Case: Hood_Capstone

Date Warrant Executed: 2024/04/20

Location: Orem, UT 84057

Devices Seized

1 Kali Box

1 Windows Computer

Chain of Custody

Kali box

Imaged on scene 2024-04-20 15:18. The machine was imaged by Christopher Hood on scene using the DD command with the OF: An external hard drive (T7Shield). T7Shield remained with investigator back to the station where the image was copied for data integrity. The copy is on the Investigators computer HDD. Autopsy was run and a case was created. Case name: Capstone. DD image was added to the case and ingest modules commenced 2024/04/21 14:00.

Windows Computer

Imaged in lab 2024-04-22. Machine was imaged by Christopher Hood using a password found on a sticky note in suspects apartment. FTK imager was added to the machine and imaging commenced at 14:07 MDT. Through the investigation there were traces of email used. A warrant was obtained for email communications from the email ralphdenizen@gmail.com. Gmail warrant issued 2024-04-23.

Device Details

Kali

MD5: 09de2a51047c0b921e4ad28e6c478e27

Size: 85.9Gb

Users: Kali (Default), Ralph. Both have root access.

Install Date: 2024-04-06

Time Zone: MDT

Windows

MD5: ce966b5b1145185b62922e791cef4b12

Size: 161Gb

Users: Ralph Denizen

OS: Windows 10 Pro

Install Date: 2024-03-22

Time Zone: MDT

Contents

Investigation

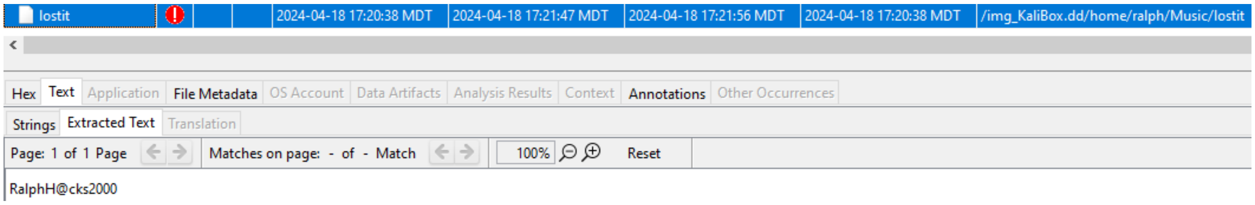
Media

2 images were found on the Kali Box. The are photographs of $100 bills on a table. One of them contains some burglary tools and a credit card reader.

1 mp4 file was found in the emails that contained a conversation between Ralph and a 3rd person. From the email it appears that Ralph altered his voice, but the other person's voice was unedited. The mp4 file is on the case flash drive.

Documents

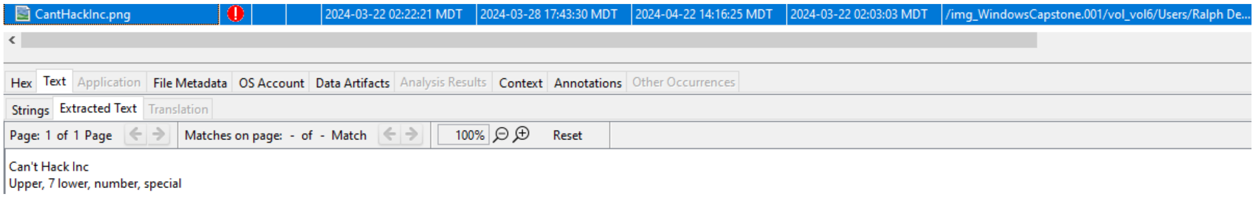
1 document was found on the user Ralph in the Kali box in the music folder titled "lostit.txt" It contained the password to his Gmail account, and might be used for other documents that are encrypted.



lostit	!			2024-04-18 17:20:38 MDT	2024-04-18 17:21:47 MDT	2024-04-18 17:21:56 MDT	2024-04-18 17:20:38 MDT	/img_KaliBox.dd/home/ralph/Music/lostit

RalphH@cks2000

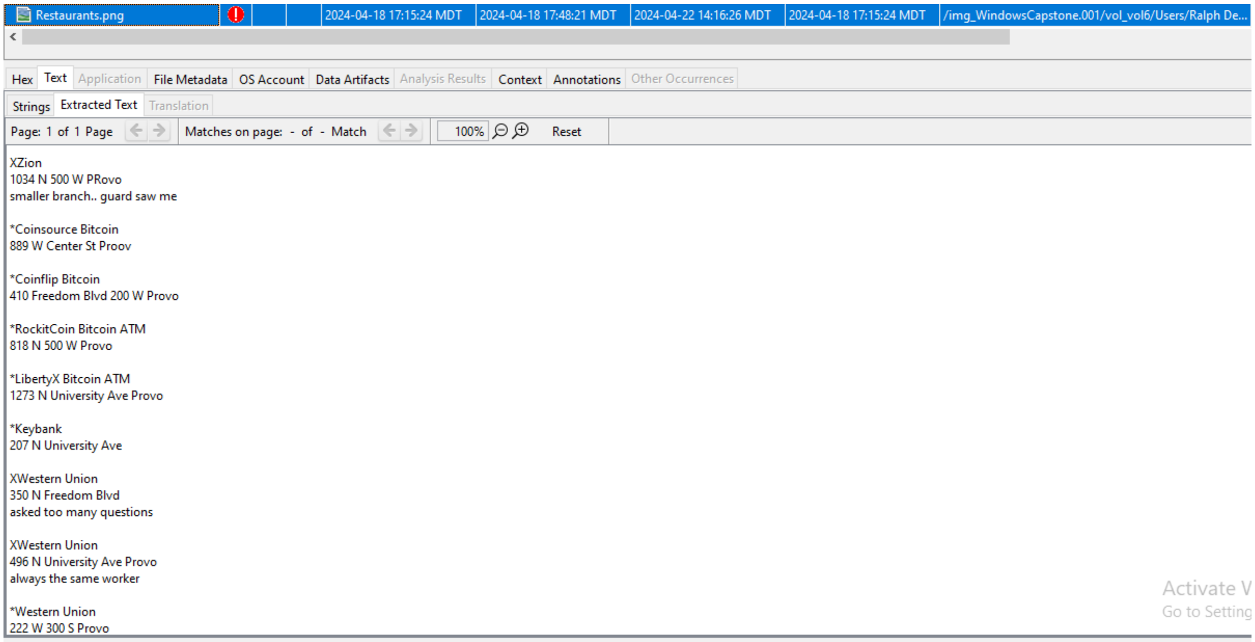
There was a file that had a mismatched file extension with a Company name and some text that appears to be password requirements.



```
CantHackInc.png | 2024-03-22 02:22:21 MDT | 2024-03-28 17:43:30 MDT | 2024-04-22 14:16:25 MDT | 2024-03-22 02:03:03 MDT | /img_WindowsCapstone.001/vol_vol6/Users/Ralph De...
```

```
Can't Hack Inc
Upper, 7 lower, number, special
```

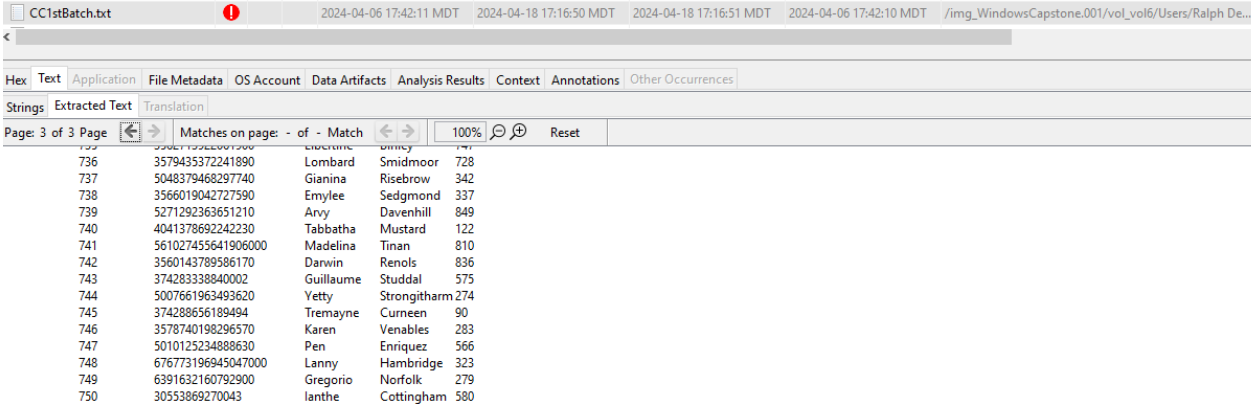
Another mismatched file contained ATM locations in Utah County with notes on the locations with what appears to be frequented locations that should be examined.



```
Restaurants.png | 2024-04-18 17:15:24 MDT | 2024-04-18 17:48:21 MDT | 2024-04-22 14:16:26 MDT | 2024-04-18 17:15:24 MDT | /img_WindowsCapstone.001/vol_vol6/Users/Ralph De...
```

```
XZion
1034 N 500 W PRovo
smaller branch.. guard saw me

*Coinsource Bitcoin
889 W Center St Proov

*Coinflip Bitcoin
410 Freedom Blvd 200 W Provo

*RockitCoin Bitcoin ATM
818 N 500 W Provo

*LibertyX Bitcoin ATM
1273 N University Ave Provo

*Keybank
207 N University Ave

XWestern Union
350 N Freedom Blvd
asked too many questions

XWestern Union
496 N University Ave Provo
always the same worker

*Western Union
222 W 300 S Provo
```

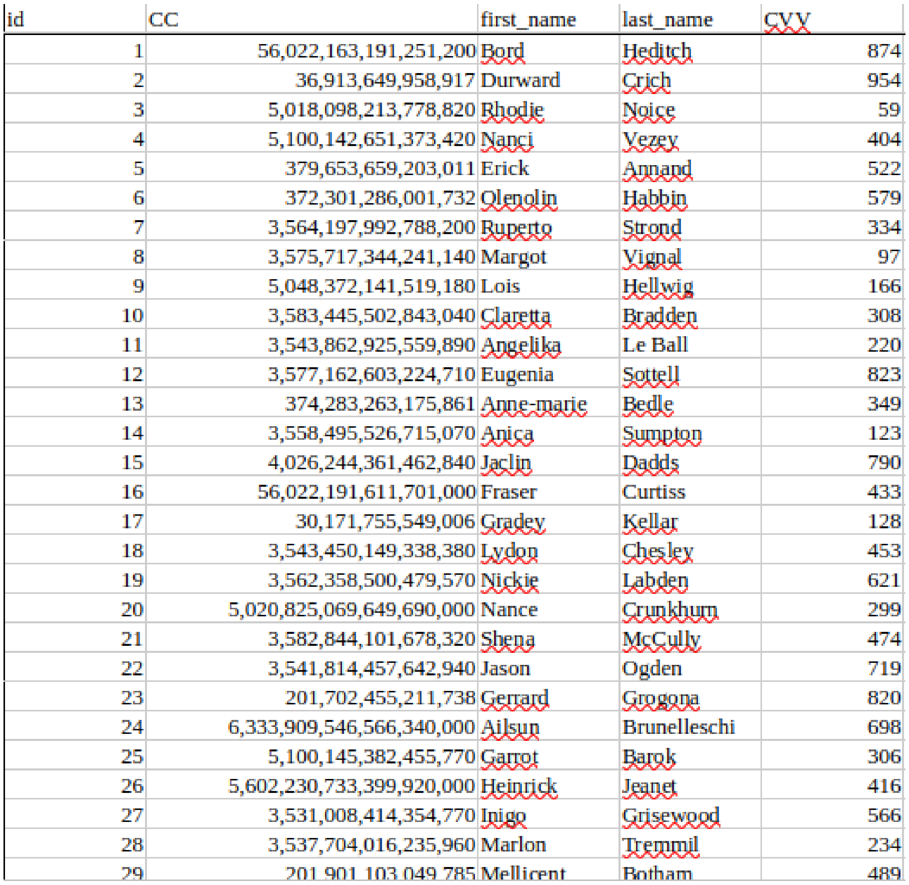
A 3rd mismatched document appears to be a .txt file but is an xls file containing 750 credit cards, names, and CVV numbers. The document is titled CC1stBatch. The creator is a Christopher and the document was downloaded on 2024-04-06 from an email sent from Christopher Hood. Because there is email communications and nothing on the image, a warrant was issued to Gmail to release his account to us.



```
CC1stBatch.txt | 2024-04-06 17:42:11 MDT | 2024-04-18 17:16:50 MDT | 2024-04-18 17:16:51 MDT | 2024-04-06 17:42:10 MDT | /img_WindowsCapstone.001/vol_vol6/Users/Ralph De...
```

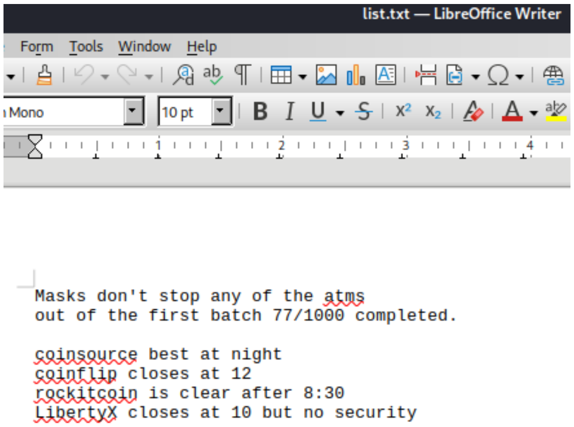
736	3579435372241890	Lombard	Smidmoor	728
737	5048379468297740	Gianina	Risebrow	342
738	3566019042727590	Emylee	Sedgmond	337
739	5271292363651210	Arvy	Davenhill	849
740	4041378692242230	Tabbatha	Mustard	122
741	561027455641906000	Madelina	Tinan	810
742	3560143789586170	Darwin	Renols	836
743	374283338840002	Guillaume	Studdal	575
744	5007661963493620	Yetty	Strongitharm	274
745	374288656189494	Tremayne	Curneen	90
746	3578740198296570	Karen	Venables	283
747	5010125234888630	Pen	Enriquez	566
748	676773196945047000	Lanny	Hambridge	323
749	6391632160792900	Gregorio	Norfolk	279
750	30553869270043	Ianthe	Cottingham	580

The encrypted 1stBatch.ods.cpt file on the Kali box contained 1750 credit cards with names and CVV numbers. 750 of them were the same as the CC1stBatch mismatched file. With some pentesting tools the password was cracked in a Kali Linux Forensic Machine. The password was RalphH@cks. The document was double encrypted with the ccrypt tool and a password through libreoffice, an application similar to Excel for Microsoft. The document was created on 2024-04-06 and edited on 2024-04-18. How the data was acquired was not found.



id	CC	first_name	last_name	CVV
1	56,022,163,191,251,200	Bord	Heditch	874
2	36,913,649,958,917	Durward	Crich	954
3	5,018,098,213,778,820	Rhodie	Noice	59
4	5,100,142,651,373,420	Nanci	Vezey	404
5	379,653,659,203,011	Erick	Annand	522
6	372,301,286,001,732	Olenolin	Habbin	579
7	3,564,197,992,788,200	Ruperto	Strond	334
8	3,575,717,344,241,140	Margot	Vignal	97
9	5,048,372,141,519,180	Lois	Hellwig	166
10	3,583,445,502,843,040	Claretta	Bradden	308
11	3,543,862,925,559,890	Angelika	Le Ball	220
12	3,577,162,603,224,710	Eugenia	Sottell	823
13	374,283,263,175,861	Anne-marie	Bedle	349
14	3,558,495,526,715,070	Anica	Sumpton	123
15	4,026,244,361,462,840	Jaclin	Dadds	790
16	56,022,191,611,701,000	Fraser	Curtiss	433
17	30,171,755,549,006	Gradey	Kellar	128
18	3,543,450,149,338,380	Lydon	Chesley	453
19	3,562,358,500,479,570	Nickie	Labden	621
20	5,020,825,069,649,690,000	Nance	Crunkhurn	299
21	3,582,844,101,678,320	Shena	McCully	474
22	3,541,814,457,642,940	Jason	Ogden	719
23	201,702,455,211,738	Gerrard	Grogona	820
24	6,333,909,546,566,340,000	Ailsun	Brunelleschi	698
25	5,100,145,382,455,770	Garrot	Barok	306
26	5,602,230,733,399,920,000	Heinrick	Jeanet	416
27	3,531,008,414,354,770	Inigo	Grisewood	566
28	3,537,704,016,235,960	Marlon	Tremmil	234
29	201,901,103,049,785	Mellicent	Botham	489

The other encrypted document was a .txt file that had a little further information about some of the ATMs.



```
Masks don't stop any of the atms
out of the first batch 77/1000 completed.

coinsource best at night
coinflip closes at 12
rockitcoin is clear after 8:30
LibertyX closes at 10 but no security
```

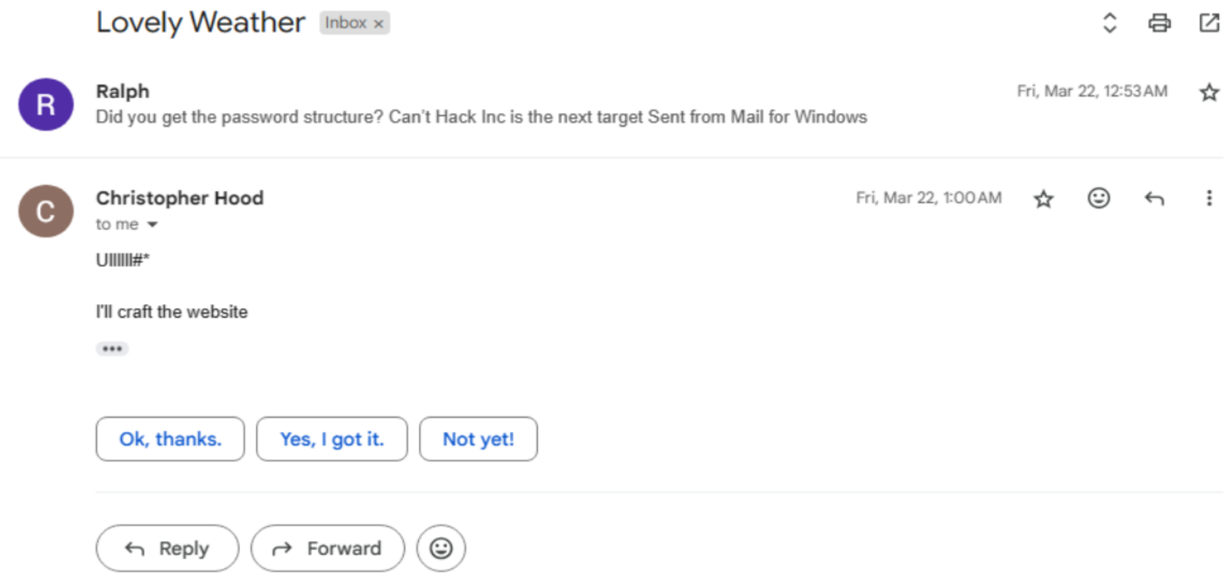
Emails

Christopher Hood (not the same as the investigator) is associated with firefighterhood20@gmail.com

Ralph's email is ralphdenizen@gmail.com

Harry's email is harrybellskin@gmail.com

Ralph emailed Christopher requesting the password structure for a company called Can't Hack Inc. Christopher responded with some characters presumably the structure for passwords in the company, and told Ralph he would craft a website. This appears to be tied to the mismatched file title CantHackInc. Potentially setting up for the social engineering toolkit and setting up a phishing campaign. Can't Hack Inc should be reached out to.



Lovely Weather

Ralph — Fri, Mar 22, 12:53 AM

Did you get the password structure? Can't Hack Inc is the next target Sent from Mail for Windows

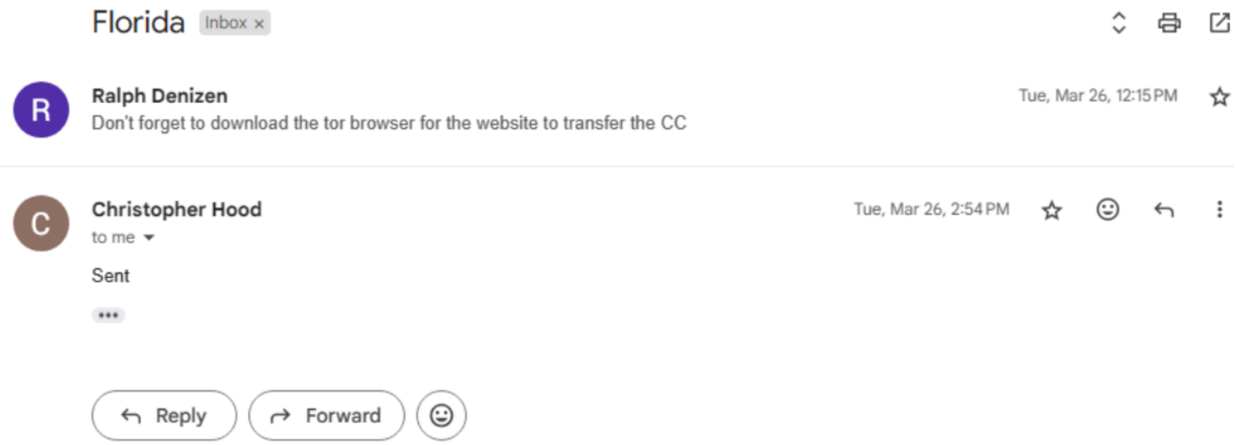
Christopher Hood — Fri, Mar 22, 1:00 AM

to me

Ullllll#*

I'll craft the website

Ralph messaged Christopher telling him to download TOR to get to a secure website for data transfer. No files appear to be downloaded around this time frame.



Florida

Ralph Denizen — Tue, Mar 26, 12:15 PM

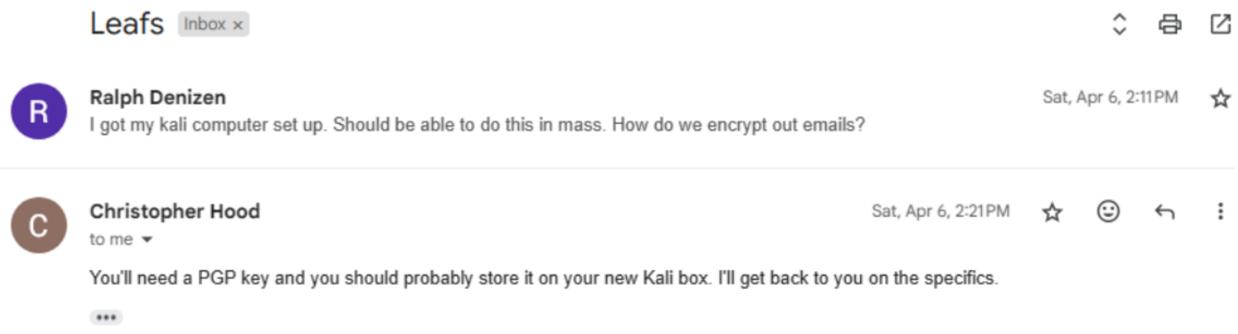
Don't forget to download the tor browser for the website to transfer the CC

Christopher Hood — Tue, Mar 26, 2:54 PM

to me

Sent

Ralph let Christopher know he set up his Kali box. He also asked for encryption methods. No PGP key was found on any seized evidence.



Leafs

Ralph Denizen — Sat, Apr 6, 2:11 PM

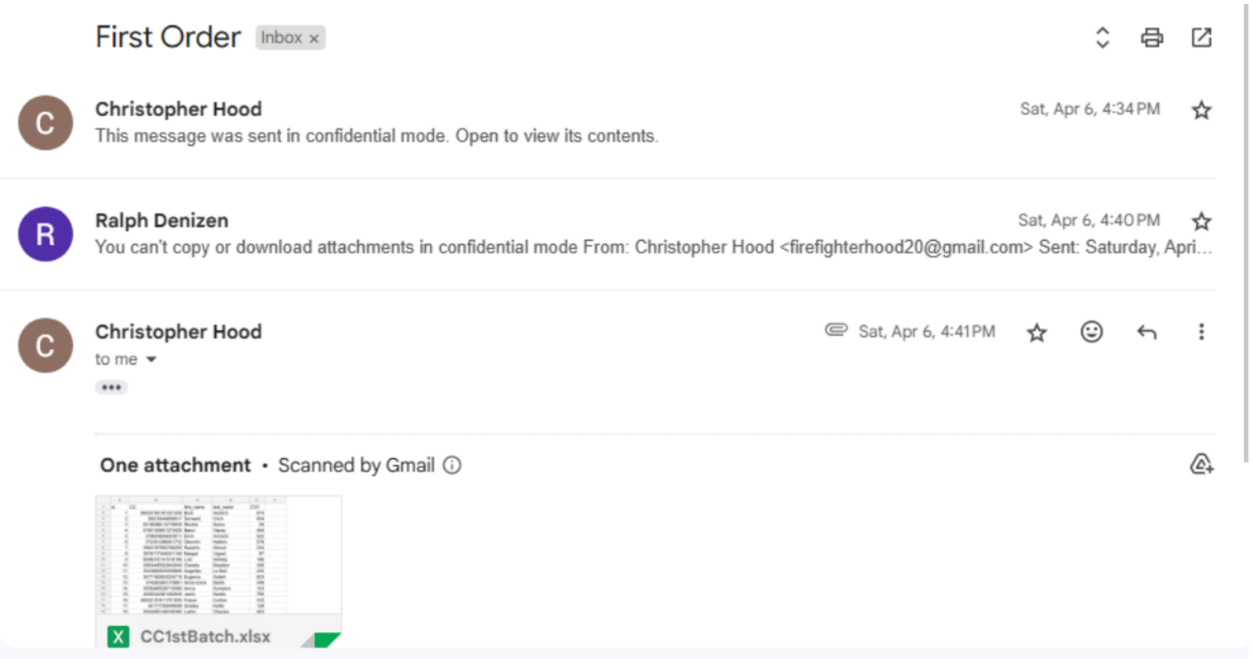
I got my kali computer set up. Should be able to do this in mass. How do we encrypt out emails?

Christopher Hood — Sat, Apr 6, 2:21 PM

to me

You'll need a PGP key and you should probably store it on your new Kali box. I'll get back to you on the specifics.

Christopher sent Ralph a confidential email with a document that Ralph said he wasn't able to see. The CC1stBatch.xlsx file was sent and Ralph downloaded it then changed the file extension.



First Order

Christopher Hood — Sat, Apr 6, 4:34 PM

This message was sent in confidential mode. Open to view its contents.

Ralph Denizen — Sat, Apr 6, 4:40 PM

You can't copy or download attachments in confidential mode From: Christopher Hood <firefighterhood20@gmail.com> Sent: Saturday, Apri…

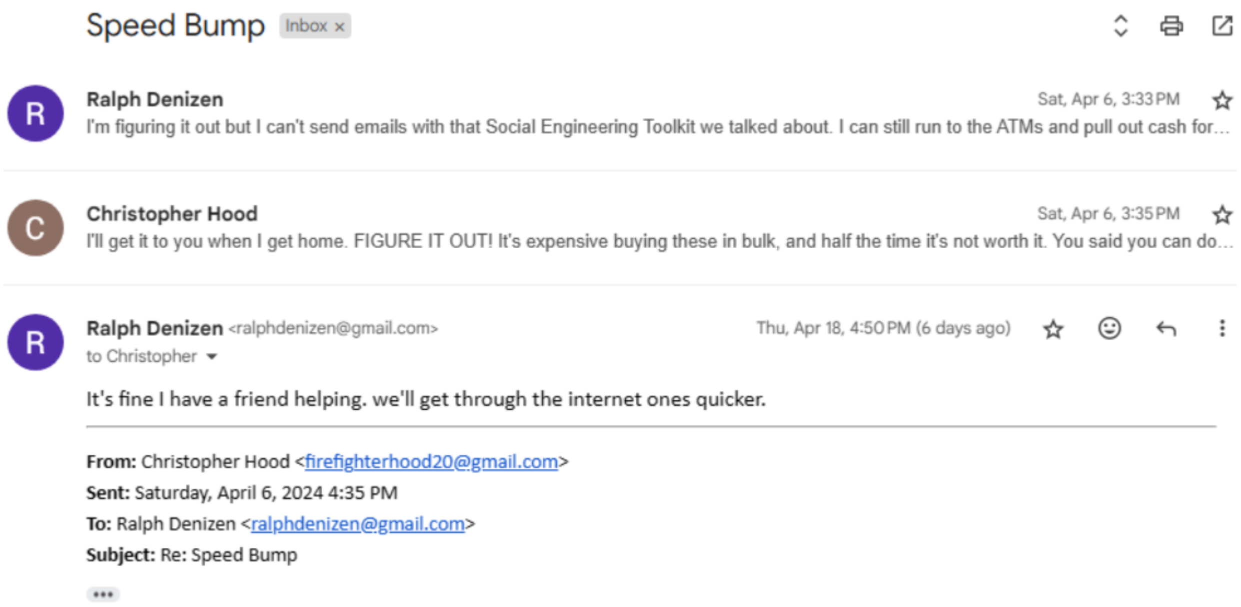
Christopher Hood — Sat, Apr 6, 4:41 PM

to me

One attachment • Scanned by Gmail

CC1stBatch.xlsx

Ralph ran into issues with the SEToolkit which corresponds to the search history. Christopher seemed to get upset at Ralph. Christopher seems to be in charge of the operation, and should be reviewed. From this email and the prior one with the Credit Card numbers there is enough evidence to obtain a warrant for Christopher.



Speed Bump

Ralph Denizen — Sat, Apr 6, 3:33 PM
I'm figuring it out but I can't send emails with that Social Engineering Toolkit we talked about. I can still run to the ATMs and pull out cash for…

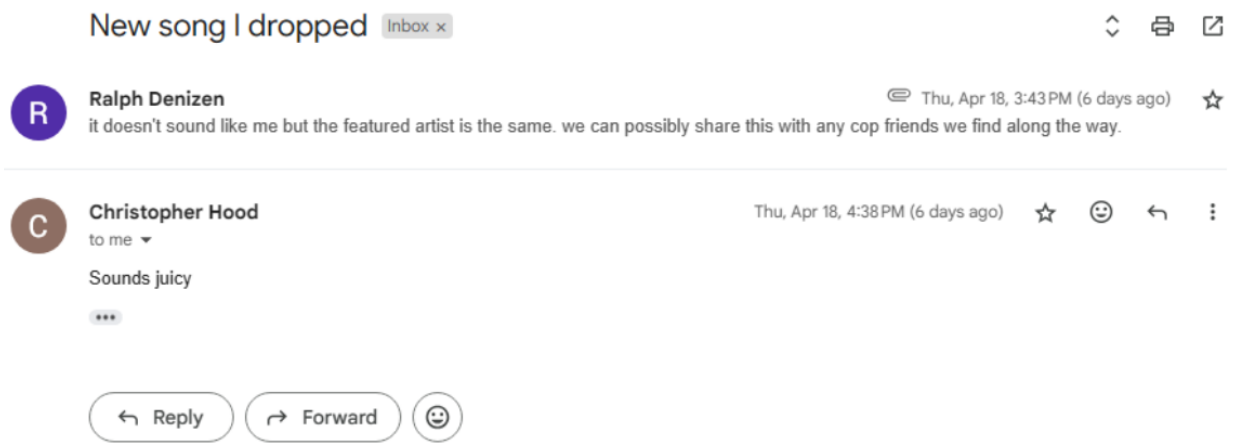
Christopher Hood — Sat, Apr 6, 3:35 PM
I'll get it to you when I get home. FIGURE IT OUT! It's expensive buying these in bulk, and half the time it's not worth it. You said you can do…

Ralph Denizen <ralphdenizen@gmail.com> — Thu, Apr 18, 4:50 PM (6 days ago)
to Christopher

It's fine I have a friend helping. we'll get through the internet ones quicker.

From: Christopher Hood <firefighterhood20@gmail.com>
Sent: Saturday, April 6, 2024 4:35 PM
To: Ralph Denizen <ralphdenizen@gmail.com>
Subject: Re: Speed Bump

The “new song” was an mp4 file with Ralph and another person talking about a card reader and paying $100 for 10.



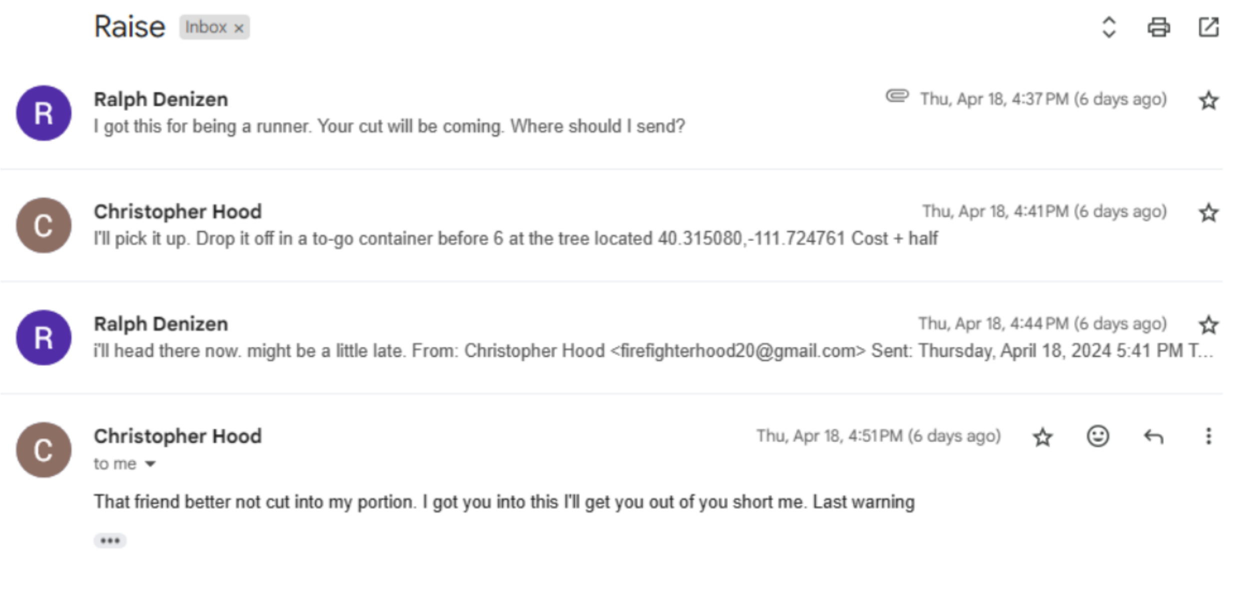
New song I dropped

Ralph Denizen — Thu, Apr 18, 3:43 PM (6 days ago)
it doesn't sound like me but the featured artist is the same. we can possibly share this with any cop friends we find along the way.

Christopher Hood — Thu, Apr 18, 4:38 PM (6 days ago)
to me

Sounds juicy

Ralph had a 3rd person to help him. Around this time he created a slack channel and Harry joined that channel. A warrant should be obtained for slack messages, and the focus should be seeing Harry’s involvement. From the last response on this thread Christopher got Ralph into these criminal activities and should be investigated as well.



Raise

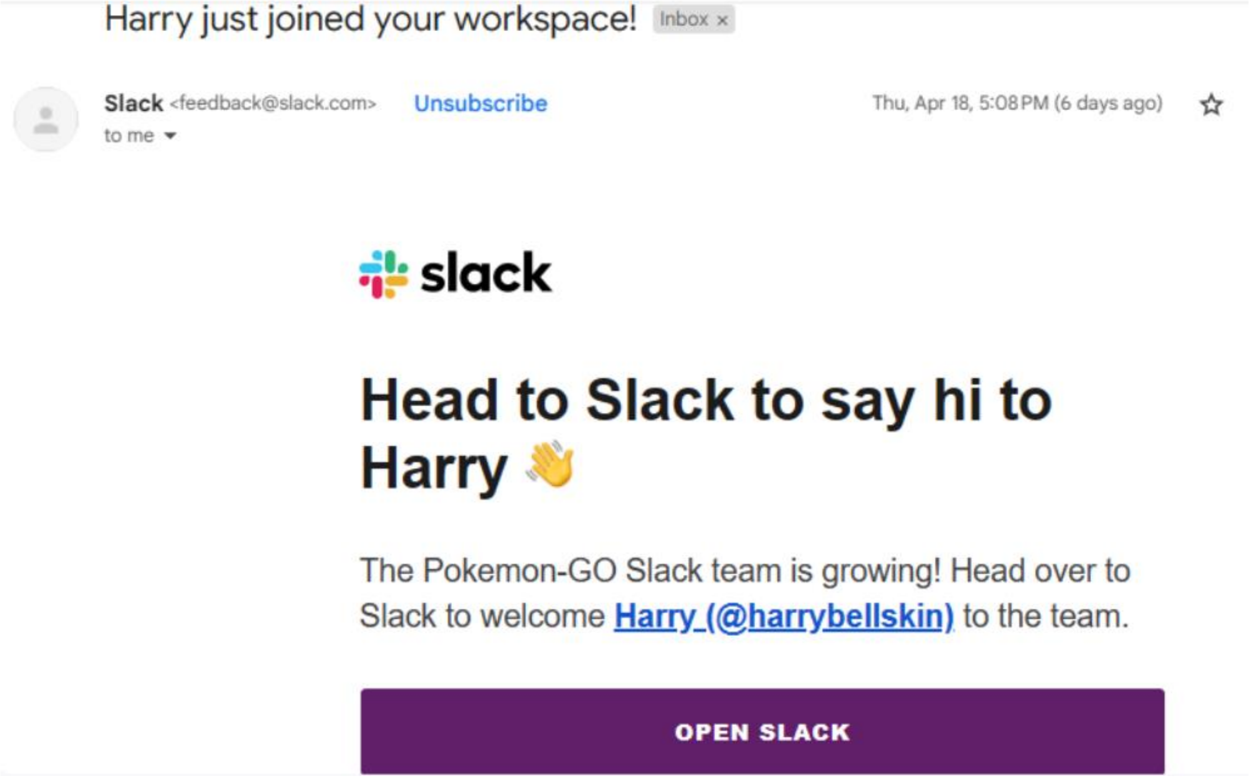
Ralph Denizen Thu, Apr 18, 4:37 PM (6 days ago)
I got this for being a runner. Your cut will be coming. Where should I send?

Christopher Hood Thu, Apr 18, 4:41 PM (6 days ago)
I'll pick it up. Drop it off in a to-go container before 6 at the tree located 40.315080,-111.724761 Cost + half

Ralph Denizen Thu, Apr 18, 4:44 PM (6 days ago)
i'll head there now. might be a little late. From: Christopher Hood <firefighterhood20@gmail.com> Sent: Thursday, April 18, 2024 5:41 PM T...

Christopher Hood Thu, Apr 18, 4:51 PM (6 days ago)
to me

That friend better not cut into my portion. I got you into this I'll get you out of you short me. Last warning



Harry just joined your workspace!

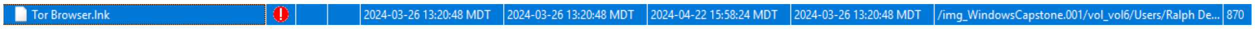
Slack <feedback@slack.com> Unsubscribe Thu, Apr 18, 5:08 PM (6 days ago)
to me

Head to Slack to say hi to Harry 👋

The Pokemon-GO Slack team is growing! Head over to Slack to welcome Harry (@harrybellskin) to the team.

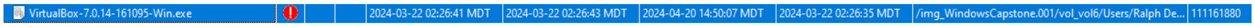
Suspicious Applications

The Onion Router (TOR) was downloaded on the Windows machine. It was frequently visited. The browser does not save local data but is frequently used for connecting to websites on the dark web. The browser was downloaded 2024-03-26



Tor Browser.lnk	!			2024-03-26 13:20:48 MDT	2024-03-26 13:20:48 MDT	2024-04-22 15:58:24 MDT	2024-03-26 13:20:48 MDT	/img_WindowsCapstone.001/vol_vol6/Users/Ralph De...	870

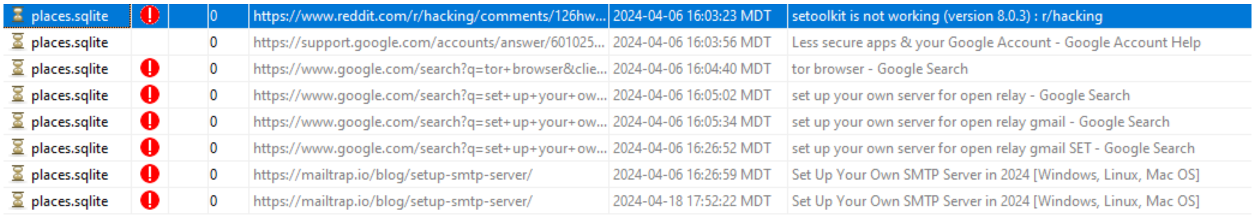
VirtualBox was downloaded on 2024-03-22 but no VM's were found on either machine.



VirtualBox-7.0.14-161095-Win.exe	❗			2024-03-22 02:26:41 MDT	2024-03-22 02:26:43 MDT	2024-04-20 14:50:07 MDT	2024-03-22 02:26:35 MDT	/img_WindowsCapstone.001/vol_vol6/Users/Ralph De...	111161880

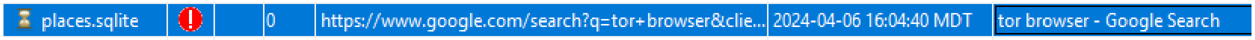
Search History

User Ralph searched on 2024-04-06 for a solution to setoolkit a Kali command line application that assists in phishing campaigns. Furthermore, the user searched for setting up their own server for open relay and SMTP servers. This is used for creating your own email domains and servers so that a user can modify email addresses and redirect traffic to a dedicated server. This can be used in creating a phishing campaign and collecting data on a server.



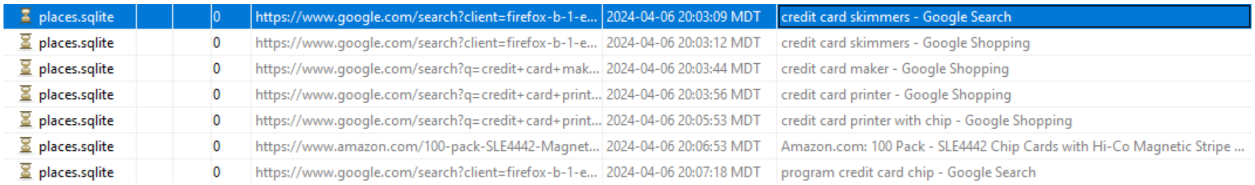
places.sqlite	❗		0	https://www.reddit.com/r/hacking/comments/126hw...	2024-04-06 16:03:23 MDT	setoolkit is not working (version 8.0.3) : r/hacking
places.sqlite			0	https://support.google.com/accounts/answer/601025...	2024-04-06 16:03:56 MDT	Less secure apps & your Google Account - Google Account Help
places.sqlite	❗		0	https://www.google.com/search?q=tor+browser&clie...	2024-04-06 16:04:40 MDT	tor browser - Google Search
places.sqlite	❗		0	https://www.google.com/search?q=set+up+your+ow...	2024-04-06 16:05:02 MDT	set up your own server for open relay - Google Search
places.sqlite	❗		0	https://www.google.com/search?q=set+up+your+ow...	2024-04-06 16:05:34 MDT	set up your own server for open relay gmail - Google Search
places.sqlite	❗		0	https://www.google.com/search?q=set+up+your+ow...	2024-04-06 16:26:52 MDT	set up your own server for open relay gmail SET - Google Search
places.sqlite	❗		0	https://mailtrap.io/blog/setup-smtp-server/	2024-04-06 16:26:59 MDT	Set Up Your Own SMTP Server in 2024 [Windows, Linux, Mac OS]
places.sqlite	❗		0	https://mailtrap.io/blog/setup-smtp-server/	2024-04-18 17:52:22 MDT	Set Up Your Own SMTP Server in 2024 [Windows, Linux, Mac OS]

On 2024-04-06 User Ralph looked up TOR browser which is commonly used to connect to the dark web and websites that require a .onion url and anonymity. Note, the windows computer has TOR downloaded, the Kali box did not.



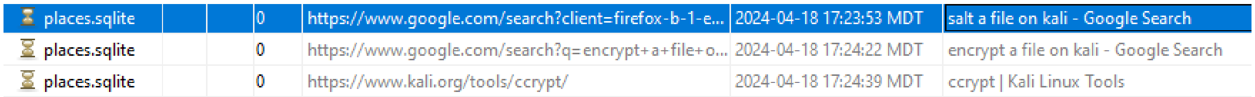
places.sqlite	❗		0	https://www.google.com/search?q=tor+browser&clie...	2024-04-06 16:04:40 MDT	tor browser - Google Search

User Ralph on the Kali box searched for credit card skimmers, credit card makers, credit card printers with chip, program credit card chip, and went to amazon.com looking to purchase 100 pack of blank credit cards with a chip and the magnetic stripe on 2024-04-06.



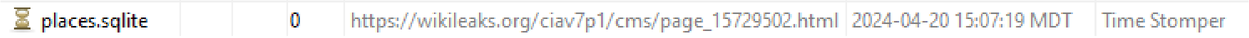
places.sqlite			0	https://www.google.com/search?client=firefox-b-1-e...	2024-04-06 20:03:09 MDT	credit card skimmers - Google Search
places.sqlite			0	https://www.google.com/search?client=firefox-b-1-e...	2024-04-06 20:03:12 MDT	credit card skimmers - Google Shopping
places.sqlite			0	https://www.google.com/search?q=credit+card+mak...	2024-04-06 20:03:44 MDT	credit card maker - Google Shopping
places.sqlite			0	https://www.google.com/search?q=credit+card+print...	2024-04-06 20:03:56 MDT	credit card printer - Google Shopping
places.sqlite			0	https://www.google.com/search?q=credit+card+print...	2024-04-06 20:05:53 MDT	credit card printer with chip - Google Shopping
places.sqlite			0	https://www.amazon.com/100-pack-SLE4442-Magnet...	2024-04-06 20:06:53 MDT	Amazon.com: 100 Pack - SLE4442 Chip Cards with Hi-Co Magnetic Stripe ...
places.sqlite			0	https://www.google.com/search?client=firefox-b-1-e...	2024-04-06 20:07:18 MDT	program credit card chip - Google Search

On 2024-04-18 User Ralph searched how to salt a file and encrypt files on Kali Linux. He alsos searched the Kali utility ccrypt which is a tool to encrypt/decrypt files on Kali. This is consistent with a few documents that have mismatched extensions that are the results of the ccrypt function when used. Analyzing the image for the password.



places.sqlite			0	https://www.google.com/search?client=firefox-b-1-e...	2024-04-18 17:23:53 MDT	salt a file on kali - Google Search
places.sqlite			0	https://www.google.com/search?q=encrypt+a+file+o...	2024-04-18 17:24:22 MDT	encrypt a file on kali - Google Search
places.sqlite			0	https://www.kali.org/tools/ccrypt/	2024-04-18 17:24:39 MDT	ccrypt | Kali Linux Tools

On 2024-04-20 at 15:07 a few minutes before the warrant was executed the user Ralph looked up timestomper an application used to change dates and times of metadata in files. It does not appear that any of the files metadata has been changed in regards to time accesses, changed, created, but examiner is evaluating the potential for this.



places.sqlite			0	https://wikileaks.org/ciav7p1/cms/page_15729502.html	2024-04-20 15:07:19 MDT	Time Stomper

Expert Witness Report

Executive Summary of Findings

Detectives consulted Digital Forensic Examiner Christopher Hood on creating a warrant for Ralph Denizen with fraudulent activities with credit cards. Examiner Hood executed the warrant and imaged the devices found on scene. Through examination, evidence was found on activities pointing to printing credit cards, fraudulent use of those cards, and conspiracy to commit fraud. Email communications and work chats were used in collaboration with a Christopher Hood and a Harry Bellskin. Search history shows potential locations for ATM use and points to locations for further examination. Further warrants for investigating Ralph's cellular device is requested, as well as warrants for coconspirators Harry Bellskin, and Christopher Hood.

Conclusion

From the evidence presented, Ralph Denizen appears to have committed fraud by working with a partner to gather credit card information and then using that information to print credit cards and use those cards in stealing money from ATM's in the Orem/Provo area. Christopher Hood provided 750 credit card numbers, names associated with, and CVV numbers. ATM's were searched for, and notes were taken on each location. Ralph attempted to hide these activities on his devices and encrypt files to prevent investigations. There is an encrypted file that we were unable to crack through a Kali Forensic Machine using some pentesting tools and the ccrypt tool. The encrypted file had an additional 1000 credit card numbers on it, the origins of that file were not found as the metadata did not reveal information other than the creation of the document. We put the file in a Kali box and used the ccrypt function with the password found in the lostit file and found 1000 more credit card entries. Money was distributed to Christopher Hood and Harry Bellskin and the evidence was found on emails and slack chats.