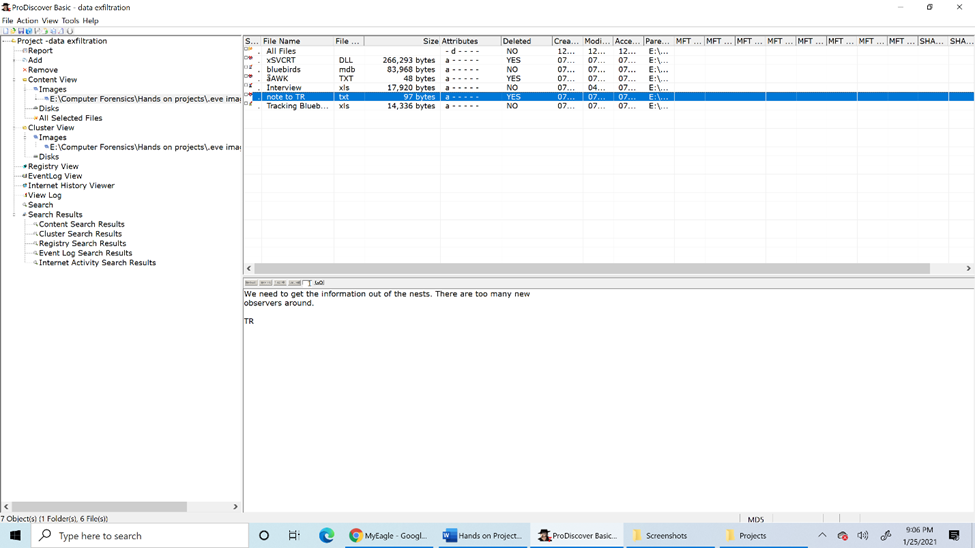
Hands on Project 1-2 Data exfiltration

This case tasked me with seeing the contents of the USB drive left by a former employee. This employee is suspected of taking sensitive data with them when they left the company to go work for a competitor. My job is to find any evidence of this data, as these files contain the word “book”, and how many times I happen to find them.

As I scoured the contents of the drive, I came across various file types, such as DLL and TXT. Reading the TXT files I found: **"The hawk is nearby. What should we do?**

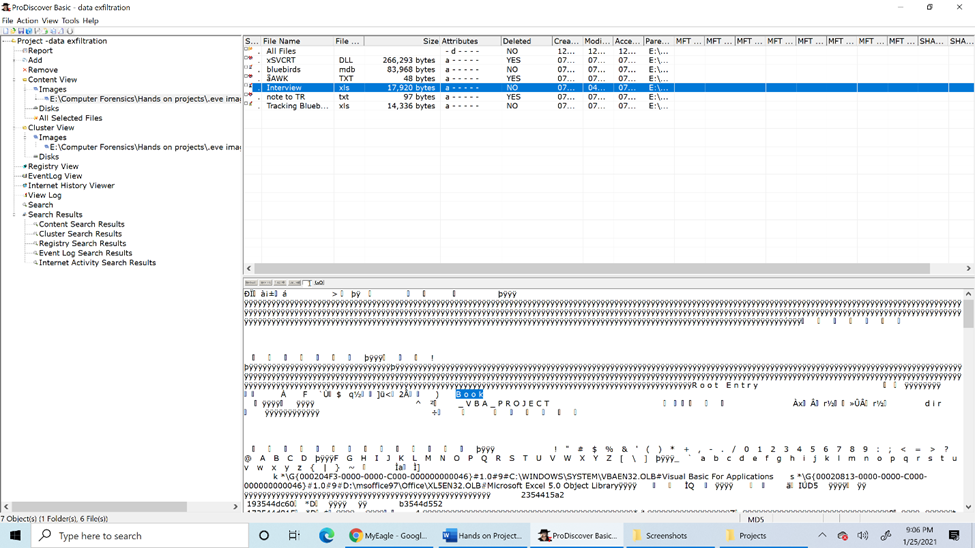
*Courtesy of Nelson, B. et al. 2016. Guide To Computer Forensics And Investigations. 5th ed. Boston, MA: Cengage Learning.*

" as well as **"We need to get the information out of the nests. There are too many new observers around.TR".**



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

What does this mean? Was the employee under the impression that they were being watched?

I found an instance of the word “Book” in ***Interview.xls*** file using the Search feature. I also did the same using the Cluster Search feature and found several more instances of the word appearing.

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

*Memo to Ms. Jones*:

Instances of the word “book” found in ***Interview.xls*** and several other clusters.

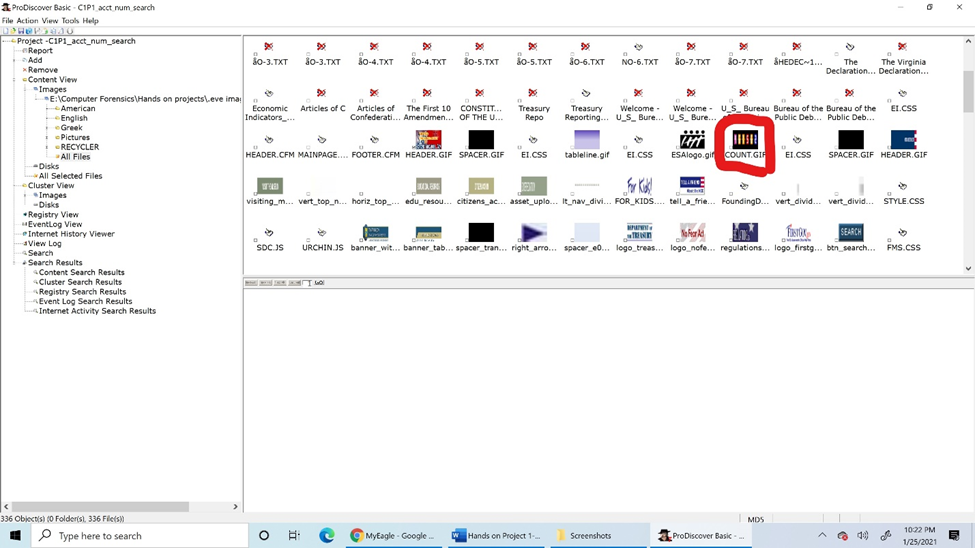
Hands on 1-3 Account Number Search

It appears the former employee has used another drive, according to Ms. Jones. My next job is to find instances of the account number 461562 appearing and documenting the instances in which it appears. This number belongs to the senior vice president and is used to access the company’s banking service over the Internet.

Use View 🡪 Gallery view to aid in search.

Files found include a variety of literature and US tax and crime laws/codes/statutes and data.

After using Search option, no results emerged, but as it turns out, graphical images can also contain text (hence, no results when using Search).

Here is what I found: **COUNT.GIF** (search under All Files)

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

*Memo to Ms. Jones*:

The account number 461562 was located under an image file called **COUNT.GIF** when searching through the drive under ‘All Files’.

The examples shown above are some of the things a forensics investigator can hope to see when working in the field and requires some prior knowledge on what to look for, such as the case with the data exfiltration.

This next case demonstrates the use of another tool called OSForensics and how it is also employed in data recovery. The USB drive of the IT person, Terry, is searched to see whether they have acted against company policy by participating in illicit activity.

Hands on Assignment 4-3

Investigator: Andy Martinez

Case: M57 Patents case

Tools used: OSForensics, M57 - Terrys USB drive image, investigator's detective skills.

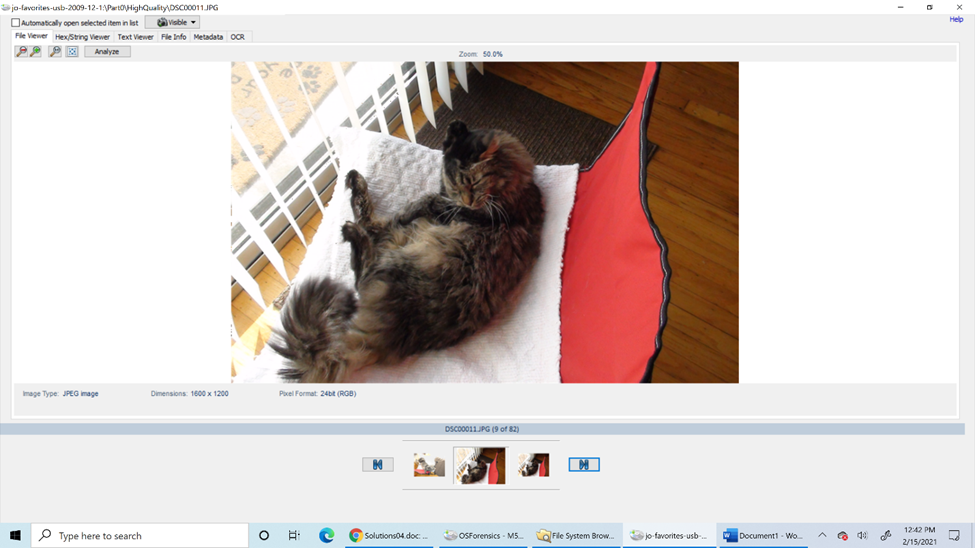
Date: 15/2/2021, 12:00 pm, CST

To whom it may concern,

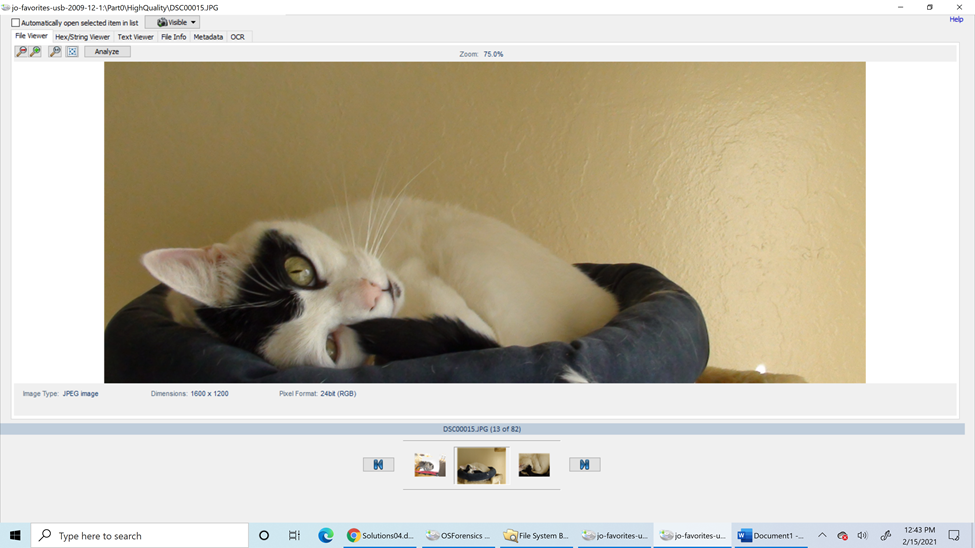
The use of the OSForensics software kit allowed the investigator to further explore the contents of the given USB drive to uncover evidence of illicit activity.

The investigator used the Manage Case feature to start a new case and uploaded the image of the thumb drive in question. Using the search feature, the investigator searched for the term "kitty\*" to find the "kitty porn" in question. No results came from this search, perhaps as an attempt by the owner to cover their tracks.

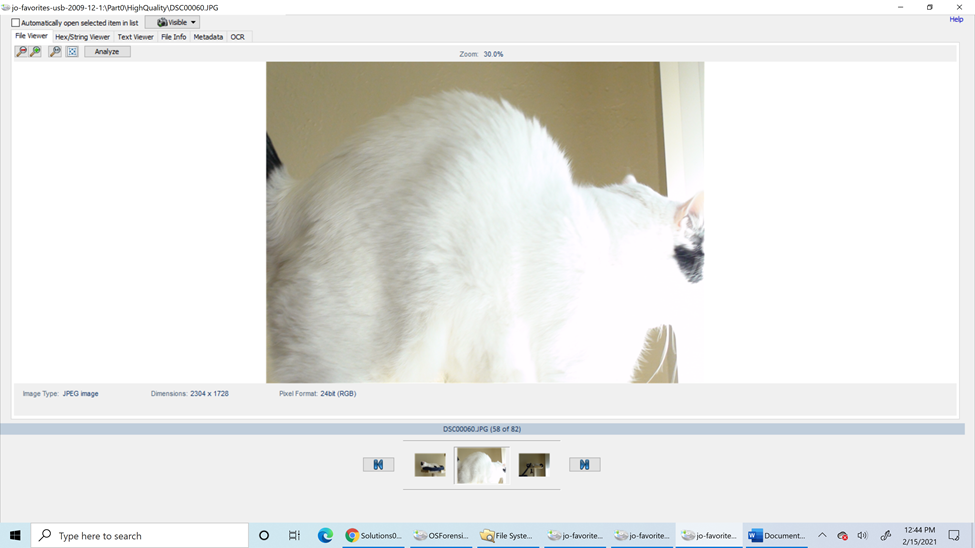
The investigator then used the Create an Index function to gather the files found on the drive in one place, with as many different file formats as possible. After the process was done, the contents of the drive were once again searched, and this is what was found during the investigation. (WARNING: GRAPHIC CONTENT AHEAD. VIEWER DISCRETION IS ADVISED.)



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



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



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

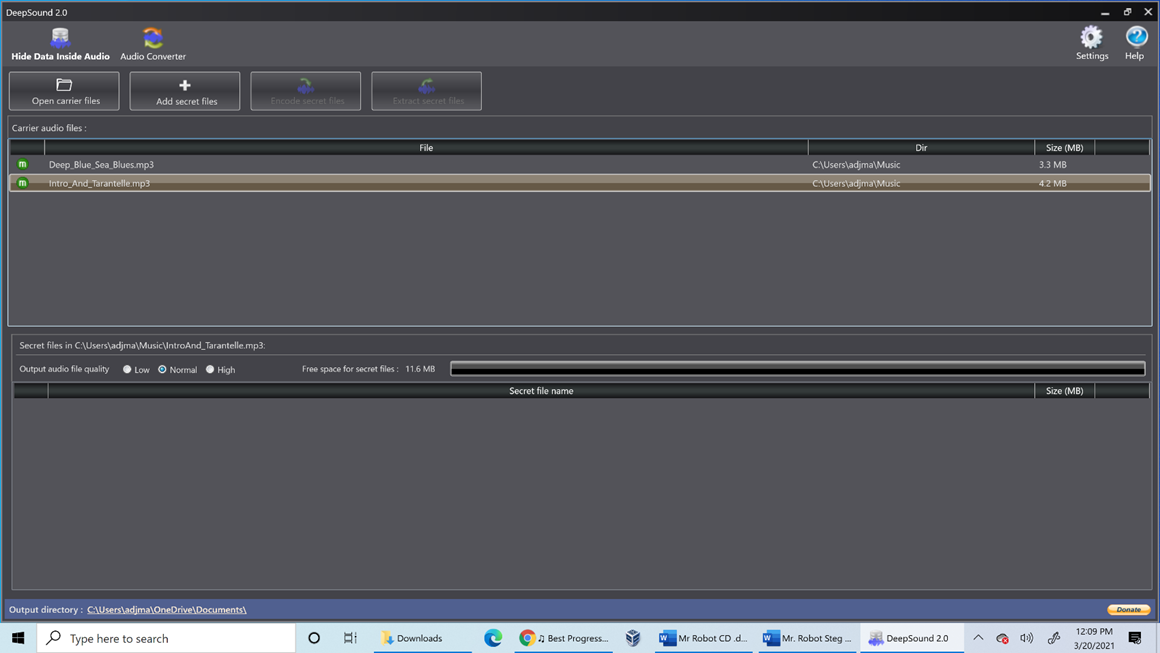
The images presented are indeed incriminating and the suspect (or suspects if more people are found to be complicit) could face a long incarceration (decades worth of jail time). This is worrisome because of the nature of work the company that the suspect works for requires a higher moral compass and good standing with the law. This will indeed damage the company’s reputation and credibility when the findings of this investigation go public. It is hard to justify working or partnering with a company that employs a person who is accused of kitty pornography and animal endangerment, let alone several people involved in such a crime.

Of course, this example was very tongue-in-cheek but speaks to the harsh reality of the job of a digital investigator within law enforcement. It is very possible to come across child pornography or other disturbing content in such a way and is quite common today. Criminals are becoming smarter in how and where they hide data, and in some cases, they can store data in another person’s computer or a company’s servers without their knowledge. When the data is discovered, the owner(s) of the device is/are prosecuted instead of the actual criminal who put the data there.

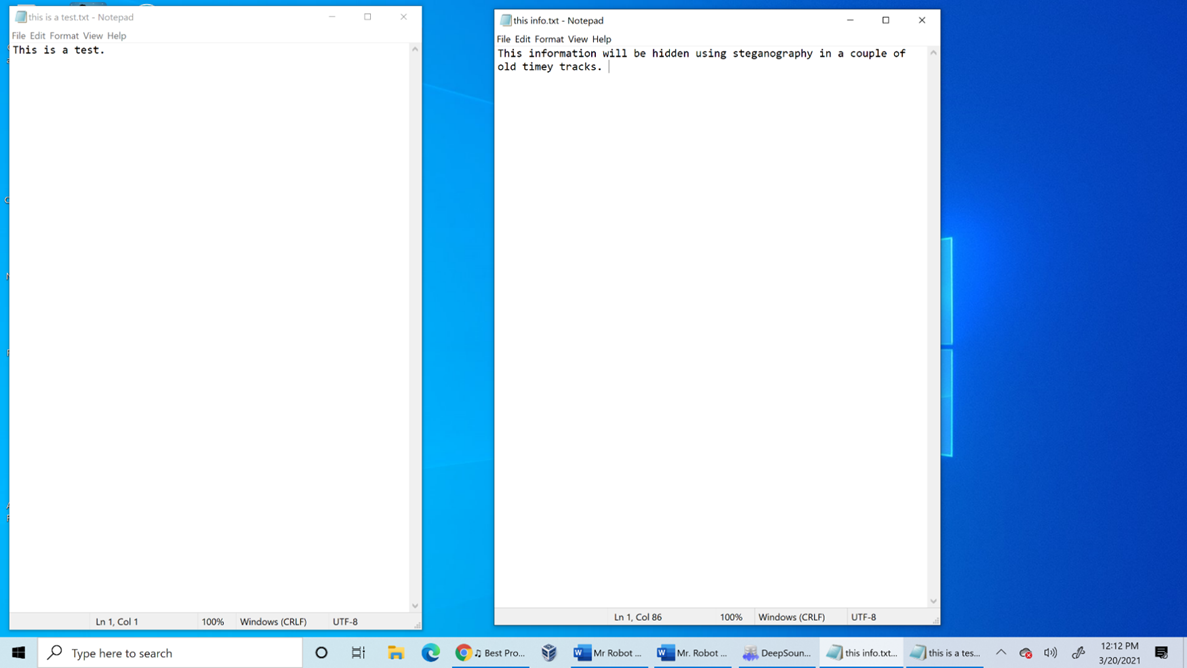
This next work presents a concept that is very common in communications and espionage: steganography. A basic definition of steganography is the art of hiding data within other data. Instances of steganography can be found throughout history from ancient Greece to the 20th century during the World Wars. Female spies would encode messages within their knitting, and photosensitive glass was used to carry covert messages. When exposed to the correct wavelength of light, the glass would reveal its hidden content.

Mr. Robot Steg Hack

My task here is to hide a secret message within a couple of music tracks that I fetched from the Public Domain. I made use of the DeepSound program to make this happen. The dashboard of the program looks like this:

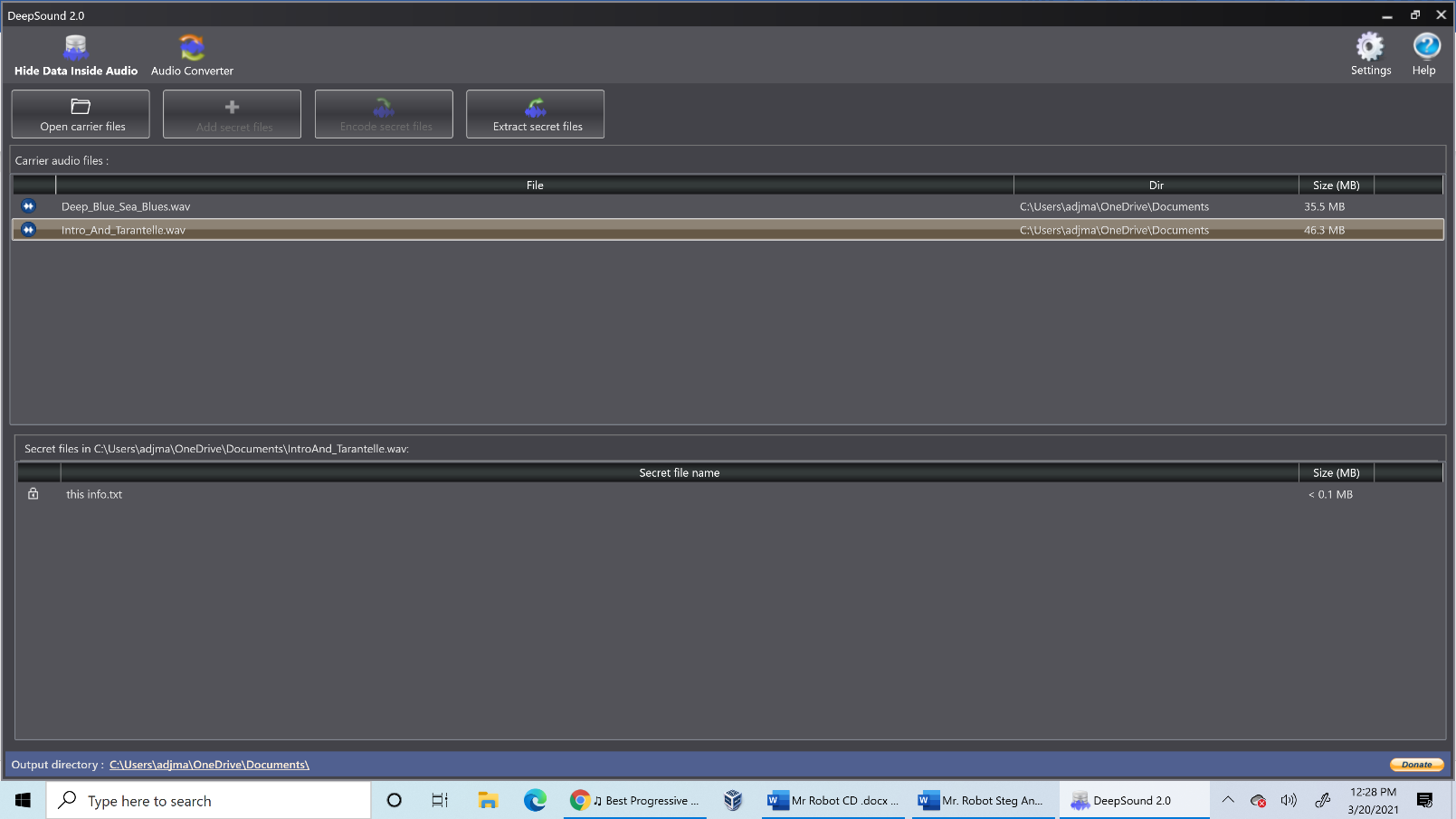


*Deepsound dashboard.*

**

*These are the messages that will be hidden within the tracks.*

The process of hiding the text happens when I select an audio file and hit ‘encode secret files.’ I closed and re-opened DeepSound, went to ‘Open carrier files’, selected my files and entered my password.

Success! The hack worked! The hidden files are seen under the ‘Secret Files’ tab. Mission accomplished.

*Files successfully hidden.*

**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

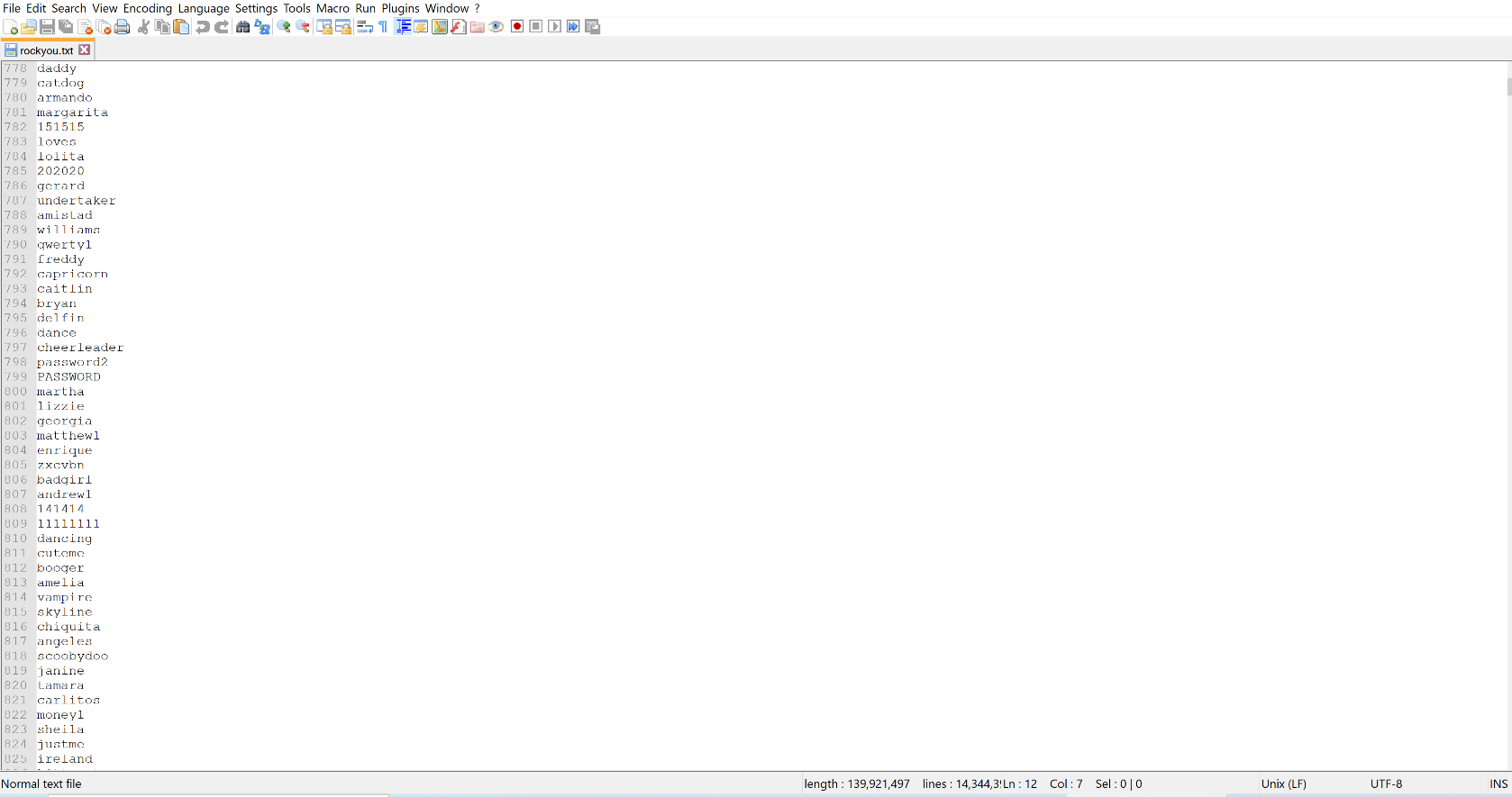


[This Photo](http://www.allwhitebackground.com/red-background.html) by Unknown Author is licensed under [CC BY-NC](https://creativecommons.org/licenses/by-nc/3.0/)

Cyber Capstone Portfolio

*An end-of-term report*

This final section will showcase just a few examples of the type of work that I have done in my studies. Topics that will exhibited include cyberattacks, competition challenges, and independent research.

Let us look at a couple of attacks on passwords, which I believe will be very eye-opening. The first of these is called a brute force attack. It is very straightforward, as an attacker just tries to guess a password repeatedly until they get it right. The more devious attack is called a dictionary attack. The attacker downloads a list of common words or phrases that are often used as passwords. This list is run through a program to guess their way into a particular restricted area, like a web server to steal sensitive information. By locating the rockyou.txt wordlist, I can share a screenshot of my findings.

*rockyou.txt wordlist*

The screenshot above shows an instance of the rockyou.txt that was used to perform a dictionary attack in the 2009 RockYou data breach. (Be aware that to open this file, a different text editor must be used, as it is too big to open with Notepad. Also, this list contains strong language.)

Notice anything familiar? These are words or phrases that people commonly use as passwords. They are displayed here in cleartext, rather than ciphertext, meaning the passwords were not encrypted. This is a failure on the website’s part, as they did not take the necessary measures to safeguard the data they were responsible for. Still, it is good for the user to be proactive in doing their fair share in using more complex passwords, and not using the same password for every site.

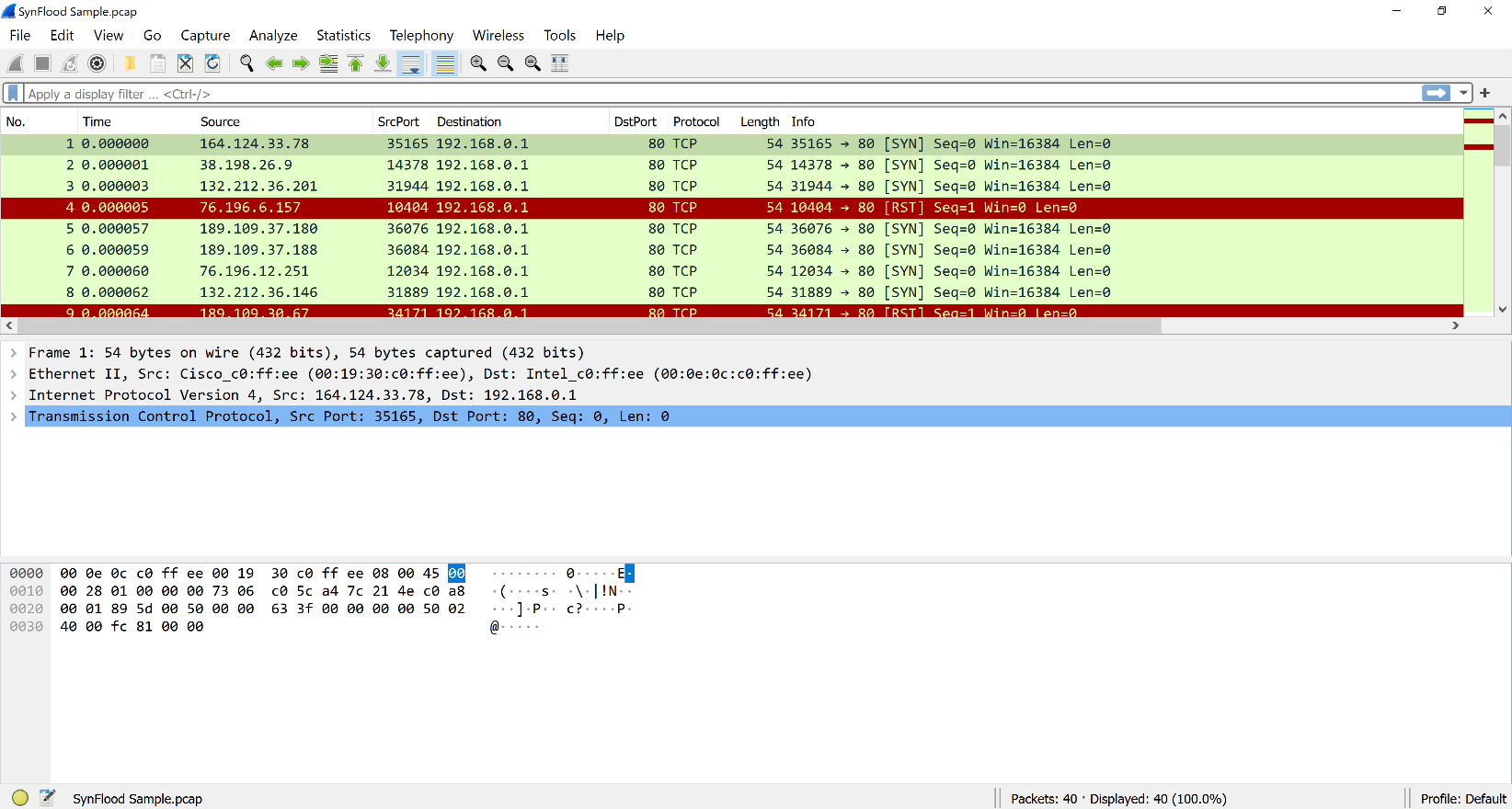
The National Cyber League is a hackathon that consists of challenges such as open-source intelligence, password cracking, cryptography, and more. I want to highlight one of the topics that was seen during the competition but due to copyright reasons, I will not be showing a specific example from there.

Instead, I want to demonstrate a type of cyberattack called a SYN flood attack. This is classified as a denial-of-service attack, which means that this prevents access to certain resources for the end user. To really know what is going on, the TCP three-way handshake must be understood. When a computer wants to make a connection to another, a three-way handshake is done. The initiating computer sends a SYN packet which tells the other computer, “Hey, I want to give you something but just so know I’m trustworthy, let’s do our handshake!”. The receiving computer sends out a SYN/ACK packet in response, which means, “Ok, sounds good, and I am letting you know that I got your request and am ready.” The first computer finally sends an ACK packet, saying, “Thanks for accepting my request. Let’s do this!”, and the connection is established.

To reiterate, the three-way handshake takes the form of:

**SYN** 🡪 **SYN/ACK** 🡪 **ACK**

That was probably a very long-winded explanation, but bear with me, it is important to understand what happens for the attack.



*SynFlood sample.pcap*

The example shown here is from a program called Wireshark which listens in on network traffic and logs the results in data called .pcap files. A closer look at the file will show various SYN packets thrown to the receiving computer repeatedly before resetting. Every time a SYN packet is sent, the receiving computer will attempt to respond to it with the next packet, but if the packets are sent out like this, then the second computer (in this case, the victim) will not have time to react because it is still trying to respond to the previous packet. The victim computer will not know what to do, exhaust all its resources, and eventually crash. This type of attack can devastate a network and bring it to its knees.

To simplify all of this, imagine two people having a conversation. One person comes along and asks one of them a question while they are talking. Another person comes and asks a different question, and then another, and another. Suddenly, 30 people are trying to talk to this one individual, and they cannot focus on the person they were having a conversation with in the first place. They might just get angry enough and storm off with finishing the conversation. Such a thing could happen to disrupt a working network if steps are not taken to prevent it.

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