# **Data Acquisition on a Virtual Machine: Three Scenarios**

Saritha Narahari California State University, Sacramento 1550 IronPoint Road apt711 Folsom, ca-95630

## ABSTRACT

Virtual machine computing is becoming more and more prevalent. Companies are providing virtual desktops for their employees and using virtual machines to run server software. Additionally, the use of Infrastructure as a Service has placed virtual machines within the reach of even more people. Virtual machines can pose a challenge because of their transient nature. Also, the nature of how virtual machines store data could prove problematic.

#### **Keywords**

Data Acquisition, Virtual Machine

## 1. INTRODUCTION

The Virtual Machine is the concept where a software application is behaved as a host machine. Virtual machine application runs on the host (Actual) machine Operating System as the Guest which runs inside the Physical computer. A Hypervisor is used to create the virtual machine and manage by allocating the machine requirements on a host. There are two types of Hypervisors. In Type-1 Hypervisor virtualization has direct access to the resources. In this type the performance is like the actual performance of the system. Whereas in the Type-02 Hypervisor, the Virtualization incurs overhead as the host's Operating System takes the requests from VM and allocates the resources.

"Performing Forensic investigation on the Virtual Machine is the challenge because the nature of the systems that's is virtualized and isolated from the host must be analyzed prior before performing investigation."

Performing Forensic Investigation on a host machine involutes four steps to recognize, acquire and analyze a virtual machine

- Forensic Image Creation
- Sensitive Information Identification and recovery
- Virtual machine analysis
- Documentation

Forensic Image Creation phase involves creation of the image which has the record of all the activities performed inside the virtual machine." While creating the image we need to ensure that the data is complete, and the data is not modified. After acquiring the Image investigation is done on it as investigation on the original disk data is not recommended which may result in data modifications, therefore it is important to create the disk image of the original data."

"Sensitive information Identification and recovery phase, Operating Systems create the keep logs of the activities I.e., debugging, management, record purposes". The Investigator should understand and be aware of the host operating system before performing analysis which helps in identifying the sensitive information and recover the traces of the VM and the illegal activities. The File associations in the registry reveal the information about the applications installed and used in the host machine. Even if the hypervisor is uninstalled, the .vbox, .vmdk, .vmx etc files in the host machine confirm the usage of virtual machine.

Investigators face some challenges in the recovery of the data deleted and files corrupted. Sometime deleted files can be recovered from the temporary locations." Deleted snapshots, VM configuration files etc can be recovered by using some application such as UNDELETE, Handy Recovery etc., which can be analyzed once they are recovered investigation can be continued". They are some limitations in the file recovery like file encryption, Physical Destruction, Degaussing, Gutmann Method which cause file corruption.

Virtual Machine Analysis Phase, Virtual Machine analysis consume more time compared to the normal machine analysis. In order to analyze the VM, we need to get access to it." The virtual machine is analyzed by mounting it as the hard drive in another machine or by using it with a hypervisor to get access into the virtual environment". Once the disk image is extracted from the original disk, it is analyzed with the tools when the VM access is granted. Most of the physical machine forensic tools support the virtual machine with the Virtual machine operating system compatible software.

"In Documentation phase, every record of the investigation is documented, and all the activities related to analysis, evidence transfer, validation, storage must be documented so that everything will be available for the further investigation. It is important to have report forms in each phase for the documentation."

# 2. PROJECT GOAL

The goal of the project was to analyze the use of a traditional forensics data acquisition to acquire data in a virtual machine environment. Here the main sought is to compare the integrity of data gathered to see if it would reflect the true actions of a scenario enacted in each environment. The choosen three data acquisition scenarios to enact are

- 1. Perform data acquisition from within a local Virtual Machine environment. This scenario is meant to simulate an instance where the company has complete control of the virtual environment and wished to acquire data from the virtual machine given to the suspect.
- 2. Perform data acquisition from a disk image of a local virtual machine. This scenario is meant to simulate an instance where the company controls the storage device upon which the virtual image disk is stored but may not have complete access to get inside of the VM while it is running.
- 3. Perform data acquisition from within a cloud Virtual Machine. This scenario is meant to simulate an instance where the company or individual is using

Infrastructure as Service from a cloud provider. Access to the actual disk image or storage device is not possible, however access to the virtual environment itself is.

#### 3. IMPLEMENTATION

To illustrate the differences between the results the three different scenarios we performed same set of activities in the cloud and virtual environments and Autopsy is the forensic tool used for investigating the differences.

Here these environments are seeded with data that could later attempt to acquire. 1. Did a web search on Spiderman and downloaded few similar images and deleted one image. 2. created a document with the text written 'Trump Trump Trump' so that a keyword search can be performed using the keyword 'Trump'. Using Autopsy, the aim is to find out the traces of these files and other interested data that is present.

In the First Scenario, the Oracle VM Virtual Box, which is freely available on internet is selected and installed for investigation. We also download a Windows virtual machine from Microsoft Developer to act as the OS within our Virtual box environment. Within the Virtual box virtual environment, Virtual disk image must be seeded with data so that the record of activities is stored. In this environment, the activities are listed and created the text document as the first step. In the second step, Autopsy forensic tool is installed, and investigation is performed on the Virtual machine.

For the Second Scenario, we extracted disk image of the virtual machine which has the record of the activities performed in the first scenario's first step. The disk image was extracted immediately after performing the "seeding" steps, before Autopsy was installed and run on the virtual machine. The extracted disk image is in the .vmdk file format. Autopsy doesn't recognize .vmdk files so a file conversion was done. For the file conversion qemu-img software is used, through which .vmdk disk image is converted to .raw file. Thereby Autopsy can perform analysis on the .raw file.



Fig 1: vmdk file converted to Raw file using qemu-img software

Raw file is added as the data source selected as disk image in autopsy.

In the Third Scenario, using the Microsoft Azure Cloud Services, a premium account is created and MS Windows Virtual Machine is setup using their standard process. The standard MS Azure virtual machine for a premium comes with 127GiB storage on SSD. The disk is not encrypted in this type of account. Additionally, MS Azure does not guarantee to persist local SSD data. If persistent data is desired, one must sign up for a different type of MS Azure File Storage account in addition to the virtual machine account. The environment was "seeded" following the steps outlined previously. Autopsy was then installed on the virtual machine. It took two days between seeding the data and running Autopsy to perform the acquisition.

# 4. RESULT

During the data acquisition, we examined each environment for the following data:

- 1. Keyword search for "Trump".
- 2. Searches for Spiderman related data/images and traces of our Spiderman browsing.
- 3. Records of email address.
- 4. Records of bookmarks
- 5. Record of the deleted files, including the Spiderman image that was deleted.

Comparison between the scenario 1 and scenario 2 results:

- 1. The number of Deleted files in both scenarios' is divergent. As analysis is performed on the same the virtual disk image there is a time lapse between the data acquisition in virtual environment.
- 2. There are some files with the modified date and time listed as 0000-00-00 00:00, as we used a freely available virtual box and the disk image from online there are the chances we need to expect from other usages
- 3. The Recent Accessed files are similar in the both cases.
- 4. There are some email addresses listed which are cached and the Bing.url as saved bookmark in the both scenarios.
- 5. While browsing for spider man images, there are few .html files stored in the cache memory, some of them with metadata and some with unknown metadata. With the spider man keyword search we were able to retrieve the same set of files in both cases.
- 6. With Trump keyword search we retrieved files which common in the both scenarios.

Case View Teols Window Help									- • ×
🕂 Add Cata Source 📠 Images/Mdeos	Timeline 🔓 Generate Report	😸 Close Cose						🔔 🐵 + Keyword Lists	Qr Keyword Search
Processory Tree       Image: State of the s	Sum Rejected Results	Leting Data Rearrow Table Shurbhal Nane PhysicaDineo	Турс 3ладо	522 (Bytos) 42399072500	Sector Size (Bytes) 512	MDSHazh	Trease Anerics Los Anoeks	a Device 19 Justification of the official officia	( ) * C
		Data Content	etadata Resulta	Nessage Indexed	Text   Media   Other Oc	currences			
			<b>i i</b>					æ ^ 1	

## 4.1 Scenario 1 Results

Fig 2: Disk image added as the data source in the virtual environment:

# finalproject - Autopsy 4.6.0 Case View Tools Window Help				- п	×
🐈 Add Data Source 📠 Images/Videos 🧮 Timeline 🔟 Genera	ite Report  Gose Gase	<u> </u>	<ul> <li>Keyward lids</li> </ul>	Og Keyward Search	
Directory Tree	- Using			( )	
€ → Show Reject	tod Results Table Thurlevel			2 1	hesu
■         ■ 20 Acces           ■         ■           ■ <td< td=""><td>1000 <u>γ</u> = 4 Coto+6 <u>γ</u> = 4 Coto+6</td><td></td><td></td><td></td><td></td></td<>	1000 <u>γ</u> = 4 Coto+6 <u>γ</u> = 4 Coto+6				
E Mai Nessages Katinesting Rens Accords Accords Reports	Rest Controll           Merri: Dengo: [1:k Headers   Kesule   Message   Undexed   ent   Header   Other Occurrences				
So Type here to search	0 0 0 0 0 0 0		el ^ B	10:00 PM 5/6/2018	ل.

Fig 3: Deleted Files retrieved from virtual machine analysis

ase View Tools Window Help						- с ×
🕂 Add Data Source 📠 Images/lideos 🗮 Timeline 🚡 Generate Report	😸 Cose Case		<u> </u>	🐵 - Keyword Li	155	Qr Keyword Search
Directory Tree -	Tisting					
Show Rejected Results	Recent Documents Table Trumbnai					7 Results
🗧 🔜 Data Sources	Source File	Path	Cate/Time	Data Source	Tags	
E- 66 Views	I_LGFTMUC835ni UPF7Ux.0.jpg.ink	C (Users(FELser)Pictures)1_LGFTMLCE(EntPF7Use0.jpg	2018 01 24 15:15:28 FDT	PhysicalD-9408		
* S. File Types	i eula bruink	C Whice wsj@ustem02/eula.bit	2010-04-24 15:15:55 FDT	PhysicalD tive0		
File System (10354)	MyTestFile.tat.ink	< 10sers()Ece*(2000 ments(MsTest File.tx);	2018-34-34 15:15:58 FDT	PrysicalDrive0		
L - χ All (10354)	PeterParker.png.ink	C (Users(IELser)Pictures(PeterParker.and	2018 24 24 15:11:14 FDT	Ny sical04+c0		
MB hie bae	Pictures.ink	C (Users)(IILse (Pictures	2010-04-24 15:09:02 FDT	PhysicalD tive0		
計画 Results	System32.14	C (Minuses)System82	2018-04-24 15:15:55 FDT	PrysicalDrive0		
EXPERIENCE (1)	Web of Spider-Nan Vol 1 129-Lpng.ink	C (UsersQELser)Pictures(Web of Spider-Pion Vol 1, 129-1	2018-04-24 15:00:02 FDT	PhysicalD (1+c)		
di - S. Stripti Uteral Nervice Scaroft (154)     di - S. Stripti Program Società (154)     di - S. Final Aktionemen (1558)     S. Final Aktionemen (1558)     S. Final Indentitio     S. Telle Interesting Stemes     S. Telle Interesting Stemes     S. Telle Interesting Stemes     S. Telle Interesting Stemes	Eats Content           HEX         Strings         Re-Metacular         Reserve (1)	nkoolTeg: Maia [Olar Gammeran]				-
Taps						

Fig 4: Recent Documents accessed in the virtual environment

Case View Tools Window Help							:			
🕂 Add Data Source 📠 Images/videos 🗮 In	neline 🔝 Generate Report					4	· · Key	word Lists	Qr Keywa	
Eirectory Tree		Listing Web Bookmarks Table Thumbrid								-< ) ♥ ( 1 Resul
- Dele Saures - Wron	Source File	URL	Title	Date Created	Program Name	Demain	Data Source	Tags		
Image: Section 2016         Fragment           Image: Section 2016         Fraddette		<b>₽</b> tinguni	http://ponecodi.com/WH/polosic=2034	tirg.u-1	a1/40-a 0-00-5-60	preux the re	go mer ossifution	Phyciel Druse.		
E-Mail Messages     Kinteresting Items		Data Content								-
Accounts		Hex Strings   Eb	Molekieler (Results: [Henneyer   ItaleureTreat : Birder							
Type here to search	4 (D)	2 .	1					<b>-</b>	10.02	PM



₩ finalproject - Autopsy 4.6.0 Case View Tools Window Help						– a ×
🛨 Act Data Source 📠 Inagesylldros 🧮 Tin	olno 🗽 Generale Report	😸 Core Case		<u> </u>	• Keyword Lists	Qr Keyword Search
Directory Tree	Show Rejected Results	Listing Enal Addresses Table Thumphal				4 → ♥ □ 1 Results
Beneficial Servers     Beneficial Serve	9%+, \\]-위기((1)(@(b+24-30-3	In Name (5,00) and 2014 - 13-0.5-1 (0) and 2014 - 13-0.5-1 Data Context The Sings (1-2) Weshing (4).				
<	>	2 🖬 🏦 🖨				토 10:03 PM 5/3/2018 나

Fig 6: Email addresses stored

finalpreject - Autopsy 4.6.0 Case View Tools Window Help						-	o ×
🕂 Add Data Source 🙇 Images/Videos 🗮 Timeline 🚡	Generate Report	😸 Close Case			<u> </u>	Keyword Licts Q-1	leyword Search
Directory Tree		Listing Keyword search Reyword search Table Thumbnal	1-tunp ×		trunp	Subdia Math. C Broak	Q Search N
■         Const           ■         Stores           ■         Stores <td>]+)*();/)¤([==1-23-9</td> <td>Name Officer/u/Ko/S3.exe My/Test/8.bc</td> <td>kootio 3 rg3 rg4 d3 in third _ n3 thir 3 na Prystal: d-chird vealer</td> <td>оры Бюлій Сольфрадь</td> <td>Charge mile 2018-0+2+16:11:00 FD</td> <td>2018-04-04 16:09-41 PC</td> <td>0.60 PS-P0-8005</td>	]+)*();/)¤([==1-23-9	Name Officer/u/Ko/S3.exe My/Test/8.bc	kootio 3 rg3 rg4 d3 in third _ n3 thir 3 na Prystal: d-chird vealer	оры Бюлій Сольфрадь	Charge mile 2018-0+2+16:11:00 FD	2018-04-04 16:09-41 PC	0.60 PS-P0-8005
Construction of vessels broad vessels	ų <b>D</b>		Renalis   Mensage   Stalenet Text   M	ede   Oter Ormanemer		서· < 다 및	10:04 PM 🖵

Fig 7: Trump keyword search returning the files with trump in it

Case View Tools Window Help												- 0	×
🕂 Add Data Source 📠 Inages/Vdeos 🗮	Timeline 📗 Generate Report	🍵 Otee Case							<u> </u>	🐵 - Keywar	dlies C	Keyward Search	<u>.</u>
Directory Tree		Tiding Keyna Keyword search Table Thurbnal	nd seech 1 - Inc	mp × 1	Gegeneril severi	h 2 - spitler-mar	×						₩ ( Resul
Deta Sources     Wews     Deta Sources     Wews     Deta Sources     Deta Sources	Fage: 1 of 1	Pages:	€ ⇒	Go to Page:	ir.	1ages: 1-12	Medium Thumbnais	Sort Sort	Sorted by:				
E V Deleted Files													
		WebCacheV01.da	t marvel-spider-r	n 300px4	Baradk_Ob	spider-man-civi	1-2-spder-man	NTUSER.CAT m	nvel-homecom S	pider-Han-Hovi	marvel-spider-m	Avengers-Onfin	
Results     H     Ditracted Content													
- 🔛 EXI' Netadata (4)		marvel-spider-m	spder-man-fro	e									
			spider-man-fro	e									
Image: Section (A)           Image: Section Removed Detected (171)           Image: Section Removed Detected (171)           Image: Section Removed Remo					e Indexed ie	at Media U	Fer Occurrences						_
Head and the set of the set		Data Content			e   Lindexed I e	at   Media   Gd	Her Uccurrences						-
European Read Concerned (1)     European Read Concerned (1/2)     European Read Concerned (1/2)     European Read Concerned (1/2)     European Read Concerned (1/2)     European Read Concerned Search (1/2)		Data Content			e   Indexed Te	at, Meda Ud	her Usourrences						

Fig 8: Spiderman keyword search retries the files stored in the cache and the virtual storage



4.2 Scenario 2 Results

Fig 9: MSConvert.raw (the converted disk image) as the data source

🐈 Add Data Source 📠 Images/Videos 🗮 Ti	meine 📗 Generate Report 🏾 🛞 Close Case	🔔 💿 - Keyword Lists	Q- Keyword Search
Dels Sources     D	Lettro Dettor File Table Trutonal Type X Ric System (9257) X Al (H433)		( ) > 2 Results
· · · · · · · · · · · · · · · · · · ·		በ ላ በ	

Fig 10: Deleted number files analyzed from the disk image

						$\leftrightarrow \tau$
F ⇒ Show Rejected Results	Listing Recent Documents					7 Resul
Data Sources	Table Thumbnail					7 10200
© Views	Source File	Path	Date/Time	Data Source	Tags	
B- 🖞 File Types	1_LGFTIvUIC8J5mi-UPF7Uw.0.jpg.lnk	C:\Users\IEUser\Pictures\1_LGFTIvUK805mi-UPF7Uw.0.tpg	2018-04-24 16:15:28 PDT	MSConvert.raw		
y Deleted Fies     y Deleted Fies     y Deleted Fies     y, Deleted Fies     y, Deleted Fies     y, Deleted Fies     w, Deleted Fies     Deleted     Deleted Fies     Deleted     Deleted	eula.txt.ink	C:\Windows\System32\eula.bd	2018-04-24 16:15:55 PDT	MSConvert.raw		
	MyTestFile.txt.lnk	C:\Users\IEUser\Documents\MyTestFile.txt	2018-04-24 16:16:58 PDT	MSConvert.raw		
	PeterParker.png.ink	C:\Users\IEUser\Pictures\PeterParker.png	2018-04-24 16:11:44 PDT	MSConvert.raw		
	Pictures.Ink	C:\Users\IEUser\Pictures	2018-04-24 16:09:02 PDT	MSConvert.raw		
	System32.lnk	C:\Windows\System32	2018-04-24 16:15:55 PDT	MSConvert.raw		
	Web_of_Spider-Man_Vol_1_129-1.png.ink	C:\Users\IEUser\Pictures\Web_of_Spider-Man_Vol_1_129+	2018-04-24 16:09:02 PDT	MSConvert.raw		
NB Fire Size         Preside           ■ Extracted Context         Extracted Context           ■ Statement Context						
Percent Documents (7)     Web Boolmants (1)     Keyword His     Single Literal Keyword Search (1344)     Single Regular Expression Search (104     Sing	9 Tex Strops Pie Metadata Results Message In	deved Text [Media   Other Occurrences]				





Fig 12: Web Bookmarks saved on the virtual disk image

⊨ Add Data Source 📠 Images/Videos 🗮 1	imeline 📗 Generate Report 🍙 Close Case 🛕 💿 • Keyword Lists	Q Keyword Search
	Listing	() <b>+</b> 1
<ul> <li>Show Rejected Results</li> </ul>	Email Addresses	1 Result
Data Sources	Table Thumbnal	
Wiews	List Name Files with Hits	
File Types	(\{?)[a:zA-Z0-9%+_]-]+(\-[a:zA-Z0-9%+_]-]+)*(\}?)\Φ([a:zA-Z0 2738     )     )	
Deleted Files		
All (9433)		
B MB File Size		
E Results		
🖨 📑 Extracted Content		
📴 EXIF Metadata (6)		
Description Suspected (1)		
Extension Mismatch Detected (134)		
<ul> <li>Recent Documents (7)</li> <li>Web Bookmarks (1)</li> </ul>		
Keyword Hits		
Single Literal Keyword Search (3344)		
- Single Regular Expression Search (104		
💼 🖳 Email Addresses (2738)		
🌪 Hashset Hits		
- 😤 E-Mail Messages		
Interesting Items     Accounts		
Tags	Hex Strings File Metadata Results Message Indexed Text Media Other Occurrences	
Reports	tikk sunga mermetauata Resulta mesata mesata mesata mesata terte mesata una dene Occurrences	
>		
,	1	

Fig 13: Email Addresses accessed over virtual disk image

Image         Location         Proces         Product Time         Dot                w Detected (SS)               More this Lot               Wore this Lot               Sold (A-Linked PD T)	ange Time 18-04-24 16:16:58 PDT 18-04-24 16:11:00 PDT 17-10-23 09:53:30 PDT	Access Time 2018-04-24 16: 2018-04-24 16:
Catals source         Marce         Location         Modeling Time         Other           Verse         Name         Location         Modeling Time         Other           MS Firster         Image Time         Image Time         Distance	18-04-24 16:16:58 PDT 18-04-24 16:11:00 PDT 17-10-23 09:53:30 PDT	Access Time 2018-04-24 16:
Version         Name         Location         V Hodified Time         Other	18-04-24 16:16:58 PDT 18-04-24 16:11:00 PDT 17-10-23 09:53:30 PDT	2018-04-24 16:
<ul></ul>	18-04-24 16:16:58 PDT 18-04-24 16:11:00 PDT 17-10-23 09:53:30 PDT	2018-04-24 16:
Image: Second Content         Image: Second Content and Image: S	17-10-23 09:53:30 PDT	2018-04-24 16:
with a (pess)               perf		
MB: First Size         Decksoft arge(CompCl, COEL ) big uni -lack         Incg. (Second Lack) and (July CompCl and (Ju		2017-10-23 09
Beautis         OfficeHulWin32.ese         Img_JFSConvet.ran/vol_wol2/Windowij/thues/logo/Padu2017-09-29 07:45:47 PDT         2011           B Strated Content         apps.inf         Img_JFSConvet.ran/vol_wol2/Windowij/thues/logo/Padu2017-09-29 06:41189 PDT         2011           D Stratedate (0)         apps.inf         Img_JFSConvet.ran/vol_wol2/Windowij/thues/logo/Padu2017-09-29 06:41189 PDT         2011           D Stratedate (0)         apps.inf         Img_JFSConvet.ran/vol_wol2/Windowij/WinSclemded (m2017-09-29 06:41189 PDT         2011           D Stratedate (0)         Dop.inf         Img_JFSConvet.ran/vol_wol2/Windowij/WinSclemded (m2017-09-29 06:41189 PDT         2011           D Stratedate (0)         Dop.inf         Img_JFSConvet.ran/vol_wol2/Windowij/WinSclemded (m2017-09-29 06:41189 PDT         2011	18-04-24 16:11:28 PDT	2018-04-24 16
DDF Pretodes (i)         asses if         l/mg_/5Gconvert.am/vd_vd2/l/Vrdom/INF2/spc.if         D11-09-29 06411.59 PDT         D11-09-29 06411.59 P	18-04-24 16:14:56 PDT	2017-09-29 07:
Curr Pressed (p)     Dur Pressed (p)	17-10-23 09:54:59 PDT	2017-09-29 06:
Extension Mismatch Detected (134) PrintConfig.dl //img_MSConvert.raw/vol_yvol2/Windows/Win5x5/x86_prm 2017-09-29 06:41:08 PDT 2011	17-10-23 09:54:59 PDT	2017-09-29 06
Recent Documents (7)     PrintConfig.dl     Intro. MSConvert. raw/vol. vol2/Windows/System32/DriverS 2017-09-29 D6:41:08 PDT 2011	17-10-23 09:00:18 PDT	2017-09-29 06
	17-10-23 09:00:18 PDT	2017-09-29 06:
Web Bookmarks (1)     PrintConfig.dl     Img_MSConvert.ran/vol_vol2/Windows/System32/spool/d 2017-09-29 06:41:08 PDT     201	17-10-23 09:00:13 PDT	2017-09-29 06
	17-10-23 09:55:37 PDT	2017-09-29 06:
	17-10-23 09:00:14 PDT	2017-10-23 09
	17-10-23 09:55:37 PDT	2017-09-29 05
- ★ Hashaet His // Hearaace /	17-10-23 09:00:21 PDT	2017-09-29 06
	17-10-23 09:00:21 PDT	2017-09-29 06:
Accounts     Counts		>
Tegen     T		



Data         Description         Description <thdescription< th=""> <thde< th=""><th>Add Data Source 🜆 Images/Videos</th><th>Timeline 📗 Generate Report 🍙 Close Case</th><th></th><th>🛕 💿 • Keywor</th><th>d Lists Qr Keyword</th><th>Search</th></thde<></thdescription<>	Add Data Source 🜆 Images/Videos	Timeline 📗 Generate Report 🍙 Close Case		🛕 💿 • Keywor	d Lists Qr Keyword	Search
Desk Sovces         Table         Desk Model         Desk Model<	→ Show Rejected		earch 2 - trump X Keyword search 3 - spider-man X	spider-man	Q	Search
Verse         Location         Verse         Verse           Wins         Industrial factor         Industrial factor         Verse         Verse           Wins         Industrial factor         Industrial factor         Industrial factor         Verse	Data Sources			Evact Match     Substi	ring Match	ssinn
Proceeding File		Name	Location	· ·		ALLEDON
Picketter fres         RundL132.DEE #SD-VEE.gr <sup>4</sup> dak         //m_2/H5Convert.am/nd_vd2/NM:dmcRPH*fetzh@ILALL         2016-04-24 161556 F0T         2016-04-24 161550 F0T         2016		eula.txt.ink-slack	/img_MSConvert.raw/vol_vol2/Users/IEUser/AppData/Roa	2018-04-24 16:15:55 PDT	2018-04-24 16:15:55 PDT	2018-0
A (Picts)     A (Picts)	File System (9257)	RUNDLL32.EXE-#52D40E6.pf-slack			2018-04-24 16:15:54 PDT	2017-1
Reads         (m)_0000mst (m)_00000mst (m)_0000mst (m)_0000mst (m)_0000mst (m)_000						2017-1
Read/s         Image: Start Signal Sta	MB File Size	V0100026.log	/img_MSConvert_raw/vol_vol2/Users/IEUser/AppData/Loca.	2018-04-24 16:15:05 PDT	2018-04-24 16:15:05 PDT	2018-0
Constraint Content     Constraint Constraint Content     Constraint Content     Constraint Constraint Constraint Content     Constraint Co					2018-04-24 16:15:02 PDT	2018-0
Comparison Superchard (s)     C					2018-04-24 16:15:02 PDT	2018-0
Extension Netwick1 Detected (14)     Extens			ance-c4f244 /img_MSConvert.raw/vol_vol2/Users/IEUser/AppData/Loca.	2018-04-24 16:14:59 PDT	2018-04-24 16:14:59 PDT	2018-0
% Spring of this factores (728)               mage-root lost               magee-root lost               magee-root lost               magee-root lost             magee-root lost             magee:root lost             m					2018-04-24 16:14:59 PDT	2018-0
Segmed htt         Imposed htt		TX82FRXKJ.txt	/img_MSConvert.raw/vol_vol2/Users/IEUser/AppData/Loca	. 2018-04-24 16:14:52 PDT	2018-04-24 16:14:52 PDT	2018-0
0		search[1].htm	/img_M5Convert.raw/vol_vol2/Users/IEUser/AppData/Loca	. 2018-04-24 16:14:38 PDT	2018-04-24 16:14:38 PDT	2018-0
Image: Socie Engine Enginesion Search (10)         Image: Socie Engine EngineEngine EngineEngine Engine Engine Engine Engine Engine Engine E		(2029) [8F139D03-7678-4977-8885-CCC757E1E814}.dat	/img_MSConvert_raw/vol_vol2/Users/IEUser/AppData/Loca	. 2018-04-24 16:14:08 PDT	2018-04-24 16:14:08 PDT	2018-0
Homesentes     H			/img_MSConvert.raw/vol_vol2/Users/IEUser/AppData/Loca	. 2018-04-24 16:13:38 PDT	2018-04-24 16:13:38 PDT	2018-0
Constant Results     Constant Results     Results	🕢 🔍 Email Addresses (2738)	ajax-actions[1].json	/img_MSConvert.raw/vol_vol2/Users/IEUser/AppData/Loca	. 2018-04-24 16:13:30 PDT	2018-04-24 16:13:30 PDT	2018-0
Interesting Tees     Tops     Tops		V0100021.log	/img_MSConvert.raw/vol_vol2/Users/IEUser/AppData/Loca	. 2018-04-24 16:13:27 PDT	2018-04-24 16:13:27 PDT	2018-0
Tags Hex Strings File Metadata Results Message Indexed Text Media Other Occurrences			/img_M5Convert.raw/vol_vol2/Users/IEUser/AppData/Loca.	2018-04-24 16:13:22 PDT	2018-04-24 16:13:22 PDT	2018-0
	Tags Reports	Hex Strings   File Metadata   Results   Message   Indexe	d Text   Media   Other Occurrences			

Fig 15: Spiderman Keyword search which retries all the files with the Spiderman along with images

Add Data Source 📠 Images/Videos 🗮 Ti	meline 🔚 Generate Report	😸 Close Case			<u> </u>	Keyword Lists	Qr Keyword Search
E → Show Rejected Results		1 - trump X Keyword sear	rch 2 - trump X Keyword s	earch 3 - spider-man 🛛 🗙			
and a set of the set o	Keyword search						140 Res
Data Sources Views Generation File Types X Deleted Files	Table Thumbnail Page: 1 of 1	Pages: 🔄 🎐 Go to Page	: Images: 1-17	Medium Thum	bnails 🗸 🛛 Sort	Sorted by: 1. Modified Time 🖲	
				-			
Encryption Suspected (1) Extension Mismatch Detected (134) Recent Documents (7)	WebCacheV01.dat	{8F139D03-7678	marvel-homecomi	spider-man-civi	spider-man-fron	{A918A44F-83FE	
Web Bookmank (1)     Web Bookmank (1)     Keyword Hits     Single Literal Keyword Search (3528)     Single Regular Expression Search (104)							
- 😤 E-Mail Messages - 🔆 Interesting Items	1-2-soider-man	(600AC235-FCAE	marvel-spider-m	marvel-soider-m	(76F50BAF-75E5	Avencers-Infini	
Leff Accounts © Tage ≩ Reports >	Hex Strings File Metadata	Results Message Indexed 1	Text Media Other Occurrence	55			

Fig 16: Spiderman Images

	meline 📗 Generate Report 🍙 Close Case		🔔 💿 • Ке	yword Lists	Keyword Search
Show Rejected Results	Listing				$\cdots \to \mathbf{v}$
Data Sources	All Table Thumbnail				9433 Res.
Views	Name	Location	Modified Time	Change Time	Access Time
🖒 File Types	x ja-JP	/img_MSConvert.raw/vol_vol2/Boot/ja-JP	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00
By Extension     By MIME Type	x ja	/img_MSConvert.raw/vol_vol2/Program Files/Microsoft Silv	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:0
Deleted Files	v cygwin1.dl	/img_MSConvert.raw/vol_vol2/Program Files/OpenSSH/bin/		0000-00-00 00:00:00	0000-00-00 00:0
File System (9257)	y minitar	/img_MSConvert.raw/vol_vol2/Program Files/Puppet Labs/	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:0
All (9433)	v ri.rb	/img_MSConvert.raw/vol_vol2/Program Files/Puppet Labs/		0000-00-00 00:00:00	0000-00-00 00:0
MB File Size MB 50 - 200M8 (28)	y DynamicLibrary.c	/img_MSConvert.raw/vol_vol2/Program Files/Puppet Labs/	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:0
	x nested_struct2.c	/img_MSConvert.raw/vol_vol2/Program Files/Puppet Labs/		0000-00-00 00:00:00	0000-00-00 00:0
MB 1G8+(3)	ssl_uc3_dphers.rb	/img_MSConvert.raw/vol_vol2/Program Files/Puppet Labs/	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:0
Results	¥ 164.png	/img_MSConvert.raw/vol_vol2/Program Files/WindowsApps.		00:00-00-00 00:00:00	0000-00-00 00:0
Extracted Content	¥ 185.png	/img_MSConvert.raw/vol_vol2/Program Files/WindowsApps.	. 0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:0
EXIF Metadata (6)	WindowsCameraAppList.contrast-black_targetsize-40.png	/img_MSConvert.raw/vol_vol2/Program Files/WindowsApps	. 0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:0
Extension Mismatch Detected (134)	WindowsCameraAppList.contrast-white targetsize-256.png	/img_MSConvert.raw/vol_vol2/Program Files/WindowsApps		0000-00-00 00:00:00	0000-00-00 00:0
Recent Documents (7)	WindowsCameraLargeTile.scale-100.png	/img_MSConvert.raw/vol_vol2/Program Files/WindowsApps.		0000-00-00 00:00:00	0000-00-00 00:0
Web Bookmarks (1)	AppList.targetsize-36.png	/img_MSConvert.raw/vol_vol2/Program Files/WindowsApps.	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:0
Keyword Hits	AppList.targetsize-30_contrast-black.png	/img_MSConvert.raw/vol_vol2/Program Files/WindowsApps.	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:0
Grand Contraction Contrac	AppList.targetsize-64_altform-unplated_contrast-black.png	/img_MSConvert.raw/vol_vol2/Program Files/WindowsApps.	. 0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:0
Email Addresses (2738)	AppList.targetsize-30_contrast-white.png	/img_MSConvert.raw/vol_vol2/Program Files/WindowsApps.	. 0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:0
💺 Hashset Hits	AppList.targetsize-64_altform-unplated_contrast-white.png	/img_MSConvert.raw/vol_vol2/Program Files/WindowsApps.	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:0
E-Mail Messages	AppList.targetsize-96.png	/img_MSConvert.raw/vol_vol2/Program Files/WindowsApps.	00:00:00 00:00:00	00:00-00-00 00:00:00	0000-00-00 00:0
Interesting Items     Accounts	<				>
Tags	Hex Strings File Metadata Results Message Indexed Text I	Media Other Occurrences			

Fig 17: List of the Deleted files: (with 0000-00-00 00:00 modified time)



Fig 18: Images with Metadata

## 4.3 Scenario 3 Results

- 1. It is easy to find the file with the "Trump" keyword, using Autopsy's keyword search. The metadata did not include date/time information for the file.
- 2. There were several references found referring to .html files that were browsed during our Spiderman web browsing. These files were in the cache for the Microsoft web browser. We were able to locate the Spiderman images that we downloaded off the internet. These images did not have any date metadata associated with them. For dates/time metadata the value was 00-00-0000 00:00:00.
- 3. The emails acquired by Autopsy from this VM are interesting. There were 160+ email addresses listed. Since we did not conduct any email activity or store any email addresses during our "seeding" we were surprised to see so many emails. We had a few theories regarding how these emails came to reside in the VM, such that Autopsy would acquire them. 1. The email addresses were gathered from various files that were browsed during our web searching. 2. The email addresses reside(d) in files that came with the

Virtual Machine image that we installed from MS Azure.

- There were no bookmarks acquired other than the standard Bing bookmark included with MS browser software.
- 5. There were 0 deleted files recovered by Autopsy. In our "seeding" process we deleted one file. This file was not show, nor any other files as with the local VM scenarios. There are few theories about why there were zero deleted files and gathered various theories from our CSC 253 classmates during our presentation. 1. Because the file storage system is SSD, the gap between seeding the data and acquiring the data was too long (two days). A know fact regarding SSD acquisitions is that the data should be gathered as soon as possible because SSD wear leveling will not necessarily preserve deleted data. Additionally, because the SSD drive is a shared drive amongst several Azure VMs, wear leveling might be even more prevalent and allow for an even shorter period that data could be recovered. 2. Cloud services use multiple distributed hard disk drives. Given MS Azures own caveat about the lack of persistence for

standard VM data, there is no reason to assume that deleted files would be stored, or that were, in fact,

accessing the same physical disk that the file had been deleted from.

= Add Data Source 🜆 Images/Videos 🇧	Timeline 📗 Generate Report 🍙 Close	Case	👍 💿 🕶 Keyword Lists	Qr Keyword Search
⇒ Show Rejec	Listing			$\leftrightarrow \mathbf{v}$
	Email Addresses			1 Res.
Data Sources	<ul> <li>Table Thumbnail</li> </ul>			
<ul> <li>Views</li> <li>Results</li> </ul>	List Name	Files with Hits		
Extracted Content	S (){?)[a-zA-Z0-9%+ \-1+().[i	a-zA-Z0-9%+ \-]+)*(\}?)\@([a-zA-Z0 161		
EXISTED Content				
Extension Mismatch Detected (2)				
Recent Documents (5)				
Web Bookmarks (1)				
- Keyword Hits				
- Single Literal Keyword Search (21)				
- Single Regular Expression Search				
Email Addresses (161)				
	zA-20-9%			
🔍 JMGuilemette@gmail.com	(1)			
🔍 Jan.Bruusgaard@ssb.no (	(1)			
- 9@RcQ.TK (1)				
- 🔍 aaron@sendthisfile.com (:				
- 🔍 amichai2@amichais.net (1	Hex Strings File Metadata Be			
andi@splitbrain.org (1)				
- 🤐 andreas.barton@web.de				
- 🔍 apache@dave.dribin.org (				
	b.edu (1)			
<u>C</u> b.carmon.colvin@gmail.co	m (1)			
🔍 bayard@apache.org (4) 🔍 bdunbar@dunbarconsultin				
- S ben@walstrum.com (1)	ig.org (1)			
bird@noir.crocodie.org (1)				
- S bloritsch@apache.org (1)				
biolischigapache.org (1)				
- Ca@trustwave.com (1)				
Cale chi@chimaric da (1)	~			
	>			

Fig19: Email addresses - MS Azure

1 · · · · ·	🚡 Generate Report 🏾 🍘	Close Case			🔔 💿 • Ке	yword Lists Q	Keyword Searc	h
€ → Show Rejected Results	Listing Keyword sea	ch 1 - Trump X						
Data Sources	Keyword search Table Thumbnail						1	Resu
Views	Name	Location	Modified Time	Change Time	Access Time	Created Time	Size	Fla
Results	testCloud.rtf	/LogicaFileSet1/Users/csc253admin/Documents/testCloud.rt		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	368	Ak
CUP Medida (1)     CUP Medida (1)     Cup Medida (1)     Cup Medida (1)     Recent Documents (5)     Web Boolmark (1)     Single Requel Toproteion Search (2)     Cup Medida (1)     Single Requel Toproteion Search (1)     Cup Medida (1)	Matches on page: 1 c testCloud.rtf This is 1 machine Microsoft Ar Bad word. Bad stuff. ( 	a test file that we will try to look for data from ore. Criminal: Ecomp. Trump Trump Trump.	· >	00 a vietna		Text Source: Search R	es/ts	~

Fig 20: Trump Keyword - MS Azure

Add Data Source	Images/Videos 🧮 Timeline	Senerate Report 🛛 🙀 Close Case	<u>A</u>	Keyword Lists	Qr Keyword Search
6 ->	Show Rejected Results	Listing Keyword search 1 - Trump × Keyword sear	ch 2 - Spiderman 🛛 🗙		< ) ¥1
<u>an en</u>		Keyword search			19 Resu
Data Sources	et1 (1)	Table Thumbnal			
in Users (		Name edb00007.ttx	Location		
(i) 🔛 Al i			/LogicalFieSet1/Users/All Users/Microsoft/Search/Data/Applications/Windows/edb0000		
	253admin (33)	95C9889A-54C7-4043-8542-910F3FAA286D}.dat	/LogicalFileSet1/Users/csc2S3admin/AppData/Local/Packages/Microsoft.MicrosoftEdge_		ge/User/Dehauk/Recover
Def	ault (29) ault User (0)	0 1000 18.log	/LogicalFileSet1/Lisers/csc253admin/AppData/Local/Microsoft/Windows/WebCache/V01		
P Put		V0100019.log	(LogicalFReSet1,Users/csc2S3admin/AppData(Local/Microsoft/Windows/WebCache/VDI	1000 C 1007	
w Views		V010001A.log	[LogicalFleSet1]Users/csc253admin/AppData/Local/Microsoft/Windows/WebCache/VD1		
		edb.log	(LogicalFileSet1)/Users/csc2S3admin/AppData/Locial/Packages/Microsoft.MicrosoftEdge_		
		5f7b5f1e01b83767.automaticDestinations-ms	[LogicalFleSet1]Users/csc253admin/AppData/Roaming/Microsoft/Windows/Recent/Auto		
		IndexedD8.edb	/LogicalFReSet1/Users/csc253admin/csc253_acquisition/ModuleOutput/keywordsearch/		
- MB File Size			[LogicalFileSet1]Users/csc253adwn/AppData/Local/Packages/MicrosoftEdge_	joweryb3ddbbwe/AppData/User/t	serault/Indexed Depinde:
E Results		autopsy.db	/LogicalFReSet1/Users/csc253admin/csc253_acquisition/autopsy.db		
Tags		Spiderman-spider-man-3979149-1024-768[1].jpg	/LogicalFileSet1/Users/csc253admin/Desktop/Spiderman-spider-man-3979149-1024-768	3(1).ipg	
Reports					,
		Hex Strings File Metadata Results Message Indexed T	txt Media (Other Occurrences)		
		Matches on page: 1 of 4 Match	age: 1 of 4 Page 🍝 À	Text Source: Sea	rch Results 🗸 🗸
	Vision: celliadmingEls:///C/Uses/celliadmin/ 1959 1959 Tilo Tilo Editmine(100104;2010042) C/User/selliadmin/UpgDes/Local/Microsoft/Window collians, 20 C/User/selliadmin/UpgDes/Local/Microsoft/Window collians, 20 Contains, 20	Factores ( <mark>Backerson</mark> -spackerson-99,97,92-169)-1895-1999 er Mannay/Mannay, TEFMBlandJ2013444(E2)29447			

Fig 21: Cache of Spiderman activity - MS Azure

Add Data Source 🛔	🚺 Images/Videos 🗮 Timeline	📔 Generate Report 🍙 Close Case		<u> </u>	Keyword Lis	ts Qr Keyword	d Search
>	Show Rejected Results	Listing Keyword search 1 - Trum	X Keyword search 2 - Spiderman X				$\leftrightarrow \mathbf{v}$
Data Sources		Keyword search Table Thumbnail					19 Resul
LogicalFileSet1 (1)     LogicalFileSet1 (6)	Name	Location	Modified Time	Change Time	Access Time	Created	
	edb00007.jtx	JuogicalFileSet1/Users/All Users/Microsoft/Search/Data/Applications/Windows/		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00	
🕀 📜 All Use		-	3FAA /LogicalFileSet1/Users/csc253admin/AppData/Local/Packages/Microsoft. Micro		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00
<ul> <li>B CSC253</li> <li>B Default</li> </ul>	admin (33)	V0100018.log	/LogicalFileSet1/Users/csc2S3admin/AppDeta/Local/Microsoft/Windows/WebC		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00
	t User (0)	V0100019.log	/LogicalFileSet1/Users/csc253admin/AppData/Local/Microsoft/Windows/WebC		0000-00-00 00:00:00	0000-00-00 00:00:00	10-0000
Public (9)  Viens Fit: Types Fit: Types Deleted Files Fit: System (0) X (0)	V010001A.log	J.ogicalFileSet1JUsers/csc2S3admin/AppData/Local/Mcrosoft/Windows/WebC		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00	
	edb.log	/LogicalFileSet1/Users/csc2S3admin/AppData/Local/Packages/Microsoft.Micro		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00	
		nation /LogicalFileSet1/Users/csc253admin/AppData/Roaming/Microsoft/Windows/Re.		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00	
	1.fdt	/LogicalFileSet1/Users/csc2S3admin/csc2S3_acouisition/ModuleOutput/keywor.		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00	
	IndexedD8.edb	/LogicalFileSet1/Users/csc253admin/AppData/Local/Packages/Microsoft.Micro		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00	
MB File Size	MB File Size	autopsy.db	/LogicalFileSet1/Users/csc2S3admin/csc2S3_acouisition/autopsy.db	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00
Results			124-7 /LogicalFileSet1/Users/csc253admin/Desktop/Spiderman-spider-man-3979149		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00
Tags Reports		<					>
incporta		New Chines Ele Metadate Dan de	Message Indexed Text Media Other Occurrences				
		nex surings memeratura Results	Pleasage Increase Pleas Other Occurrences				
		Matches on page: 1 of 4 Ma	tch 🗧 🌶 Page: 1 of 4 Page 🧲 🌶		Text Sc	ource: Search Results	~
		1595 1598 T61Q T61Q 2M3Nisc012010041620100423	Svers/cec222admin/Flowers/ <mark>Systemman</mark> -spider-man-5849784-260-1200.jp al/Microwsfe/Windows/Misecory/Misecory.IES/MSMise012018044201804221				



-	Images/Videos 🧮 Timeline	🗽 Generate Report 🏾 🍘 Close Case		<u> </u>	<ul> <li>Keyword Lists</li> </ul>	Q Keyword S	iearch
>	Show Rejected Results		rch 2 - Spiderman ×			4	) <b>v</b> (
		Keyword search					19 Resul
<ul> <li>Data Sources</li> <li>Views</li> </ul>		Table Thumbnail					
E Results		Name	Location	Modified Time	Change Time	Access Time	Crea
- 🔄 Extracted Content		Recent Documents Artifact	/LogicalFileSet1/Users/csc253admin/AppData/Roaming/Micr		0000-00-00 00:00:00	0000-00-00 00:00:00	0000
- 📴 EXIF Metadata		Dispiderman-spider-man-5848734-1600-1280.lnk	/LogicalFileSet1/Users/csc253admin/AppData/Roaming/Micr		0000-00-00 00:00:00	0000-00-00 00:00:00	0000
	match Detected (2)	📄 drawable.db	/LogicalFileSet1/Users/csc253admin/csc253_acquisition/Mo		0000-00-00 00:00:00	0000-00-00 00:00:00	0000
Recent Docum     Web Bookmark		_1_Lucene41_0.tm	/LogicalFileSet1/Users/csc253admin/csc253_acquisition/Mo	00:00:00:00:00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000
Keyword Hits	(1)	📑 tika.log.0	/LogicalFileSet1/Users/csc253admin/AppData/Roaming/aut	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000
	(evword Search (41)	Spiderman-spider-man-5848734-1600-1280.jpg	/LogicalFileSet1/Users/csc253admin/Pictures/Spiderman-spi	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000
	Expression Search (0)	📄 tika.log. 1	/LogicalFileSet1/Users/csc253admin/AppData/Roaming/aut	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000
🗄 – 🔍 Email Addresse	es (161)	{15826497-2482-46D5-88D5-8D392F0D3CC8}.dat	/LogicalFileSet1/Users/csc253admin/AppData/Local/Packag	0000-00-00 00:00:00	00:00:00-00-00:00:00	0000-00-00 00:00:00	0000
- 🔶 Hashset Hits		edb00007.jtx	/LogicalFileSet1/Users/All Users/Microsoft/Search/Data/Ap	00:00-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000
E-Mail Messages		95C9889A-54C7-4043-8542-910F3FAA286D}.dat	/LogicalFileSet1/Users/csc253admin/AppData/Local/Packag	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000
<ul> <li>Interesting Items</li> <li>Accounts</li> </ul>		V0100018.log	/LogicaFileSet1/Users/csc253admin/AppData/Local/Microso	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000
Tags		<					>
👠 Reports		rtex Strings File Metadata Results (Manager Endered)					ſ
			BFILLER MARK				

Fig 23: Spiderman image file - MS Azure

🛉 Add Data Source 🚛	Images/Videos 🧮 Timeline	🚡 Generate Report 🍙 Clo	ise Case	A	• Keyword Lists	Qr Keyword Sea	arch
€ ⇒		Listing Keyword search	1 - Trump × Keyword search 2 - Sp	iderman ×		4	) <b>- v</b>
	Show Rejected Results	Keyword search				19	9 Res
Data Sources     Data Sources     LogicalFileSet1 (1)		Table Thumbnail					
<ul> <li>Views</li> </ul>		Name		Location	Modified Time	Change Time	A
🖶 🍰 File Types		tka.log.0		/LogicalFileSet1/Users/csc253admin/AppData/Roaming/autopsy/var/logitika.l		0000-00-00 00:00:00	0
X     Deleted Files		Spiderman-spider-man-58	48734-1600-1280.jpg	/LogicalFileSet1/Users/csc253admin/Pictures/Spiderman-spider-man-5848734		0000-00-00 00:00:00	0
File System (0)		tika.log.1		/LogicalFileSet1/Users/csc253admin/AppData/Roaming/autopsy/var/log/tika.l		0000-00-00 00:00:00	0
MB File Size		15826497-2482-46D5-88	3D5-BD392F0D3CCB}.dat	/LogicalFileSet1/Users/csc253admin/AppData/Local/Packages/Microsoft.Micro		0000-00-00 00:00:00	0
E Results		edb00007.jtx		/LogicalFileSet1/Users/All Users/Microsoft/Search/Data/Applications/Windows/		0000-00-00 00:00:00	0
Tags		95C9889A-54C7-4043-8	542-910F3FAA286D}.dat	/LogicalFileSet1/Users/csc253admin/AppData/Local/Packages/Microsoft.Micro		0000-00-00 00:00:00	0
Reports	V0100018.log		/LogicalFileSet1/Users/csc253admin/AppData/Local/Microsoft/Windows/WebC	. 0000-00-00 00:00:00	0000-00-00 00:00:00	0	
		Hex Strings File Metadata	Results Message Indexed Text Mer	a Other Occurrences			
		Name	/LogicalFileSet1/Users/csc253	admin/Pictures/Spiderman-spider-man-5848734-1600-1280.jpg			
		Туре	Local				
		MIME Type	image/jpeg				
		Size	599436				
		File Name Allocation	Allocated				
		Metadata Allocation	Allocated				
		Modified	0000-00-00 00:00:00				
		Accessed	0000-00-00 00:00:00				
		Created	0000-00-00 00:00:00				
		Changed	00:00-00-00 00:00:00				
		MD5	48c37dbdb4a6ccb8197441d2	22c89d76			
		Hash Lookup Results	UNKNOWN				

Fig 24: Date metadata missing from Spiderman image file - MS Azure

- → Show Rejected Results		Close Case				<u> </u>	• Keyword L	ists	$\mathbf{Q}_{\overline{\mathbf{v}}}$ Keyword Search
<ul> <li>Show Rejected Results</li> </ul>	Listing Keywo	ord search 1 - Trump X Keyword search 2 - Spide	man ×						
	Web Bookmarks								1 Re
Data Sources	Table Thumbnail								
Views     Results	Source File	URL	Title	Date Created	Program Name	Domain	Data Source	Tags	
E Results	🧳 Bing.url	http://go.microsoft.com/fwlink/p/?Link1d=255142	Bing.url	0000-00-00 00:00:00	Internet Explorer	go.microsoft.com	LogicalFileSet1		
DUF Netadata (1)     Extension Mmatch Detected (2)     Extension Mmatch Detected (2)     Second Second (1)     We bookmats (1)     Single Literal Keyword Second (41)     Single Literal Keyword (41)     Single		Aetadata Results Message Indexed Text Mesla	Other Occurr	ences					
	Result: 1 of	1 Result ( >		Web Bookma	rks				
		Value							
	Type	YOIUC							Source(s)
	Type URL	http://go.microsoft.com/fwlink/p/?LinkId=255142							Source(s) RecentActivity
	URL	http://go.microsoft.com/fwlink/p/?LinkId=255142							RecentActivity
	URL Title	http://go.microsoft.com/fwlink/p/?LinkId=255142 Bing.url							RecentActivity RecentActivity
	URL Title Date Created	http://go.microsoft.com/fwlink/p/7LinkId=255142 Bing.url 0000-00-00 00:00:00							RecentActivity RecentActivity RecentActivity
	URL Title Date Created Program Name	http://go.microsoft.com/fwink/p/7LinkId=255142 Bing.url 0000-00-00 00:00:00 Internet Explorer	url						RecentActivity RecentActivity RecentActivity RecentActivity

Fig 25: Bookmarks - MS Azure

🕂 Add Data Source 📠	Images/Videos 🧮 Timeline	🚡 Generate Report 🛛 👩 Close Case	🛕 💿 - Keyword Lists	Q Keyword Search
€ >	Show Rejected Results	Listing Keyword search 1 - Trump X Keyword search 2 - Spiderman X Deleted Files		∢ → ▼ □ 2 Result
Data Sources     Data Sources     Difference     Difference		Table Trubunai True True File System (0) X Al (0)		
		Hex   Strings   File Metadata   Results   Message   Indexed Text   Media   Other Occurrences		
Type here	to search	4 💷 🔁 🔚 🏦 🗨 🐰	A Ap	투 4») <sup>9:21 PM</sup> 다

Fig 26: Deleted Files - MS Azure

# 5. CONCLUSION

M CSC253-CloudVM - Autopry 4.6.0

The goal of the project was to analyze the use of a traditional forensics data acquisition to acquire data in a virtual machine environment. The sought to compare the integrity of data gathered to see if it would reflect the true actions of a scenario enacted in each environment. In each environment, the results found both expected results and discrepancies between the expectations to find and acquired. These discrepancies lead us to believe that establishing the integrity of data acquired from a Virtual Machine using traditional forensic software was not possible for our project.

Expected results.

- In all scenarios we found the file containing the word "Trump" that was seeded in the environment.
- 2. In all scenarios we were able to find trails of our web surfing activity located in the browser cache. These trails included date metadata.
- 3. In all scenarios we were able to locate the files that

we downloaded, which were not deleted. However, only the local VM(Scenarios 1 and 2) retained data metadata for the file. For MS Azure, non-standard settings must be applied to the configuration to ensure that date metadata is stored for files. If one wanted to ensure that metadata for files would be stored in the cloud VM, that configuration setting would need to be made upon setting up the VM, otherwise such data would not be accessible upon later investigation.

n x

4. In the case of the local VM(Scenarios 1 and 2), were able to acquire the deleted Spiderman image.

#### The discrepancies fell into two broad categories.

#### 1. The presence of unexpected data

In all three scenarios Autopsy software found emails that could not have been placed there by the user (us). There were 1,500+ emails acquired in Scenario 1, 2,700+ emails in Scenario 2 and XXX emails in Scenario 3. Despite the web browsing that we performed in order to seed these environments, it is unlikely that we came across that many email addresses during our process. These emails may have already been present on the Virtual Image and were inherited by us as the user. Therefore, in a real investigative case, it could be difficult to establish that the suspect was, in fact, in contact with any of the listed emails.

Additionally, one would expect the number of emails from Scenarios 1 and 2 to be the same since, essentially, it was the same environment. The excess number of email in Scenario 2 might be attributable to extra data located inside the .vmdk image that is necessary to operate it. Further investigation is needed to determine the exact reason for the discrepancy.

In Scenarios 1 and 2, there were also deleted images present in the Autopsy results. These are not images that we deleted as the user and we have no prior knowledge of these images. Some of the deleted images contained metadata describing their usage date and some did not. In the case of a true forensic investigation, deleted criminal images would not necessarily be attributable to the suspect. How can we prove that deleted images without accurate metadata belong to suspect activity? On that same note, if some of the data acquired from the forensic investigation cannot be relied upon, how can any of it be? Even those images that contain date metadata could be brought under suspicion in a court of law. Further investigation is needed to determine if/how can truly distinguish between the user's deleted files and deleted files that came as part of the virtual image.

As with the emails, there is also a discrepancy between the number of deleted files reported by Scenario 1 (9000+) and Scenario 2 (10000+). The excess number of email in Scenario 2 might be attributable to extra data located inside the .vmdk image that is necessary to operate it. Further investigation is needed to determine the exact reason for the discrepancy.

#### 2. The absence of expected data.

We had expected a record of the deleted file from the cloud VM in Scenario 3. However, there was no record of any deleted files in this environment. The standard configuration of VM storage for MS Azure does not guarantee persistence of data. While there are options for persisting VM data/files via MS Azure we cannot be sure that deleted files would be preserved. Further investigation is called for to understand if/how deleted VM data could be made to persist for a distinct period.

It was expected that date metadata would exist for the

Spiderman images that was downloaded from the web. This metadata was not present. Again, the standard configuration of MS Azure VM local storage does not guarantee file metadata preservation. If this type of record is needed, it needs to be configured during VM storage setup.

#### 6. SUMMARY

It is clear from our project that more work needs to be done to solidify how forensic data acquisition from virtual machines can be made trust-worthy. Any company or service that utilizes virtual machines as a regular part of their business will need to decide if there is any anticipated or possible need for future forensic data acquisition. If future forensic investigation is to be accommodated for, a few conclusions can be made as a result of our project.

The local virtual machine, which is completely under the control of the owning organization, seems to be more reliable than the cloud VM machine. To compensate for the discrepancies discovered during our investigation, creators of local virtual images should ensure that the image is clean and free of any historical data. Theoretically, a clean virtual image could be trusted to contain only data placed there by the current user, and not data present from the image itself. This hypothesis warrants further investigation.

For MS Azure cloud virtual machines, standard configurations do not facilitate accurate data acquisition. Further investigation needs to be made into how cloud VMs can be configured in such a way to preserve data should a forensic investigation be necessary at a future data.

#### 7. REFERENCES

- [1] Digital Forensics on a Virtual Machine; University of Alabama website, undated; Juan Carlos Flores Cruz, Travis Atkinson http://atkison.cs.ua.edu/papers/ACMSE11\_JF.pdf
- [2] Acquiring forensic evidence from infrastructure-as-aservice cloud computing: Exploring and evaluating tools, trust, and techniques; Digital Investigation Volume 9, Supplement, August 2012, Pages S90-S98; Josiah Dykstra, Alan T.Sherman https://www.sciencedirect.com/science/article/pii/S17422 87612000266
- [3] Evolution of Traditional Digital Forensic in Virtualization; ACMSE '13 Proceedings of the 51st ACM Southeast Conference Article No. 30; Savannah, Georgia — April 04 - 06, 2013; Juan Carlos Flores Cruz, Travis Atkinson https://dl.acm.org/citation.cfm?id=2500078.