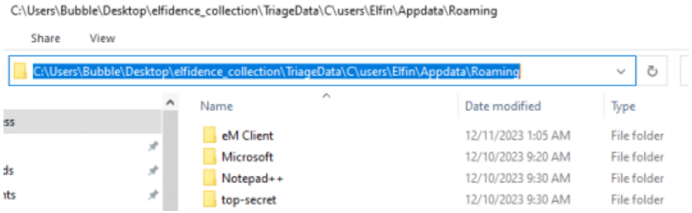
OpTinselTrace-1 Challenge

Sherlock Scenario
An elf named "Elfin" has been acting rather suspiciously lately. He's been working at odd hours and seems to be bypassing some of Santa's security protocols. Santa's network of intelligence elves has told Santa that the Grinch got a little bit too tipsy on egg nog and made mention of an insider elf! Santa is very busy with his naughty and nice list, so he's put you in charge of figuring this one out. Please audit Elfin's workstation and email communications. Please note - these Sherlocks are built to be completed sequentially and in order!

Task 1:
What is the name of the email client that Elfin is using?

Checking inside the user folder Elfin Appdata\Roaming there is a folder eM Client

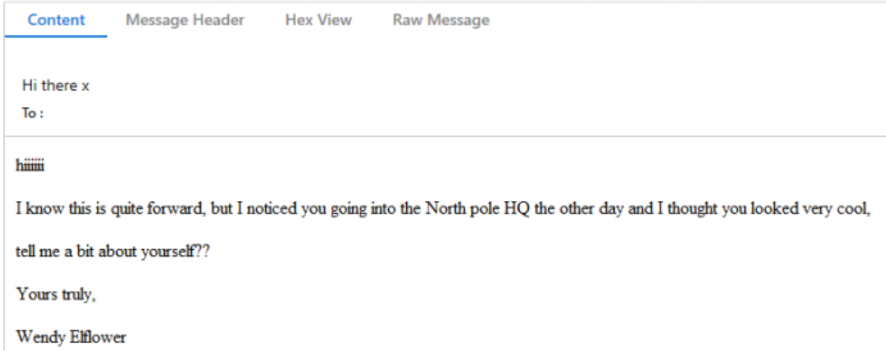

C:\Users\Bubble\Desktop\elfidence_collection\TriageData\C\users\Elfin\Appdata\Roaming
Share
View
C:\Users\Bubble\Desktop\elfidence_collection\TriageData\C\users\Elfin\Appdata\Roaming

Name	Date modified	Type
eM Client	12/11/2023 1:05 AM	File folder
Microsoft	12/10/2023 9:20 AM	File folder
Notepad++	12/10/2023 9:30 AM	File folder
top-secret	12/10/2023 9:30 AM	File folder

Answer: eM client

Task 2:
What is the email the threat is using?

I downloaded a tool "eM Client Forensics Wizard" and then open all the eM Client folder.
The first email from 11/27/2023 is from unknown sender



Hi there x
To :

hiiiiii

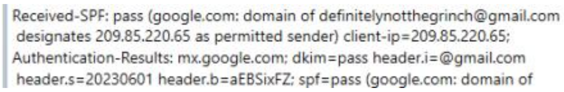
I know this is quite forward, but I noticed you going into the North pole HQ the other day and I thought you looked very cool,

tell me a bit about yourself??

Yours truly,

Wendy Elflower

Inside the Message Header I found the sender email

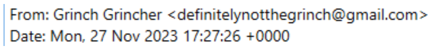


```
Received-SPF: pass (google.com: domain of definitelynotthegrinch@gmail.com
 designates 209.85.220.65 as permitted sender) client-ip=209.85.220.65;
Authentication-Results: mx.google.com; dkim=pass header.i=@gmail.com
 header.s=20230601 header.b=aEBSixFZ; spf=pass (google.com: domain of
```

Answer: definitelynotthegrinch@gmail.com

Task 3:
When does the threat actor reach out to Elfin?

Inside the Message Header

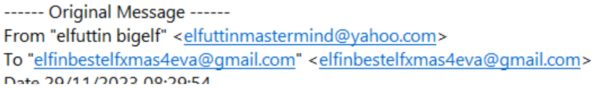


```
From: Grinch Grincher <definitelynotthegrinch@gmail.com>
Date: Mon, 27 Nov 2023 17:27:26 +0000
```

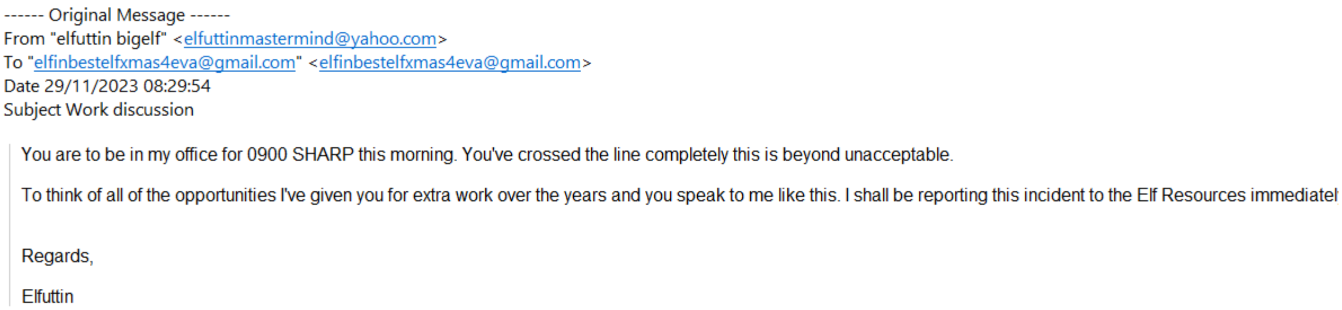
Answer: 2023-11-27 17:27:26

Task 4:
What is the name of Elfins boss?

Found this after the boss sent emails



------ Original Message ------
From "elfuttin bigelf" <elfuttinmastermind@yahoo.com>
To "elfinbestelfxmas4eva@gmail.com" <elfinbestelfxmas4eva@gmail.com>
Date 29/11/2023 08:29:54



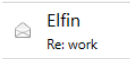
------ Original Message ------
From "elfuttin bigelf" <elfuttinmastermind@yahoo.com>
To "elfinbestelfxmas4eva@gmail.com" <elfinbestelfxmas4eva@gmail.com>
Date 29/11/2023 08:29:54
Subject Work discussion

> You are to be in my office for 0900 SHARP this morning. You've crossed the line completely this is beyond unacceptable.
>
> To think of all of the opportunities I've given you for extra work over the years and you speak to me like this. I shall be reporting this incident to the Elf Resources immediatel
>
> Regards,
>
> Elfuttin

Answer: elfuttin bigelf

Task 5:
What is the title of the email in which Elfin first mentions his access to Santas special files?

Emails titles

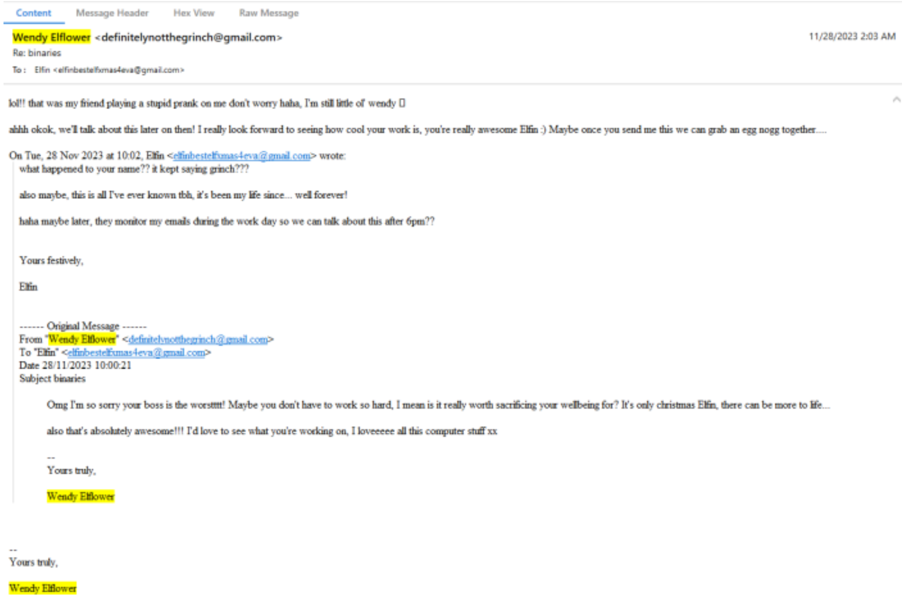


Elfin
Re: work

Answer: Re: work

Task 6:
The threat actor changes their name, what is the new name + the date of the first email Elfin receives with it?

There is an email when Elfin asked what happened to your name



Wendy Elflower <definitelynotthegrinch@gmail.com> 11/28/2023 2:03 AM
Re: binaries
To : Elfin <elfinbestelfxmas4eva@gmail.com>

lol!! that was my friend playing a stupid prank on me don't worry haha, I'm still little ol' wendy □

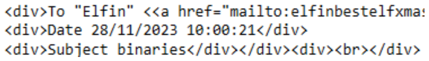
ahhh okok, we'll talk about this later on then! I really look forward to seeing how cool your work is, you're really awesome Elfin :) Maybe once you send me this we can grab an egg nogg together....

On Tue, 28 Nov 2023 at 10:02, Elfin <elfinbestelfxmas4eva@gmail.com> wrote:

> what happened to your name?? it kept saying grinch???
>
> also maybe, this is all I've ever known tbh, it's been my life since... well forever!
>
> haha maybe later, they monitor my emails during the work day so we can talk about this after 6pm??
>
> Yours festively,
>
> Elfin
>
> ------ Original Message ------
> From "Wendy Elflower" <definitelynotthegrinch@gmail.com>
> To "Elfin" <elfinbestelfxmas4eva@gmail.com>
> Date 28/11/2023 10:00:21
> Subject binaries
>
> Omg I'm so sorry your boss is the worstttt! Maybe you don't have to work so hard, I mean is it really worth sacrificing your wellbeing for? It's only christmas Elfin, there can be more to life...
>
> also that's absolutely awesome!!! I'd love to see what you're working on, I loveeeee all this computer stuff xx
>
> --
> Yours truly,
>
> Wendy Elflower

--
Yours truly,

Wendy Elflower

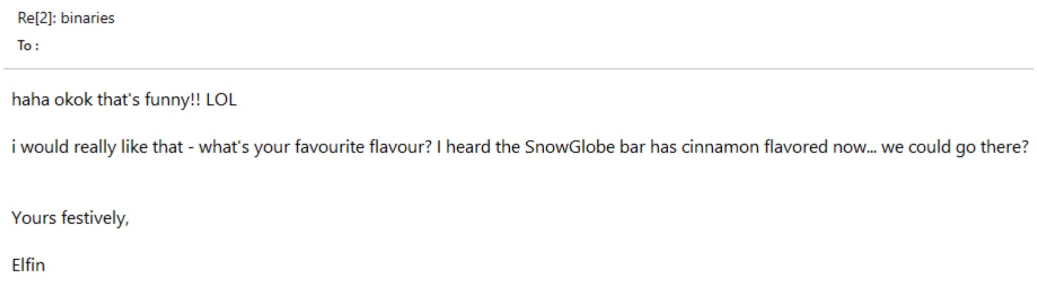


```
<div>To "Elfin" <<a href="mailto:elfinbestelfxma:
<div>Date 28/11/2023 10:00:21</div>
<div>Subject binaries</div></div><div><br></div>
```

Answer: wendy elflower, 2023-11-28 10:00:21

Task 7:
What is the name of the bar that Elfin offers to meet the threat actor at?

Found it when Elfin send email to Wendy



Re[2]: binaries

To :

haha okok that's funny!! LOL

i would really like that - what's your favourite flavour? I heard the SnowGlobe bar has cinnamon flavored now... we could go there?

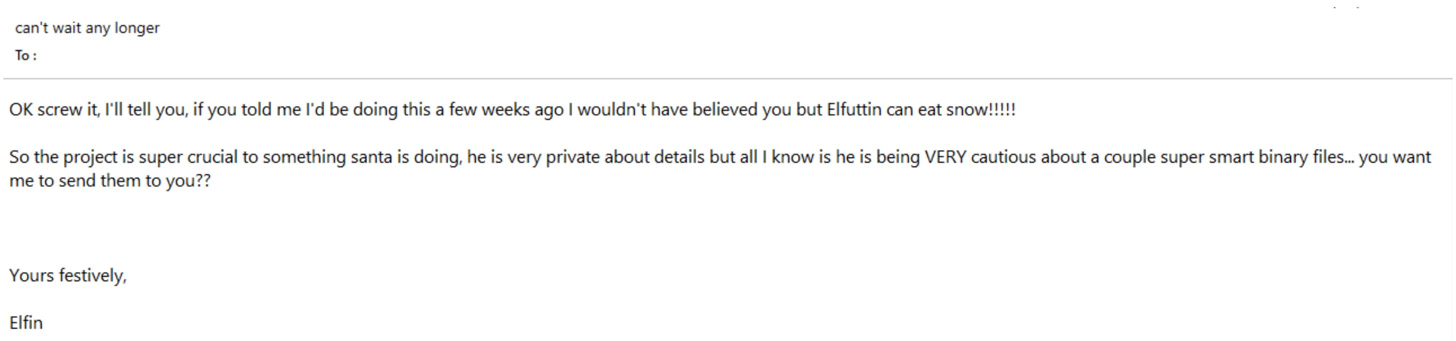
Yours festively,

Elfin

Answer: SnowGlobe

Task 8:
When does Elfin offer to send the secret files to the actor?

Found it when Elfin send email to Wendy



can't wait any longer

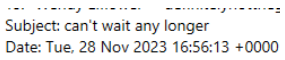
To :

OK screw it, I'll tell you, if you told me I'd be doing this a few weeks ago I wouldn't have believed you but Elfuttin can eat snow!!!!!

So the project is super crucial to something santa is doing, he is very private about details but all I know is he is being VERY cautious about a couple super smart binary files... you want me to send them to you??

Yours festively,

Elfin

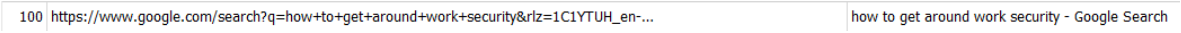


Subject: can't wait any longer
Date: Tue, 28 Nov 2023 16:56:13 +0000

Answer: 2023-11-28 16:56:13

Task 9:
What is the search string for the first suspicious google search from Elfin? (Format: string)

Checked the Chrome History with DB Browser

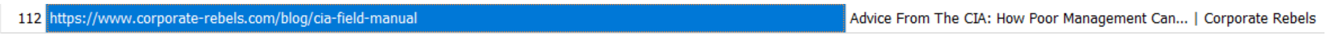


100	https://www.google.com/search?q=how+to+get+around+work+security&rlz=1C1YTUH_en-...	how to get around work security - Google Search

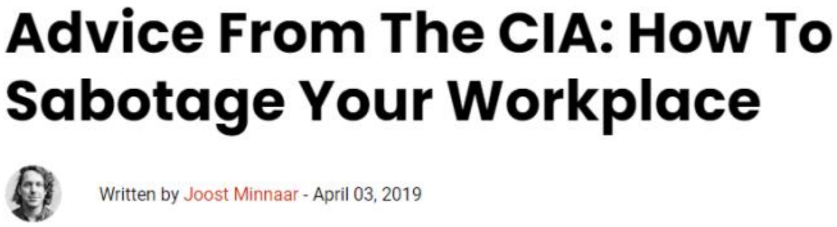
Answer: how to get around work security

Task 10:
What is the name of the author who wrote the article from the CIA field manual?

Checked the Chrome History with DB Browser



112	https://www.corporate-rebels.com/blog/cia-field-manual	Advice From The CIA: How Poor Management Can... | Corporate Rebels



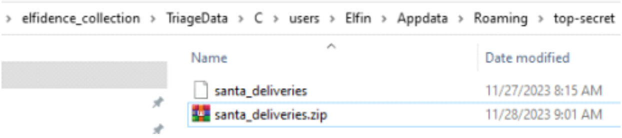
Advice From The CIA: How To Sabotage Your Workplace

Written by Joost Minnaar - April 03, 2019

Answer: Joost Minnaar

Task 11:
What is the name of Santas secret file that Elfin sent to the actor?

Searched the user files and found it inside the Appdata\Roaming



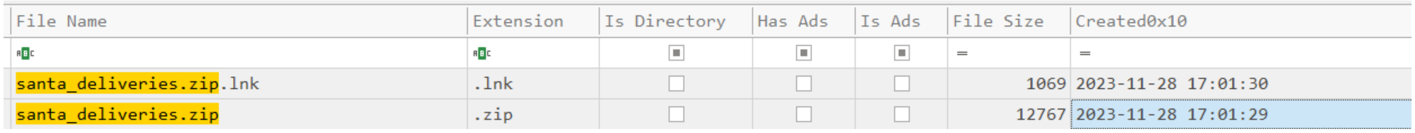
› elfidence_collection › TriageData › C › users › Elfin › Appdata › Roaming › top-secret

Name	Date modified
santa_deliveries	11/27/2023 8:15 AM
santa_deliveries.zip	11/28/2023 9:01 AM

Answer: santa_deliveries.zip

Task 12:
According to the filesystem, what is the exact CreationTime of the secret file on Elfins host?

Parsed the MFT with MFTECMD and searched the file name santa_deliveries.zip

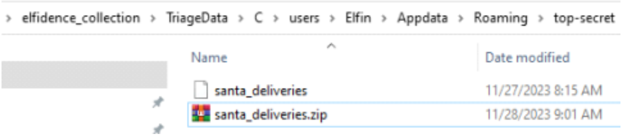


File Name	Extension	Is Directory	Has Ads	Is Ads	File Size	Created0x10
ABC	ABC	▣	▣	▣	=	=
santa_deliveries.zip.lnk	.lnk	□	□	□	1069	2023-11-28 17:01:30
santa_deliveries.zip	.zip	□	□	□	12767	2023-11-28 17:01:29

Answer: 2023-11-28 17:01:29

Task 13:
What is the full directory name that Elfin stored the file in?

Same like task 11 and also we can see it in the MFT



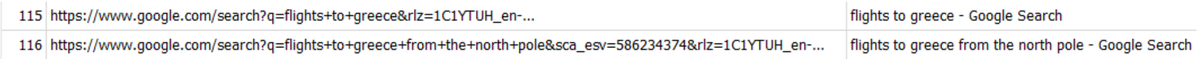
› elfidence_collection › TriageData › C › users › Elfin › Appdata › Roaming › top-secret

Name	Date modified
santa_deliveries	11/27/2023 8:15 AM
santa_deliveries.zip	11/28/2023 9:01 AM

Answer: C:\users\Elfin\Appdata\Roaming\top-secret

Task 14:
Which country is Elfin trying to flee to after he exfiltrates the file?

Checked the Chrome History

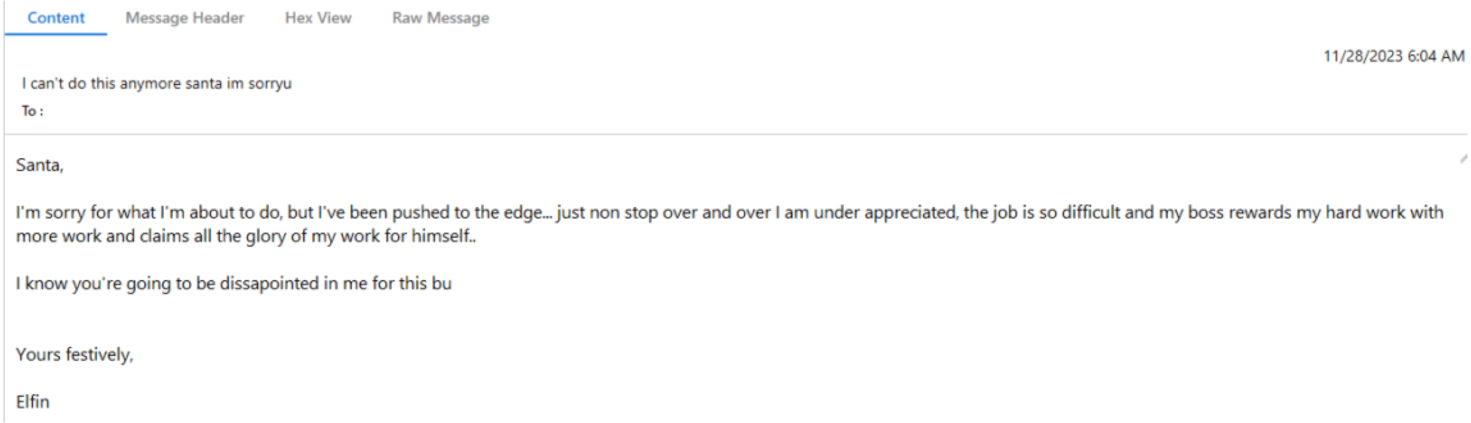


115	https://www.google.com/search?q=flights+to+greece&rlz=1C1YTUH_en-...	flights to greece - Google Search
116	https://www.google.com/search?q=flights+to+greece+from+the+north+pole&sca_esv=586234374&rlz=1C1YTUH_en-...	flights to greece from the north pole - Google Search

Answer: Greece

Task 15:
What is the email address of the apology letter the user (elfin) wrote out but didn't send?

Inside the eM Client in the Drafts folder



11/28/2023 6:04 AM

I can't do this anymore santa im sorryu

To :

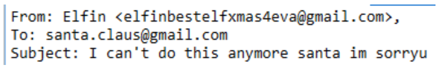
Santa,

I'm sorry for what I'm about to do, but I've been pushed to the edge... just non stop over and over I am under appreciated, the job is so difficult and my boss rewards my hard work with more work and claims all the glory of my work for himself..

I know you're going to be dissapointed in me for this bu

Yours festively,

Elfin



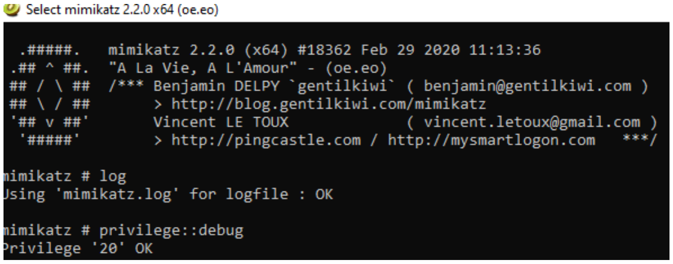
```
From: Elfin <elfinbestelfxmas4eva@gmail.com>,
To: santa.claus@gmail.com
Subject: I can't do this anymore santa im sorryu
```

Answer: santa.claus@gmail.com

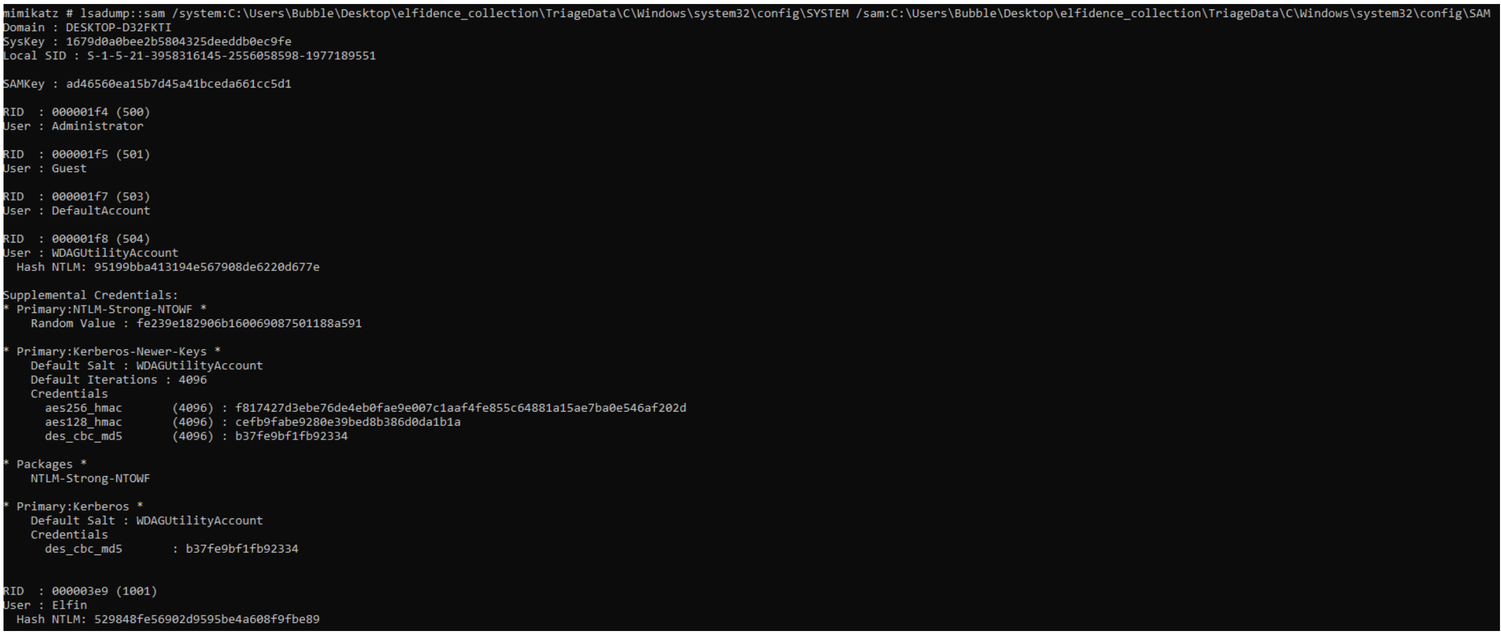
Task 16:
The head elf PixelPeppermint has requested any passwords of Elfins to assist in the investigation down the line. What's the windows password of Elfin's host?

I used mimikatz and dumped the SAM NTLM Hash

Starts with running the Mimikatz with Administrator and then used the following commands:
privilege::debug
lsadump::sam /system:C:\Users\Bubble\Desktop\elfidence_collection\TriageData\C\Windows\system32\config\SYSTEM /sam:C:\Users\Bubble\Desktop\elfidence_collection\TriageData\C\Windows\system32\config\SAM



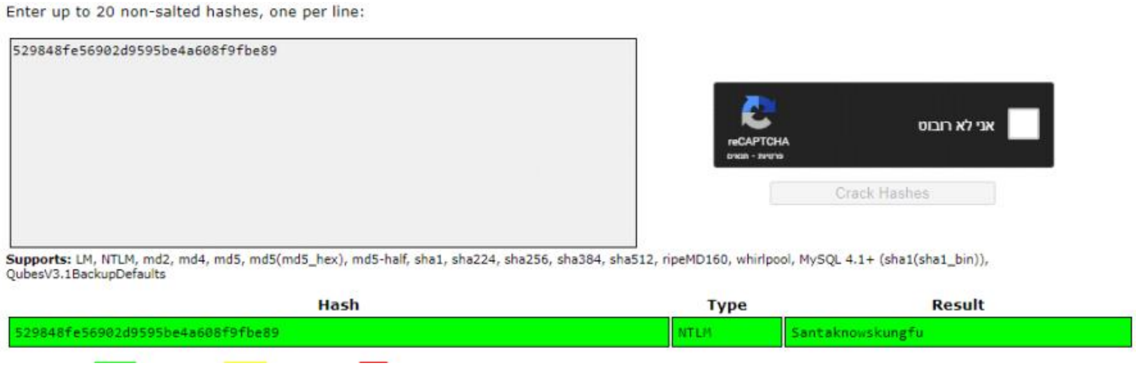
```
  .#####.   mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # log
Using 'mimikatz.log' for logfile : OK

mimikatz # privilege::debug
Privilege '20' OK
```



```
mimikatz # lsadump::sam /system:C:\Users\Bubble\Desktop\elfidence_collection\TriageData\C\Windows\system32\config\SYSTEM /sam:C:\Users\Bubble\Desktop\elfidence_collection\TriageData\C\Windows\system32\config\SAM
Domain : DESKTOP-D32FKTI
SysKey : 1679d0a0bee2b5804325deeddb0ec9fe
Local SID : S-1-5-21-3958316145-2556058598-1977189551

SAMKey : ad46560ea15b7d45a41bceda661cc5d1

RID  : 000001f4 (500)
User : Administrator

RID  : 000001f5 (501)
User : Guest

RID  : 000001f7 (503)
User : DefaultAccount

RID  : 000001f8 (504)
User : WDAGUtilityAccount
  Hash NTLM: 95199bba413194e567908de6220d677e

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : fe239e182906b160069087501188a591

* Primary:Kerberos-Newer-Keys *
    Default Salt : WDAGUtilityAccount
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : f817427d3ebe76de4eb0fae9e007c1aaf4fe855c64881a15ae7ba0e546af202d
      aes128_hmac       (4096) : cefb9fabe9280e39bed8b386d0da1b1a
      des_cbc_md5       (4096) : b37fe9bf1fb92334

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : WDAGUtilityAccount
    Credentials
      des_cbc_md5       : b37fe9bf1fb92334


RID  : 000003e9 (1001)
User : Elfin
  Hash NTLM: 529848fe56902d9595be4a608f9fbe89
```

Hash NTLM: 529848fe56902d9595be4a608f9fbe89

Then I cracked the password in the crackstation.net website


Enter up to 20 non-salted hashes, one per line:
529848fe56902d9595be4a608f9fbe89
אני לא רובוט
reCAPTCHA
פרטיות - תנאים
Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
529848fe56902d9595be4a608f9fbe89	NTLM	Santaknowskungfu

Answer: Santaknowskungfu