

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.

The screenshot displays a forensic analysis tool interface. On the left, a tree view under 'Results' > 'Extracted Content' has 'Operating System Information (2)' selected and circled in blue. The main pane shows a table titled 'Operating System Information' with two results. The first result, for the 'SYSTEM' source file, has 'Version' circled in blue and shows 'Windows_NT'. The second result, for the 'SOFTWARE' source file, has 'Program Name' circled in blue and shows 'Windows 10 Education'. The table columns include Source File, S, C, Name, Domain, Version, Processor Architecture, Temporary Files Directory, Data Source, Program Name, Path, Owner, and Organization.

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

The screenshot displays a forensic analysis application interface. On the left, a sidebar lists various data sources and results, with 'Operating System User Account (8)' highlighted. The main window shows a table titled 'Operating System User Account' with 8 results. The table columns are: Source File, S, C, User ID, Username, Date Created, Count, Description, and Password. The data rows are as follows:

Source File	S	C	User ID	Username	Date Created	Count	Description	Password
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				

Below the table, there are tabs for 'Hex', 'Text', 'Application', 'File Metadata', 'Context', 'Results', 'Annotations', and 'Other Occurrences'. The 'Results' tab is currently selected.

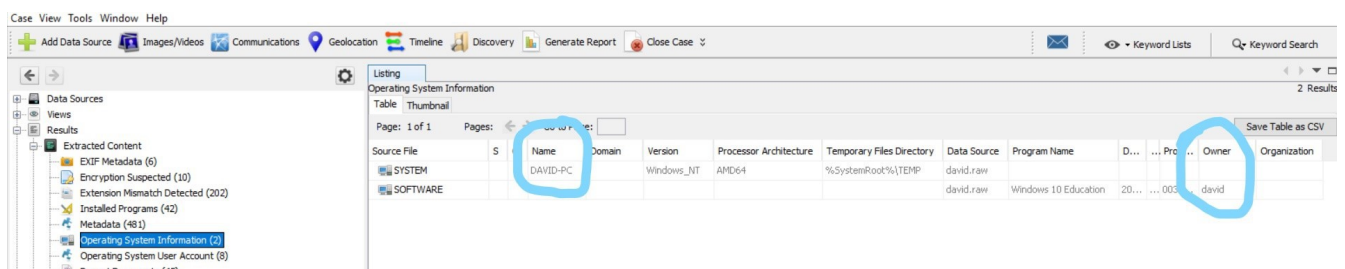
The mapped user accounts are:

- **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.

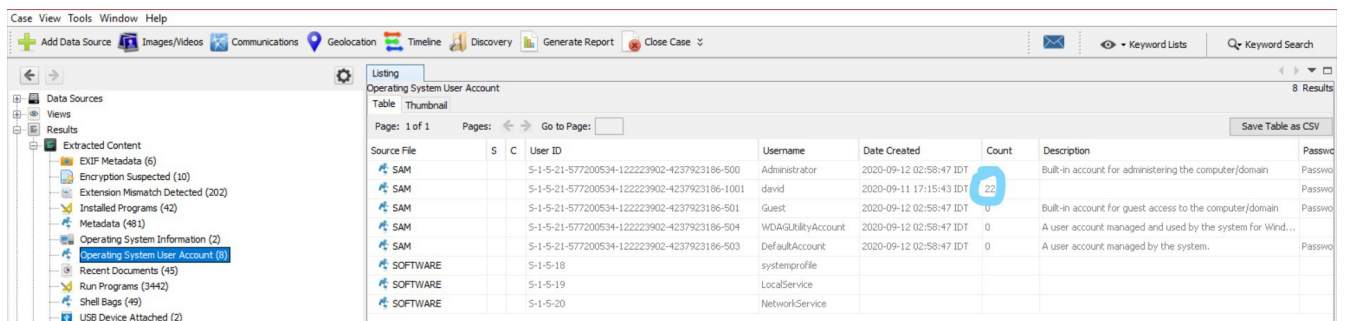
We can further use information from the “**Operating System User Account**” folder, where we learn that only one of all the user accounts found on the system is an actual non-system non-default account managed by a human, and it is of course **David**.

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



The screenshot shows the SOFTWRAE interface with the 'Listing' tab selected. The 'Operating System Information' table is displayed, showing two results. The 'Name' column contains 'DAVID-PC' and the 'Owner' column contains 'david'. Both are circled in blue.

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



The screenshot shows the SOFTWRAE interface with the 'Listing' tab selected. The 'Operating System User Account' table is displayed, showing 8 results. The 'Count' column for the 'david' user account is circled in blue, showing a value of 22.

Source File	S	C	User ID	Username	Date Created	Count	Description	Password
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	Password
SAM			S-1-5-21-577200534-122223902-4237923186-1001	david	2020-09-11 17:15:43 IDT	22	Built-in account for guest access to the computer/domain	Password
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	Password
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...	Password
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.	Password
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

The screenshot shows a forensic analysis tool interface. The main window displays a list of installed programs. The left sidebar shows a tree view of the file system, with 'Installed Programs' selected. The bottom pane shows details for the selected program, including its name, date/time, and source file path.

Source 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 4.1.0 v.4.1.0-v.4.1.0	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			D3M_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

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 Internet 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.

The screenshot shows a forensic analysis tool interface. On the left, a file system tree displays folders like 'SendTo (2)', 'Start Menu (2)', 'Templates (2)', 'Videos (3)', 'Default (28)', 'Default User (2)', 'Public (11)', 'Windows (108)', and 'vol4 (Unallocated: 167768064-167772031)'. Below this is a 'Results' pane with categories such as 'Extracted Content', 'EXIF Metadata (6)', 'Encryption Suspected (10)', 'Extension Mismatch Detected (202)', 'Installed Programs (42)', 'Metadata (481)', 'Operating System Information (2)', 'Operating System User Account (8)', 'Recent Documents (45)', 'Run Programs (3442)', 'Shell Bags (49)', 'USB Device Attached (2)', 'User Content Suspected (6)', 'Web Bookmarks (6)', 'Web Cache (98)', 'Web Cookies (91)', 'Web Downloads (12)', 'Web Form AutoFill (6)', 'Web History (102)', and 'Web Search (13)'. The 'Web History' category is selected. On the right, a table titled 'Web History' displays the following data:

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	

At the bottom of the table, there are tabs for 'Hex', 'Text', 'Application', 'File Metadata', 'Context', 'Results', 'Annotations', and 'Other Occurrences'. The 'Results' tab is currently selected.

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'**.

The screenshot shows a forensic analysis tool interface. The sidebar on the left displays a file tree with folders like 'SendTo (2)', 'Start Menu (2)', 'Templates (2)', 'Videos (3)', 'Default (28)', 'Default User (2)', 'Public (11)', 'Windows (108)', and 'vol4 (Unallocated: 167768064-167772031)'. The 'Web Search' folder is selected, showing 13 items. The main pane displays a table of search results with columns: Source File, S, C, Domain, Text, Program Name, and Date Accessed. Two entries are highlighted in blue: one from 'places.sqlite' with the text 'how to spoof email address in thunderbird' and another from 'WebCacheV01.dat' with the text 'how to spoof sender email address in thunderbird'. The bottom pane shows a detailed view of the selected entry, including its Artifact ID, Source File Path, Date Accessed, Program Name, Text, and Domain.

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

Type	Value
Artifact ID	-9223372036854775343
Source File Path	/img_david.raw/vol_vol3/Users/david/AppData/Roaming/Mozilla/Firefox/Profiles/hxbnbn.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
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
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
2020-10-01 17:49:56 IDT	https://addons.thunderbird.net/en-US/thunderbird/extensions/...	Privacy and Security :: Add-ons for Thunderbird	Firefox	addons.thunderbird.net
2020-10-01 17:50:50 IDT	https://addons.thunderbird.net/en-US/thunderbird/extensions/...	Privacy and Security :: Add-ons for Thunderbird	Firefox	addons.thunderbird.net
2020-10-01 17:51:23 IDT	https://addons.thunderbird.net/en-US/thunderbird/extensions/...	proxy :: Add-ons for Thunderbird	Firefox	addons.thunderbird.net
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
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
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
2020-10-03 14:51:56 IDT	https://www.google.com/search?client=firefox-b-d&sq=ho...	how to spoof email address in thunderbird - 3 870171-Google	Firefox	www.google.com
2020-10-03 14:52:07 IDT	https://www.google.com/url?sa=t&rcct=j&q=besrc=s&sour...	email - How can I fake a "from" address in Thunderbird? - 5...	Firefox	superuser.com
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? - 5...	Firefox	superuser.com
2020-10-05 16:27:46 IDT	https://www.google.com/url?sa=t&rcct=j&q=besrc=s&sour...	email - How can I fake a "from" address in Thunderbird? - 5...	Firefox	superuser.com
2020-10-05 16:27:50 IDT	https://www.google.com/url?sa=t&rcct=j&q=besrc=s&sour...	email - How can I fake a "from" address in Thunderbird? - 5...	Firefox	superuser.com
2020-10-03 14:54:09 IDT	https://www.google.com/search?client=firefox-b-d&sq=ho...		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)

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing Default 54 Results

Source File	S	C	E-Mail From	E-Mail To	Subject	Date Received	Message ID	Path	Thread ID
Drafts-1			ezm0n3y@jalme.vox	carol@malme.com	\$\$\$GoodchoicE\$\$\$	2020-10-05 16:54:49 IDT	Not available	/malme-1.com/Drafts-1	b7486327-9372-4d3d-9965-2ace9ed1c
INBOX			carol@malme.com	anon@malme.com		2020-10-03 17:06:06 IDT	Not available	/malme-1.com/INBOX	854a9ca1-9631-4b95-ac03-8477467c8
Drafts-1			ezm0n3y@jalme.vox	carol@malme.com	\$\$\$GoodchoicE\$\$\$	2020-10-05 16:54:49 IDT	Not available	/malme-1.com/Drafts-1	b7486327-9372-4d3d-9965-2ace9ed1c
INBOX			carol@malme.com	anon@malme.com		2020-10-05 16:48:03 IDT	Not available	/malme-1.com/INBOX	80bb7156-4099-4120-b027-54e3db88f
Sent-1			kingpin@cartel.com	carol@malme.com	Fine choice	2020-10-03 16:34:41 IDT	Not available	/malme-1.com/Sent-1	b977ba64-7ba5-41f1-ba29-f68788767
Sent-1			kingpin@cartel.com	carol@malme.com	Fine choice	2020-10-03 16:34:41 IDT	Not available	/malme-1.com/Sent-1	b977ba64-7ba5-41f1-ba29-f68788767
Sent-1			anon@malme.com	carol@malme.com	????????	2020-10-05 15:46:01 IDT	Not available	/malme-1.com/Sent-1	f66886ff-2756-48a7-aa7b-ab1d64a-9f7

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Result: 4 of 11

E-Mail Messages

From: ezm0n3y@jalme.vox;
To: carol@malme.com;
CC:
Subject: \$\$\$GoodchoicE\$\$\$

2020-10-05 16:54:49 IDT

Headers Text HTML RTF Attachments (0) Accounts

-----HEADERS-----

X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
FCC: imap:/anon%40malme.com@malme.com/Sent
X-Identity-Key: id2
X-Account-Key: account3
To: carol<carol@malme.com>
From: ezm0n3y@jalme.vox
Subject: \$\$\$GoodchoicE\$\$\$
Message-ID: <a22ba543-eadd-b6a4-e3d4-f03cf6-46a2@malme.com>
Date: Mon, 5 Oct 2020 16:54:49 +0300
X-Mozilla-Draft-Info: internal/draft; ucard=0; receipt=0; DSN=0; uencode=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.

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing
Installed Programs

Table Thumbnail

Page: 1 of 1 Pages: Go to Page:

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

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Result: 23 of 60 Result

Type	Value
Program Name	Mozilla Thunderbird 78.3.1 (x86 en-US) v.78.3.1
Date/Time	2020-10-01 14:45:49 IDT
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

The screenshot displays a forensic analysis interface. On the left, a tree view shows the file system structure, including 'Data Sources', 'david.raw', and various file types like 'ScaphFiles', 'PerfLogs', 'Program Files', 'Recovery', 'System Volume Information', 'Users', and 'Windows'. The main pane shows a listing of files in the 'Instructions' folder. The table below lists the files with their metadata.

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[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...

The bottom pane shows the text content of the selected file, 'TASK02'. The text is as follows:

```
#####
TASK2
#####

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

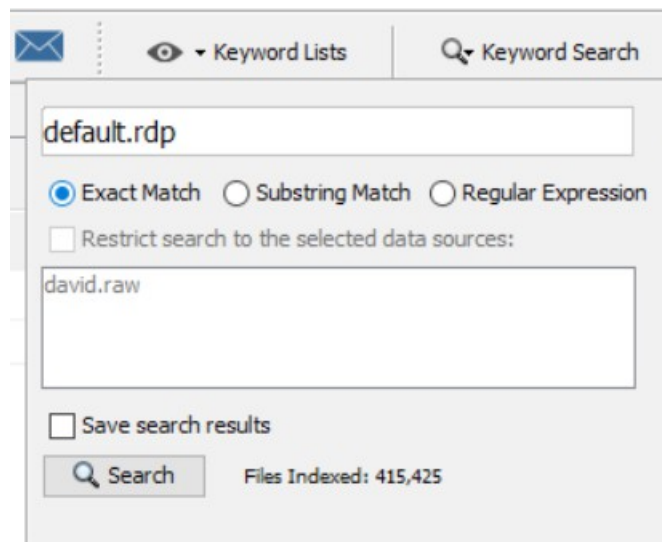
TIME LIMIT: 2 hours

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> Default 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.



The screenshot shows a software interface with a top bar containing an envelope icon, an eye icon with a dropdown arrow, and a magnifying glass icon. Below the top bar, there are two tabs: "Keyword Lists" (selected) and "Keyword Search". The "Keyword Search" tab is active, displaying a search input field with the text "default.rdp". Below the input field, there are three radio buttons: "Exact Match" (selected), "Substring Match", and "Regular Expression". Below these radio buttons, there is a checkbox labeled "Restrict search to the selected data sources:" which is unchecked. Below the checkbox, there is a text input field containing the text "david.raw". Below the text input field, there is a checkbox labeled "Save search results" which is unchecked. At the bottom left, there is a "Search" button with a magnifying glass icon. At the bottom right, there is a status label "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.

The screenshot displays a forensic analysis application with a search results table and an indexed text view.

Search Results Table:

Name	Keyword Preview	Location	Modified Time
Unaloc_423706_23341916160_25121570816	bing[1].xml<<Default.rdp><Default.rdp>,<Terminal Server	/img_david.raw/vol_vol3/(\$Unaloc/Unaloc_423706_23341...	0000-00-00 00:00:00
mstsc.exe	rDIGetClassObject<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
Unaloc_423706_21849481216_23340806144	bing[1].xml<<Default.rdp><Default.rdp>,<Terminal Server	/img_david.raw/vol_vol3/(\$Unaloc/Unaloc_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
Unaloc_423706_570125748_20015163136	C:\Users\david\Documents\Default.rdp%7F%4C\Windows	/img_david.raw/vol_vol3/(\$Unaloc/Unaloc_423706_57012...	0000-00-00 00:00:00

Indexed Text View:

Page: 1 of 1 Page | Matches on page: 1 of 1 Match | 100% | Reset | Text Source: Search Results

```
keyboardhook:i:1
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
#enablemenuimaging:i:1
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**.

The screenshot displays a forensic analysis tool interface. The left sidebar shows a tree view of the file system, including 'Templates (2)', 'Videos (3)', 'Default (28)', 'Default User (2)', 'Public (11)', 'Windows (108)', and 'voH4 (unallocated: 167768064-167772031)'. The main window shows a 'Keyword search' results table for the keyword 'bob@mailme.com'. The table has columns for 'Name', 'Keyword Preview', 'Location', and 'Modified Time'. The selected row is 'E-Mail Messages Artifact', which has a preview showing an email header and body text. The body text includes a reminder about a flight on 20-10-06, with a return time of two weeks. The email header shows 'From: bob@mailme.com' and 'Subject: reminder'. The email body text includes 'Just in case', 'On 10/5/2020 4:34 PM, david wrote:', 'of course bob,', 'enjoy your trip', 'On 05/10/2020 16:32, bob wrote:', 'Just a reminder that i'm flying home tomorrow.', and 'be back in two weeks.'.

Name	Keyword Preview	Location	Modified Time
DAV_Merge.pcap	Hx4@<26 3 login "bob@mailme.com" "bob" "Hx5@3 login	/img_david.raw/vol3/Users/david/Desktop/David_pcap...	2020-10-05 18:15:15 IDT
E-Mail Messages Artifact	0000000Return-Path: <bob@mailme.com>Received: from...	/img_david.raw/vol3/Users/david/AppData/Roaming/T...	2020-10-05 18:00:15 IDT
dav_pt1.pcap	Hx4@<26 3 login "bob@mailme.com" "bob" "Hx5@3 login	/img_david.raw/vol3/Users/david/Desktop/David_pcap...	2020-10-05 17:40:17 IDT
wireshark_Ethernet_20201005160213_a03888.pcap	Hx4@<26 3 login "bob@mailme.com" "bob" "Hx5@3 login	/img_david.raw/vol3/Users/david/AppData/Local/Temp...	2020-10-05 17:38:50 IDT
E-Mail Messages Artifact	HEADERS--E-Mail From : <bob@mailme.com>;E-Mail To : ds...	/img_david.raw/vol3/Users/david/AppData/Roaming/T...	2020-10-05 18:00:15 IDT
Sent.msf-slack	6691) (115=bob <bob@mailme.com>)(116=reminder)(...	/img_david.raw/vol3/Users/david/AppData/Roaming/T...	2020-10-03 16:51:40 IDT
cpv_Meridian	Hx4@<26 3 login "bob@mailme.com" "bob" "Hx5@3 login	/img_david.raw/vol3/Users/david/AppData/Roaming/T...	2020-10-05 18:00:15 IDT

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

---END HEADERS---

E-Mail From : bob@mailme.com

E-Mail To : david@mailme.com

Subject : e: reminder

Date Received : 2020-10-05 17:29:25 IDT

Date Sent : 2020-10-05 17:29:25 IDT

Message ID : ... details

Just in case

On 10/5/2020 4:34 PM, david wrote:

> of course bob,

>

> enjoy your trip

On 05/10/2020 16:32, bob wrote:

> Just a reminder that i'm flying home tomorrow.

>

> be back in two weeks.

Message ID : ...

Path : /mailme.com/INBOX

Thread ID : 00a466ac-f2c4-42a2-ab9d-4b90502db9fc