Universidad
Carlos III de Madrid

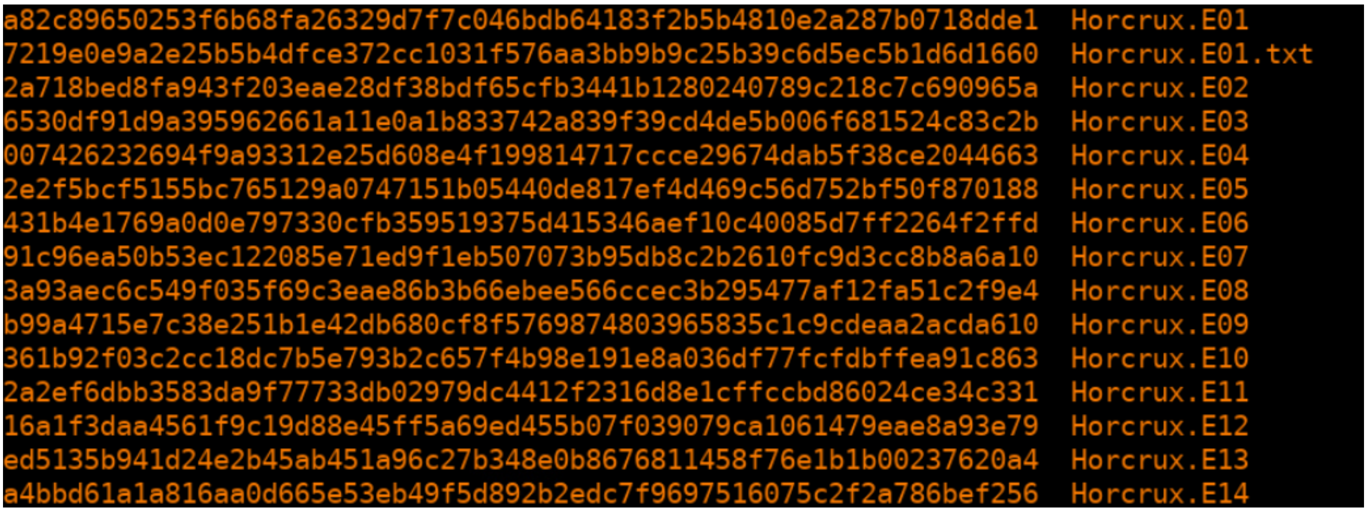
Report for Windows Analysis

Juan Diego Llano Miraval

Fecha: 19/05/2024

procedure

We validate the sha256:



```
a82c89650253f6b68fa26329d7f7c046bdb64183f2b5b4810e2a287b0718dde1  Horcrux.E01
7219e0e9a2e25b5b4dfce372cc1031f576aa3bb9b9c25b39c6d5ec5b1d6d1660  Horcrux.E01.txt
2a718bed8fa943f203eae28df38bdf65cfb3441b1280240789c218c7c690965a  Horcrux.E02
6530df91d9a395962661a11e0a1b833742a839f39cd4de5b006f681524c83c2b  Horcrux.E03
007426232694f9a93312e25d608e4f199814717ccce29674dab5f38ce2044663  Horcrux.E04
2e2f5bcf5155bc765129a0747151b05440de817ef4d469c56d752bf50f870188  Horcrux.E05
431b4e1769a0d0e797330cfb359519375d415346aef10c40085d7ff2264f2ffd  Horcrux.E06
91c96ea50b53ec122085e71ed9f1eb507073b95db8c2b2610fc9d3cc8b8a6a10  Horcrux.E07
3a93aec6c549f035f69c3eae86b3b66ebee566ccec3b295477af12fa51c2f9e4  Horcrux.E08
b99a4715e7c38e251b1e42db680cf8f5769874803965835c1c9cdeaa2acda610  Horcrux.E09
361b92f03c2cc18dc7b5e793b2c657f4b98e191e8a036df77fcfdbffea91c863  Horcrux.E10
2a2ef6dbb3583da9f77733db02979dc4412f2316d8e1cffccbd86024ce34c331  Horcrux.E11
16a1f3daa4561f9c19d88e45ff5a69ed455b07f039079ca1061479eae8a93e79  Horcrux.E12
ed5135b941d24e2b45ab451a96c27b348e0b8676811458f76e1b1b00237620a4  Horcrux.E13
a4bbd61a1a816aa0d665e53eb49f5d892b2edc7f9697516075c2f2a786bef256  Horcrux.E14
```

For the adquisition process

1. What is the name of the examiner who created the E01?

we can look inside the txt file and see:

```
Created By AccessData® FTK® Imager 4.1.1.1

Case Information:
Acquired using: ADI4.1.1.1
Case Number: 9.75
Evidence Number: 394
```

```
Unique description: Lbh'er n jvmneq Uneel!
Examiner: Minerva
Notes: Why does Voldemort only use Twitter and not Facebook? --Because he has
followers not friends...

--------------------------------------------------------------

Information for C:\Users\amanda.johnson01\Downloads\Horcrux\Horcrux:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 6,527
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 104,857,600
[Physical Drive Information]
 Drive Interface Type: lsilogic
[Image]
 Image Type: VMWare Virtual Disk
 Source data size: 51200 MB
 Sector count:    104857600
[Computed Hashes]
 MD5 checksum:    3422bde521801901155f73f7de5cd8fe
 SHA1 checksum:   0fa6ab4bd9a707d49ded70e8b9198fe18114b369

Image Information:
 Acquisition started:   Fri Mar 22 20:08:08 2019
 Acquisition finished:  Fri Mar 22 20:25:53 2019
 Segment list:
  C:\Users\amanda.johnson01\Downloads\Horcrux\Horcrux.E01
  C:\Users\amanda.johnson01\Downloads\Horcrux\Horcrux.E02
  C:\Users\amanda.johnson01\Downloads\Horcrux\Horcrux.E03
  C:\Users\amanda.johnson01\Downloads\Horcrux\Horcrux.E04
  C:\Users\amanda.johnson01\Downloads\Horcrux\Horcrux.E05
  C:\Users\amanda.johnson01\Downloads\Horcrux\Horcrux.E06
  C:\Users\amanda.johnson01\Downloads\Horcrux\Horcrux.E07
  C:\Users\amanda.johnson01\Downloads\Horcrux\Horcrux.E08
  C:\Users\amanda.johnson01\Downloads\Horcrux\Horcrux.E09
  C:\Users\amanda.johnson01\Downloads\Horcrux\Horcrux.E10
  C:\Users\amanda.johnson01\Downloads\Horcrux\Horcrux.E11
  C:\Users\amanda.johnson01\Downloads\Horcrux\Horcrux.E12
  C:\Users\amanda.johnson01\Downloads\Horcrux\Horcrux.E13
  C:\Users\amanda.johnson01\Downloads\Horcrux\Horcrux.E14

Image Verification Results:
 Verification started:  Fri Mar 22 20:25:53 2019
 Verification finished: Fri Mar 22 20:42:12 2019
 MD5 checksum:    3422bde521801901155f73f7de5cd8fe : verified
 SHA1 checksum:   0fa6ab4bd9a707d49ded70e8b9198fe18114b369 : verified
```

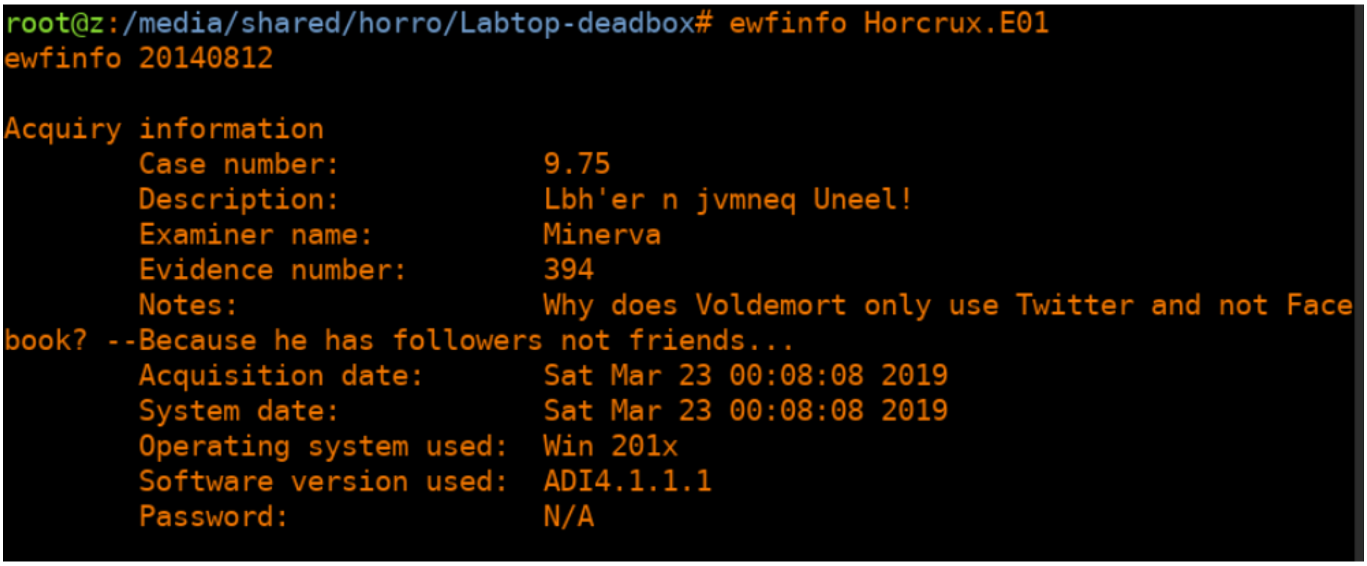
The examiner is Minerva

2. What is the SHA1 hash of the evidence?

From the .txt information provided before, it says that the sha1 is `0fa6ab4bd9a707d49ded70e8b9198fe18114b369`

3. What time was the image created?

Using ewfinfo command we get: Saturday March 23 00:08:08 2019



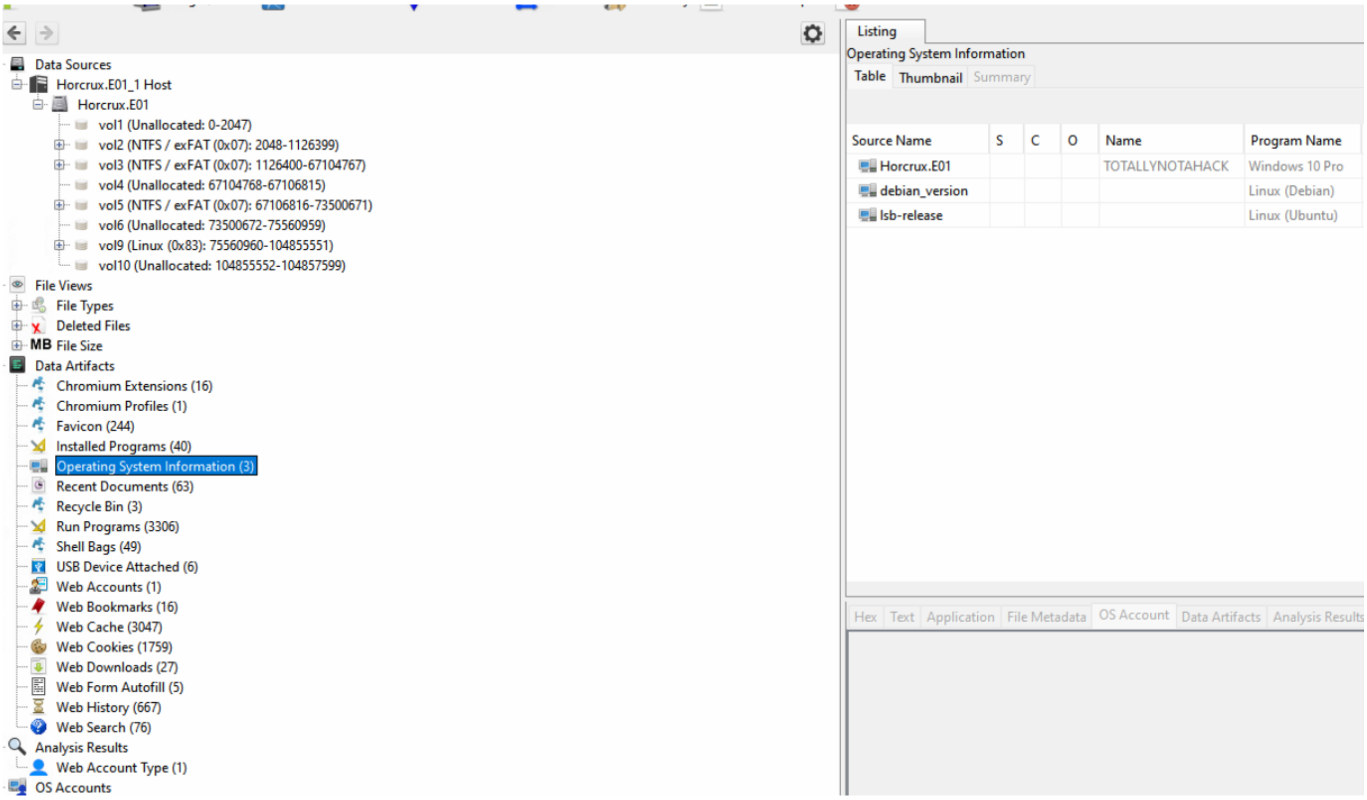
```
root@z:/media/shared/horro/Labtop-deadbox# ewfinfo Horcrux.E01
ewfinfo 20140812

Acquiry information
        Case number:              9.75
        Description:              Lbh'er n jvmneq Uneel!
        Examiner name:            Minerva
        Evidence number:          394
        Notes:                    Why does Voldemort only use Twitter and not Face
book? --Because he has followers not friends...
        Acquisition date:         Sat Mar 23 00:08:08 2019
        System date:              Sat Mar 23 00:08:08 2019
        Operating system used:    Win 201x
        Software version used:    ADI4.1.1.1
        Password:                 N/A
```

Concerning the image

1. What OS is installed on this computer? Windows_?

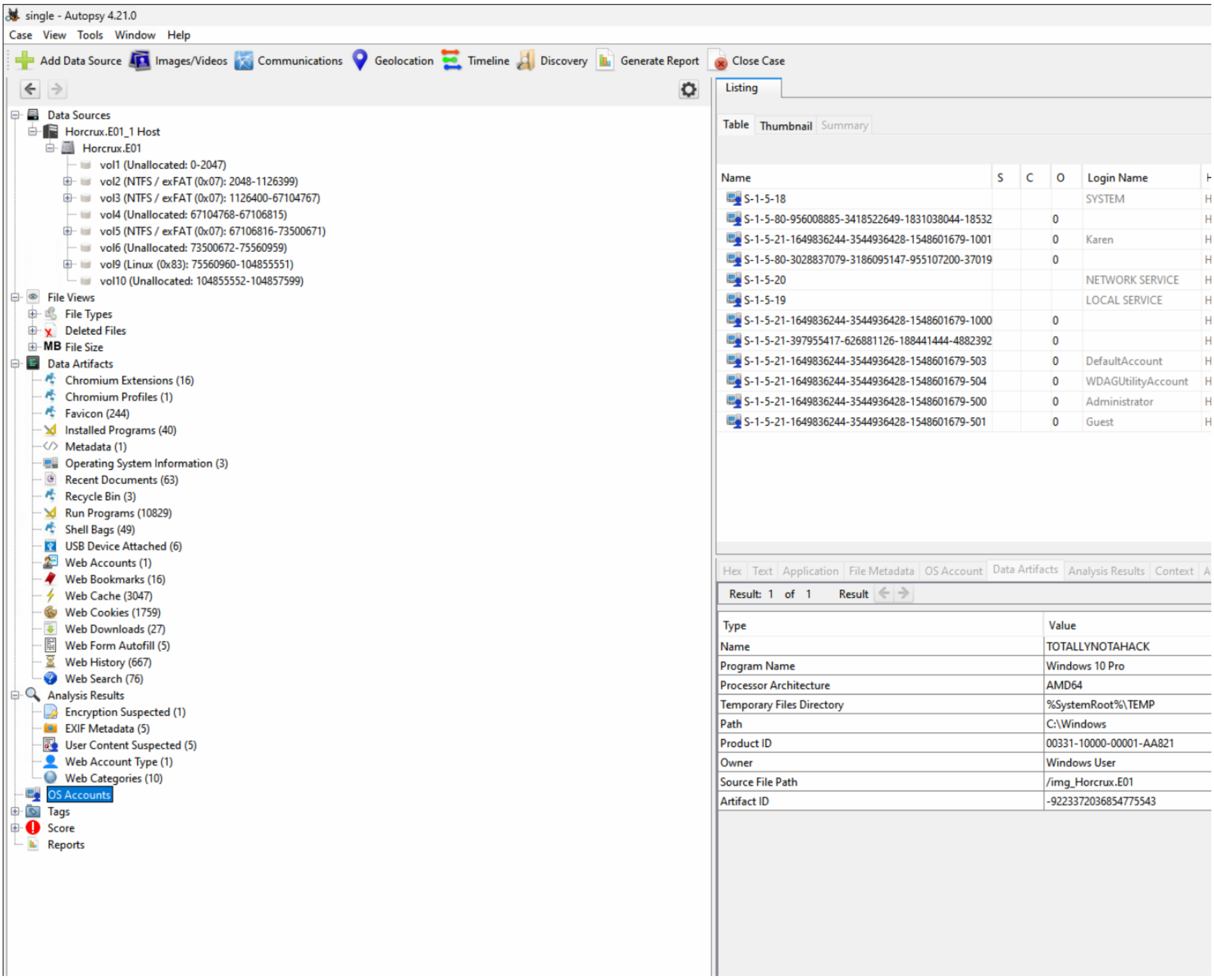
With the help of Autopsy we can retrieve the OS: Windows 10 Pro



Source Name	S	C	O	Name	Program Name
Horcrux.E01				TOTALLYNOTAHACK	Windows 10 Pro
debian_version					Linux (Debian)
lsb-release					Linux (Ubuntu)

2. What is the username of the primary user of the machine?

On the OS accounts section of autopsy we can see: Karen as a user of the system:



Name	S	C	O	Login Name	H
S-1-5-18				SYSTEM	H
S-1-5-80-956008885-3418522649-1831038044-18532			0		H
S-1-5-21-1649836244-3544936428-1548601679-1001			0	Karen	H
S-1-5-80-3028837079-3186095147-955107200-37019			0		H
S-1-5-20				NETWORK SERVICE	H
S-1-5-19				LOCAL SERVICE	H
S-1-5-21-1649836244-3544936428-1548601679-1000			0		H
S-1-5-21-397955417-626881126-188441444-4882392			0		H
S-1-5-21-1649836244-3544936428-1548601679-503			0	DefaultAccount	H
S-1-5-21-1649836244-3544936428-1548601679-504			0	WDAGUtilityAccount	H
S-1-5-21-1649836244-3544936428-1548601679-500			0	Administrator	H
S-1-5-21-1649836244-3544936428-1548601679-501			0	Guest	H

Result: 1 of 1 Result

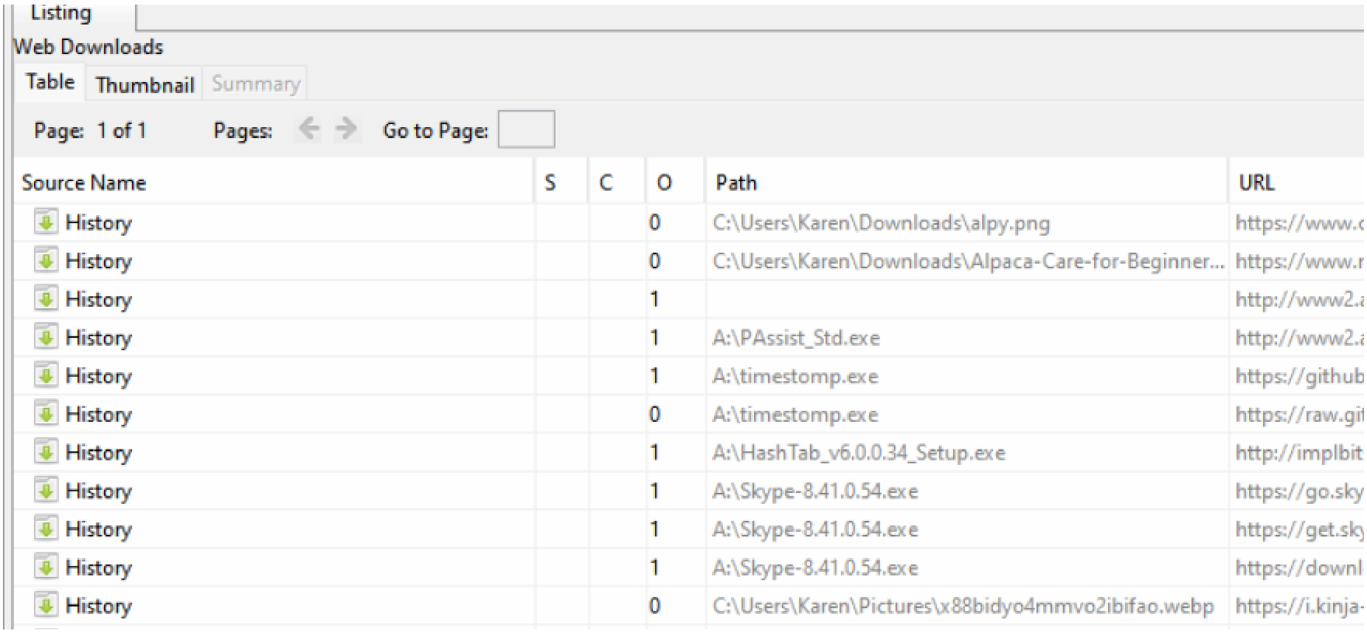
Type	Value
Name	TOTALLYNOTAHACK
Program Name	Windows 10 Pro
Processor Architecture	AMD64
Temporary Files Directory	%SystemRoot%\TEMP
Path	C:\Windows
Product ID	00331-10000-00001-AA821
Owner	Windows User
Source File Path	/img_Horcrux.E01
Artifact ID	-9223372036854775543

3. What is the hostname of the Windows partition?

On the question 1 image, we can see the name being: TOTALLYNOTAHACK

4. A messaging platform was used to communicate with a fellow Alpaca enthusiast, what is the name of the software?

First we looked at the downloads:

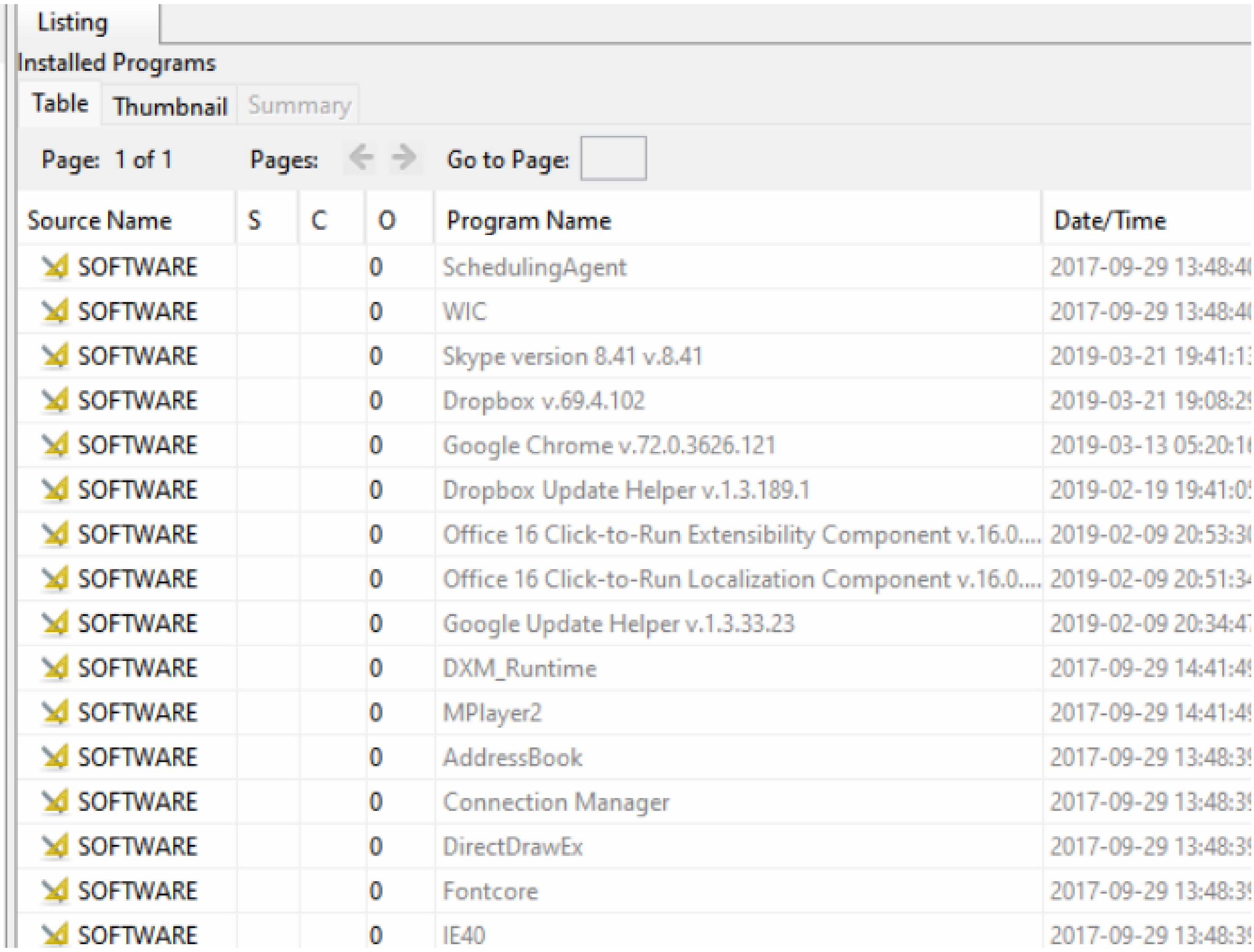


Web Downloads

Page: 1 of 1

Source Name	S	C	O	Path	URL
History			0	C:\Users\Karen\Downloads\alpy.png	https://www.c
History			0	C:\Users\Karen\Downloads\Alpaca-Care-for-Beginner...	https://www.r
History			1		http://www2.a
History			1	A:\PAssist_Std.exe	http://www2.a
History			1	A:\timestomp.exe	https://github
History			0	A:\timestomp.exe	https://raw.git
History			1	A:\HashTab_v6.0.0.34_Setup.exe	http://implbit
History			1	A:\Skype-8.41.0.54.exe	https://go.sky
History			1	A:\Skype-8.41.0.54.exe	https://get.sky
History			1	A:\Skype-8.41.0.54.exe	https://downl
History			0	C:\Users\Karen\Pictures\x88bidyo4mmvo2ibifao.webp	https://i.kinja-

And we found alpaca related content, and later we see a skype download, we checked the installed apps there it is: Skype



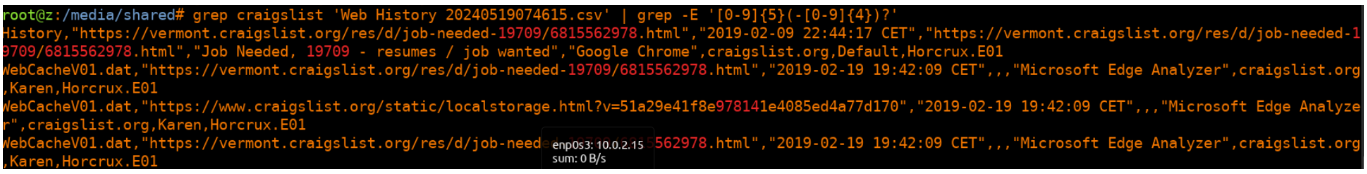
Installed Programs

Page: 1 of 1

Source Name	S	C	O	Program Name	Date/Time
SOFTWARE			0	SchedulingAgent	2017-09-29 13:48:4
SOFTWARE			0	WIC	2017-09-29 13:48:4
SOFTWARE			0	Skype version 8.41 v.8.41	2019-03-21 19:41:1
SOFTWARE			0	Dropbox v.69.4.102	2019-03-21 19:08:2
SOFTWARE			0	Google Chrome v.72.0.3626.121	2019-03-13 05:20:1
SOFTWARE			0	Dropbox Update Helper v.1.3.189.1	2019-02-19 19:41:0
SOFTWARE			0	Office 16 Click-to-Run Extensibility Component v.16.0....	2019-02-09 20:53:3
SOFTWARE			0	Office 16 Click-to-Run Localization Component v.16.0....	2019-02-09 20:51:3
SOFTWARE			0	Google Update Helper v.1.3.33.23	2019-02-09 20:34:4
SOFTWARE			0	DXM_Runtime	2017-09-29 14:41:4
SOFTWARE			0	MPlayer2	2017-09-29 14:41:4
SOFTWARE			0	AddressBook	2017-09-29 13:48:3
SOFTWARE			0	Connection Manager	2017-09-29 13:48:3
SOFTWARE			0	DirectDrawEx	2017-09-29 13:48:3
SOFTWARE			0	Fontcore	2017-09-29 13:48:3
SOFTWARE			0	IE40	2017-09-29 13:48:3

5. What is the zip code of Karen’s craigslist post?

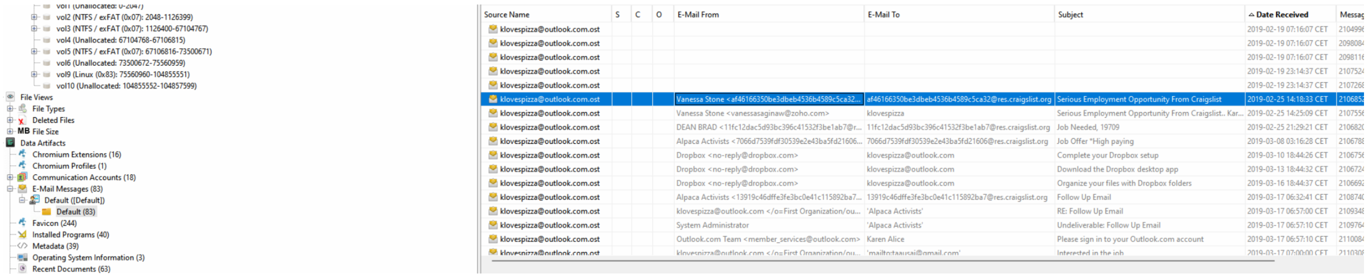
For this i downloaded the web history csv from autopsy and I run a double grep, one for craiglist and the other one for a zip number, and i got: 19709



```
root@z:/media/shared# grep craigslist 'Web History 20240519074615.csv' | grep -E '[0-9]{5}(-[0-9]{4})?'
History,"https://vermont.craigslist.org/res/d/job-needed-19709/6815562978.html","2019-02-09 22:44:17 CET","https://vermont.craigslist.org/res/d/job-needed-1
9709/6815562978.html","Job Needed, 19709 - resumes / job wanted","Google Chrome",craigslist.org,Default,Horcrux.E01
WebCacheV01.dat,"https://vermont.craigslist.org/res/d/job-needed-19709/6815562978.html","2019-02-19 19:42:09 CET",,,"Microsoft Edge Analyzer",craigslist.org
,Karen,Horcrux.E01
WebCacheV01.dat,"https://www.craigslist.org/static/localstorage.html?v=51a29e41f8e978141e4085ed4a77d170","2019-02-19 19:42:09 CET",,,"Microsoft Edge Analyze
r",craigslist.org,Karen,Horcrux.E01
WebCacheV01.dat,"https://vermont.craigslist.org/res/d/job-need enp0s3: 10.0.2.15 562978.html","2019-02-19 19:42:09 CET",,,"Microsoft Edge Analyzer",craigslist.org
,Karen,Horcrux.E01                                  sum: 0 B/s
```

6. What are the initials of the person who contacted Karen? a. Hint: OST (Offline Outlook Data).

There are 3 people who contacted Karen:



vol1 (Unallocated: 0-2047)
vol2 (NTFS / exFAT (0x07): 2048-1126399)
vol3 (NTFS / exFAT (0x07): 1126400-67104767)
vol4 (Unallocated: 67104768-67106815)
vol5 (NTFS / exFAT (0x07): 67106816-73500671)
vol6 (Unallocated: 73500672-75560959)
vol9 (Linux (0x83): 75560960-104855551)
vol10 (Unallocated: 104855552-104857599)
File Views
File Types
Deleted Files
MB File Size
Data Artifacts
Chromium Extensions (16)
Chromium Profiles (1)
Communication Accounts (18)
E-Mail Messages (83)
Default ([Default])
Default (83)
Favicon (244)
Installed Programs (40)
Metadata (39)
Operating System Information (3)
Recent Documents (63)

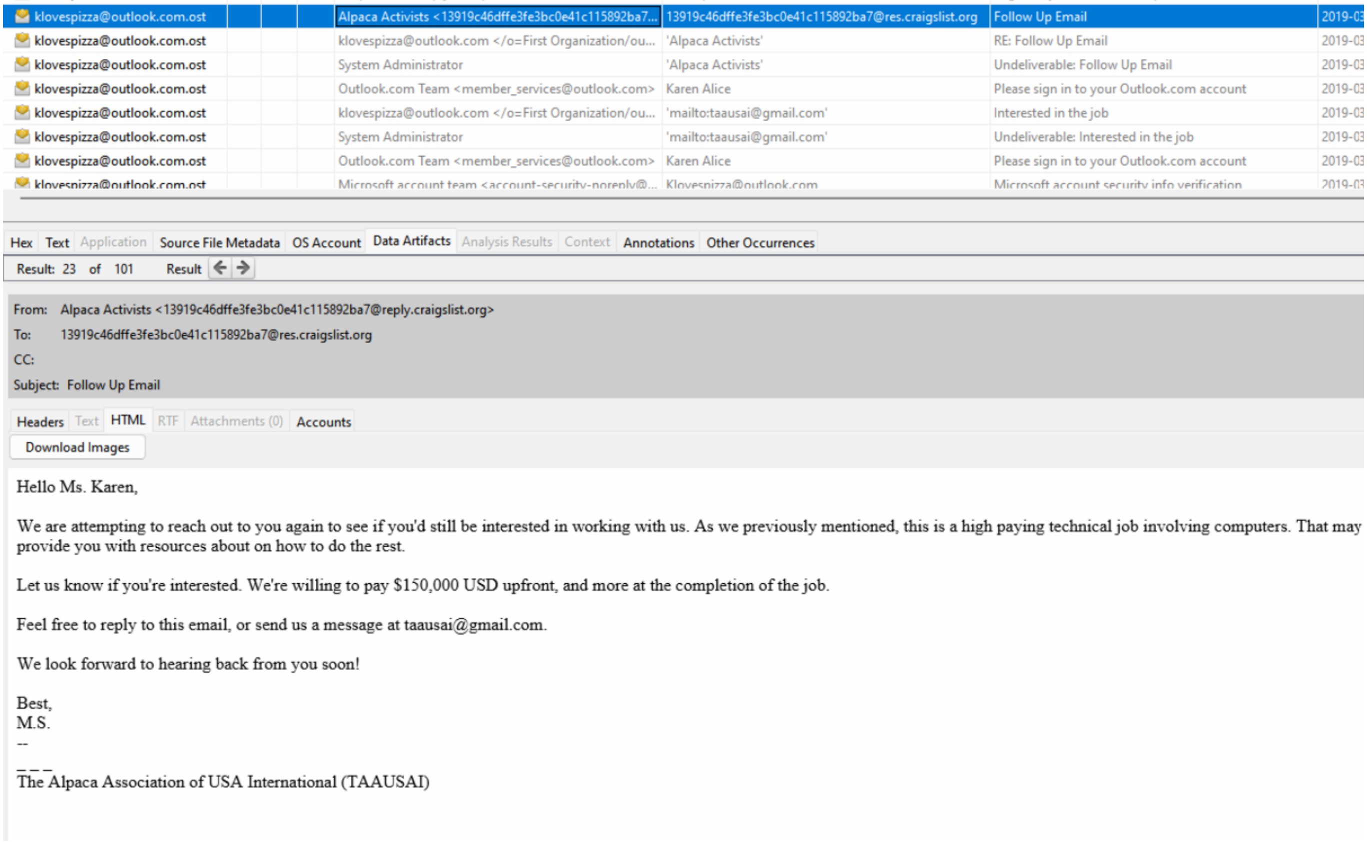
Source Name	S	C	O	E-Mail From	E-Mail To	Subject	Date Received	Messag
klovespizza@outlook.com.ost							2019-02-19 07:16:07 CET	2104996
klovespizza@outlook.com.ost							2019-02-19 07:16:07 CET	2098084
klovespizza@outlook.com.ost							2019-02-19 07:16:07 CET	2098116
klovespizza@outlook.com.ost							2019-02-19 23:14:37 CET	2107524
klovespizza@outlook.com.ost							2019-02-19 23:14:37 CET	2107268
klovespizza@outlook.com.ost				Vanessa Stone <af46166350be3dbeb4536b4589c5ca32...	af46166350be3dbeb4536b4589c5ca32@res.craigslist.org	Serious Employment Opportunity From Craigslist	2019-02-25 14:18:33 CET	2106852
klovespizza@outlook.com.ost				Vanessa Stone <vanessasaginaw@zoho.com>	klovespizza	Serious Employment Opportunity From Craigslist.. Kar...	2019-02-25 14:25:09 CET	2107556
klovespizza@outlook.com.ost				DEAN BRAD <11fc12dac5d93bc396c41532f3be1ab7@r...	11fc12dac5d93bc396c41532f3be1ab7@res.craigslist.org	Job Needed, 19709	2019-02-25 21:29:21 CET	2106820
klovespizza@outlook.com.ost				Alpaca Activists <7066d7539fdf30539e2e43ba5fd21606...	7066d7539fdf30539e2e43ba5fd21606@res.craigslist.org	Job Offer *High paying	2019-03-08 03:16:28 CET	2106788
klovespizza@outlook.com.ost				Dropbox <no-reply@dropbox.com>	klovespizza@outlook.com	Complete your Dropbox setup	2019-03-10 18:44:26 CET	2106756
klovespizza@outlook.com.ost				Dropbox <no-reply@dropbox.com>	klovespizza@outlook.com	Download the Dropbox desktop app	2019-03-13 18:44:32 CET	2106724
klovespizza@outlook.com.ost				Dropbox <no-reply@dropbox.com>	klovespizza@outlook.com	Organize your files with Dropbox folders	2019-03-16 18:44:37 CET	2106692
klovespizza@outlook.com.ost				Alpaca Activists <13919c46dffe3fe3bc0e41c115892ba7...	13919c46dffe3fe3bc0e41c115892ba7@res.craigslist.org	Follow Up Email	2019-03-17 06:32:41 CET	2108740
klovespizza@outlook.com.ost				klovespizza@outlook.com </o=First Organization/ou...	'Alpaca Activists'	RE: Follow Up Email	2019-03-17 06:57:00 CET	2109348
klovespizza@outlook.com.ost				System Administrator	'Alpaca Activists'	Undeliverable: Follow Up Email	2019-03-17 06:57:10 CET	2109764
klovespizza@outlook.com.ost				Outlook.com Team <member_services@outlook.com>	Karen Alice	Please sign in to your Outlook.com account	2019-03-17 06:57:10 CET	2110084
klovespizza@outlook.com.ost				klovespizza@outlook.com </o=First Organization/ou...	'mailto:taausai@gmail.com'	Interested in the job	2019-03-17 07:00:00 CET	2110308

Vanessa Stone (VS) Dean Brad (DB) Michael Scott (MS)

as I filter through time, the first person to use Karen's personal email was Vanessa Stone

7. How much money was TAAUSAI willing to pay Karen upfront?

When looking at the emails, I can see:



klovespizza@outlook.com.ost				Alpaca Activists <13919c46dffe3fe3bc0e41c115892ba7...	13919c46dffe3fe3bc0e41c115892ba7@res.craigslist.org	Follow Up Email	2019-03
klovespizza@outlook.com.ost				klovespizza@outlook.com </o=First Organization/ou...	'Alpaca Activists'	RE: Follow Up Email	2019-03
klovespizza@outlook.com.ost				System Administrator	'Alpaca Activists'	Undeliverable: Follow Up Email	2019-03
klovespizza@outlook.com.ost				Outlook.com Team <member_services@outlook.com>	Karen Alice	Please sign in to your Outlook.com account	2019-03
klovespizza@outlook.com.ost				klovespizza@outlook.com </o=First Organization/ou...	'mailto:taausai@gmail.com'	Interested in the job	2019-03
klovespizza@outlook.com.ost				System Administrator	'mailto:taausai@gmail.com'	Undeliverable: Interested in the job	2019-03
klovespizza@outlook.com.ost				Outlook.com Team <member_services@outlook.com>	Karen Alice	Please sign in to your Outlook.com account	2019-03
klovespizza@outlook.com.ost				Microsoft account team <account-security-noreply@...	Klovespizza@outlook.com	Microsoft account security info verification	2019-03

Result: 23 of 101 Result

From: Alpaca Activists <13919c46dffe3fe3bc0e41c115892ba7@reply.craigslist.org>
To: 13919c46dffe3fe3bc0e41c115892ba7@res.craigslist.org
CC:
Subject: Follow Up Email

Hello Ms. Karen,

We are attempting to reach out to you again to see if you'd still be interested in working with us. As we previously mentioned, this is a high paying technical job involving computers. That may provide you with resources about on how to do the rest.

Let us know if you're interested. We're willing to pay $150,000 USD upfront, and more at the completion of the job.

Feel free to reply to this email, or send us a message at taausai@gmail.com.

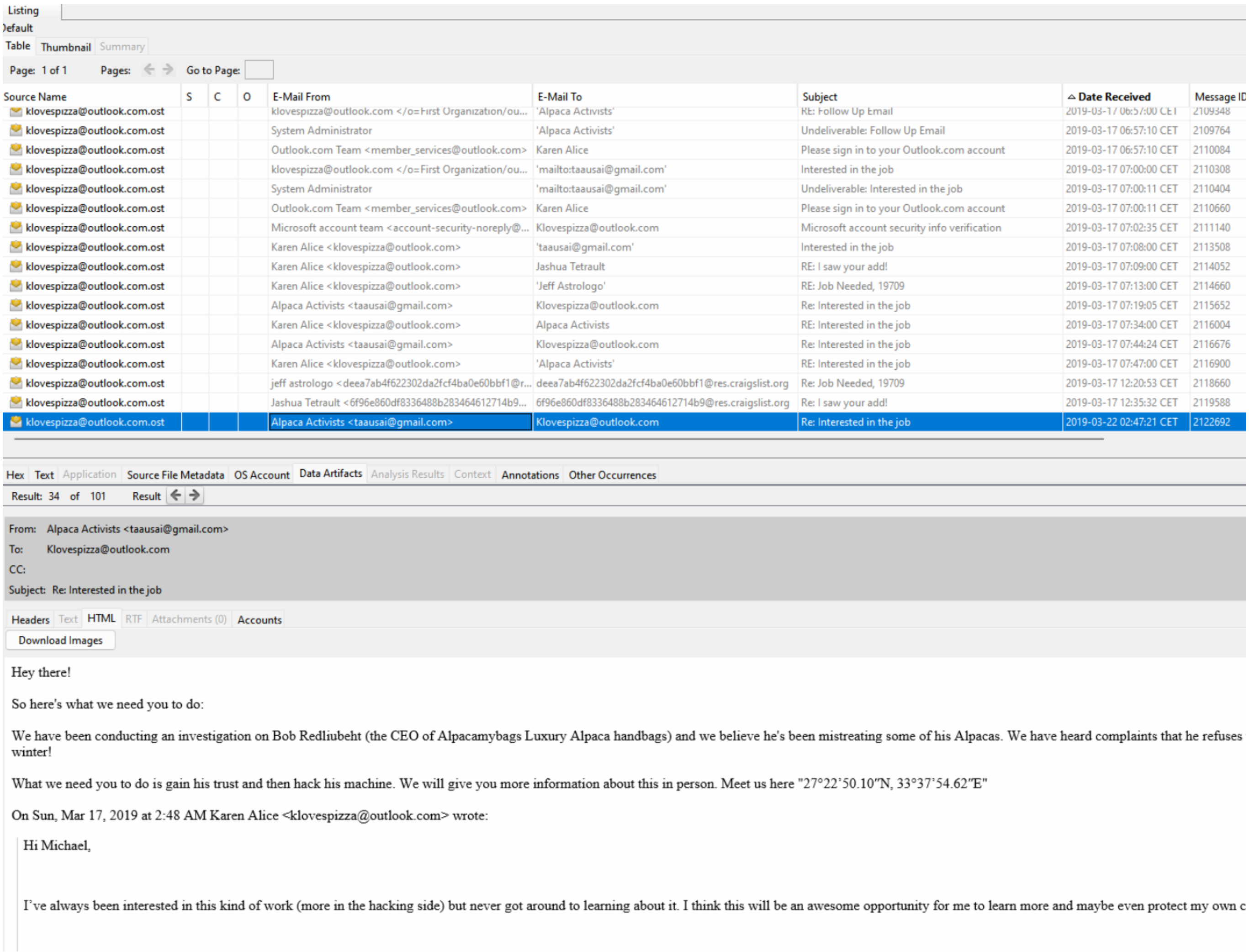
We look forward to hearing back from you soon!

Best,
M.S.
--
_ _ _
The Alpaca Association of USA International (TAAUSAI)

So they are offering 150,000 USD

8. What country is Karen meeting the hacker group in?

By looking more into the emails, I followed the thread and found the coordinates: `27°22’50.10”N, 33°37’54.62”E`



Source Name	S	C	O	E-Mail From	E-Mail To	Subject	Date Received	Message ID
klovespizza@outlook.com.ost				klovespizza@outlook.com </o=First Organization/ou...	'Alpaca Activists'	RE: Follow Up Email	2019-03-17 06:57:00 CET	2109348
klovespizza@outlook.com.ost				System Administrator	'Alpaca Activists'	Undeliverable: Follow Up Email	2019-03-17 06:57:10 CET	2109764
klovespizza@outlook.com.ost				Outlook.com Team <member_services@outlook.com>	Karen Alice	Please sign in to your Outlook.com account	2019-03-17 06:57:10 CET	2110084
klovespizza@outlook.com.ost				klovespizza@outlook.com </o=First Organization/ou...	'mailto:taausai@gmail.com'	Interested in the job	2019-03-17 07:00:00 CET	2110308
klovespizza@outlook.com.ost				System Administrator	'mailto:taausai@gmail.com'	Undeliverable: Interested in the job	2019-03-17 07:00:11 CET	2110404
klovespizza@outlook.com.ost				Outlook.com Team <member_services@outlook.com>	Karen Alice	Please sign in to your Outlook.com account	2019-03-17 07:00:11 CET	2110660
klovespizza@outlook.com.ost				Microsoft account team <account-security-noreply@...	Klovespizza@outlook.com	Microsoft account security info verification	2019-03-17 07:02:35 CET	2111140
klovespizza@outlook.com.ost				Karen Alice <klovespizza@outlook.com>	'taausai@gmail.com'	Interested in the job	2019-03-17 07:08:00 CET	2113508
klovespizza@outlook.com.ost				Karen Alice <klovespizza@outlook.com>	Jashua Tetrault	RE: I saw your add!	2019-03-17 07:09:00 CET	2114052
klovespizza@outlook.com.ost				Karen Alice <klovespizza@outlook.com>	'Jeff Astrologo'	RE: Job Needed, 19709	2019-03-17 07:13:00 CET	2114660
klovespizza@outlook.com.ost				Alpaca Activists <taausai@gmail.com>	Klovespizza@outlook.com	Re: Interested in the job	2019-03-17 07:19:05 CET	2115652
klovespizza@outlook.com.ost				Karen Alice <klovespizza@outlook.com>	Alpaca Activists	RE: Interested in the job	2019-03-17 07:34:00 CET	2116004
klovespizza@outlook.com.ost				Alpaca Activists <taausai@gmail.com>	Klovespizza@outlook.com	Re: Interested in the job	2019-03-17 07:44:24 CET	2116676
klovespizza@outlook.com.ost				Karen Alice <klovespizza@outlook.com>	'Alpaca Activists'	RE: Interested in the job	2019-03-17 07:47:00 CET	2116900
klovespizza@outlook.com.ost				jeff astrologo <deea7ab4f622302da2fcf4ba0e60bbf1@r...	deea7ab4f622302da2fcf4ba0e60bbf1@res.craigslist.org	Re: Job Needed, 19709	2019-03-17 12:20:53 CET	2118660
klovespizza@outlook.com.ost				Jashua Tetrault <6f96e860df8336488b283464612714b9...	6f96e860df8336488b283464612714b9@res.craigslist.org	Re: I saw your add!	2019-03-17 12:35:32 CET	2119588
klovespizza@outlook.com.ost				Alpaca Activists <taausai@gmail.com>	Klovespizza@outlook.com	Re: Interested in the job	2019-03-22 02:47:21 CET	2122692

From: Alpaca Activists <taausai@gmail.com>
To: Klovespizza@outlook.com
CC:
Subject: Re: Interested in the job

Hey there!

So here's what we need you to do:

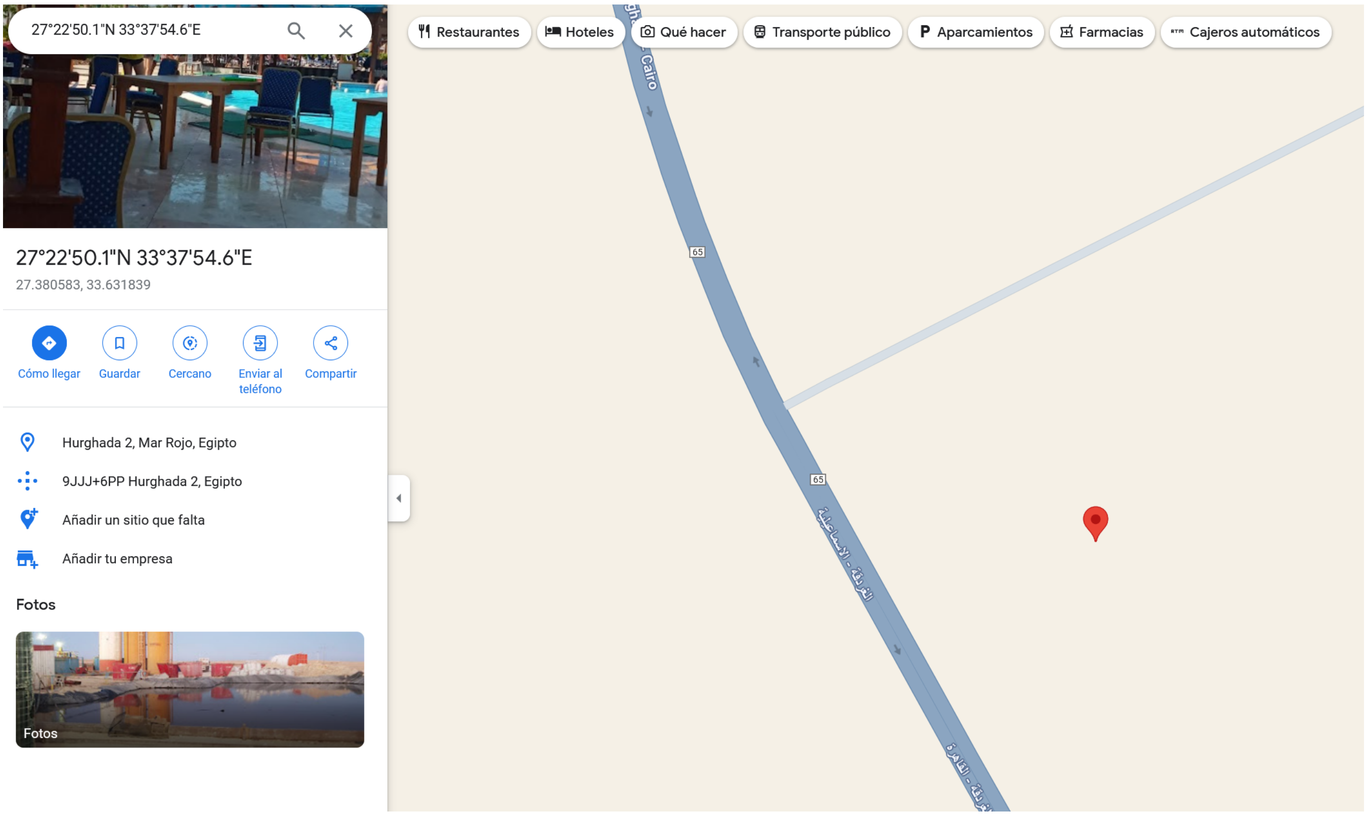
We have been conducting an investigation on Bob Redliubeht (the CEO of Alpacamybags Luxury Alpaca handbags) and we believe he's been mistreating some of his Alpacas. We have heard complaints that he refuses winter!

What we need you to do is gain his trust and then hack his machine. We will give you more information about this in person. Meet us here "27°22'50.10"N, 33°37'54.62"E"

On Sun, Mar 17, 2019 at 2:48 AM Karen Alice <klovespizza@outlook.com> wrote:

> Hi Michael,
>
> I've always been interested in this kind of work (more in the hacking side) but never got around to learning about it. I think this will be an awesome opportunity for me to learn more and maybe even protect my own c

the location is on Egypt:

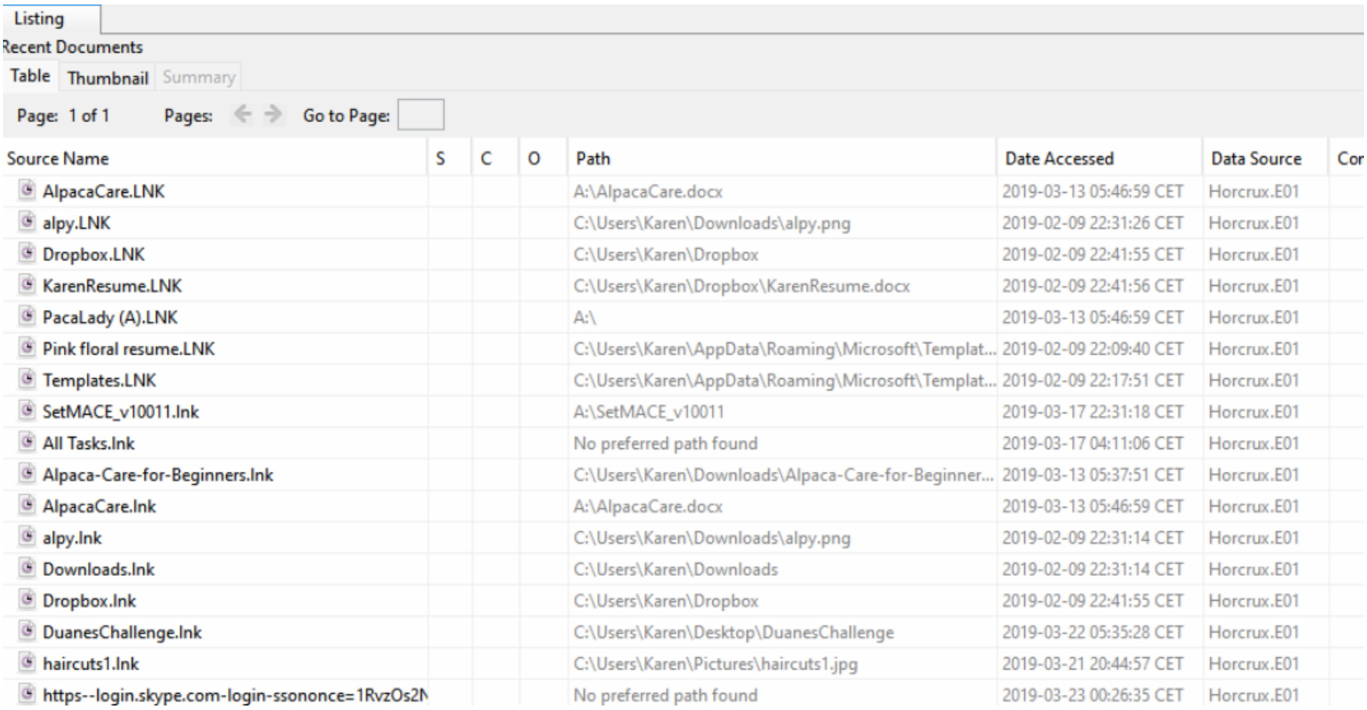

27°22'50.1"N 33°37'54.6"E

27°22'50.1"N 33°37'54.6"E
27.380583, 33.631839

Hurghada 2, Mar Rojo, Egipto
9JJJ+6PP Hurghada 2, Egipto
Añadir un sitio que falta
Añadir tu empresa

9. Karen had a second partition on the drive, what drive letter was it assigned?

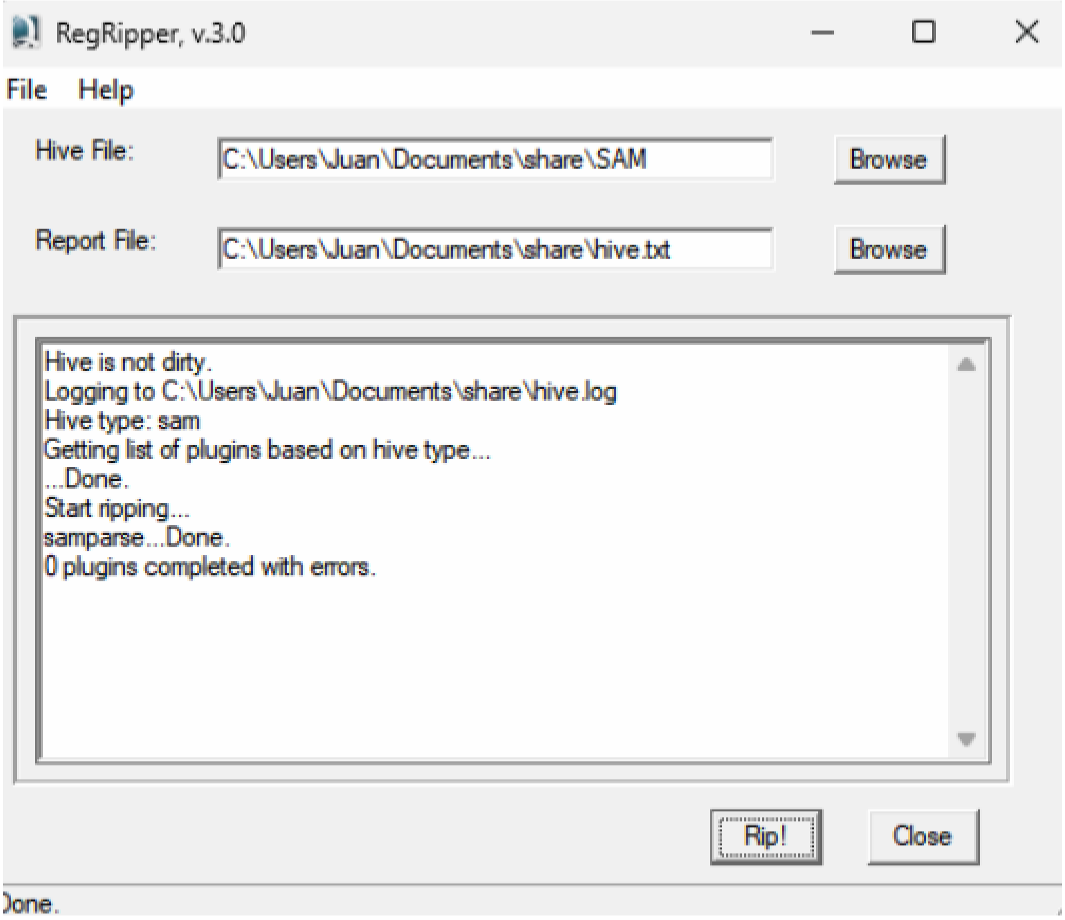
When looking at recent documents, I can see a partition: A:\



Source Name	S	C	O	Path	Date Accessed	Data Source	Cor
AlpacaCare.LNK				A:\AlpacaCare.docx	2019-03-13 05:46:59 CET	Horcrux.E01	
alpy.LNK				C:\Users\Karen\Downloads\alpy.png	2019-02-09 22:31:26 CET	Horcrux.E01	
Dropbox.LNK				C:\Users\Karen\Dropbox	2019-02-09 22:41:55 CET	Horcrux.E01	
KarenResume.LNK				C:\Users\Karen\Dropbox\KarenResume.docx	2019-02-09 22:41:56 CET	Horcrux.E01	
PacaLady (A).LNK				A:\	2019-03-13 05:46:59 CET	Horcrux.E01	
Pink floral resume.LNK				C:\Users\Karen\AppData\Roaming\Microsoft\Templat...	2019-02-09 22:09:40 CET	Horcrux.E01	
Templates.LNK				C:\Users\Karen\AppData\Roaming\Microsoft\Templat...	2019-02-09 22:17:51 CET	Horcrux.E01	
SetMACE_v10011.lnk				A:\SetMACE_v10011	2019-03-17 22:31:18 CET	Horcrux.E01	
All Tasks.lnk				No preferred path found	2019-03-17 04:11:06 CET	Horcrux.E01	
Alpaca-Care-for-Beginners.lnk				C:\Users\Karen\Downloads\Alpaca-Care-for-Beginner...	2019-03-13 05:37:51 CET	Horcrux.E01	
AlpacaCare.lnk				A:\AlpacaCare.docx	2019-03-13 05:46:59 CET	Horcrux.E01	
alpy.lnk				C:\Users\Karen\Downloads\alpy.png	2019-02-09 22:31:14 CET	Horcrux.E01	
Downloads.lnk				C:\Users\Karen\Downloads	2019-02-09 22:31:14 CET	Horcrux.E01	
Dropbox.lnk				C:\Users\Karen\Dropbox	2019-02-09 22:41:55 CET	Horcrux.E01	
DuanesChallenge.lnk				C:\Users\Karen\Desktop\DuanesChallenge	2019-03-22 05:35:28 CET	Horcrux.E01	
haircuts1.lnk				C:\Users\Karen\Pictures\haircuts1.jpg	2019-03-21 20:44:57 CET	Horcrux.E01	
https--login.skype.com-login-ssononce=1RvzOs2N				No preferred path found	2019-03-23 00:26:35 CET	Horcrux.E01	

10. When was Karen password last changed? a. Hint: SAM (Security Account Manager)

We extract the SAM file from `C:\Windows\System32\config\SAM` from the volume 3. Then we use RegRipper to extract the information about the SAM.

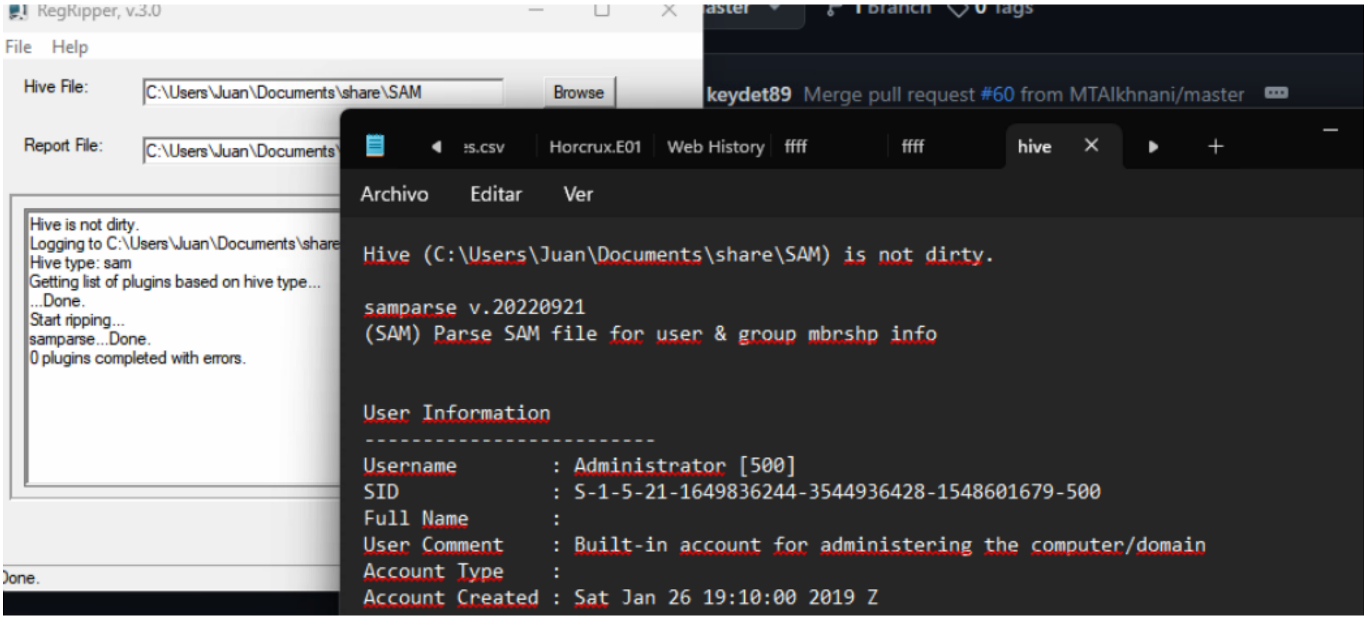


Hive File: C:\Users\Juan\Documents\share\SAM

Report File: C:\Users\Juan\Documents\share\hive.txt

```
Hive is not dirty.
Logging to C:\Users\Juan\Documents\share\hive.log
Hive type: sam
Getting list of plugins based on hive type...
...Done.
Start ripping...
samparse...Done.
0 plugins completed with errors.
```

Done.



Hive File: C:\Users\Juan\Documents\share\SAM

Report File: C:\Users\Juan\Documents\

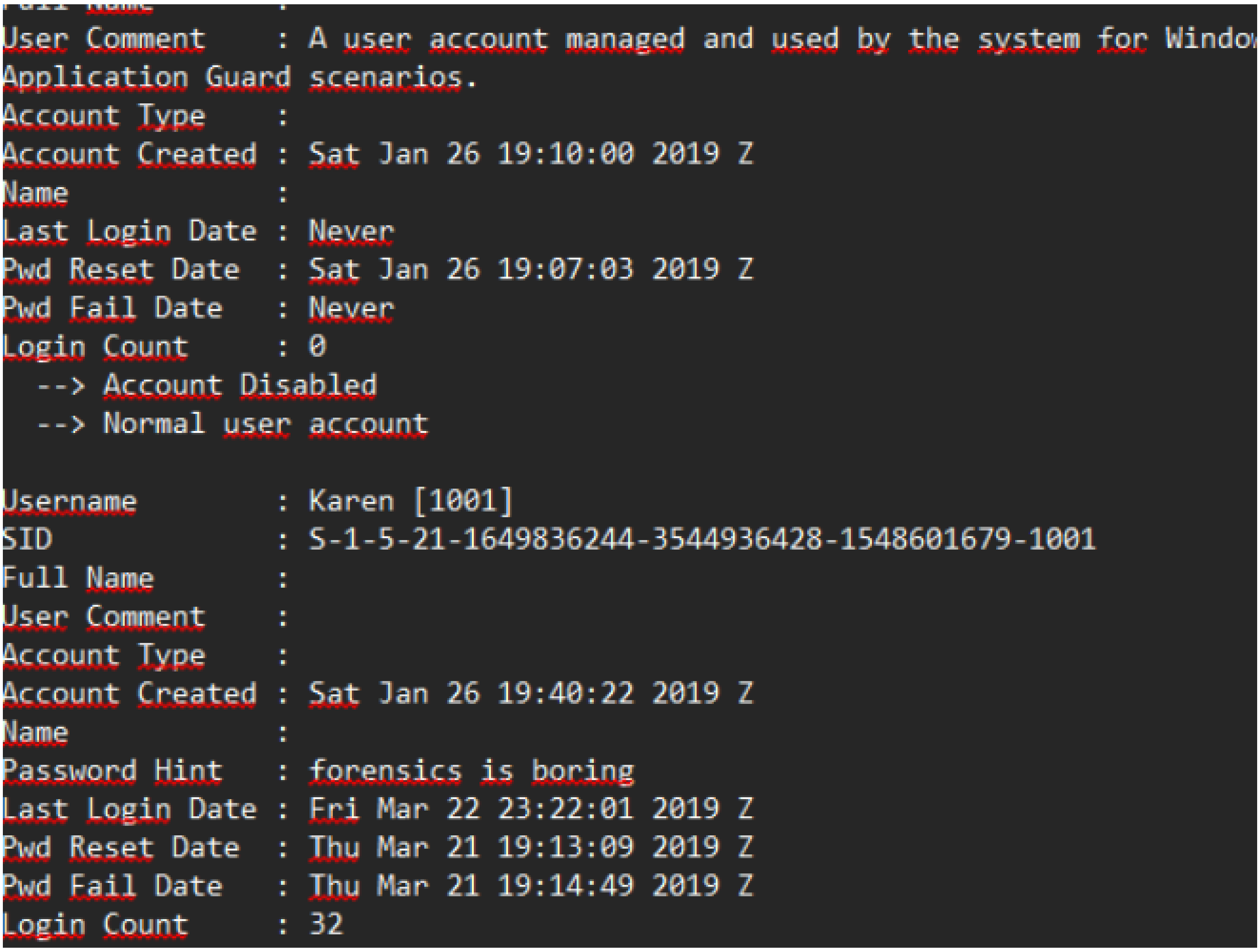
Hive is not dirty.
Logging to C:\Users\Juan\Documents\share
Hive type: sam
Getting list of plugins based on hive type...
...Done.
Start ripping...
samparse...Done.
0 plugins completed with errors.

Done.

```
Hive (C:\Users\Juan\Documents\share\SAM) is not dirty.

samparse v.20220921
(SAM) Parse SAM file for user & group mbrshp info


User Information
-------------------------
Username        : Administrator [500]
SID             : S-1-5-21-1649836244-3544936428-1548601679-500
Full Name       :
User Comment    : Built-in account for administering the computer/domain
Account Type    :
Account Created : Sat Jan 26 19:10:00 2019 Z
```



```
Full Name      :
User Comment   : A user account managed and used by the system for Windo
Application Guard scenarios.
Account Type   :
Account Created : Sat Jan 26 19:10:00 2019 Z
Name           :
Last Login Date : Never
Pwd Reset Date  : Sat Jan 26 19:07:03 2019 Z
Pwd Fail Date   : Never
Login Count     : 0
  --> Account Disabled
  --> Normal user account

Username        : Karen [1001]
SID             : S-1-5-21-1649836244-3544936428-1548601679-1001
Full Name       :
User Comment    :
Account Type    :
Account Created : Sat Jan 26 19:40:22 2019 Z
Name            :
Password Hint   : forensics is boring
Last Login Date : Fri Mar 22 23:22:01 2019 Z
Pwd Reset Date  : Thu Mar 21 19:13:09 2019 Z
Pwd Fail Date   : Thu Mar 21 19:14:49 2019 Z
Login Count     : 32
```

with the information and location of the Karen account, we can see that the date was: Thu Mar 21 19:13:09 2019 Z