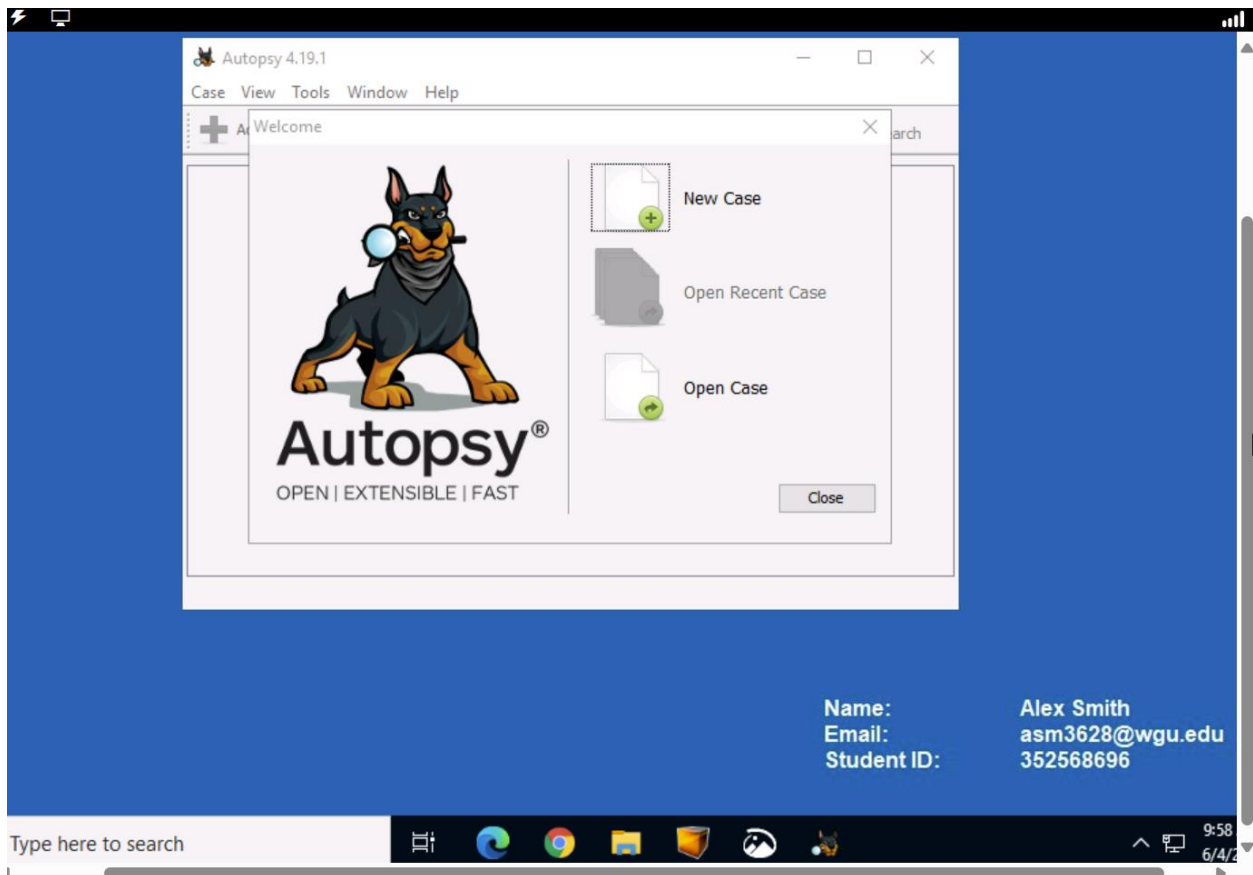Digital Forensics in Cybersecurity – D431

Alex Smith

June 04, 2024

A.1 Create a forensic system case file

The first step was to launch Autopsy on the desktop by double clicking Autopsy on the desktop then clicking on new case.

Created the Case named John Smith, manually entered the desired base directory path as C:\Users\LabUser\Desktop\Evidence Files and clicked "Select" then "Next" on following window.
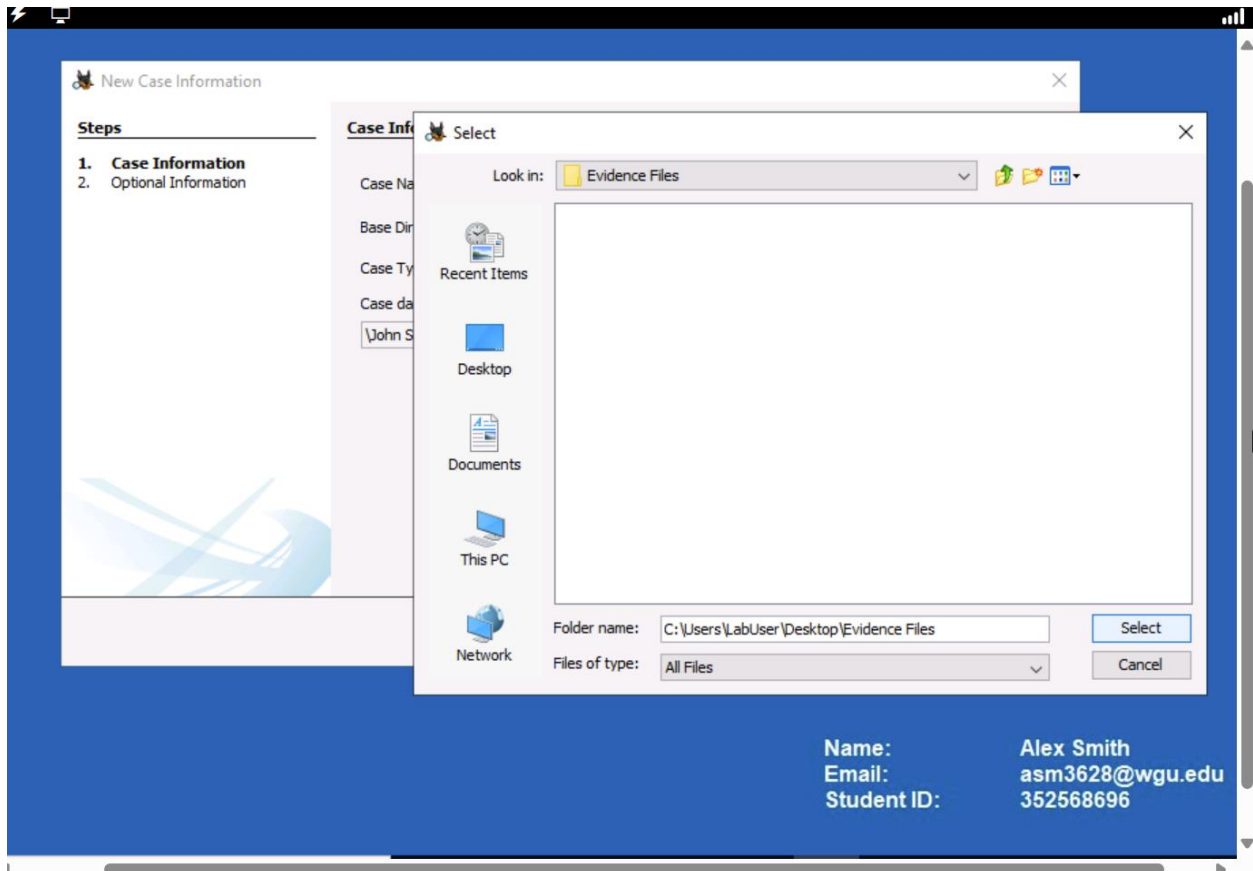
New Case Information

Steps

1. **Case Information**
2. Optional Information

Case Information

Case Name: John Smith

Base Directory: C:\Users\LabUser\Desktop\Evidence Files [Browse]

Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:

C:\Users\LabUser\Desktop\Evidence Files\John Smith

[< Back] [Next >] [Finish] [Cancel] [Help]

Name: Alex Smith
Email: asm3628@wgu.edu
Student ID: 352568696

I Entered my Student ID number as the case number and the name on the examiner details page then hit "Finish"

Selected Host accepted the default settings and clicked Next. Chose the data source type, Disk Image or VM file, and clicked "Next"

i
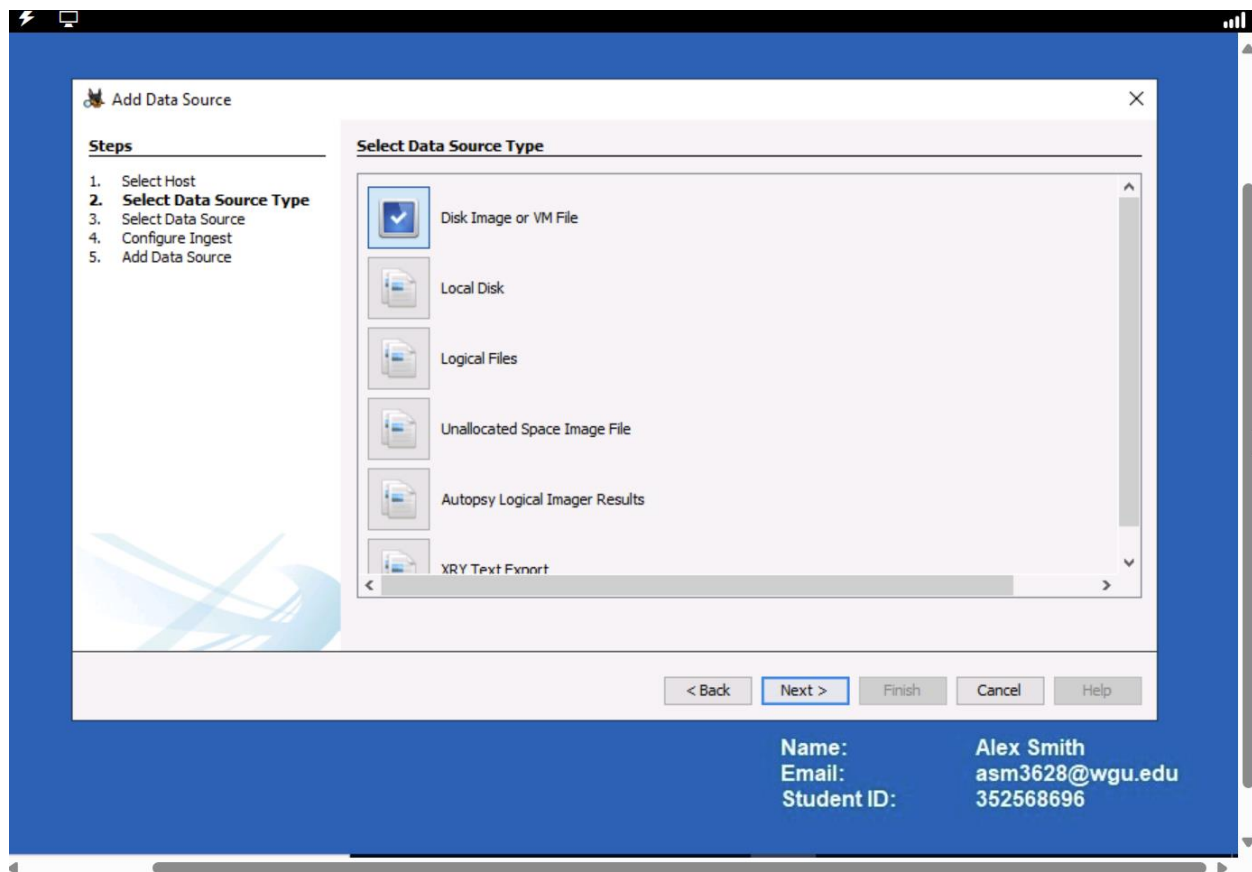
I Selected the Data Source path by browsing to: C:\Users\LabUser\Desktop\Evidence Files\JSmith_Q1.001. Chose the Data Source and accepted the defaults, then clicked Next. Configured Ingest with the default settings and clicked Next. Added the Data Source and, upon seeing the message "Data source has been added to the local database. Files are being analyzed," clicked Finish.

Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Open

Look in: Evidence Files

Recent Items

Desktop

Documents

This PC

Network

John Smith
JSmith_Q1.001

File name: JSmith_Q1.001

Files of type: All Supported Types

Open

Cancel

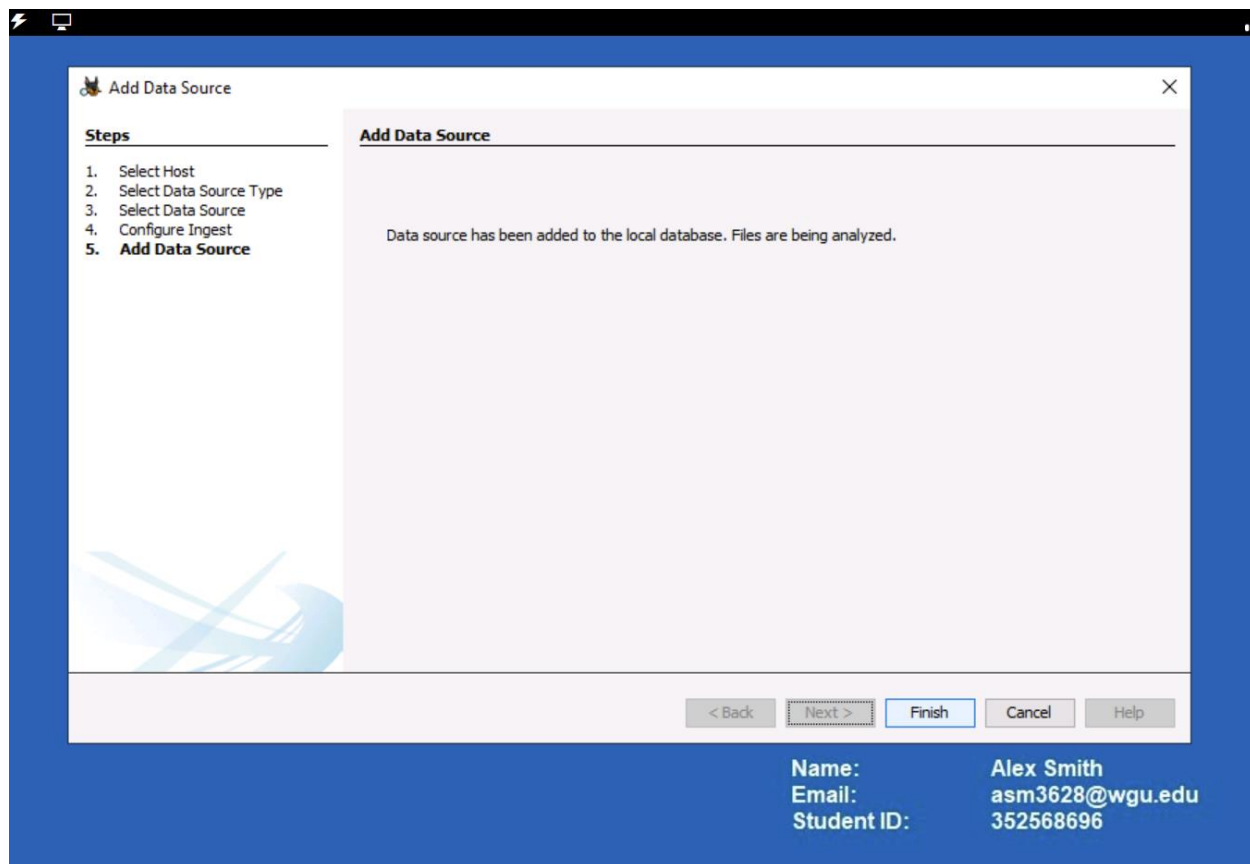< Back   Next >   Finish   Cancel   Help

Name: Alex Smith
Email: asm3628@wgu.edu
Student ID: 352568696

At this time, I begin my analysis

While performing my analysis, I locate and right-click on the desired file name. From the context menu, select "Extract File(s)." I Choose to save the files to the Export Folder located at: C:\Users\LabUser\Desktop\Evidence Files\Example\Export

File Explorer window titled "Export"

Path: « John... > Export

Search Export

Name	Date modified	Type
Business_Strategy.pdf	6/4/2024 10:38 AM	Microsoft
Drilling Methodology.pdf	6/4/2024 10:35 AM	Microsoft
f0000000_business_Strategy.pdf	6/4/2024 10:35 AM	Microsoft
f0001128_Drilling_Methodology.pdf	6/4/2024 10:35 AM	Microsoft
f0002256.pdf	6/4/2024 10:35 AM	Microsoft
f0002784.jpg	6/4/2024 10:36 AM	JPG File
f0002808.jpg	6/4/2024 10:36 AM	JPG File
f0002824.pdf	6/4/2024 10:36 AM	Microsoft
How to buy and pay with bitcoin anony...	6/4/2024 10:35 AM	Microsoft
Oil_co_Conf.jpg	6/4/2024 10:35 AM	JPG File
Oilco_Conf2.jpg	6/4/2024 10:35 AM	JPG File
The best way to hide something, is in plai...	6/4/2024 10:35 AM	Microsoft

Quick access
- Desktop
- Downloads
- Documents
- Pictures

This PC
- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures

12 items

Name: Alex Smith
Email: asm3628@wgu.edu
Student ID: 352568696

A.2 Evidence

Oil Company
CONFIDENTIAL Restricted
Business Strategies 2021

Innovating energy solutions: Research and development highlights

R&D has been part of Oil Company since our company began. Our innovations have helped provide the energy fundamental to modern life – from the clean, efficient fuels that power today's transportation to the natural gas that provides light and heat to homes and businesses.

Today, our world faces a dual challenge: meeting growing demand for energy while also reducing environmental impacts, including the risks of climate change. Oil Company is committed to doing our part.

Today, we are working to develop the next generation of energy solutions, including: advanced biofuels; carbon capture and storage; natural gas technologies; and new energy efficiency processes. In addition to our robust in-house capabilities, we collaborate with leading research and technology companies, national labs and universities, and others involved in breakthrough energy research. While all forms of energy are needed – including natural gas and renewables such as wind and solar – new technologies will be required to meet the world's emissions-

Name: Alex Smith
Email: asm3628@wgu.edu
Student ID: 352568696

Oil Company
CONFIDENTIAL Restricted
Oil Strategies 2021
Field 007-A

Field 007-A was recently located in Nigeria. Current discussions with local government have been successful and the below methods will be used in the various parcels of the field. Proprietary methods listed below will result in maximum extraction with little environmental concerns. Current business risk is competitors learning the methodology and steps used in the location based on soil conditions. The company first to deploy these technologies should be able to extract more than 75% of available oil.

Conventional Enhanced Oil Recovery Methods

- Controlled-ionic flooding
  - SmartWater flooding
  - Low salinity flooding
- Chemical EOR
  - Alkaline flooding
  - Surfactant flooding
- Gas EOR
  - CO₂ flooding
- Thermal EOR

Figure 1
Classification of conventional enhanced oil recovery methods.

comparitech

Search 🔍

VPN ▾   Antivirus   Online backup   Streaming ▾   Blog ▾   More Comparisons ▾   About Us ▾

Crypto » How to buy and pay with bitcoin anonymously

We are reader supported and may earn a commission when you buy through links on our site

How to buy and pay with bitcoin anonymously

AIMEE O'DRISCOLL · VPN AND CYBERSECURITY EXPERT
April 18, 2018

f ⓧ ⓟ G⁺ in

BITCOIN
ACCEPTED HERE

As a form of currency, bitcoin has many advantages. Based on blockchain technology, it offers a secure method of fast payments with relatively low transaction fees. While the nature of the blockchain makes bitcoin secure, it isn't very private. For those looking to pay with bitcoin anonymously, there are issues to overcome.

While it's not inherently private, there are ways to make buying and paying with bitcoin more anonymous. Even if you purchase coins through an open method, using the right steps you can mask their history and **spend them in almost completely untraceable transactions.**

Popular Posts

10 Best SFTP and FTPS Servers Reviewed 2021
February 27, 2019 / by Jon Watson

Best VPNs for Netflix: Get any version of Netflix anywhere
January 5, 2019 / by Paul Bischoff

10 Best VPNs for Torrenting Safely and Privately in 2021
January 1, 2019 / by Paul Bischoff

Die besten und schlechtesten VPNs für Torrent-Dateien und P2P-Filesharing 2018
September 20, 2018 / by Paul Bischoff

How to make your own free VPN with Amazon Web Services
May 15, 2018 / by Paul Bischoff

Latest Cloud and Online Backup

10 Best Secure File Sharing Tools & Software for Business in 2021
October 21, 2019 / by Tim Keary

Rapidshare is discontinued, try these alternatives
February 4, 2019 / by Aimee O'Driscoll

Name: Alex Smith
Email: asm3628@wgu.edu
Student ID: 352568696

1 of 3

Daily Fintech

Fintech, Crypto and Insurtech trends & analysis

Become a Member About Us Licensing Advisory Services Deans List Log In

Blockchain courseware

10/08/2020 ILIAS LOUIS HATZIS

The best way to hide something, is in plain sight. Crypto laundering.

Want unlimited access to our content and forum? Become a member today.
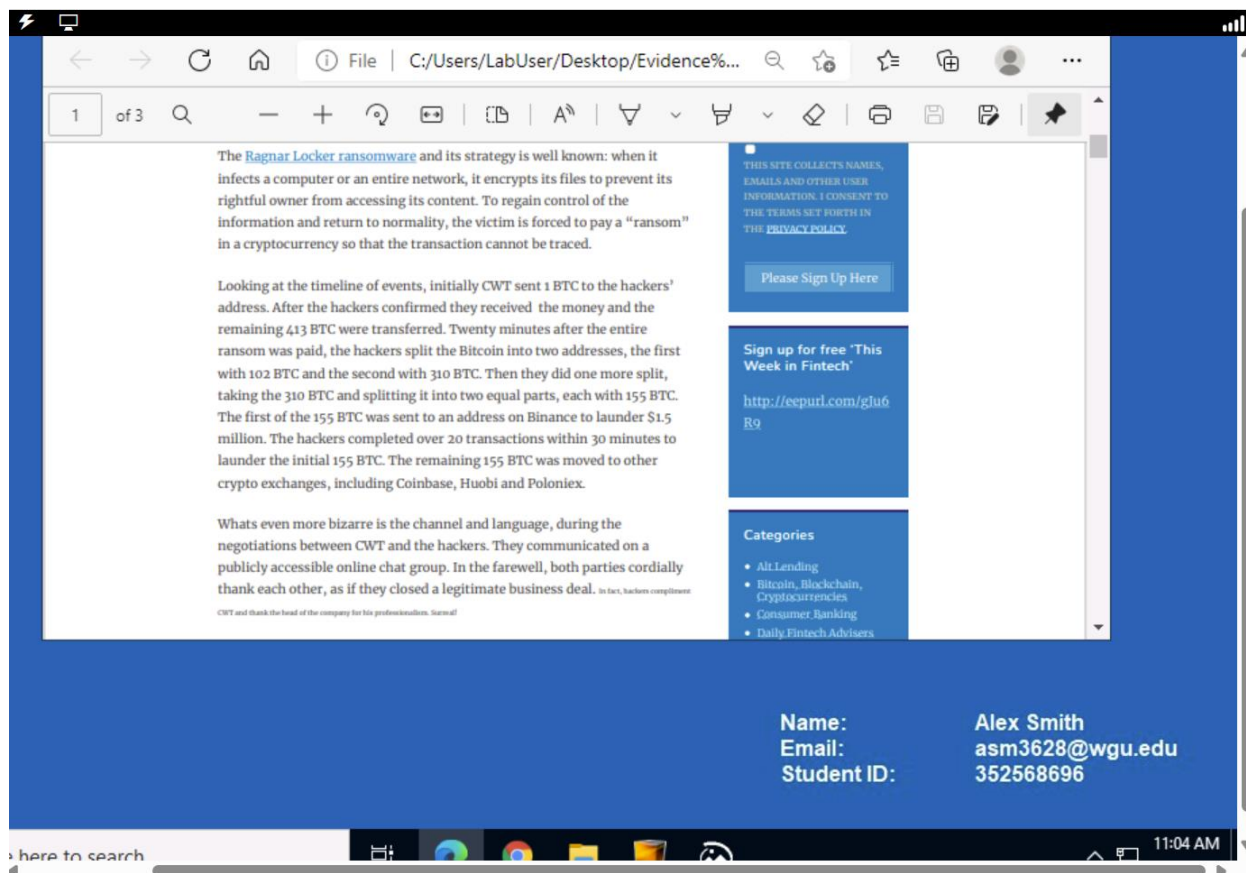
Terms: $143 / Year

FIRST NAME:*

LAST NAME:*

ADDRESS:*

Name: Alex Smith
Email: asm3628@wgu.edu
Student ID: 352568696

The Ragnar Locker ransomware and its strategy is well known: when it infects a computer or an entire network, it encrypts its files to prevent its rightful owner from accessing its content. To regain control of the information and return to normality, the victim is forced to pay a "ransom" in a cryptocurrency so that the transaction cannot be traced.

Looking at the timeline of events, initially CWT sent 1 BTC to the hackers' address. After the hackers confirmed they received the money and the remaining 413 BTC were transferred. Twenty minutes after the entire ransom was paid, the hackers split the Bitcoin into two addresses, the first with 102 BTC and the second with 310 BTC. Then they did one more split, taking the 310 BTC and splitting it into two equal parts, each with 155 BTC. The first of the 155 BTC was sent to an address on Binance to launder $1.5 million. The hackers completed over 20 transactions within 30 minutes to launder the initial 155 BTC. The remaining 155 BTC was moved to other crypto exchanges, including Coinbase, Huobi and Poloniex.

Whats even more bizarre is the channel and language, during the negotiations between CWT and the hackers. They communicated on a publicly accessible online chat group. In the farewell, both parties cordially thank each other, as if they closed a legitimate business deal. In fact, hackers compliment CWT and thank the head of the company for his professionalism. Surreal!

THIS SITE COLLECTS NAMES, EMAILS AND OTHER USER INFORMATION. I CONSENT TO THE TERMS SET FORTH IN THE PRIVACY POLICY.

Please Sign Up Here

Sign up for free 'This Week in Fintech'

http://eepurl.com/gJu6R9

Categories
- Alt Lending
- Bitcoin, Blockchain, Cryptocurrencies
- Consumer Banking
- Daily Fintech Advisers

Name: Alex Smith
Email: asm3628@wgu.edu
Student ID: 352568696

A.3 Summary

From the evidence that was gathered, John Smith seems to have made copies of documents and renamed it. He has also been doing some research on cryptocurrency laundering and how to receive cryptocurrency anonymously. The documents have "CONFIDENTIAL" watermarked on them. This leads me to believe that these documents were confidential, and John Smith may have gained unauthorized access to the confidential documents. There is unmistakable evidence that John Smith was planning to give the documents to a crime team or a competitor of the company in exchange for cryptocurrency or even worse use ransomware to withhold documents until he was given money through cryptocurrency undetected. Mr. Smith was researching ways he can launder cryptocurrency as seen in evidence above, the articles found on his computer on how to launder cryptocurrency. This is enough evidence against Mr. Smith to confirm he has wrongly taken confidential documents and was planning to use them for his own personal gain at any means necessary that would have hurt his Oil Company financially and its reputation.