

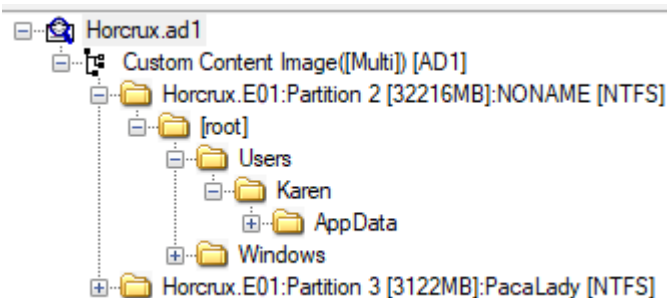
CyberDefenders: HireMe Lab

The following writeup is for [HireMe Lab](#) on CyberDefenders, it involves analysing a disk image from a Windows machine. This room requires the use of several tools, including FTK Imager, Registry Explorer, LECmd, RegRipper, and OST Viewer. This challenge took me roughly 2 hours, and I found the medium difficulty rating to be pretty accurate. This lab encompasses many skills, including registry, browser, and email forensics, making it a wonderful learning experience for aspiring DFIR professional like myself.

Scenario: Karen is a security professional looking for a new job. A company called "TAAUSAI" offered her a position and asked her to complete a couple of tasks to prove her technical competency. As a soc analyst Analyze the provided disk image and answer the questions based on your understanding of the cases she was assigned to investigate.

What is the administrator's username?

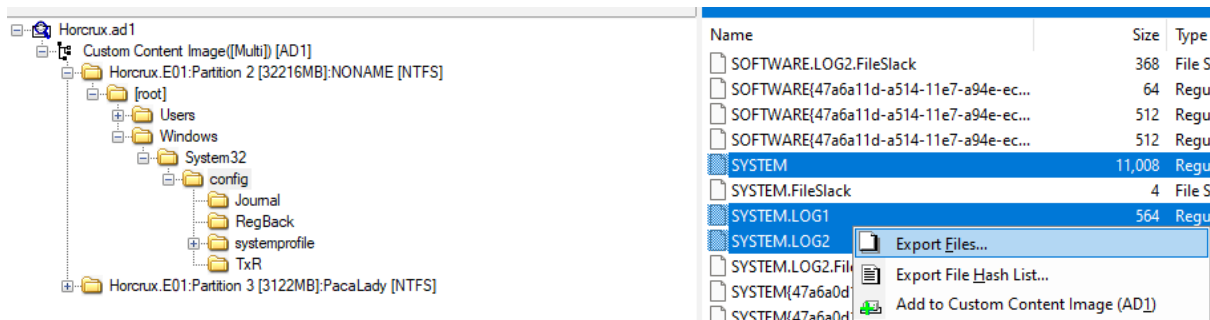
Start off by loading the disk image with FTK Imager (you can open it in Autopsy although I believe you need a custom module to load AD1 files). If you navigate to the Users directory, we can see that the administrator's username is Karen:



Answer: Karen

What is the OS's build number?

The only way I know how to find the OS build number is to inspect the SOFTWARE registry hive, we can do so by exporting all the registry hives and their transaction logs found at root/Windows/System32/config:



You can then open up the SOFTWARE hive using Registry Explorer and navigate to SOFTWARE\Microsoft\Windows NT\CurrentVersion:

CurrentBuild	RegSz	16299
--------------	-------	-------

Answer: 16299

What is the hostname of the computer?

You can find the hostname of a computer within the SYSTEM hive, located at SYSTEM\CurrentControlSet\ComputerName:

ComputerName	RegSz	TOTALLYNOTAHACK
--------------	-------	-----------------

Answer: TOTALLYNOTAHACK

A messaging application was used to communicate with a fellow Alpaca enthusiast. What is the name of the software?

In order to find the messaging application used, we should look at what applications are installed on the system. You can do so by navigating to SOFTWARE\Microsoft\Windows\CurrentVersion\AppPaths:

SKYPESEVER.EXE	C:\Program Files (x86)\Microsoft Office\Root\Office16\SkypeSrv\SKYPESEVER.EXE
----------------	---

Answer: Skype

What is the zip code of the administrator's post?

In order to find the zip code of the administrator's post, let's take a look at the Google autofill data located within an SQLite database found at C:\Users\Karen\AppData\Local\Google\Chrome\User Data\Default\Web Data. You can open this database file using whatever tool you like, in this case I used DB Browser for SQLite:

	<u>name</u>	<u>value</u>	<u>value_lower</u>
	Filter	Filter	Filter
1	email	klovespizza@outlook.com	klovespizza@outlook.com
2	PostingTitle	Job Needed, 19709	job needed, 19709
3	postal	19709	19709
4	FromEMail	klovespizza@outlook.com	klovespizza@outlook.com
5	ConfirmEMail	klovespizza@outlook.com	klovespizza@outlook.com

Answer: 19709

What are the initials of the person who contacted the admin user from TAAUSAI?

To find the initials of the person who contacted the admin user from TAAUSAI, we need to first examine the user's mailbox, which is possible via inspecting the OST file located at \\Users\\Karen\\AppData\\Local\\Microsoft\\Outlook\\klovespizza@outlook.com.ost. You can use whatever tool you like to inspect this OST file, I opted to use a Browser based tool found [here](#). After going through the emails within klovespizza's inbox, I came across this"

Job Offer *High paying

From: "Alpaca Activists" <7066d7539fdf30539e2e43ba5fd21606@reply.craigslist.org>

To: <7066d7539fdf30539e2e43ba5fd21606@res.craigslist.org>

BEST BODY

HEADERS

Hello Ms. Karen,

My name is Micheal Scotch and I work with The Alpaca Association of USA International (TAAUSAI). We he TAAUSAI are passionate about fighting for Alpaca animal rights in the United States of America and across th need your help!

We came across your Craigslist entry here and wanted to know if you'd be interested in a high paying technical use of computers. Don't worry about your skill level, we'll supply you with what you need.

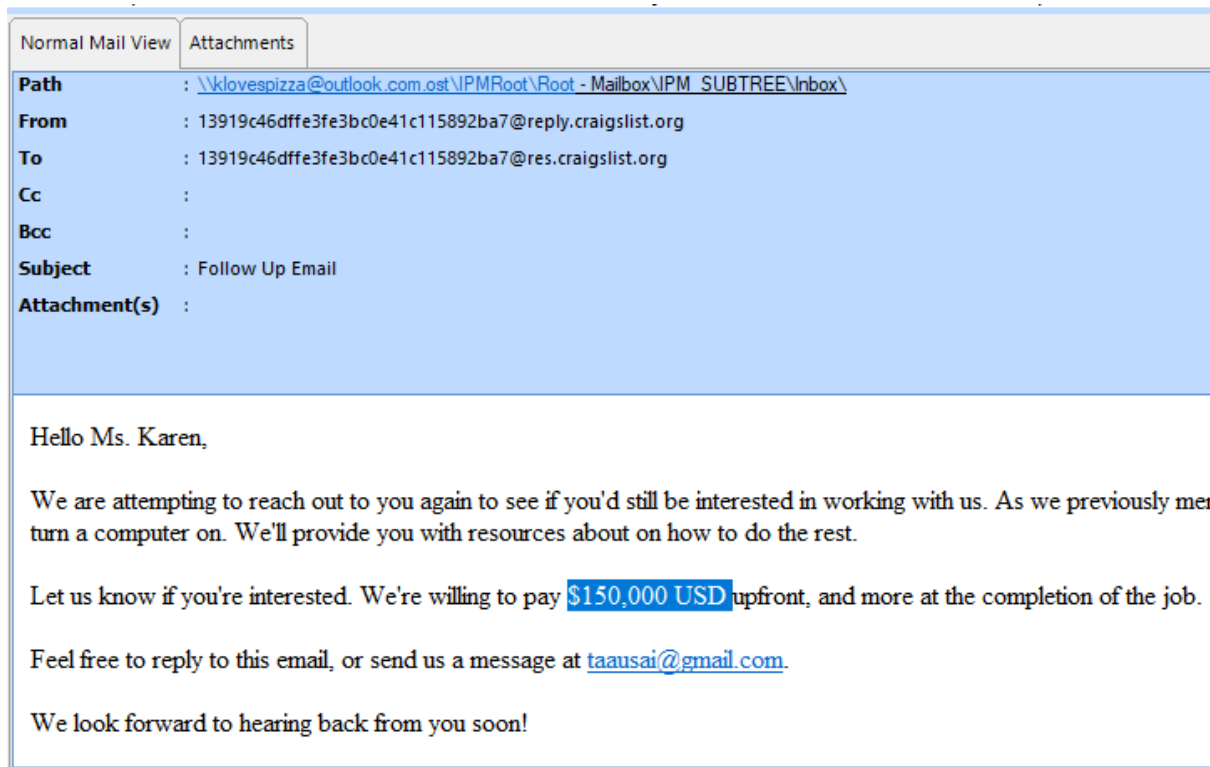
Let us know what you think.

Best,
- Micheal Scotch

The Alpaca Association of USA International (TAAUSAI)

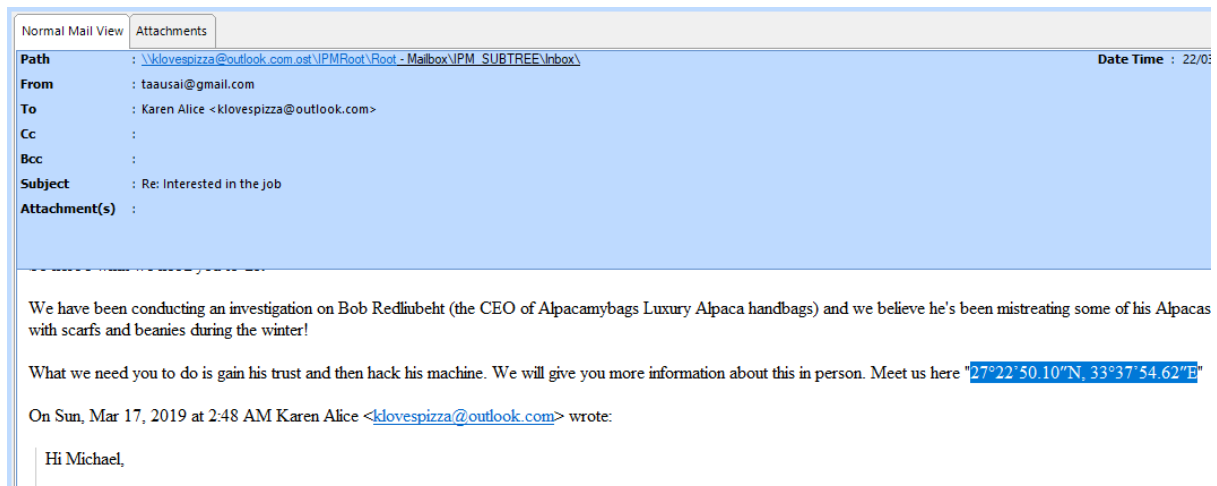
Answer: MS

How much money was TAAUSAI willing to pay upfront?

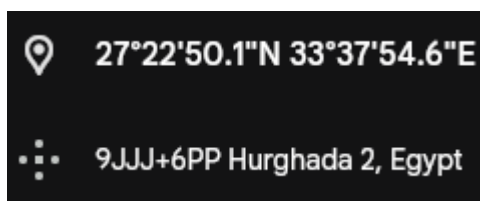


Answer: 150000

What country is the admin user meeting the hacker group in?



If you enter these GPS coordinates into Google Earth, you can find yourself in Egypt:



Answer: Egypt

What is the machine's timezone? (Use the three-letter abbreviation)


A machine's timezone is stored in the SYSTEM registry hive, located at SYSTEM\CurrentControlSet\Control\TimeZoneInformation:

Bias	0	0
DaylightBias	0	0
DaylightName	@tzres.dll,-931	@tzres.dll,-931
DaylightStart	Month 0, week of month 0, day of week 0, Hours:Minutes:Seconds:Milliseconds 0:0:0:0	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
StandardBias	0	0
StandardName	@tzres.dll,-932	@tzres.dll,-932
StandardStart	Month 0, week of month 0, day of week 0, Hours:Minutes:Seconds:Milliseconds 0:0:0:0	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
TimeZoneKeyName	UTC	UTC
ActiveTimeBias	0	0

Answer: UTC

When was AlpacaCare.docx last accessed?

The AlpacaCare.docx file can be found within the 3rd partition:

 AlpacaCare.docx	53 Regular File	17/03/2019 9:52:20 PM
---	-----------------	-----------------------

The third column is the date modified timestamp, which in this instance is 17/03/2019 9:52:20 PM, make sure to convert it to the correct format when entering it into CyberDefenders.

Answer: 03/17/2019 09:52 PM

There was a second partition on the drive. What is the letter assigned to it?

To find the second partition drive letter, we need to examine the paths contained within LNK files located in \Users\Karen\AppData\Roaming\Microsoft\Office\Recent. This is where another Eric Zimmerman tool comes in handy. The tool is called LECmd, we can use the following command to recursively analyse the LNK files within the recent directory:

```
.\LECmd.exe -d "C:\Users\timba\Desktop\Recent\" --csv "C:\Users\timba\Desktop\"
```

If you open up the csv output with a tool like Timeline Explorer, you can see the A drive letter:

C:\Users\Karen\AppData\Roaming\Microsoft\Templates\Pink floral resume.dotx
C:\Users\Karen\AppData\Roaming\Microsoft\Templates
C:\Users\Karen\Downloads\alpy.png
C:\Users\Karen\Dropbox
C:\Users\Karen\Dropbox\KarenResume.docx
A:\AlpacaCare.docx
A:\

Answer: A

What is the answer to the question Company's manager asked Karen?

Within the inbox of klovespizza, we can see a message chain where Karen is asked to answer a question given by Michael, this question is a Base64 encoded string that decodes to TheCardCriesNoMore:

Hi Karen,

No worries, it happens! We're just happy to finally hear from you.

So I may have lied, my manager is saying that before we can offer you a job, we need to give you a quick test. Can you tell me what the answer to the thing at the bottom is?

VGhlQ2FyZENyaWVzTm9Nb3Jl

On Sun, Mar 17, 2019 at 2:34 AM Karen Alice <klovespizza@outlook.com> wrote:

Hi Michael,

The answer is TheCardCriesNoMore

Answer: TheCardCriesNoMore

What is the job position offered to Karen? (3 words, 2 spaces in between)

Karen,

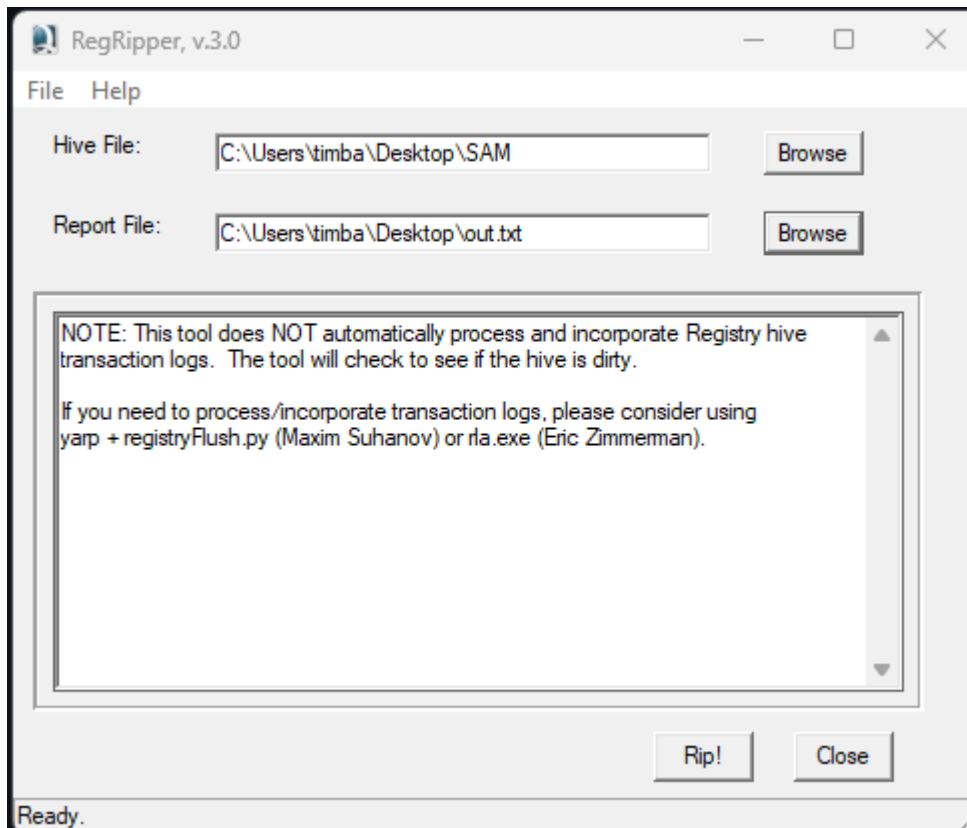
WOW! That was quick! I have confirmed with my manager that that answer is correct. We d zone.

The job position we think you'll be an awesome fit for is an entry level **cyber security analysts**. what this job entails (and the set up involved with getting you payed), but wanted to give you :

Answer: cyber security analyst

When was the admin user password last changed?

In order to find when the admin user password was last changed, I am going to use a wonderful tool called RegRipper. Within RegRipper, I will be supplying the path to the SAM registry hive like as follows:



After clicking the Rip! Button, you will be presented with a txt file, within this file you can find the last time the password was changed for the Karen 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
--> Password does not expire
--> Password not required
--> Normal user account
```

Answer: 03/21/2019 19:13:09

What version of Chrome is installed on the machine?


You can find the version of Chrome installed by navigating to SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\:

2019-03-13 05:20:16	Google Chrome	Google Chrome	72.0.3626.121	Google Inc.	20190312
2017-09-30 13:48:30	1E40				

Answer: 72.0.3626.121

What is the URL used to download Skype?

Within the 3rd partition, you are able to find the Skype executable. If you click on the Zone.Identifier stream of the Skype executable, you can see the download URL:

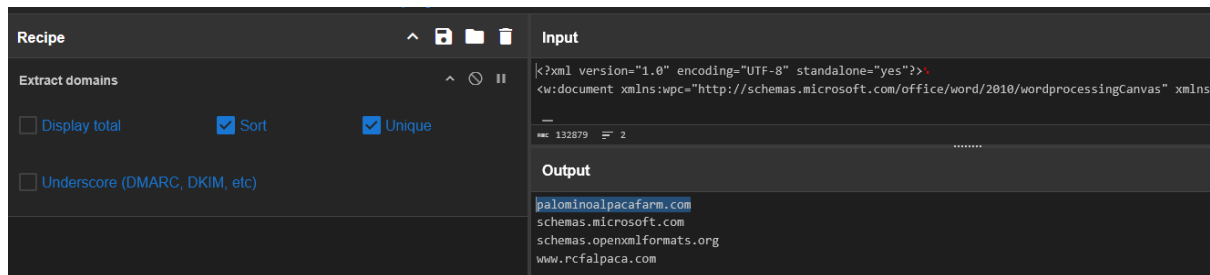
 Zone.Identifier	1	Alternate Data ...	21/03/2019 7:40:52 PM
---	---	--------------------	-----------------------

```
[ZoneTransfer]
ZoneId=3
ReferrerUrl=https://www.skype.com/en/get-skype/
HostUrl=https://download.skype.com/s4l/download/win/Skype-8.41.0.54.exe
```

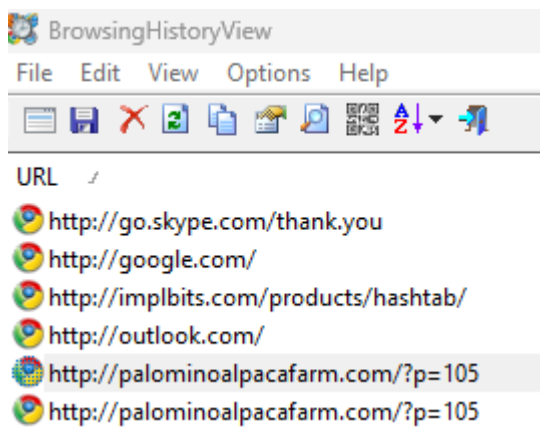
Answer: <https://download.skype.com/s4l/download/win/Skype-8.41.0.54.exe>

What is the domain name of the website Karen browsed on Alpaca care that the file AlpacaCare.docx is based on?

Unbeknownst to me, DOCX files are ZIP archives that contain XML files. In order to find hyperlinks or references to domains, you can simply extract the AlpacaCare.docx file using FTK Imager, and unzip the file using something like 7Zip. Once you have done so, navigate to word/ and open the document.xml file. Using Cyberchef, we can extract domains within this xml document:



You are also able to see palominoalpaca.com in the browsing history:



Answer: palominoalpaca.com