PART II

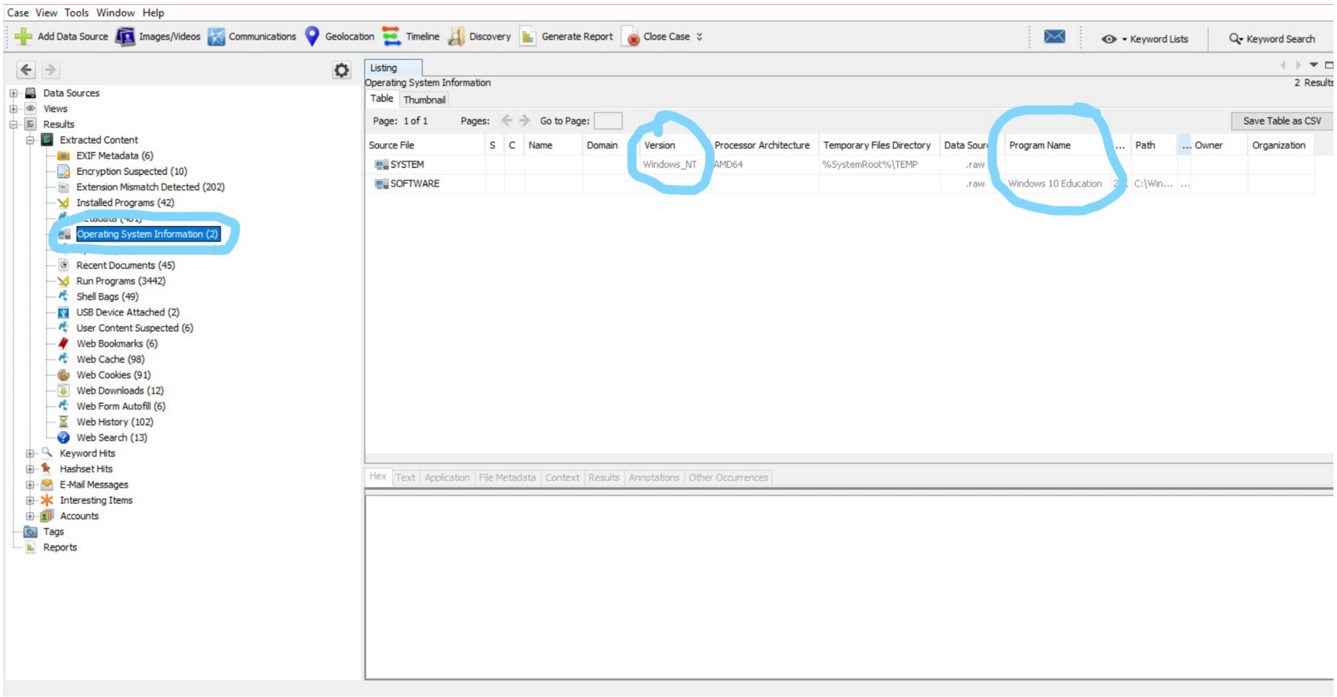
DISK FORENSICS

AUTOPSY ANALYSIS

1> From the left menu, select **“Results” >> “Extracted Content” >> “Operating System Information”**. This folder contains pointers to registry files from the SYSTEM and SOFTWARE hives, which stores system and software information and configurations.

The OS type is Windows_NT Windows 10 Education.

The same files store information that would help answer question 2.



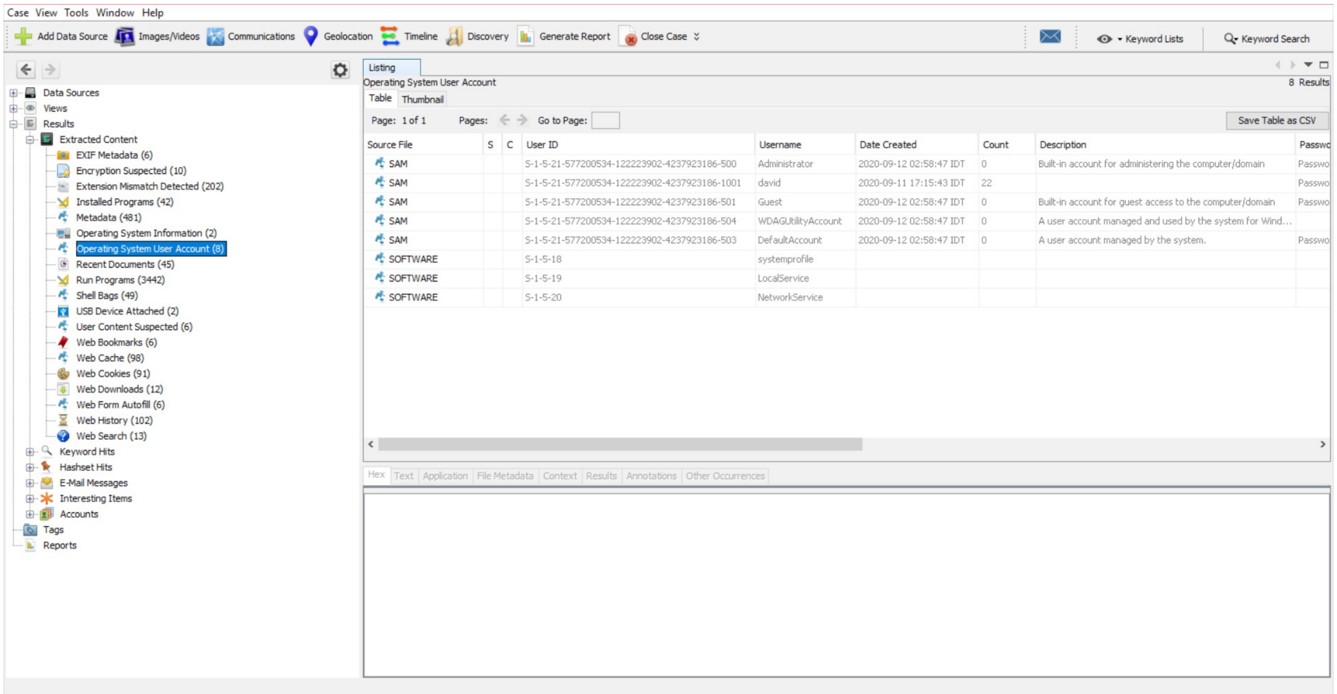
Operating System Information

2 Results

Page: 1 of 1 Pages: Go to Page:

Source File	S	C	Name	Domain	Version	Processor Architecture	Temporary Files Directory	Data Sour	Program Name	...	Path	...	Owner	Organization
SYSTEM					Windows_NT	AMD64	%SystemRoot%\TEMP	.raw						
SOFTWARE								.raw	Windows 10 Education	2	C:\Win...	...		

2> Also referring to registry files (SAM and SOFTWARE hives) this view shows 8 different users in the system, as well as a short description and a login count.



Operating System User Account

8 Results

Page: 1 of 1 Pages: Go to Page:

Source File	S	C	User ID	Username	Date Created	Count	Description	Passwo
SAM			S-1-5-21-577200534-122223902-4237923186-500	Administrator	2020-09-12 02:58:47 IDT	0	Built-in account for administering the computer/domain	Passwo
SAM			S-1-5-21-577200534-122223902-4237923186-1001	david	2020-09-11 17:15:43 IDT	22		Passwo
SAM			S-1-5-21-577200534-122223902-4237923186-501	Guest	2020-09-12 02:58:47 IDT	0	Built-in account for guest access to the computer/domain	Passwo
SAM			S-1-5-21-577200534-122223902-4237923186-504	WDAGUtilityAccount	2020-09-12 02:58:47 IDT	0	A user account managed and used by the system for Wind...	
SAM			S-1-5-21-577200534-122223902-4237923186-503	DefaultAccount	2020-09-12 02:58:47 IDT	0	A user account managed by the system.	Passwo
SOFTWARE			S-1-5-18	systemprofile				
SOFTWARE			S-1-5-19	LocalService				
SOFTWARE			S-1-5-20	NetworkService				

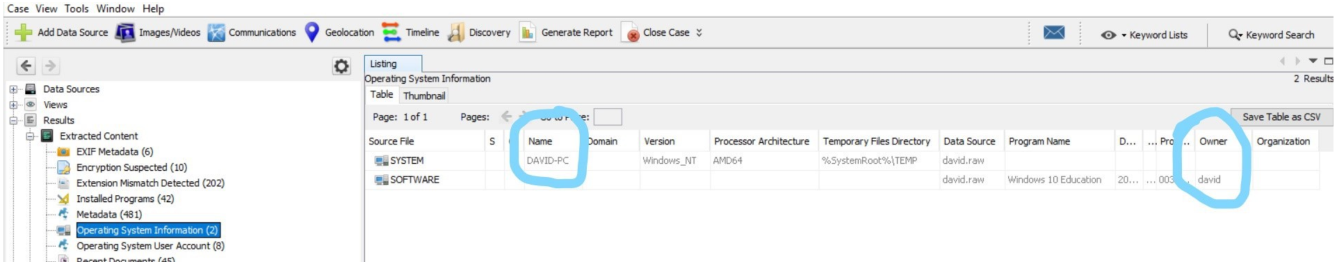
The mapped user accounts are:

- **Administrator** – Built-in account for administering the computer/domain.
- **david**
- **Guest** – Built-in account for guest access to the computer/domain.
- **WDAGUtilityAccount** – A user account managed and used by the system for Windows Defender Application Guard scenarios.
- **DefaultAccount** – A user account managed by the system.
- **SystemProfile** – Default system user running the root IIS process host.
- **LocalSystem** – Predefined local account used by the Service Control Manager.
- **NetworkService** - Predefined local account used by the Service Control Manager.

3> In the OS Information folder at SOFTWRAE hive reference we can see the name of the owner in the **“Owner” column**.

We can further use information from the **“Operating System User Account”** folder, where we learn that only one of all the user accounts found on the system is an actual non-system non-default account managed by a human, and it is of course **David**.

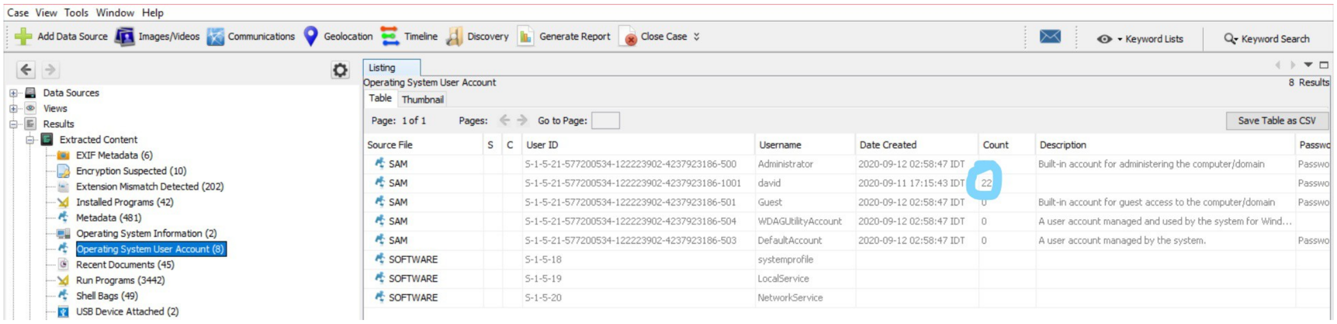
Also, in the “Count” tab we can see that David is the only user to have been in use (22 times).



Operating System Information — 2 Results

Page: 1 of 1

Source File	S		Name	Domain	Version	Processor Architecture	Temporary Files Directory	Data Source	Program Name	D...	... Pro...	Owner	Organization
SYSTEM			DAVID-PC		Windows_NT	AMD64	%SystemRoot%\TEMP	david.raw					
SOFTWARE								david.raw	Windows 10 Education	20...	... 003...	david	



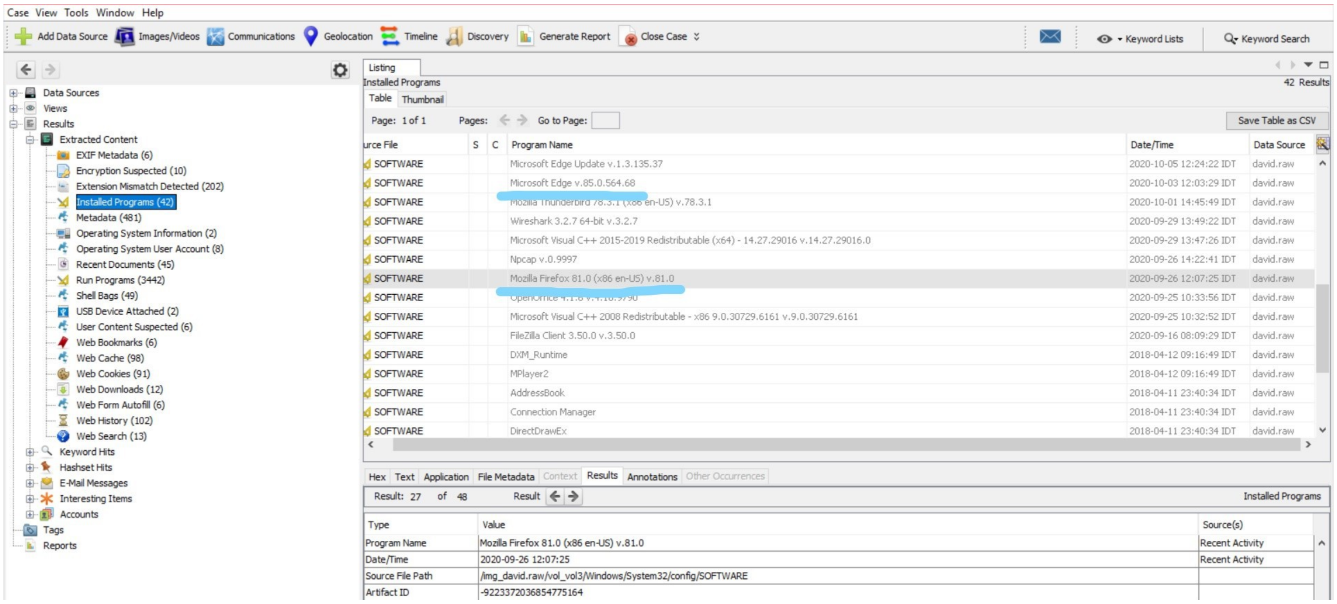
Operating System User Account — 8 Results

Page: 1 of 1 Go to Page:

Source File	S	C	User ID	Username	Date Created	Count	Description	Passwo
SAM			S-1-5-21-577200534-122223902-4237923186-500	Administrator	2020-09-12 02:58:47 IDT		Built-in account for administering the computer/domain	Passwo
SAM			S-1-5-21-577200534-122223902-4237923186-1001	david	2020-09-11 17:15:43 IDT	22		Passwo
SAM			S-1-5-21-577200534-122223902-4237923186-501	Guest	2020-09-12 02:58:47 IDT	0	Built-in account for guest access to the computer/domain	Passwo
SAM			S-1-5-21-577200534-122223902-4237923186-504	WDAGUtilityAccount	2020-09-12 02:58:47 IDT	0	A user account managed and used by the system for Wind...	
SAM			S-1-5-21-577200534-122223902-4237923186-503	DefaultAccount	2020-09-12 02:58:47 IDT	0	A user account managed by the system.	Passwo
SOFTWARE			S-1-5-18	systemprofile				
SOFTWARE			S-1-5-19	LocalService				
SOFTWARE			S-1-5-20	NetworkService				

4> Examining the **“Installed Programs”** folder we can see the browsers among programs that were installed on the PC, but it **won't show the ones that are installed by default** (like Internet Explorer).

The two browsers installed are Mozilla Firefox V.81.0 and Microsoft Edge V.85.0.564.37 updated to V.1.3.135.37



Installed Programs

42 Results

Page: 1 of 1 Pages: Go to Page:

urce File	S	C	Program Name	Date/Time	Data Source
SOFTWARE			Microsoft Edge Update v.1.3.135.37	2020-10-05 12:24:22 IDT	david.raw
SOFTWARE			Microsoft Edge v.85.0.564.68	2020-10-03 12:03:29 IDT	david.raw
SOFTWARE			Mozilla Thunderbird 78.3.1 (x86 en-US) v.78.3.1	2020-10-01 14:45:49 IDT	david.raw
SOFTWARE			Wireshark 3.2.7 64-bit v.3.2.7	2020-09-29 13:49:22 IDT	david.raw
SOFTWARE			Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.27.29016 v.14.27.29016.0	2020-09-29 13:47:26 IDT	david.raw
SOFTWARE			Npcap v.0.9997	2020-09-26 14:22:41 IDT	david.raw
SOFTWARE			Mozilla Firefox 81.0 (x86 en-US) v.81.0	2020-09-26 12:07:25 IDT	david.raw
SOFTWARE			OpenOffice 4.1.6 v.4.16.9790	2020-09-25 10:33:56 IDT	david.raw
SOFTWARE			Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 v.9.0.30729.6161	2020-09-25 10:32:52 IDT	david.raw
SOFTWARE			FileZilla Client 3.50.0 v.3.50.0	2020-09-16 08:09:29 IDT	david.raw
SOFTWARE			DXM_Runtime	2018-04-12 09:16:49 IDT	david.raw
SOFTWARE			MPlayer2	2018-04-12 09:16:49 IDT	david.raw
SOFTWARE			AddressBook	2018-04-11 23:40:34 IDT	david.raw
SOFTWARE			Connection Manager	2018-04-11 23:40:34 IDT	david.raw
SOFTWARE			DirectDrawEx	2018-04-11 23:40:34 IDT	david.raw

Result: 27 of 48 Result

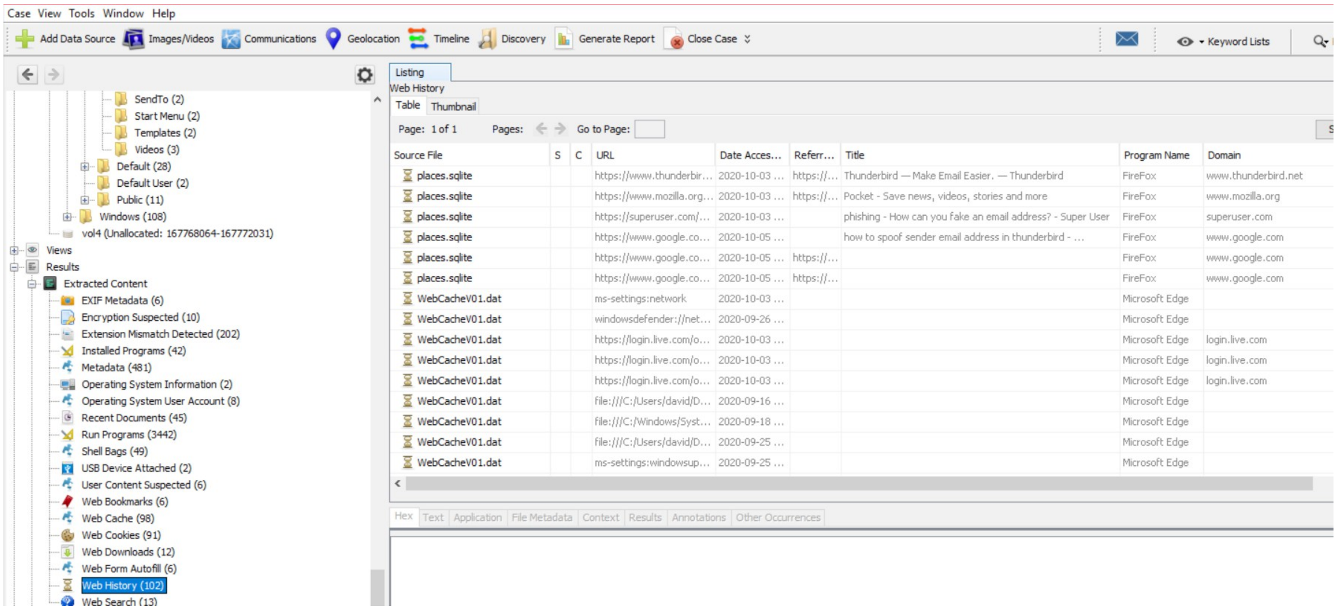
Installed Programs

Type	Value	Source(s)
Program Name	Mozilla Firefox 81.0 (x86 en-US) v.81.0	Recent Activity
Date/Time	2020-09-26 12:07:25	Recent Activity
Source File Path	/img_david.raw/vol_vol3/Windows/System32/config/SOFTWARE	
Artifact ID	-9223372036854775164	

In the **“Web History”** folder there are references to two **web cache database files;**

- **“places.sqlite”** which is the cache file for Mozilla Firefox.
- **“WebCacheV01.dat”** which is the cache file for Internret Explorer and MS Edge.

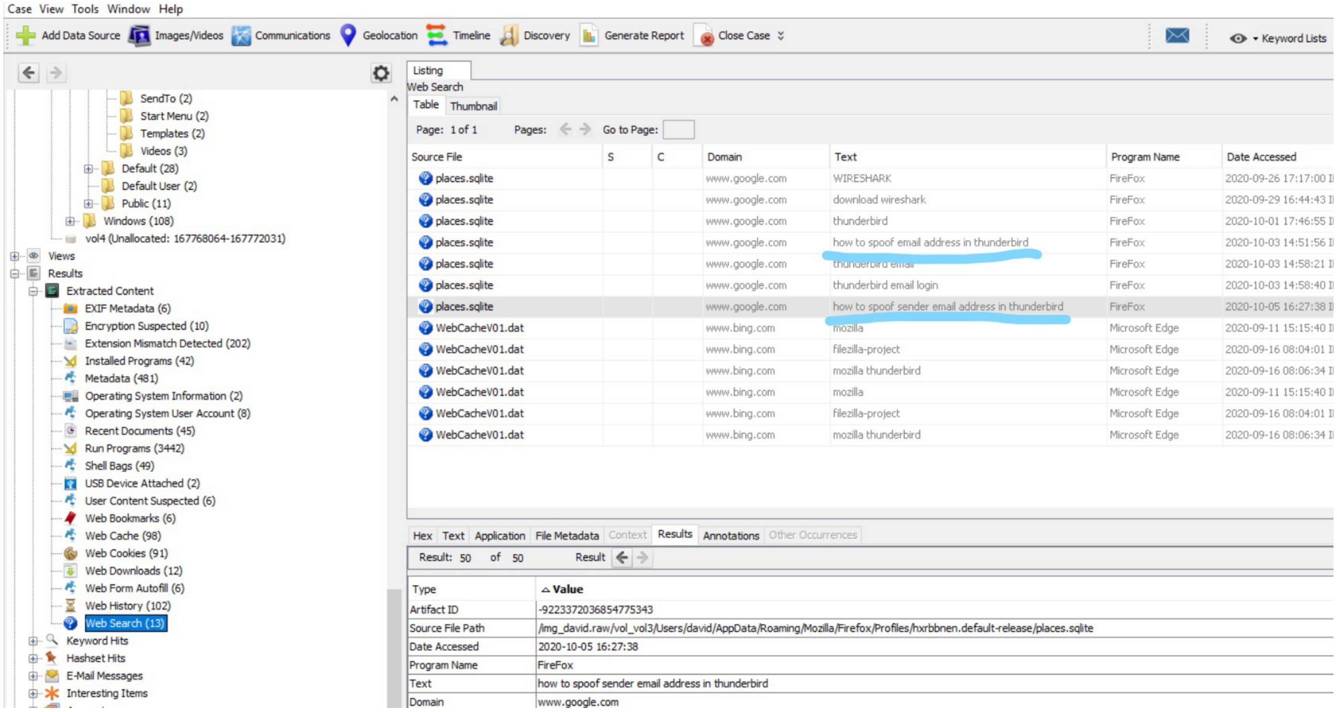
In the **“Program Name”** column there are two browsers exclusively; **Firefox and MS Edge**, which means that these are the two browsers to have been in use.



Source File	S	C	URL	Date Acces...	Referr...	Title	Program Name	Domain
places.sqlite			https://www.thunderbir...	2020-10-03 ...	https://...	Thunderbird — Make Email Easier. — Thunderbird	FireFox	www.thunderbird.net
places.sqlite			https://www.mozilla.org...	2020-10-03 ...	https://...	Pocket - Save news, videos, stories and more	FireFox	www.mozilla.org
places.sqlite			https://superuser.com/...	2020-10-03 ...		phishing - How can you fake an email address? - Super User	FireFox	superuser.com
places.sqlite			https://www.google.co...	2020-10-05 ...		how to spoof sender email address in thunderbird - ...	FireFox	www.google.com
places.sqlite			https://www.google.co...	2020-10-05 ...	https://...		FireFox	www.google.com
places.sqlite			https://www.google.co...	2020-10-05 ...	https://...		FireFox	www.google.com
WebCacheV01.dat			ms-settings:network	2020-10-03 ...			Microsoft Edge	
WebCacheV01.dat			windowsdefender://net...	2020-09-26 ...			Microsoft Edge	
WebCacheV01.dat			https://login.live.com/o...	2020-10-03 ...			Microsoft Edge	login.live.com
WebCacheV01.dat			https://login.live.com/o...	2020-10-03 ...			Microsoft Edge	login.live.com
WebCacheV01.dat			https://login.live.com/o...	2020-10-03 ...			Microsoft Edge	login.live.com
WebCacheV01.dat			file:///C:/Users/david/D...	2020-09-16 ...			Microsoft Edge	
WebCacheV01.dat			file:///C:/Windows/Syst...	2020-09-18 ...			Microsoft Edge	
WebCacheV01.dat			file:///C:/Users/david/D...	2020-09-25 ...			Microsoft Edge	
WebCacheV01.dat			ms-settings:windowsup...	2020-09-25 ...			Microsoft Edge	

5> To find evidence of suspicious activities we'll start at the “Web Search” folder.

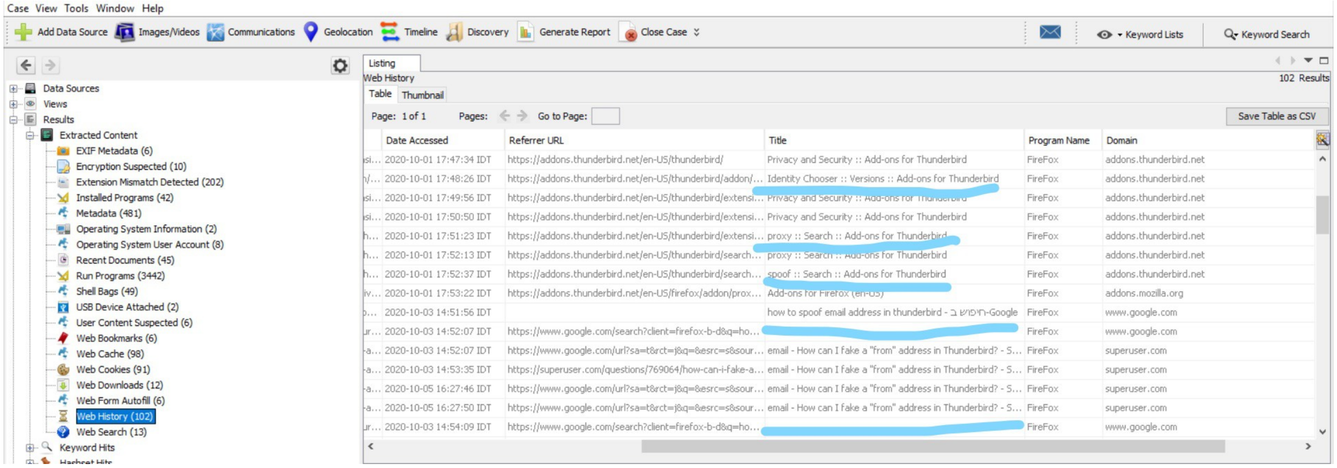
Again, referring to the **places.sqlite** and **WebCachev01.dat** files we see the actual text typed by the user in the browser. **Two suspicious searches** should raise a red flag; **'how to spoof email address in thunderbird'** and **'how to spoof sender email address in thunderbird'**.



Source File	S	C	Domain	Text	Program Name	Date Accessed
places.sqlite			www.google.com	WIRESHARK	FireFox	2020-09-26 17:17:00 I
places.sqlite			www.google.com	download wireshark	FireFox	2020-09-29 16:44:43 I
places.sqlite			www.google.com	thunderbird	FireFox	2020-10-01 17:46:55 I
places.sqlite			www.google.com	how to spoof email address in thunderbird	FireFox	2020-10-03 14:51:56 I
places.sqlite			www.google.com	thunderbird email	FireFox	2020-10-03 14:58:21 I
places.sqlite			www.google.com	thunderbird email login	FireFox	2020-10-03 14:58:40 I
places.sqlite			www.google.com	how to spoof sender email address in thunderbird	FireFox	2020-10-05 16:27:38 I
WebCacheV01.dat			www.bing.com	mozilla	Microsoft Edge	2020-09-11 15:15:40 I
WebCacheV01.dat			www.bing.com	filezilla-project	Microsoft Edge	2020-09-16 08:04:01 I
WebCacheV01.dat			www.bing.com	mozilla thunderbird	Microsoft Edge	2020-09-16 08:06:34 I
WebCacheV01.dat			www.bing.com	mozilla	Microsoft Edge	2020-09-11 15:15:40 I
WebCacheV01.dat			www.bing.com	filezilla-project	Microsoft Edge	2020-09-16 08:04:01 I
WebCacheV01.dat			www.bing.com	mozilla thunderbird	Microsoft Edge	2020-09-16 08:06:34 I

Type	△ Value
Artifact ID	-9223372036854775343
Source File Path	/img_david.raw/vol_vol3/Users/david/AppData/Roaming/Mozilla/Firefox/Profiles/hxrbbnen.default-release/places.sqlite
Date Accessed	2020-10-05 16:27:38
Program Name	FireFox
Text	how to spoof sender email address in thunderbird
Domain	www.google.com

In the “Web History” folder, under the “Title” column, we can see many more of those **spoofing queries** as well as queries for **proxy and email address spoofing add-ons** for Firefox browser.



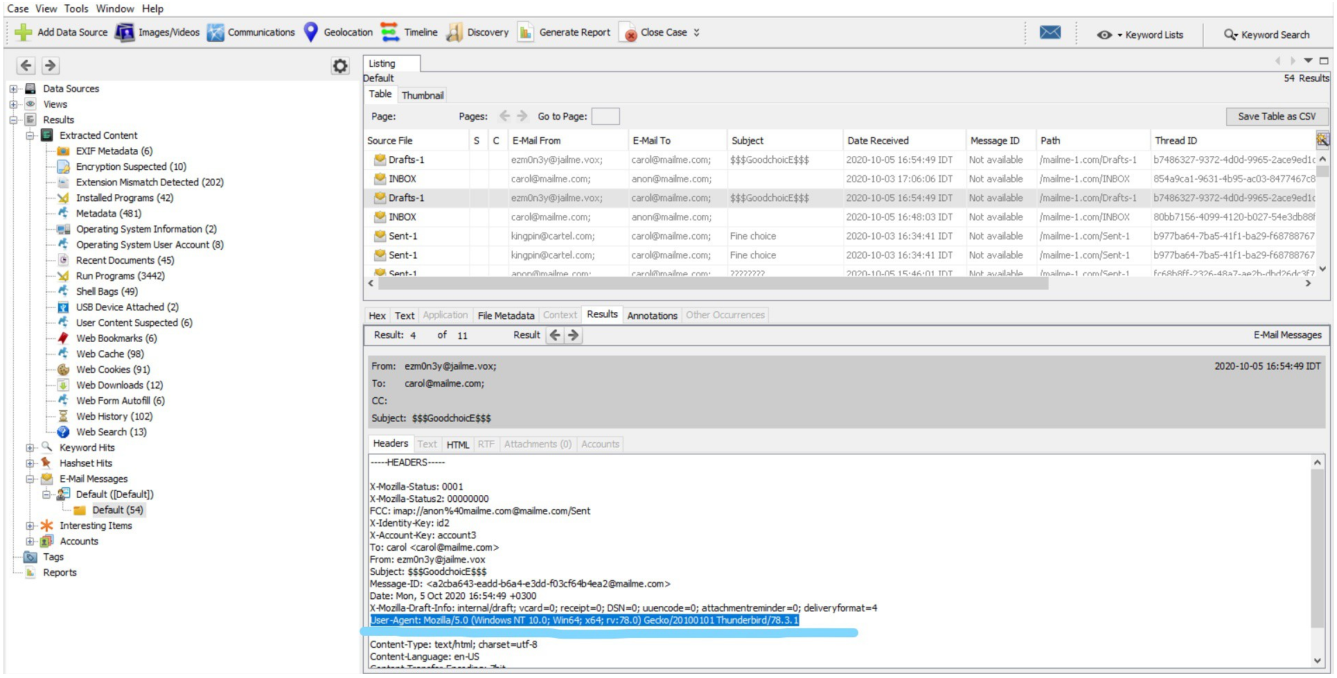
	Date Accessed	Referrer URL	Title	Program Name	Domain
si…	2020-10-01 17:47:34 IDT	https://addons.thunderbird.net/en-US/thunderbird/	Privacy and Security :: Add-ons for Thunderbird	FireFox	addons.thunderbird.net
h/…	2020-10-01 17:48:26 IDT	https://addons.thunderbird.net/en-US/thunderbird/addon/…	Identity Chooser :: Versions :: Add-ons for Thunderbird	FireFox	addons.thunderbird.net
si…	2020-10-01 17:49:56 IDT	https://addons.thunderbird.net/en-US/thunderbird/extensi…	Privacy and Security :: Add-ons for Thunderbird	FireFox	addons.thunderbird.net
si…	2020-10-01 17:50:50 IDT	https://addons.thunderbird.net/en-US/thunderbird/extensi…	Privacy and Security :: Add-ons for Thunderbird	FireFox	addons.thunderbird.net
h…	2020-10-01 17:51:23 IDT	https://addons.thunderbird.net/en-US/thunderbird/extensi…	proxy :: Search :: Add-ons for Thunderbird	FireFox	addons.thunderbird.net
h…	2020-10-01 17:52:13 IDT	https://addons.thunderbird.net/en-US/thunderbird/search…	proxy :: Search :: Add-ons for Thunderbird	FireFox	addons.thunderbird.net
h…	2020-10-01 17:52:37 IDT	https://addons.thunderbird.net/en-US/thunderbird/search…	spoof :: Search :: Add-ons for Thunderbird	FireFox	addons.thunderbird.net
iv…	2020-10-01 17:53:22 IDT	https://addons.thunderbird.net/en-US/firefox/addon/prox…	Add-ons for Firefox (en-US)	FireFox	addons.mozilla.org
o…	2020-10-03 14:51:56 IDT		how to spoof email address in thunderbird - חיפוש ב-Google	FireFox	www.google.com
ur…	2020-10-03 14:52:07 IDT	https://www.google.com/search?client=firefox-b-d&q=ho…	[illegible]	FireFox	www.google.com
-a…	2020-10-03 14:52:07 IDT	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&sour…	email - How can I fake a "from" address in Thunderbird? - S…	FireFox	superuser.com
-a…	2020-10-03 14:53:35 IDT	https://superuser.com/questions/769064/how-can-i-fake-a…	email - How can I fake a "from" address in Thunderbird? - S…	FireFox	superuser.com
-a…	2020-10-05 16:27:46 IDT	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&sour…	email - How can I fake a "from" address in Thunderbird? - S…	FireFox	superuser.com
-a…	2020-10-05 16:27:50 IDT	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&sour…	email - How can I fake a "from" address in Thunderbird? - S…	FireFox	superuser.com
ur…	2020-10-03 14:54:09 IDT	https://www.google.com/search?client=firefox-b-d&q=ho…	[illegible]	FireFox	www.google.com

Next, go to **“E-mail Messages” >> Default >> Default”**. This view contains Email messages sent and received by the user.

Scroll up and down and you'll find lots of Email messages with spoofed sender addresses.

In the bottom part of the screen, in the **“Text” tab**, we can see all the **messages in plain text**.

In the **“Results” tab** we can see the spoofed sender's **user-agent info**, (Photo #1)

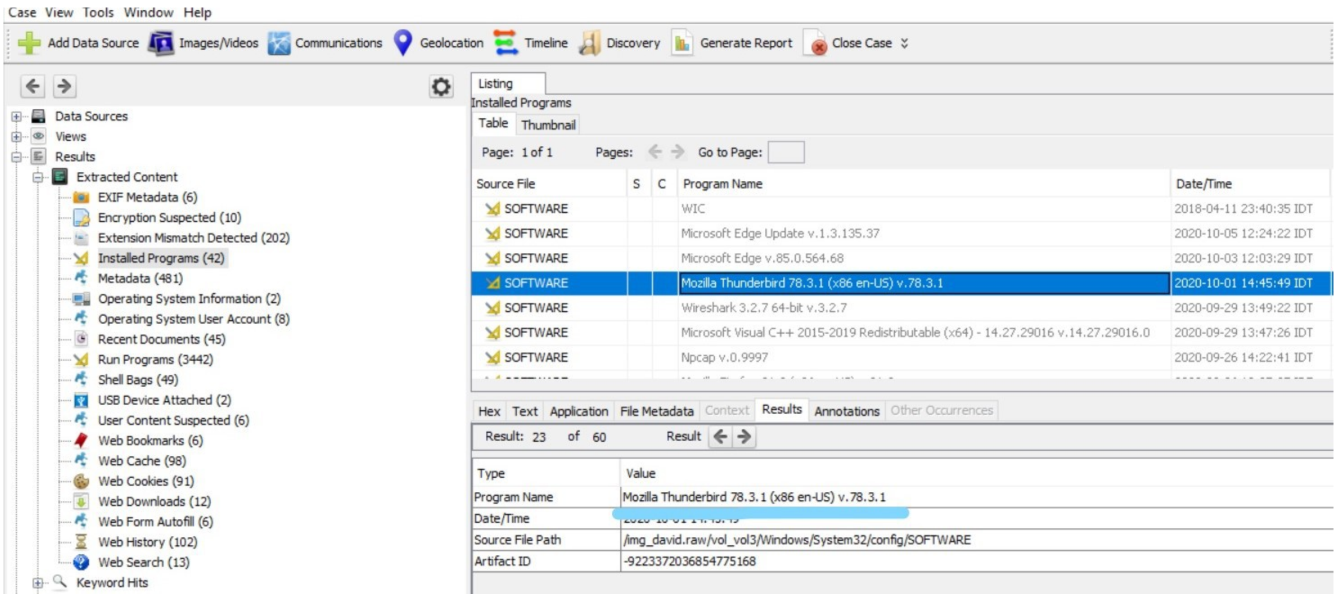


Source File	S	C	E-Mail From	E-Mail To	Subject	Date Received	Message ID	Path	Thread ID
Drafts-1			ezm0n3y@jailme.vox;	carol@mailme.com;	$$$GoodchoicE$$$	2020-10-05 16:54:49 IDT	Not available	/mailme-1.com/Drafts-1	b7486327-9372-4d0d-9965-2ace9ed1c
INBOX			carol@mailme.com;	anon@mailme.com;		2020-10-03 17:06:06 IDT	Not available	/mailme-1.com/INBOX	854a9ca1-9631-4b95-ac03-8477467c8
Drafts-1			ezm0n3y@jailme.vox;	carol@mailme.com;	$$$GoodchoicE$$$	2020-10-05 16:54:49 IDT	Not available	/mailme-1.com/Drafts-1	b7486327-9372-4d0d-9965-2ace9ed1c
INBOX			carol@mailme.com;	anon@mailme.com;		2020-10-05 16:48:03 IDT	Not available	/mailme-1.com/INBOX	80bb7156-4099-4120-b027-54e3db88f
Sent-1			kingpin@cartel.com;	carol@mailme.com;	Fine choice	2020-10-03 16:34:41 IDT	Not available	/mailme-1.com/Sent-1	b977ba64-7ba5-41f1-ba29-f68788767
Sent-1			kingpin@cartel.com;	carol@mailme.com;	Fine choice	2020-10-03 16:34:41 IDT	Not available	/mailme-1.com/Sent-1	b977ba64-7ba5-41f1-ba29-f68788767
Sent-1			anon@mailme.com;	carol@mailme.com;	????????	2020-10-05 15:46:01 IDT	Not available	/mailme-1.com/Sent-1	fc68b8ff-2326-48a7-ae2b-dbd26dc3f7

From: ezm0n3y@jailme.vox; 2020-10-05 16:54:49 IDT
To: carol@mailme.com;
CC:
Subject: $$$GoodchoicE$$$

```
-----HEADERS-----

X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
FCC: imap://anon%40mailme.com@mailme.com/Sent
X-Identity-Key: id2
X-Account-Key: account3
To: carol <carol@mailme.com>
From: ezm0n3y@jailme.vox
Subject: $$$GoodchoicE$$$
Message-ID: <a2cba643-eadd-b6a4-e3dd-f03cf64b4ea2@mailme.com>
Date: Mon, 5 Oct 2020 16:54:49 +0300
X-Mozilla-Draft-Info: internal/draft; vcard=0; receipt=0; DSN=0; uuencode=0; attachmentreminder=0; deliveryformat=4
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Thunderbird/78.3.1

Content-Type: text/html; charset=utf-8
Content-Language: en-US
```

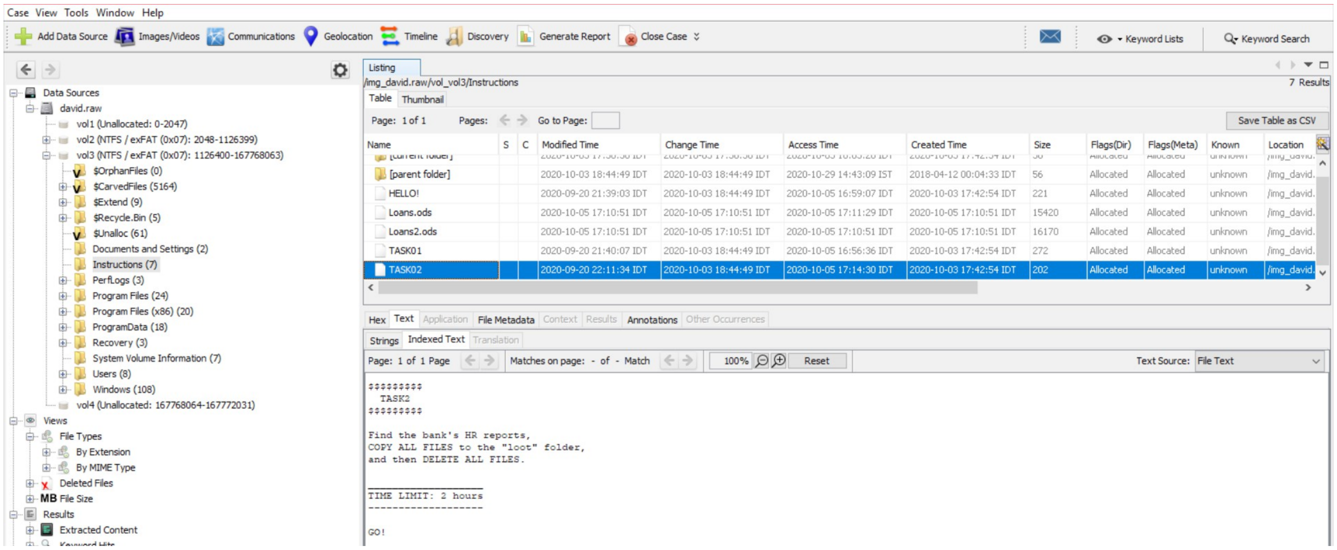
Comparing this user-agent to David's user-agent info as stored in the SOFTWRAE registry hive (Photo #2) **is a definite match**.



Source File	S	C	Program Name	Date/Time
SOFTWARE			WIC	2018-04-11 23:40:35 IDT
SOFTWARE			Microsoft Edge Update v.1.3.135.37	2020-10-05 12:24:22 IDT
SOFTWARE			Microsoft Edge v.85.0.564.68	2020-10-03 12:03:29 IDT
SOFTWARE			Mozilla Thunderbird 78.3.1 (x86 en-US) v.78.3.1	2020-10-01 14:45:49 IDT
SOFTWARE			Wireshark 3.2.7 64-bit v.3.2.7	2020-09-29 13:49:22 IDT
SOFTWARE			Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.27.29016 v.14.27.29016.0	2020-09-29 13:47:26 IDT
SOFTWARE			Npcap v.0.9997	2020-09-26 14:22:41 IDT

Type	Value
Program Name	Mozilla Thunderbird 78.3.1 (x86 en-US) v.78.3.1
Date/Time	2020-10-01 14:45:49
Source File Path	/img_david.raw/vol_vol3/Windows/System32/config/SOFTWARE
Artifact ID	-9223372036854775168

We can also view the whole “Instructions” folder located in the C: drive and view it's contents



```
Data Sources
  david.raw
    vol1 (Unallocated: 0-2047)
    vol2 (NTFS / exFAT (0x07): 2048-1126399)
    vol3 (NTFS / exFAT (0x07): 1126400-167768063)
      $OrphanFiles (0)
      $CarvedFiles (5164)
      $Extend (9)
      $Recycle.Bin (5)
      $Unalloc (61)
      Documents and Settings (2)
      Instructions (7)
      PerfLogs (3)
      Program Files (24)
      Program Files (x86) (20)
      ProgramData (18)
      Recovery (3)
      System Volume Information (7)
      Users (8)
      Windows (108)
    vol4 (Unallocated: 167768064-167772031)
Views
  File Types
    By Extension
    By MIME Type
  Deleted Files
  File Size
Results
  Extracted Content
```

/img_david.raw/vol_vol3/Instructions

7 Results

Page: 1 of 1 Pages: Go to Page:

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[current folder]			[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Allocated	Allocated	unknown	/img_david.
[parent folder]			2020-10-03 18:44:49 IDT	2020-10-03 18:44:49 IDT	2020-10-29 14:43:09 IST	2018-04-12 00:04:33 IDT	56	Allocated	Allocated	unknown	/img_david.
HELLO!			2020-09-20 21:39:03 IDT	2020-10-03 18:44:49 IDT	2020-10-05 16:59:07 IDT	2020-10-03 17:42:54 IDT	221	Allocated	Allocated	unknown	/img_david.
Loans.ods			2020-10-05 17:10:51 IDT	2020-10-05 17:10:51 IDT	2020-10-05 17:11:29 IDT	2020-10-05 17:10:51 IDT	15420	Allocated	Allocated	unknown	/img_david.
Loans2.ods			2020-10-05 17:10:51 IDT	2020-10-05 17:10:51 IDT	2020-10-05 17:10:51 IDT	2020-10-05 17:10:51 IDT	16170	Allocated	Allocated	unknown	/img_david.
TASK01			2020-09-20 21:40:07 IDT	2020-10-03 18:44:49 IDT	2020-10-05 16:56:36 IDT	2020-10-03 17:42:54 IDT	272	Allocated	Allocated	unknown	/img_david.
TASK02			2020-09-20 22:11:34 IDT	2020-10-03 18:44:49 IDT	2020-10-05 17:14:30 IDT	2020-10-03 17:42:54 IDT	202	Allocated	Allocated	unknown	/img_david.

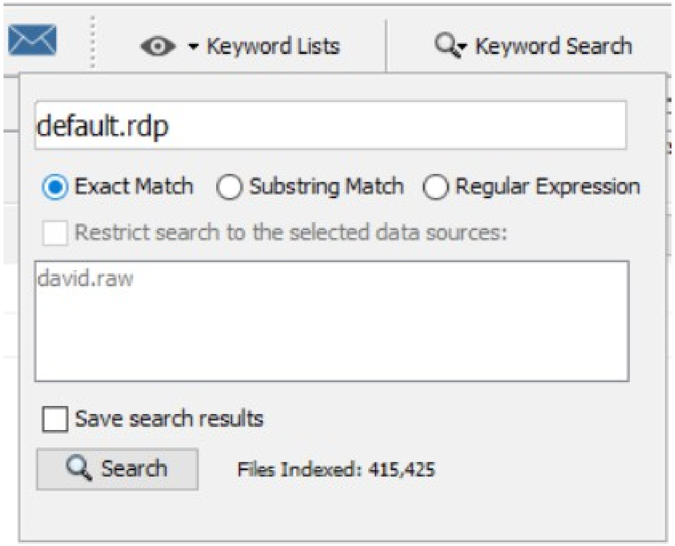
Page: 1 of 1 Page Matches on page: - of - Match 100% Text Source: File Text

```
$$$$$$$$$
  TASK2
$$$$$$$$$

Find the bank's HR reports,
COPY ALL FILES to the "loot" folder,
and then DELETE ALL FILES.


___________________
TIME LIMIT: 2 hours
-------------------


GO!
```

In conclusion, David's suspicious activities are mostly **Email address spoofing** and **covering his identity in an attempt to conspire with other FakeBank employees**.

6> Defult rdp connections information is stored in a hidden **default.rdp** file which is under the **Documents folder by default.**

If we had not known this we could simply use the “Keyword Search” option on the uppermost right hand side.



default.rdp

● Exact Match ○ Substring Match ○ Regular Expression

□ Restrict search to the selected data sources:

david.raw

□ Save search results

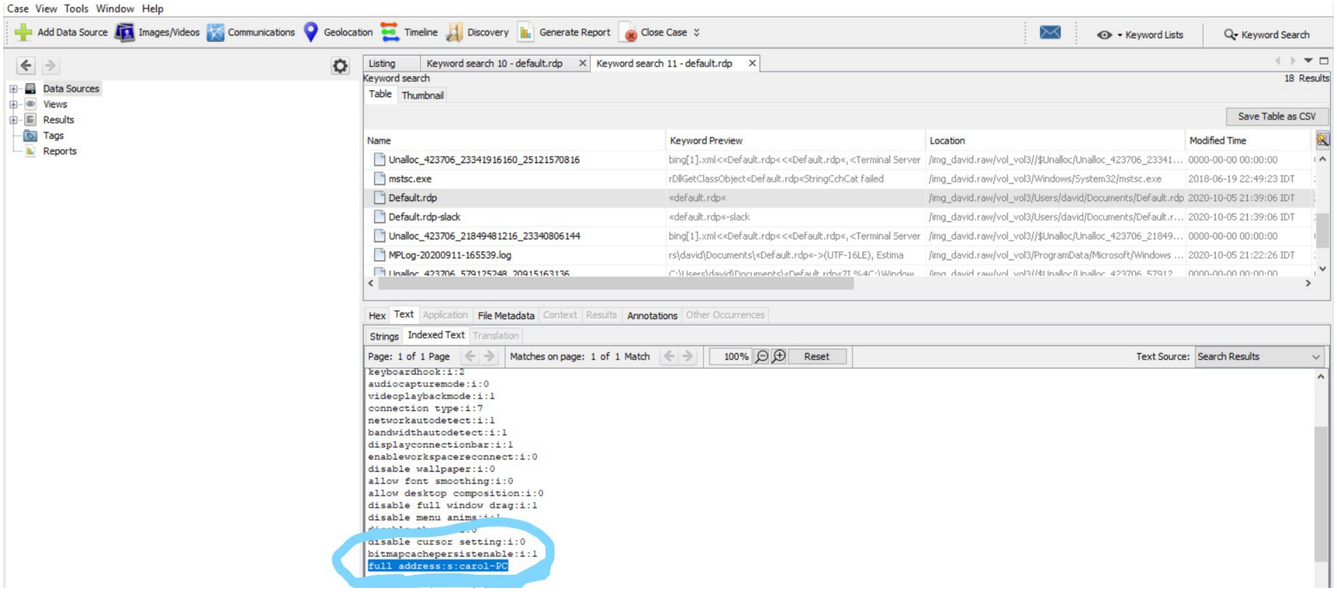
Files Indexed: 415,425

Scroll down, find and **select the default.rdp** file.

In the **“Indexed Text” tab** at screen bottom are the configurations for the default rdp connection.

Look for the **“full address”** row...

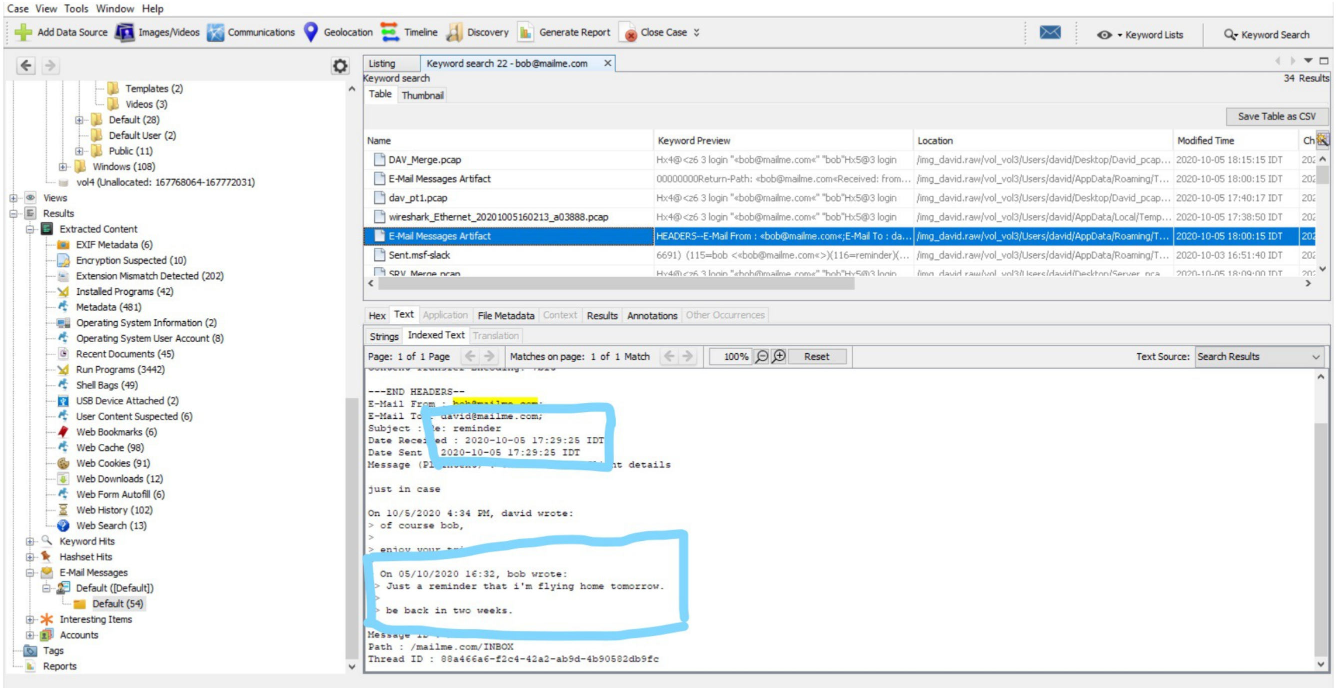
Carol-PC is the default rdp session's full address.



Name	Keyword Preview	Location	Modified Time
Unalloc_423706_23341916160_25121570816	bing[1].xml<<Default.rdp<<<Default.rdp<, <Terminal Server	/img_david.raw/vol_vol3//$Unalloc/Unalloc_423706_23341...	0000-00-00 00:00:00
mstsc.exe	rDllGetClassObject<Default.rdp<StringCchCat failed	/img_david.raw/vol_vol3/Windows/System32/mstsc.exe	2018-06-19 22:49:23 IDT
Default.rdp	<default.rdp<	/img_david.raw/vol_vol3/Users/david/Documents/Default.rdp	2020-10-05 21:39:06 IDT
Default.rdp-slack	<default.rdp<-slack	/img_david.raw/vol_vol3/Users/david/Documents/Default.r...	2020-10-05 21:39:06 IDT
Unalloc_423706_21849481216_23340806144	bing[1].xml<<Default.rdp<<<Default.rdp<, <Terminal Server	/img_david.raw/vol_vol3//$Unalloc/Unalloc_423706_21849...	0000-00-00 00:00:00
MPLog-20200911-165539.log	rs\david\Documents\<Default.rdp<->(UTF-16LE), Estima	/img_david.raw/vol_vol3/ProgramData/Microsoft/Windows ...	2020-10-05 21:22:26 IDT
Unalloc_423706_579125248_20915163136	C:\Users\david\Documents\<Default.rdp<7L%4C:\Window	/img_david.raw/vol_vol3//$Unalloc/Unalloc_423706_57912...	0000-00-00 00:00:00

```
keyboardhook:i:2
audiocapturemode:i:0
videoplaybackmode:i:1
connection type:i:7
networkautodetect:i:1
bandwidthautodetect:i:1
displayconnectionbar:i:1
enableworkspacereconnect:i:0
disable wallpaper:i:0
allow font smoothing:i:0
allow desktop composition:i:0
disable full window drag:i:1
disable menu anims:i:1
disable themes:i:0
disable cursor setting:i:0
bitmapcachepersistenable:i:1
full address:s:carol-PC
```

7> Performing a **Keyword Search for "bob@mailme.com"** (bob's email address) all files containing this expression. Search the **"Name" column** for **"E-Mail Message Artifacts"** Though there are multiple messages titled "reminder", only the last one, dated 20-10-05 indicates a return time of two weeks from the flight date. According to the email Bob's flight is "tomorrow" which is 20-10-06, meaning **Bob's due to be back on 20-10-20**.



Name	Keyword Preview	Location	Modified Time	Ch
DAV_Merge.pcap	Hx4@<z6 3 login "«bob@mailme.com«" "bob"Hx5@3 login	/img_david.raw/vol_vol3/Users/david/Desktop/David_pcap…	2020-10-05 18:15:15 IDT	202
E-Mail Messages Artifact	00000000Return-Path: «bob@mailme.com«Received: from…	/img_david.raw/vol_vol3/Users/david/AppData/Roaming/T…	2020-10-05 18:00:15 IDT	202
dav_pt1.pcap	Hx4@<z6 3 login "«bob@mailme.com«" "bob"Hx5@3 login	/img_david.raw/vol_vol3/Users/david/Desktop/David_pcap…	2020-10-05 17:40:17 IDT	202
wireshark_Ethernet_20201005160213_a03888.pcap	Hx4@<z6 3 login "«bob@mailme.com«" "bob"Hx5@3 login	/img_david.raw/vol_vol3/Users/david/AppData/Local/Temp…	2020-10-05 17:38:50 IDT	202
E-Mail Messages Artifact	HEADERS--E-Mail From : «bob@mailme.com«;E-Mail To : da…	/img_david.raw/vol_vol3/Users/david/AppData/Roaming/T…	2020-10-05 18:00:15 IDT	202
Sent.msf-slack	6691) (115=bob <«bob@mailme.com«>)(116=reminder)(…	/img_david.raw/vol_vol3/Users/david/AppData/Roaming/T…	2020-10-03 16:51:40 IDT	202
SRV_Merge.pcap	Hx4@<z6 3 login "«bob@mailme.com«" "bob"Hx5@3 login	/img_david.raw/vol_vol3/Users/david/Desktop/Server_pca…	2020-10-05 18:09:00 IDT	202

```
---END HEADERS--
E-Mail From : bob@mailme.com;
E-Mail To : david@mailme.com;
Subject : Re: reminder
Date Received : 2020-10-05 17:29:25 IDT
Date Sent : 2020-10-05 17:29:25 IDT
Message (Plaintext) : [illegible]nt details

just in case

On 10/5/2020 4:34 PM, david wrote:
> of course bob,
>
> enjoy your tri[illegible]

 On 05/10/2020 16:32, bob wrote:
> Just a reminder that i'm flying home tomorrow.
>
> be back in two weeks.

Message ID : [illegible]
Path : /mailme.com/INBOX
Thread ID : 88a466a6-f2c4-42a2-ab9d-4b90582db9fc
```