The Evil Deeds of Michael Smirnov Unraveled

Key Contributors:
Garrett Stokes, Marcus Harmon, Michael Bahre,
Abdul Abdulaziz

UNIVERSITY OF THE
INCARNATE WORD®

12-07-2023

Table of Contents

Executive Summary

This project simulates a forensic investigation of an individual, "Michael Smirnov", who regulated and appointed hired kills using his computer laptop device. The identification of Michael comes through a legal witness, Timothy Simpson. The possession of the computer laptop device in which the crime was thought to take place was seized and taken into custody through an acquired search warrant, the same day as the initial 911 call, 09/16/2023. Upon seizure of the device, which occurred on 09/16/2023, the device was then transported by the police officers at the initial scene and taken to the APD (Austin Police Department) headquarters, where the device was then stored until it was retrieved by the forensic team of agents, Garrett Stokes, Abdul Abdulaziz, and Michael Bahre. Forensic Legal Analyst Marcus Harmon serves the purpose of making sure the forensic investigation is conducted properly and thoroughly according to law, as well as presenting discovered evidence and possible violations of law of the suspect in a clear and concise manner which helps the prosecution in the case, which is not included in this report. The suspect computer laptop device was stored in the APD headquarters from 09/16/2023, to 09/28/23. On 09/28/2023, the forensic team began conducting a forensic examination on the device. This forensic examination serves the purpose of following best practices to prepare the device for forensic analysis. In the forensic examination, the suspect computer device comes in the form of a virtual desktop infrastructure. This is a VirtualBox image file, this was done for simulation purposes. The forensic examination treated this device as if it were a real physical device, and used FTK imager, a forensic tool which creates a bit-by-bit copy of the device and converted it to a .raw file which could be used for analysis by two forensic machines – Virtualized Kali Linux, and Host Windows 10. The primary tool used for analysis was Autopsy, both the Kali and Windows version. To make the FTK imager copy of the suspect drive available to the forensic software, it was placed in a shared folder called "KaliShared". This shared folder was linked to the virtual Kali machine on VirtualBox. This made the file available to not only the Host Windows 10 machine, but also the virtualized Kali Machine. The rest of the forensic examination included a conversion of the FTK imager copied .raw file to a .vdi, which could be used for direct access to the box on VirtualBox, as well as updating of the Kali Machine and the analysis software used, Autopsy, to ensure no issues arose related to deprecation. The examination successfully prepared the suspect machine to be analyzed and was completed on 10/06/2023. The next step of the forensic investigation was the Forensic Analysis, which began on 10/10/2023. This is when the suspect image file was actually analyzed by forensic software for evidence and key findings. The first section of the forensic analysis is the Preliminary Analysis, which details how the forensic agents were able to add the raw image file as a data source in both the Kali version of Autopsy, as well as the Windows version of Autopsy. The second section of the Forensic Analysis is the File System Meta Data Analysis, which was conducted on Kali Linux's version of Autopsy. The goal of this section is to gain valuable insight into suspicious activities being conducted on the device that could be related to the crime. There were three specific MFT entries that were analyzed, all of which provided insight into the investigation. These insights included suspicious downloading and altering of logos related to “weather”, as well as the presence of discord on the system, a popular communications application. The third section of the analysis, Keyword Search, utilizes these insights. The goal of this section was to find direct evidence linked to the murders of Matthew Latkin on Michael’s device. A keyword search was conducted using the Windows version of Autopsy, the keyword being “weather”. There was a total of 7000+ linked files which included this keyword, but multiple recent document artifacts were found, pointing to a directory in Michael’s user account on the desktop, called “Weather”. The agent explored this directory, but found the folder to be empty, indicating these recent documents had been deleted from the system. The agent continued sifting through the keyword search results, and found a file titled “weatherrecordings.txt”. Upon examination of the file, names of victims, including Matthew Latkin were found, as well as their addresses, occupation, and survival state. This file was confirmed to be in Michael’s user account backup folder. The fourth and final section of the Forensic Analysis is the Discord section. This section is different from the others, and doesn’t use forensic software to analyze the drive, but rather a live booting of a copy of the suspect image using VirtualBox to analyze Michael’s Discord for possible evidence. The machine was booted into, and Discord was immediately launched upon startup. The forensic agent quickly noticed there was a direct message conversation between Michael’s Discord account and a user with the username of “darkside8041” upon reading the messages, the agent discovered the two accounts discussing the appointment of the murders of Matthew Latkin and Alex Croyll. This concluded the forensic analysis and was complete on 10/21/2023. The Final section of the report is Evidence, which lays out all the evidence found in the forensic analysis, in a clear and concise manner and ties it to the law.

Project Information

(ALL NAMES USED IN THIS PROJECT HAVE BEEN MADE UP THIS IS FOR EDUCATIONAL PURPOSES ONLY)

Project Milestones:

1. Case Start
2. Legal Framework
3. Forensic Examination
4. Forensic Analysis
5. Evidence

Materials List:

1. Windows 10 Forensic Machine
2. Virtual Kali Linux Forensic Machine
3. VirtualBox, FTK Imager, Autopsy (Kali and Windows Version)
4. Simulated Suspect Image File

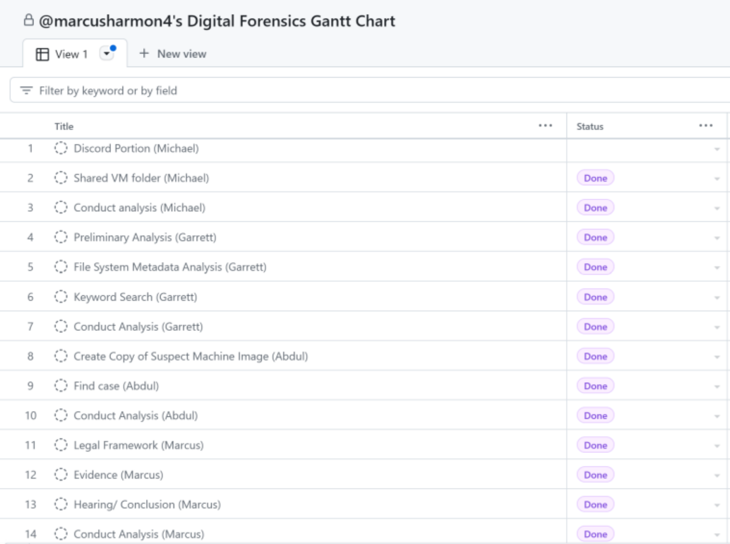
Deliverables:

1. Report and PowerPoint Presentation
2. Case Information
3. Methods to Find Evidence
4. Incriminating Evidence
5. Potentially Violated Laws

Professional Accomplishments:

1. Become familiar with FTK Imager and Autopsy on both Windows and Kali Linux
2. Gain experience working in a simulated Forensic investigation
3. Become better working on a group project with team members

Project Schedule Management Gantt Chart



@marcusharmon4's Digital Forensics Gantt Chart

	Title	Status
1	Discord Portion (Michael)	
2	Shared VM folder (Michael)	Done
3	Conduct analysis (Michael)	Done
4	Preliminary Analysis (Garrett)	Done
5	File System Metadata Analysis (Garrett)	Done
6	Keyword Search (Garrett)	Done
7	Conduct Analysis (Garrett)	Done
8	Create Copy of Suspect Machine Image (Abdul)	Done
9	Find case (Abdul)	Done
10	Conduct Analysis (Abdul)	Done
11	Legal Framework (Marcus)	Done
12	Evidence (Marcus)	Done
13	Hearing/ Conclusion (Marcus)	Done
14	Conduct Analysis (Marcus)	Done

Case Start

Commented [SJ1]: Legal Analyst Agent Marcus Harmon, 09/27/2023, 9:00AM, Austin PD Headquarters

On September 16th, at roughly 10:47am, witness Timothy Simpson was at his dorm room, at The University of Texas, and happened to notice some alarming messages on his roommate's computer. His roommate Michael Smirnov is a fine art major and is in his first year of undergraduate. According to Timothy, it is Michael's first year in the United States. Timothy happened to glance at a Discord conversation, in which he saw the name of a person he had recently seen in the news headlines – Matthew Latkin. The message read "Latkin has been taken care of –ck" This alerted Timothy instantly, so he took a screenshot of the text, left the room and called the police at 10:59am. Soon after, Michael returned to his desk, and felt something was wrong when he realized he left his WhatsApp open.

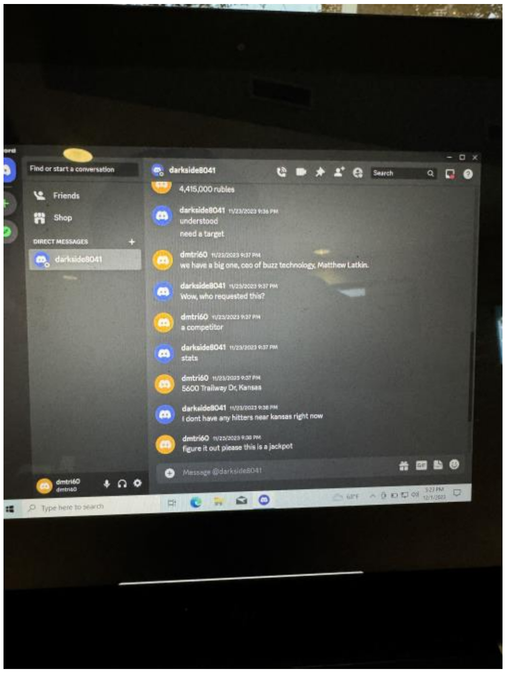
After receiving the call, Police obtained a search warrant and arrived onto the campus and at Andrews Hall, room 227, in which Timothy, Michael, Kyle, and Eriktan lived in. The search warrant allowed the Austin Police Department to search the room and confiscate the suspects laptop the same day, September 16th at 1PM. After a week and a half had passed by the examiners started to search the computer and create a copy of the suspects machine using FTK imager, this happened on September 28th at 8:05AM and this was conducted by agent Abdul. The next step was conducted by Agent Michael and his role was VirtualBox Image Environment Shared Folders, his investigation was conducted on October 2nd 9: 32AM.

The Forensic Kali Linux Virtual Machine setup was next on the list, and this was conducted by Agent Abdul on October 6th 6:15AM. The next step in the investigation was the Preliminary Analysis and this was conducted on October 10th, by Agent Garrett. The next step to do was Filesystem Metadata Analysis and this was conducted on October 14th 4:35PM by agent Garrett, he also conducted the Keyword Search a few days later October 17th at 7:01AM. The investigation was followed up by the Discord Analysis and this was conducted on October 21st at 9:01AM by agent Michael.

Legal Framework

Probable Cause

This case starts off with Timothy Simpson seeing the computer of Michael Smirnov. Michael's computer is seen to have messages and a discord chat open. The discord chat details Matthew Latkin's address, his job, and what time he usually leaves his house and gets home from work. The messages were talking about the murder of Matthew Latkin and how the job has been "completed". Timothy sees these messages and the discord chat when Michael left the room and had his computer open, this is the probable cause of this case. Michael also feels like something is going on and his suspicions are brewing so to cover up his tracks he deletes the files in his "Weather" folder, which contains details of the killings.



darkside8041

4,415,000 rubles

darkside8041 11/23/2023 9:36 PM
understood
need a target

dmtri60 11/23/2023 9:37 PM
we have a big one, ceo of buzz technology, Matthew Latkin.

darkside8041 11/23/2023 9:37 PM
Wow, who requested this?

dmtri60 11/23/2023 9:37 PM
a competitor

darkside8041 11/23/2023 9:37 PM
stats

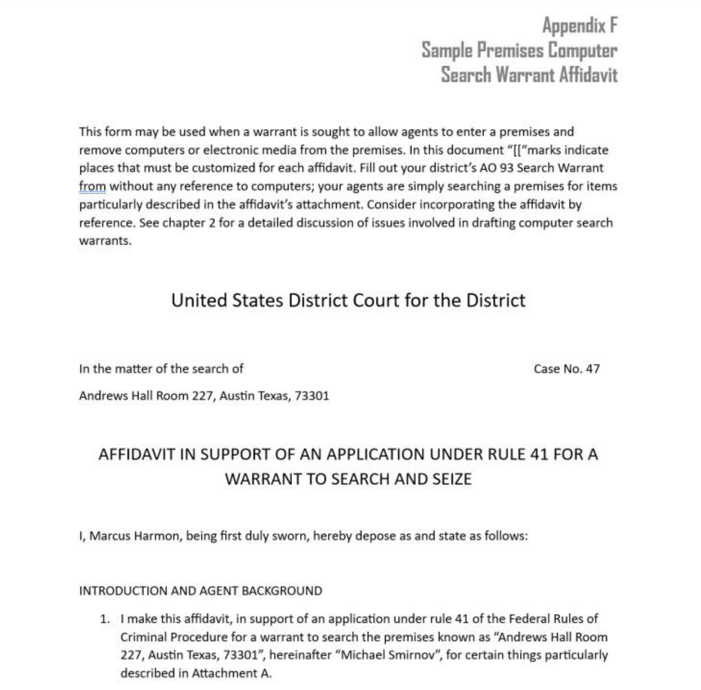
dmtri60 11/23/2023 9:37 PM
5600 Trailway Dr, Kansas

darkside8041 11/23/2023 9:38 PM
I dont have any hitters near kansas right now

dmtri60 11/23/2023 9:38 PM
figure it out please this is a jackpot

Search Warrant and Device Seizure

This leads Timothy to call the cops and he believes that Dimitri is an accomplice to the murder of Matthew Latkin. Search warrants can take up to a few hours, up to a few days, or even weeks based on the severity of the case. The case that we have though has an extremely high level of importance so after Timothy called the cops and gave out the information of what he has seen the cops then make an affidavit and this provides detailed information about the case including the facts and the evidence. The affidavit is then given to a judge who reviews the affidavit, and they determine whether or not a search warrant can be given out. The judge's review is a very critical step because under the fourth amendment the people of the United States are protected against unreasonable searches and seizures. In our case the judge did provide the cops with a search warrant and that allowed the cops to then be able to search Dimitri's dorm room and confiscate his computer for further investigations.



Appendix F
Sample Premises Computer
Search Warrant Affidavit

This form may be used when a warrant is sought to allow agents to enter a premises and remove computers or electronic media from the premises. In this document "[["marks indicate places that must be customized for each affidavit. Fill out your district's AO 93 Search Warrant from without any reference to computers; your agents are simply searching a premises for items particularly described in the affidavit's attachment. Consider incorporating the affidavit by reference. See chapter 2 for a detailed discussion of issues involved in drafting computer search warrants.

United States District Court for the District

In the matter of the search of — Case No. 47

Andrews Hall Room 227, Austin Texas, 73301

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Marcus Harmon, being first duly sworn, hereby depose as and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit, in support of an application under rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as "Andrews Hall Room 227, Austin Texas, 73301", hereinafter "Michael Smirnov", for certain things particularly described in Attachment A.

Chain Of Custody

The police are the ones who handled the evidence, the evidence was handled some hours after the phone call to the police was made inside of the witness's dorm room. The file isn't physical evidence, it's digital evidence so the condition of it is good, the hard part of the investigation for the cops is going to be the analysis and finding concrete evidence that ties Michael to the case.

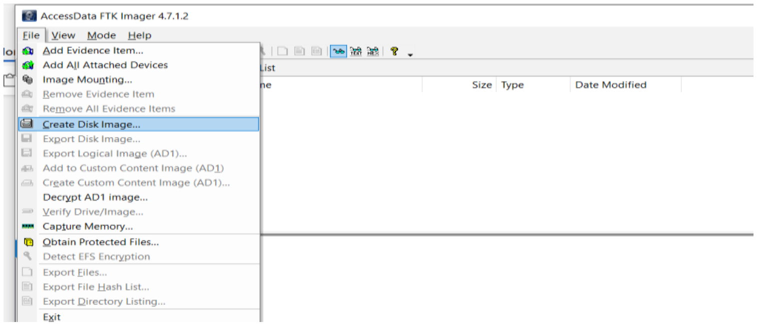
(September 16th 1PM the laptop is retrieved)

Forensic Examination Procedure

Creating A Copy of The Suspect Machine Image with FTK Imager

Commented [SJ2]: Forensic Examiner Agent Abdul Abdulaziz, 09/28/2023, 8:05AM, Austin PD Headquarters

This forensics examination on Michael Smirnov’s file system was performed using virtualization, for simulation purposes, our suspect drive is not physical, and starts as a .vdi VirtualBox image file. Given this scenario, we treat the image file as if it was a true physical drive. To initiate the forensic examination, we must prepare the drive to be analyzed by the forensic analyzation team. This starts by creating a bit-by-bit copy of the drive using FTK Imager on the host Forensic Examiner computer.



09/28/2023, 8:05AM, FTK Imager on host examiner machine, creating disk image

The examination is initiated at 8:05AM on 09/28/2023 by using a utility called FTK imager, which allows us to create an exact copy of the virtual drive while converting it to raw format. Simply copying and pasting the drive is not an option, as metadata changes can occur, and for a forensic investigation, the least number of conversions and changes to a drive are expected for accurate analysis later down the forensic investigation.

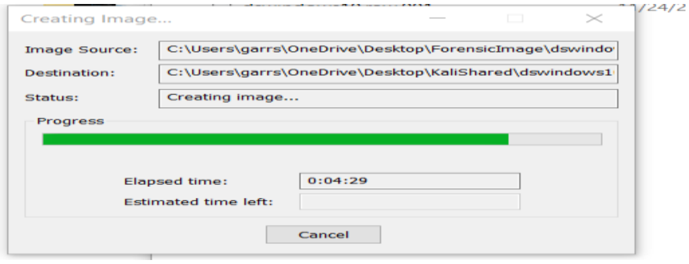

Creating Image...

Image Source: C:\Users\garrs\OneDrive\Desktop\ForensicImage\dswindo

Destination: C:\Users\garrs\OneDrive\Desktop\KaliShared\dswindows1

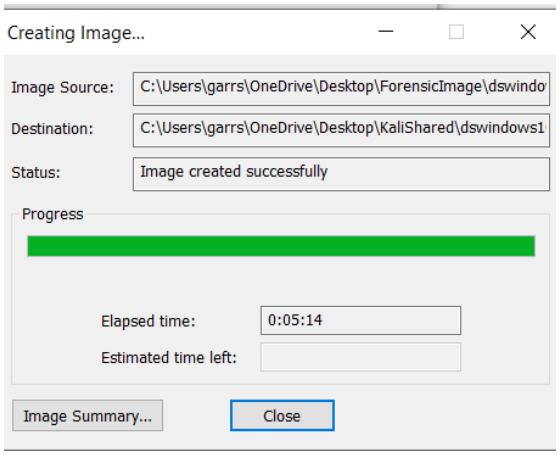
Status: Creating image...

Elapsed time: 0:04:29

Estimated time left:

09/28/2023, 8:19AM, FTK Imager drive creation in progress

The image source is specified in the Desktop folder known as “ForensicImage” which includes the .vdi image being replicated, “dswindows10.vdi”. The destination folder is marked as “KaliShared” which is another desktop folder on the host forensic examiner machine. The folder “KaliShared”, will later serve as a shared folder using Virtual Box, and will allow access to the Kali Linux Forensic Machine to access the image file. The image file will also be accessed from the Windows 10 host analysis machine after for further analysis.



Creating Image...

Image Source: C:\Users\garrs\OneDrive\Desktop\ForensicImage\dswindo

Destination: C:\Users\garrs\OneDrive\Desktop\KaliShared\dswindows1

Status: Image created successfully

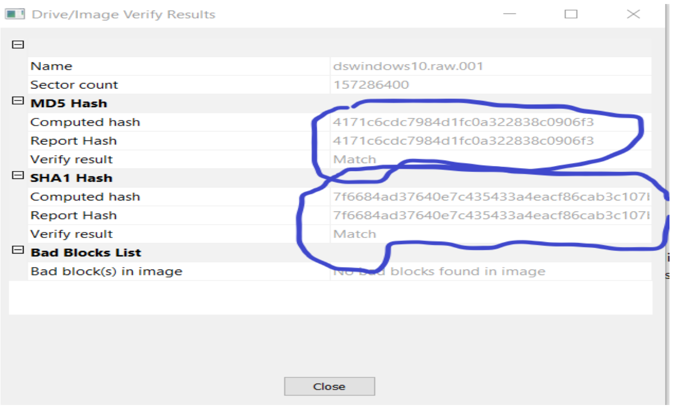
Progress

Elapsed time: 0:05:14

Estimated time left:

09/28/2023, 8:28AM, FTK Imager image created successfully

Upon completion of FTK Imager, the image file was successfully created, and we get a hash value comparison matcher to indicate if the image file was changed any way during the creation.

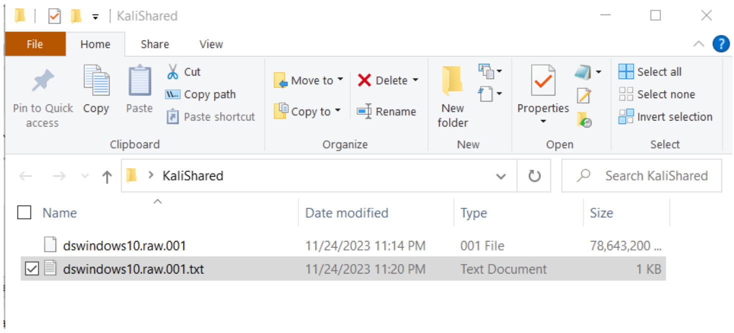


Drive/Image Verify Results

Name	dswindows10.raw.001
Sector count	157286400
MD5 Hash	
Computed hash	4171c6cdc7984d1fc0a322838c0906f3
Report Hash	4171c6cdc7984d1fc0a322838c0906f3
Verify result	Match
SHA1 Hash	
Computed hash	7f6684ad37640e7c435433a4eacf86cab3c107
Report Hash	7f6684ad37640e7c435433a4eacf86cab3c107
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

09/28/2023, 8:29AM, FTK Imager hash value comparison

As seen above, the hash values are an exact match, indicating that no change occurred during the image creation of the file. This allows the forensic examination team to continue working with the created image file knowing there are no unwanted changes to the copy.

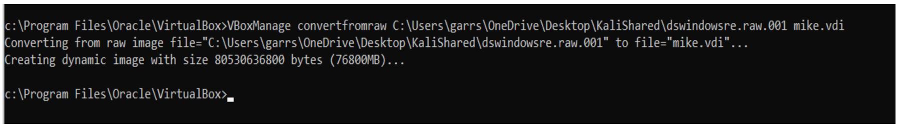


Name	Date modified	Type	Size
dswindows10.raw.001	11/24/2023 11:14 PM	001 File	78,643,200 ...
☑ dswindows10.raw.001.txt	11/24/2023 11:20 PM	Text Document	1 KB

09/28/2023, 8:30AM, verification of FTK Imager Image file

Looking into the destination in which the file was to be added to, we can see that the. raw image copy created by FTK Imager has successfully been added to the “KaliShared” Directory. The .txt file serves to provide case information details about when the image was created and by whom.

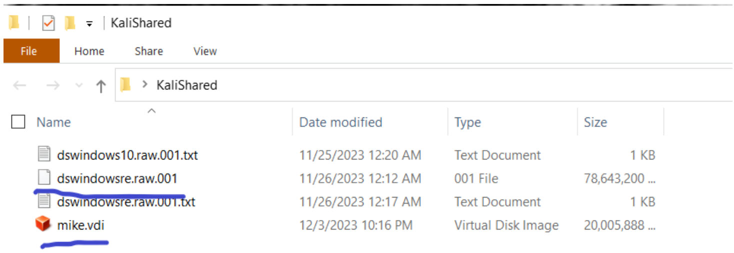
Lastly, Agent Abdul creates a copy of and conversion of this .raw file to a .vdi file so the machine can be analyzed directly via VirtualBox. This is done using VBoxManage with the command seen below.



```
c:\Program Files\Oracle\VirtualBox>VBoxManage convertfromraw C:\Users\garrs\OneDrive\Desktop\KaliShared\dswindowsre.raw.001 mike.vdi
Converting from raw image file="C:\Users\garrs\OneDrive\Desktop\KaliShared\dswindowsre.raw.001" to file="mike.vdi"...
Creating dynamic image with size 80530636800 bytes (76800MB)...

c:\Program Files\Oracle\VirtualBox>
```

09/28/2023, 8:43AM, .raw image file copy to .vdi

There is now a .vdi copy of the suspect image file, which can be accessed directly through a virtual machine using VirtualBox.



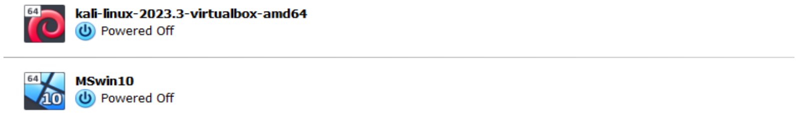
Name	Date modified	Type	Size
dswindows10.raw.001.txt	11/25/2023 12:20 AM	Text Document	1 KB
dswindowsre.raw.001	11/26/2023 12:12 AM	001 File	78,643,200 ...
dswindowsre.raw.001.txt	11/26/2023 12:17 AM	Text Document	1 KB
mike.vdi	12/3/2023 10:16 PM	Virtual Disk Image	20,005,888 ...

09/28/2023, 8:45AM, verification of .vdi conversion from .raw

VirtualBox Image Environment and Shared Folders

Commented [SJ3]: Forensic Examiner Agent Michael Bahre, 10/02/2023, 9:32AM, Austin PD Headquarters

With a copy of the suspect drive in .raw format on the forensic Windows 10 host machine, the forensic examination team must get it to be accessible over the Kali Linux virtual box, who will be doing the first file metadata analysis of the .raw image file. Thankfully, this is easily done by using shared folders via VirtualBox.

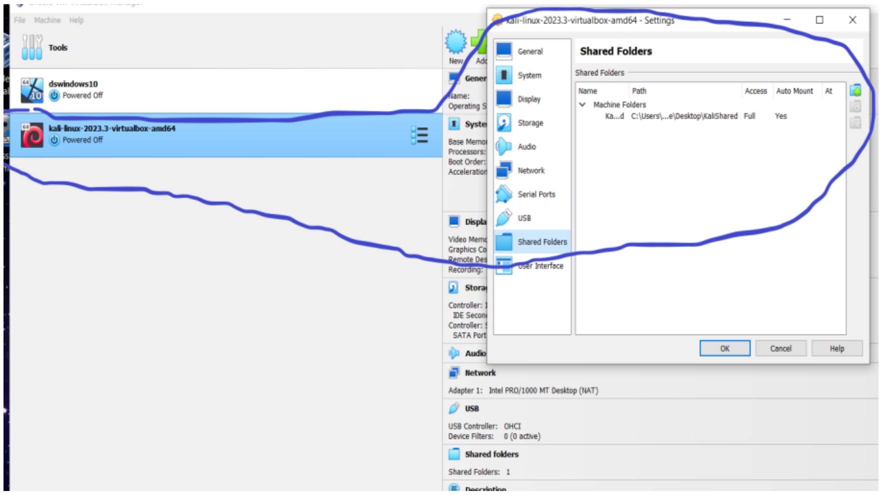


kali-linux-2023.3-virtualbox-amd64
Powered Off

MSwin10
Powered Off

10/02/2023, 9:32AM, VirtualBox Environment

Above is pictured the forensic examination VirtualBox environment. A copy of suspect drive “dswindows10” in VDI form, which will remain untouched until needed, and the forensic examination Kali Linux box, which the team will now appoint its attention in order to prepare it for forensic drive analysis. A shared folder will be linked and automatically mounted to the Kali Box, the folder being the one the team previously appointed the FTK Image copy to, known as “KaliShared”



kali-linux-2023.3-virtualbox-amd64 - Settings

Shared Folders

Name	Path	Access	Auto Mount	At
Machine Folders				
Ka...d	C:\Users\...e\Desktop\KaliShared	Full	Yes	

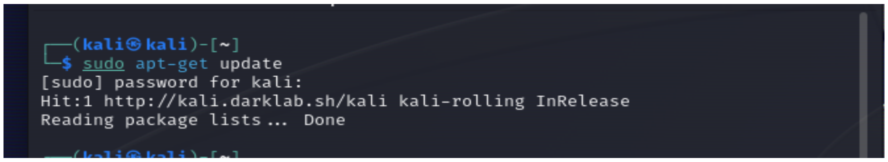
10/02/2023, 9:35AM, Kali Linux shared folder “KaliShared”

This shared folder allows the Kali Linux virtual forensic machine, as well as the host windows 10 forensic machine to have direct access to the file, without having to copy or transfer the image file to the VM, which could lead to unintentional changes in the image file.

Forensic Kali Linux Virtual Machine Setup

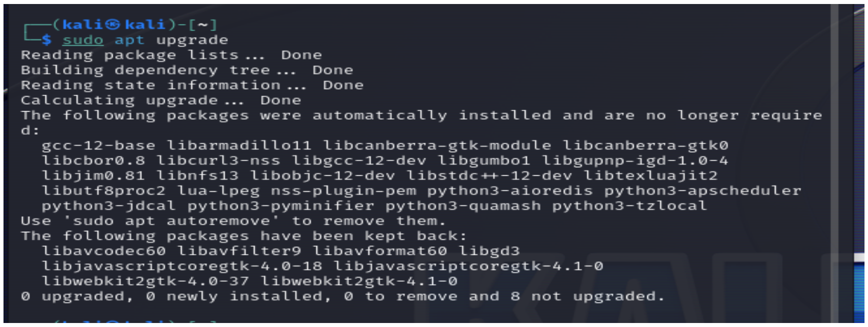
Commented [SJ4]: Forensic Examiner Agent Abdul Abdulaziz, 10/06/2023, 6:15AM, Austin PD Headquarters

Now that the forensic team has shared access to the .raw suspect image, the examination team will begin preparing the box for file metadata analysis on the virtual Kali forensic box. To begin this, the team ensures the machine is fully upgraded and up to date.



```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get update
[sudo] password for kali:
Hit:1 http://kali.darklab.sh/kali kali-rolling InRelease
Reading package lists ... Done
```

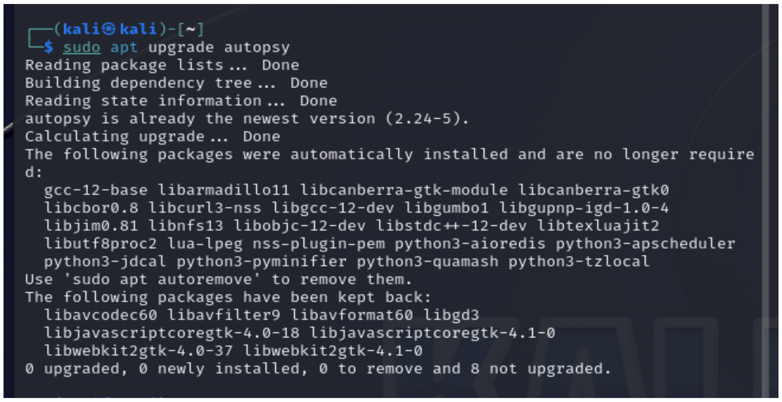
10/06/2023, 6:15AM, Kali Machine Update



```
┌──(kali㉿kali)-[~]
└─$ sudo apt upgrade
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Calculating upgrade ... Done
The following packages were automatically installed and are no longer require
d:
  gcc-12-base libarmadillo11 libcanberra-gtk-module libcanberra-gtk0
  libcbor0.8 libcurl3-nss libgcc-12-dev libgumbo1 libgupnp-igd-1.0-4
  libjim0.81 libnfs13 libobjc-12-dev libstdc++-12-dev libtexluajit2
  libutf8proc2 lua-lpeg nss-plugin-pem python3-aioredis python3-apscheduler
  python3-jdcal python3-pyminifier python3-quamash python3-tzlocal
Use 'sudo apt autoremove' to remove them.
The following packages have been kept back:
  libavcodec60 libavfilter9 libavformat60 libgd3
  libjavascriptcoregtk-4.0-18 libjavascriptcoregtk-4.1-0
  libwebkit2gtk-4.0-37 libwebkit2gtk-4.1-0
0 upgraded, 0 newly installed, 0 to remove and 8 not upgraded.
```

10/06/2023, 6:17AM, Kali Machine Upgrade

After the team performs routine updating and upgrading of the Kali forensic system, they upgrade Autopsy, the main forensic tool being used by the forensic analysis team.

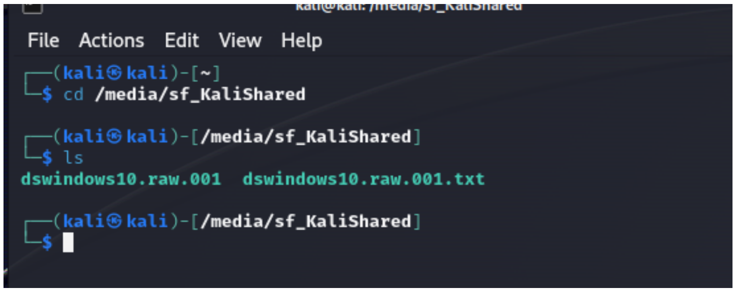


```
┌──(kali㉿kali)-[~]
└─$ sudo apt upgrade autopsy
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
autopsy is already the newest version (2.24-5).
Calculating upgrade ... Done
The following packages were automatically installed and are no longer require
d:
  gcc-12-base libarmadillo11 libcanberra-gtk-module libcanberra-gtk0
  libcbor0.8 libcurl3-nss libgcc-12-dev libgumbo1 libgupnp-igd-1.0-4
  libjim0.81 libnfs13 libobjc-12-dev libstdc++-12-dev libtexluajit2
  libutf8proc2 lua-lpeg nss-plugin-pem python3-aioredis python3-apscheduler
  python3-jdcal python3-pyminifier python3-quamash python3-tzlocal
Use 'sudo apt autoremove' to remove them.
The following packages have been kept back:
  libavcodec60 libavfilter9 libavformat60 libgd3
  libjavascriptcoregtk-4.0-18 libjavascriptcoregtk-4.1-0
  libwebkit2gtk-4.0-37 libwebkit2gtk-4.1-0
0 upgraded, 0 newly installed, 0 to remove and 8 not upgraded.
```

10/06/2023, 6:20AM, Kali Autopsy Upgrade

Having the Kali system updated and upgraded, as well as the Autopsy forensic software upgraded to its latest version, is paramount for any forensic investigation. Using deprecated software is never a wise choice, as it can lead to issues that will hurt the investigation, as well as slow the investigation process entirely.

Finally, the team ensures the shared folder is accessible on the Kali machine, which is looking into the shared folder directory, /media/sf_KaliShared.



```
┌──(kali㉿kali)-[~]
└─$ cd /media/sf_KaliShared

┌──(kali㉿kali)-[/media/sf_KaliShared]
└─$ ls
dswindows10.raw.001  dswindows10.raw.001.txt

┌──(kali㉿kali)-[/media/sf_KaliShared]
└─$ 
```

10/06/2023, 6:30AM, dswindows.raw.001 in shared folder verification

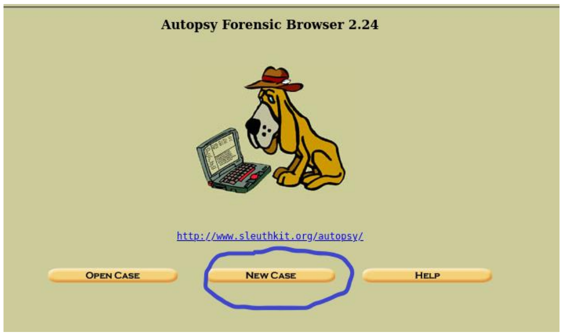
With the updating and upgrading of the primary components that will be used on the forensic Kali machine, as well as the verification that the machine can access the raw suspect image file, the examination portion of the investigation is concluded. The next natural step of the investigation is the forensic analysis, which will be conducted by the forensic analysis team.

Forensic Analysis Procedure

Preliminary Analysis (Kali Linux and Windows 10)

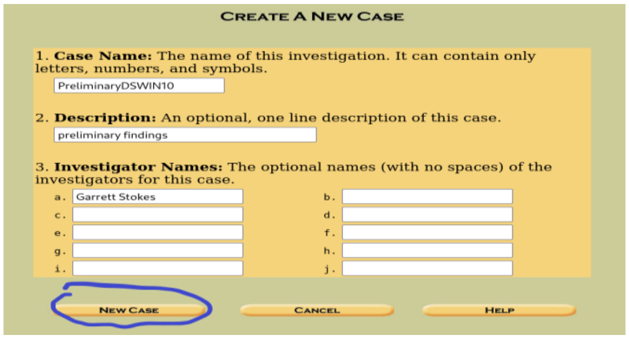
Commented [SJ5]: Forensic Examiner Agent Garrett Stokes, 10/10/2023, 11:05AM, Austin PD Headquarters

In the preliminary analysis, the details of how the suspect image file data source is added, for both the Virtual Kali Forensic machine as well as the Windows 10 machine, are defined. This preliminary Analysis was conducted on 10/10/2023, starting at 11:05AM by Agent Stokes.


Autopsy Forensic Browser 2.24
http://www.sleuthkit.org/autopsy/
OPEN CASE
NEW CASE
HELP

10/10/2023, 11:05AM, Autopsy case creation

Step 1: Autopsy is started on the virtual Kali Linux Forensic machine and navigated to through the local host port. At this point, the Autopsy forensic browser is accessed.



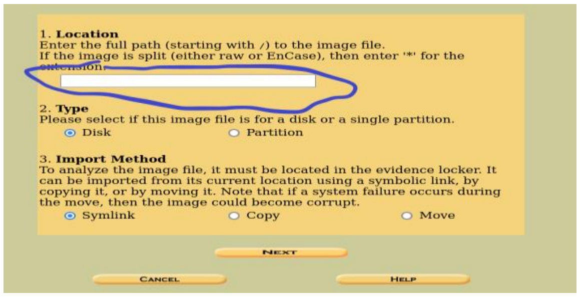
1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.
PreliminaryDSWIN10

2. **Description:** An optional, one line description of this case.
preliminary findings

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.
a. Garrett Stokes
b.
c.
d.
e.
f.
g.
h.
i.
j.

10/10/2023, 11:06AM, Case details

Step 2: After this, agent Stokes adds the host (source of data) and links the image path utilizing a symbolic link. In this case, the suspect image is in the shared folder, /media/sF_KaliShared/dswindows10.raw.001



1. **Location**
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

2. **Type**
Please select if this image file is for a disk or a single partition.
● Disk ○ Partition

3. **Import Method**
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.
● Symlink ○ Copy ○ Move

10/10/2023, 11:08AM, location of image path with symbolic link

Step 3: After linking the image, Autopsy will recognize the image as a NTFS/ ExFat, and ask for an md5 hash calculation of the image. Agent Stokes selects this option, to ensure the image has not been altered in any way since it was created by FTK imager.

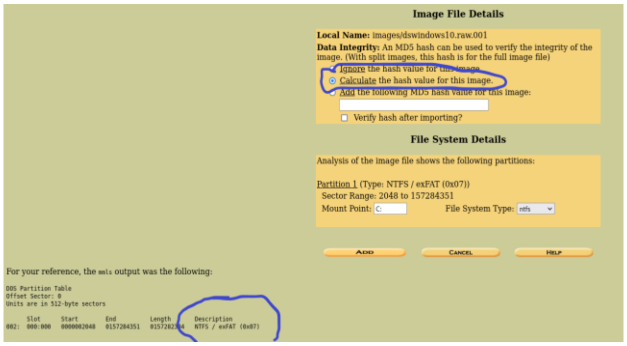


Image File Details

Local Name: images/dswindows10.raw.001
Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)
○ Ignore the hash value for this image.
● Calculate the hash value for this image.
○ Add the following MD5 hash value for this image:
□ Verify hash after importing?

File System Details

Analysis of the image file shows the following partitions:

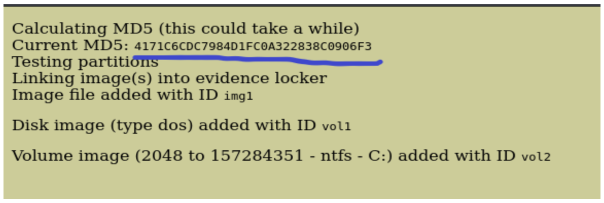
Partition 1 (Type: NTFS / exFAT (0x07))
Sector Range: 2048 to 157284351
Mount Point: C: File System Type: ntfs

For your reference, the mmls output was the following:

```
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
002:  000:000   0000002048   0157284351   0157282304   NTFS / exFAT (0x07)
```

10/10/2023, 11:12AM, Calculate hash?

Step 4: The hash is calculated after a long amount of time, because the drive is 80GB. The hash matches that of which the examination team had when the image file was copied with FTK Imager. This ensures the image file has not been altered.

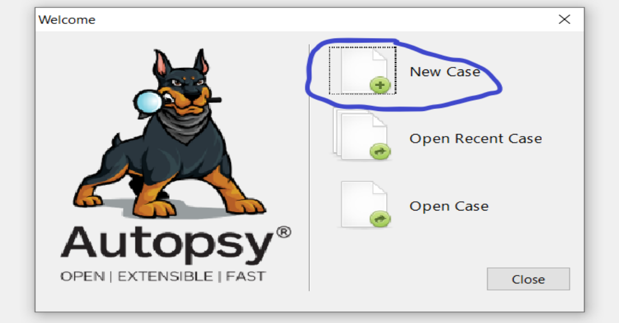


```
Calculating MD5 (this could take a while)
Current MD5: 4171C6CDC7984D1FC0A322838C0906F3
Testing partitions
Linking image(s) into evidence locker
Image file added with ID img1

Disk image (type dos) added with ID vol1

Volume image (2048 to 157284351 - ntfs - C:) added with ID vol2
```

10/28/2023, 12:35PM, MD5 Hash

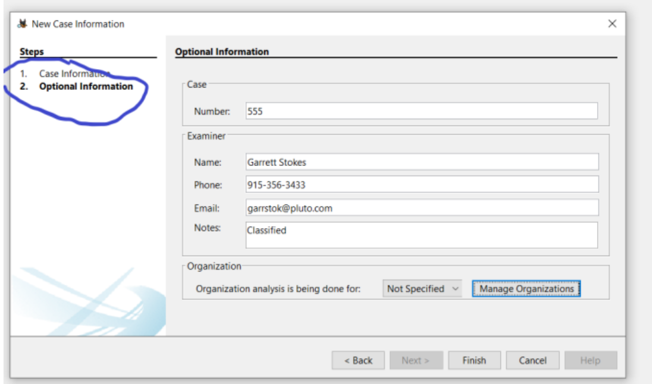
(End of Kali Linux Virtual Forensic Machine Preliminary Analysis)

Step 1: Autopsy is started on the Windows 10 Forensic machine, and the create new case option is selected.



10/10/2023, 12:40PM, Windows 10 Autopsy create new case

Step 2: After creating the case, case information and optional information are entered. This is a feature that is more robust than that of the Kali version of Autopsy and allows us to enter more information that is pertinent to the case.



Optional Information

Case

Number: 555

Examiner

Name: Garrett Stokes

Phone: 915-356-3433

Email: garrstok@pluto.com

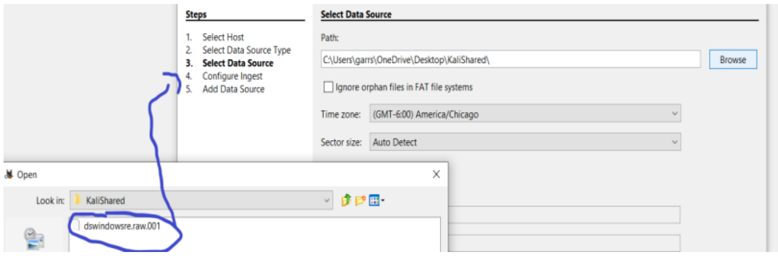
Notes: Classified

Organization

Organization analysis is being done for: Not Specified

10/10/2023, 12:41PM, case details

Step 3: After The next steps involve inputting the data source that is to be ingested by autopsy. This is very similar to how it was conducted with the Kali machine, as the suspect image copy resided in the same folder “KaliShared” and is named “dswindows.raw.001”. The type of data source is defined as “Image/VM File”. This file is pointed at to be the data source for Autopsy.



Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Path: C:\Users\garrs\OneDrive\Desktop\KaliShared\

□ Ignore orphan files in FAT file systems

Time zone: (GMT-6:00) America/Chicago

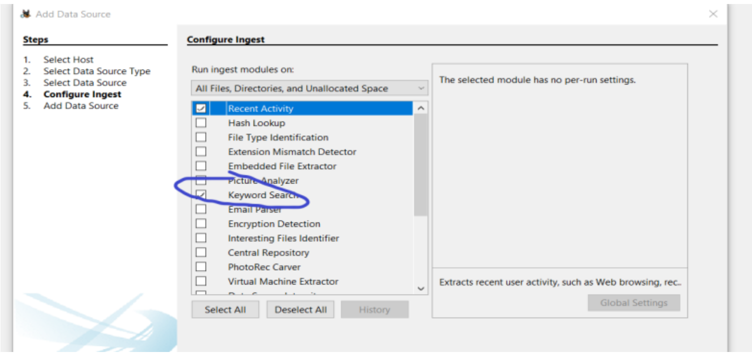
Sector size: Auto Detect

Look in: KaliShared

dswindowsre.raw.001

10/10/2023, 12:46PM, add data source

Step 4: After Another feature that is specific to the Windows version of Autposy is ingest modules. These are different configurations that can be run before the ingest to look for certain things during the ingest. In this scenario, we only use the “Keyword Search” and “Recent Activity” modules. This will give us more specific information for these modules but will also include other basic information about all the files in the image file, which is perfect for this investigation.



Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. **Configure Ingest**
5. Add Data Source

Configure Ingest

Run ingest modules on: All Files, Directories, and Unallocated Space

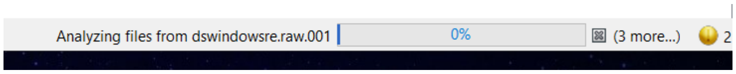
☑ Recent Activity
□ Hash Lookup
□ File Type Identification
□ Extension Mismatch Detector
□ Embedded File Extractor
□ Picture Analyzer
☑ Keyword Search
□ Email Parser
□ Encryption Detection
□ Interesting Files Identifier
□ Central Repository
□ PhotoRec Carver
□ Virtual Machine Extractor

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, rec..

10/10/2023, 12:48PM, configure ingest modules

Step 5: After the ingest modules are configured, Autopsy will begin the ingest of the image file. This is a very long process, even with only two ingest modules selected. It took about two hours for the Windows 10 forensic machine to ingest the image file, which was sized around 80GB.



Analyzing files from dswindowsre.raw.001 0% (3 more...) 2

10/10/2023, 12:49PM, ingest begins

(End of Windows 10 Forensic Machine Preliminary Analysis)

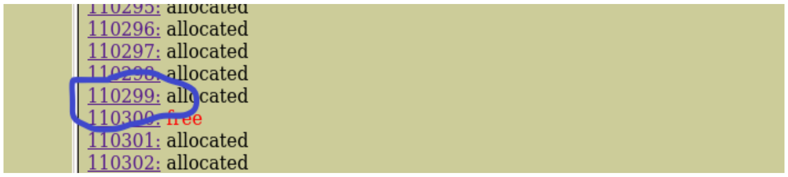
File System Metadata Analysis

Commented [SJ6]: Forensic Examiner Agent Garrett Stokes, 10/14/2023, 4:35PM, Austin PD Headquarters

The file system metadata analysis is the first real look into the suspect image. It took place on 10/14/2023, starting at 4:35PM, and was conducted by forensic agent Garrett Stokes.

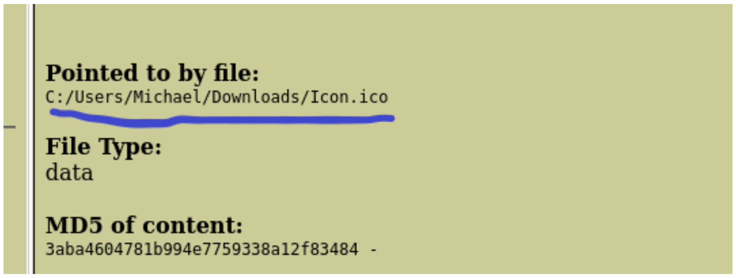
In the duration of the file system analysis, metadata for MFT entries, which are records of each file and directory on an NTFS volume, were analyzed to find general information regarding the file system as well as any suspicious behavior with files and directories on the suspect image drive.

To begin, an allocated MFT entry is analyzed, which indicates the entry is in use, and is associated with specific files or directories on the suspect image drive. The first MFT entry agent Stokes examined was 110299.



```
110295: allocated
110296: allocated
110297: allocated
110298: allocated
110299: allocated
110300: free
110301: allocated
110302: allocated
```

10/14/2023, 4:35PM, MFT Entry 110299



Pointed to by file:
C:/Users/Michael/Downloads/Icon.ico

File Type:
data

MD5 of content:
3aba4604781b994e7759338a12f83484 -

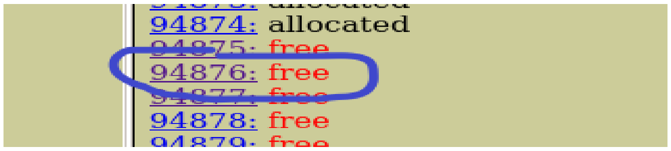
10/14/2023, 4:36PM, MFT Entry 110299 file pointer to /Users/Michael/Downloads/Icon.ico

Upon further analysis, there are some key takeaways that help further the investigation.

1. The MFT entry 110299 corresponds to a file named “Icon.ico” and is located at "C:/Users/Michael/Downloads/Icon.ico.". It is classified as a data file.
2. The file was created on November 10, 2023, at 15:33:52 (EST), last modified on November 10, 2023, at 15:33:52 (EST), and last accessed on November 24, 2023, at 23:30:03 (EST).
3. The file has an allocated size of 172,032 bytes and an actual size of 171,867 bytes. It contains various attributes, including standard information, file name, object ID, and data attributes.

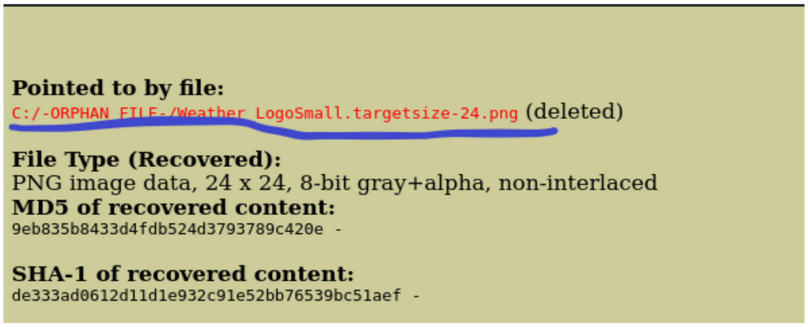
Taking everything into account, the fact that this file is identified as a data file suggests that it contains binary / non-textual information, such as that of an icon file would include. This suggests that Michael may have downloaded an icon file and was altering images within the system.

The next MFT entry analyzed by agent Stokes was that of a “free” entry, indicating that the file was deleted.



```
94873: allocated
94874: allocated
94875: free
94876: free
94877: free
94878: free
94879: free
```

10/14/2023, 4:51PM, MFT Entry 94876



Pointed to by file:
C:/-ORPHAN_FILE-/Weather_LogoSmall.targetsize-24.png (deleted)

File Type (Recovered):
PNG image data, 24 x 24, 8-bit gray+alpha, non-interlaced
MD5 of recovered content:
9eb835b8433d4fdb524d3793789c420e -

SHA-1 of recovered content:
de333ad0612d11d1e932c91e52bb76539bc51aef -

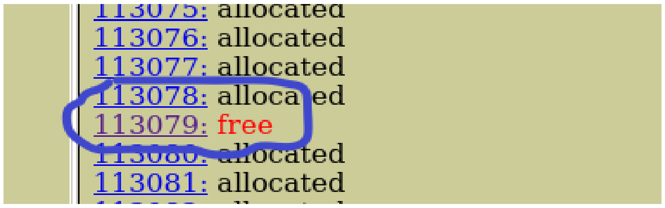
10/14/2023, 4:52PM, MFT Entry 94876, Weather Logo deleted

The three notes made by agent Stokes are as follows:

1. The MFT entry (94876) corresponds to a file named "Weather_LogoSmall.targetsize-24.png" located at "C:/-ORPHAN_FILE-/Weather_LogoSmall.targetsize-24.png (deleted)." It is identified as a PNG image.
2. The file was created on November 10, 2023, at 17:20:34 (EST), last modified on November 10, 2023, at 17:20:34 (EST), and last accessed on November 10, 2023, at 17:20:34 (EST). Notably, the MFT Modified timestamp is updated more recently on November 24, 2023, at 01:03:41 (EST).
3. The file has an allocated size of 0 bytes, indicating that it is not taking up space in the file system, but its actual size is also 0 bytes. The presence of an EA (Extended Attribute) and EA_INFORMATION attributes may suggest additional metadata associated with the file.

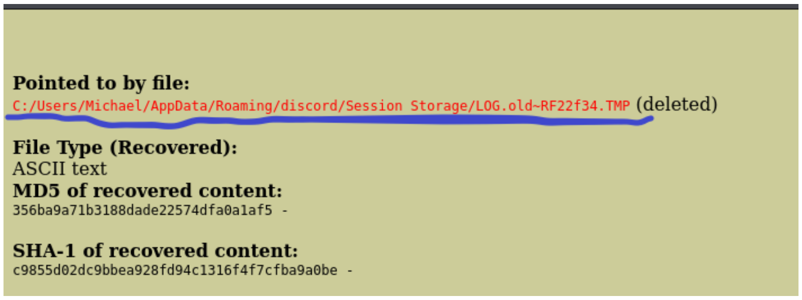
This deleted file is somewhat like the previously analyzed MFT entry, which involved an icon file, but this time it is a deleted .png image which is no longer accessible on the system. It is a .png image related to weather, perhaps the user (Michael) was doing something on the system related to adding /altering images related to weather.

The third analyzed MFT entry is yet again another deleted entry, which provides the team with valuable insight for further analysis.



```
113075: allocated
113076: allocated
113077: allocated
113078: allocated
113079: free
113080: allocated
113081: allocated
```

10/14/2023, 5:15PM, MFT Entry 113079



Pointed to by file:
C:/Users/Michael/AppData/Roaming/discord/Session Storage/LOG.old~RF22f34.TMP (deleted)

File Type (Recovered):
ASCII text
MD5 of recovered content:
356ba9a71b3188dade22574dfa0a1af5 -

SHA-1 of recovered content:
c9855d02dc9bbea928fd94c1316f4f7cfba9a0be -

10/14/2023, 5:17PM, MFT Entry 113079, Discord

Notes on this MFT entry:

1. The MFT entry (113079) corresponds to a file named "LOG.oldRF22f34.TMP" located at "C:/Users/Michael/AppData/Roaming/discord/Session Storage/LOG.oldRF22f34.TMP (deleted)." It is identified as an ASCII text file.
2. The file was created on November 10, 2023, at 15:48:08 (EST), last modified on November 23, 2023, at 21:15:59 (EST), and last accessed on November 23, 2023, at 21:15:59 (EST). The MFT Modified timestamp is updated on November 24, 2023, at 01:04:34 (EST).
3. The file has an allocated size of 280 bytes, and its actual size is also 280 bytes. It contains Standard Information, File Name, and Data attributes. The Data attribute indicates that the file is of type ASCII text.

Most importantly this deleted file seems to be some kind of log generated from the software Discord, a popular communications app used online. This discovery is huge, as the team can analyze Michael's discord for information as well as potential evidence.

The File System Analysis portion of the investigation, conducted by forensic analysis agent Garrett Stokes, is concluded at this point. There are a few major takeaways from this file system analysis for the remainder of the investigation

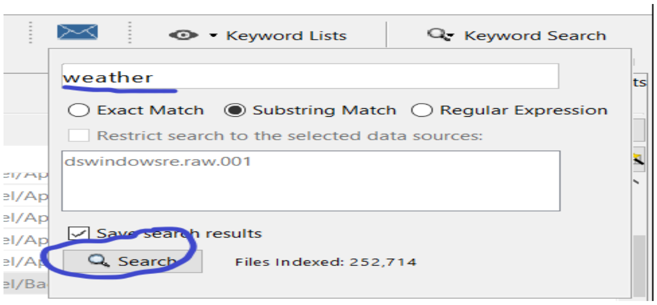
- There was activity with icon and .png files under the user account "Michael". With the .png image, it was related to "weather".
- Discord is installed and operating under the user account "Michael".

Keyword Search

Commented [SJ7]: Forensic Examiner Agent Garrett Stokes, 10/17/2023, 7:01AM, Austin PD Headquarters

On 10/17/2023, starting at 7:01AM, Forensic Agent Garrett Stokes conducted a keyword search on the image file, using Autopsy on Windows, based on the findings from the previous File system metadata analysis.

Based on previous findings, Agent Stokes knew there was something going on related to weather, so that is the keyword that was used for the search.



weather

○ Exact Match ● Substring Match ○ Regular Expression

□ Restrict search to the selected data sources:

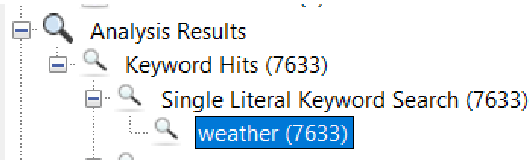
dswindowsre.raw.001

☑ Save search results

Files Indexed: 252,714

10/17/2023, 7:01AM, “weather” keyword search

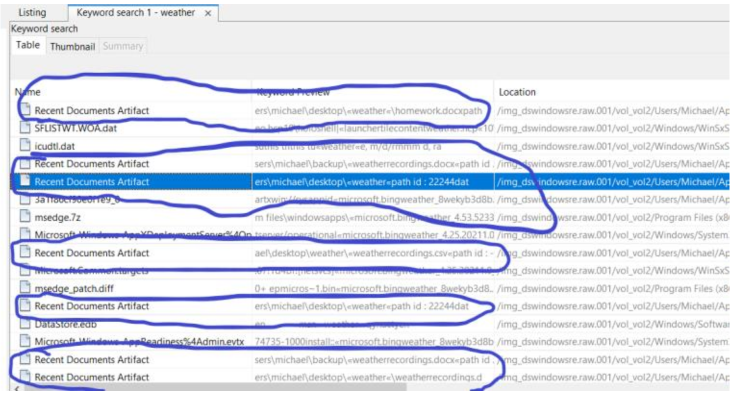
After the keyword search for “Weather” was complete, there was a total of 7633 hits. Agent Stokes began to analyze the findings.



- Analysis Results
  - Keyword Hits (7633)
    - Single Literal Keyword Search (7633)
      - weather (7633)

10/17/2023, 7:11AM, “weather” keyword search hits (7633)

Interestingly enough, immediately there were “Recent Document Artifacts” found in the search, all of them related to activity with various files related to “weather”.



Listing | Keyword search 1 - weather

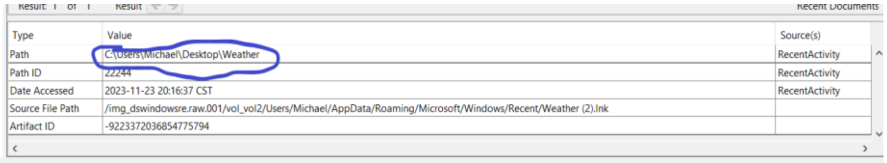
Keyword search

Table | Thumbnail | Summary

Name	Keyword Preview	Location
Recent Documents Artifact	ers\michael\desktop\«weather«\homework.docxpath	/img_dswindowsre.raw.001/vol_vol2/Users/Michael/Ap
SFLISTWT.WOA.dat	[illegible]oshell|«launchertilecontent[illegible]cp«10	/img_dswindowsre.raw.001/vol_vol2/Windows/WinSxS
icudtl.dat	[illegible] tt«weather«e, m/d/mmm d, ra	/img_dswindowsre.raw.001/vol_vol2/Windows/WinSxS
Recent Documents Artifact	sers\michael\backup\«weatherrecordings.docx«path id .	/img_dswindowsre.raw.001/vol_vol2/Users/Michael/Ap
Recent Documents Artifact	ers\michael\desktop\«weather«path id : 22244dat	/img_dswindowsre.raw.001/vol_vol2/Users/Michael/Ap
3a118bcf90e0f1e9_0	artxwin[illegible]appid«microsoft.bingweather_8wekyb3d8b.	/img_dswindowsre.raw.001/vol_vol2/Users/Michael/Ap
msedge.7z	m files\windowsapps\«microsoft.bingweather_4.53.5233	/img_dswindowsre.raw.001/vol_vol2/Program Files (x8
Microsoft-Windows-AppXDeploymentServer%4Op	tserver/operational«microsoft.bingweather_4.25.20211.0	/img_dswindowsre.raw.001/vol_vol2/Windows/System
Recent Documents Artifact	ael\desktop\weather\«weatherrecordings.csv«path id : -	/img_dswindowsre.raw.001/vol_vol2/Users/Michael/Ap
Microsoft.Commontargets	[illegible]	/img_dswindowsre.raw.001/vol_vol2/Windows/WinSxS
msedge_patch.diff	0+ epmicros~1.bin«microsoft.bingweather_8wekyb3d8..	/img_dswindowsre.raw.001/vol_vol2/Program Files (x8
Recent Documents Artifact	ers\michael\desktop\«weather«path id : 22244dat	/img_dswindowsre.raw.001/vol_vol2/Users/Michael/Ap
DataStore.edb	[illegible]	/img_dswindowsre.raw.001/vol_vol2/Windows/Softwai
Microsoft-Windows-AppReadiness%4Admin.evtx	74735-1000install::«microsoft.bingweather_8wekyb3d8b	/img_dswindowsre.raw.001/vol_vol2/Windows/System
Recent Documents Artifact	sers\michael\backup\«weatherrecordings.docx«path id .	/img_dswindowsre.raw.001/vol_vol2/Users/Michael/Ap
Recent Documents Artifact	ers\michael\desktop\«weather«\weatherrecordings.d	/img_dswindowsre.raw.001/vol_vol2/Users/Michael/Ap

10/17/2023, 7:23AM, recent document artifacts

Agent Stokes checked the path in which these Document Artifacts were pointing to and found them to be pointing to the directory "C:\Users\Michael\Desktop\Weather". At this point, it was time to investigate this directory and see if there is something of value to analyze in this directory.

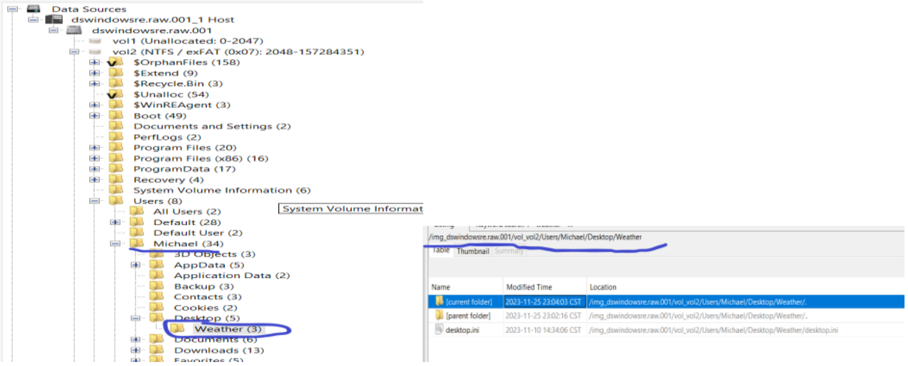


Result: 1 of 1 Result | Recent Documents

Type	Value	Source(s)
Path	C:\Users\Michael\Desktop\Weather	RecentActivity
Path ID	22244	RecentActivity
Date Accessed	2023-11-23 20:16:37 CST	RecentActivity
Source File Path	/img_dswindowsre.raw.001/vol_vol2/Users/Michael/AppData/Roaming/Microsoft/Windows/Recent/Weather (2).lnk	
Artifact ID	-9223372036854775794	

10/17/2023, 7:23AM, recent document artifact directory path

After navigating to the Weather folder located on the desktop, there were no files related to weather in the folder. The Folder was empty. This indicates that all the artifacts were remnants of deleted files, and likely the suspect was trying to cover his tail.



```
Data Sources
  dswindowsre.raw.001_1 Host
    dswindowsre.raw.001
      vol1 (Unallocated: 0-2047)
      vol2 (NTFS / exFAT (0x07): 2048-157284351)
        $OrphanFiles (158)
        $Extend (9)
        $Recycle.Bin (3)
        $Unalloc (54)
        $WinREAgent (3)
        Boot (49)
        Documents and Settings (2)
        PerfLogs (2)
        Program Files (20)
        Program Files (x86) (16)
        ProgramData (17)
        Recovery (4)
        System Volume Information (6)
        Users (8)
          All Users (2)
          Default (28)
          Default User (2)
          Michael (34)
            3D Objects (3)
            AppData (5)
            Application Data (2)
            Backup (3)
            Contacts (3)
            Cookies (2)
            Desktop (5)
              Weather (3)
            Documents (6)
            Downloads (13)
            Favorites (5)
```

System Volume Informat

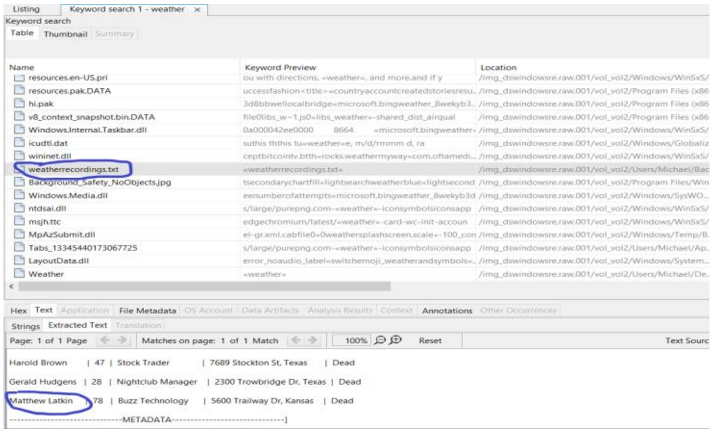
/img_dswindowsre.raw.001/vol_vol2/Users/Michael/Desktop/Weather

Table | Thumbnail | Summary

Name	Modified Time	Location
[current folder]	2023-11-25 23:04:03 CST	/img_dswindowsre.raw.001/vol_vol2/Users/Michael/Desktop/Weather/.
[parent folder]	2023-11-25 23:02:16 CST	/img_dswindowsre.raw.001/vol_vol2/Users/Michael/Desktop/Weather/..
desktop.ini	2023-11-10 14:34:06 CST	/img_dswindowsre.raw.001/vol_vol2/Users/Michael/Desktop/Weather/desktop.ini

10/17/2023, 7:29AM, checking the path for any files, no results

At this point, there is no concrete evidence, but there is a highly suspicious activity going on in this Weather Folder on the desktop on Michael's user account. Agent stokes continued to analyze findings of the keyword search and found a much more concrete piece of evidence. Further down the long list of results, the agent locates a file called "weatherrecordings.txt", and upon examining the file there are contents including names, age, profession, address, and status. This is direct evidence and includes information of victims that have been found dead by police.

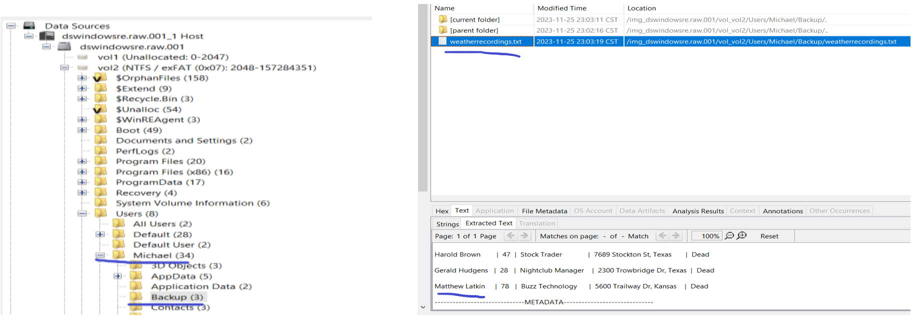


Name	Keyword Preview	Location
resources.en-US.pri	ou with directions, «weather«, and more.and if y	/img_dswindowsre.raw.001/vol_vol2/Windows/WinSxS/
resources.pak.DATA	uccessfashion<title>«countryaccountcreatedstoriesresu...	/img_dswindowsre.raw.001/vol_vol2/Program Files (x86
hi.pak	3d8bbwellocalbridge«microsoft.bingweather_8wekyb3...	/img_dswindowsre.raw.001/vol_vol2/Program Files (x86
v8_context_snapshot.bin.DATA	file0libs_w~1.js0«libs_weather«-shared_dist_airqual	/img_dswindowsre.raw.001/vol_vol2/Program Files (x86
Windows.Internal.Taskbar.dll	0a000042ee0000 8664 «microsoft.bingweather«	/img_dswindowsre.raw.001/vol_vol2/Windows/WinSxS/
icudtl.dat	suthis ththis tu«weather«e, m/d/rmmm d, ra	/img_dswindowsre.raw.001/vol_vol2/Windows/Globaliz
wininet.dll	ceptbitcointv.btth«rocks.weathermyway«com.oftamedi...	/img_dswindowsre.raw.001/vol_vol2/Windows/WinSxS/
weatherrecordings.txt	«weatherrecordings.txt«	/img_dswindowsre.raw.001/vol_vol2/Users/Michael/Bac
Background_Safety_NoObjects.jpg	tsecondarychartfill«lightsearchweatherblue«lightsecond	/img_dswindowsre.raw.001/vol_vol2/Program Files/Win
Windows.Media.dll	eenumberofattempts«microsoft.bingweather_8wekyb3d	/img_dswindowsre.raw.001/vol_vol2/Windows/SysWO...
ntdsai.dll	s/large/purepng.com-«weather«-iconsymbolsiconsapp	/img_dswindowsre.raw.001/vol_vol2/Windows/WinSxS/
msjh.ttc	edgechromium/latest/«weather«-card-wc-init-accoun	/img_dswindowsre.raw.001/vol_vol2/Windows/WinSxS/
MpAzSubmit.dll	el-gr.xml.cabfile0«0weathersplashscreen.scale«-100_con	/img_dswindowsre.raw.001/vol_vol2/Windows/Temp/B...
Tabs_13345440173067725	s/large/purepng.com-«weather«-iconsymbolsiconsapp	/img_dswindowsre.raw.001/vol_vol2/Users/Michael/Ap...
LayoutData.dll	error_noaudio_label«switchemoji_weatherandsymbols«...	/img_dswindowsre.raw.001/vol_vol2/Windows/System...
Weather	«weather«	/img_dswindowsre.raw.001/vol_vol2/Users/Michael/De...

```
Harold Brown    | 47 | Stock Trader       | 7689 Stockton St, Texas    | Dead
Gerald Hudgens  | 28 | Nightclub Manager  | 2300 Trowbridge Dr, Texas | Dead
Matthew Latkin  | 78 | Buzz Technology    | 5600 Trailway Dr, Kansas   | Dead
-----------------------------METADATA-----------------------------]
```

10/17/2023, 7:51AM, further analysis of keyword search results, suspicious file located

After this, the agent browses to the directory in which this file resides, in "C:\Users\Michael\Backup". It seems that this file was a last resort for Michael that he could see when needed, but perhaps he forgot this file existed as he did not delete it off the system before the device was seized, unlike the other files that could not be found directly within the file system hierarchy.



```
Data Sources
  dswindowsre.raw.001_1 Host
    dswindowsre.raw.001
      vol1 (Unallocated: 0-2047)
      vol2 (NTFS / exFAT (0x07): 2048-157284351)
        $OrphanFiles (158)
        $Extend (9)
        $Recycle.Bin (3)
        $Unalloc (54)
        $WinREAgent (3)
        Boot (49)
        Documents and Settings (2)
        PerfLogs (2)
        Program Files (20)
        Program Files (x86) (16)
        ProgramData (17)
        Recovery (4)
        System Volume Information (6)
        Users (8)
          All Users (2)
          Default (28)
          Default User (2)
          Michael (34)
            3D Objects (3)
            AppData (5)
            Application Data (2)
            Backup (3)
            Contacts (3)
```

Name	Modified Time	Location
[current folder]	2023-11-25 23:03:11 CST	/img_dswindowsre.raw.001/vol_vol2/Users/Michael/Backup/.
[parent folder]	2023-11-25 23:02:16 CST	/img_dswindowsre.raw.001/vol_vol2/Users/Michael/Backup/..
weatherrecordings.txt	2023-11-25 23:03:19 CST	/img_dswindowsre.raw.001/vol_vol2/Users/Michael/Backup/weatherrecordings.txt

```
Harold Brown    | 47 | Stock Trader       | 7689 Stockton St, Texas    | Dead
Gerald Hudgens  | 28 | Nightclub Manager  | 2300 Trowbridge Dr, Texas | Dead
Matthew Latkin  | 78 | Buzz Technology    | 5600 Trailway Dr, Kansas   | Dead
-----------------------------METADATA-----------------------------
```

10/17/2023, 7:55AM, confirming existence of suspicious file, and displaying of evidence

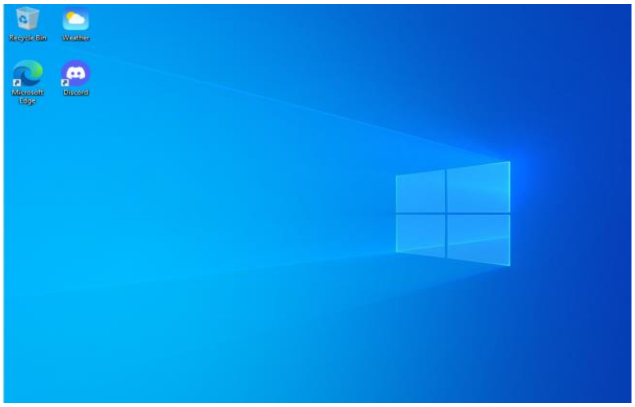
At this point in the analysis, there was no point in conducting a deleted file recovery retrieval on the weather folder, as this finding provided sufficient evidence that Michael was highly likely to be involved in this case.

Discord Analysis

Commented [SJ8]: Forensic Examiner Agent Michael Bahre, 10/21/2023, 9:07AM, Austin PD Headquarters

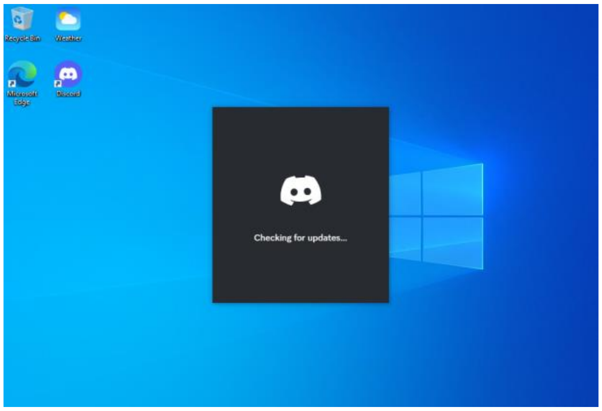
The third and final portion of the analysis is conducted by Agent Bahre, started at 9:07AM, 10/21/2023. This analysis was performed hands on with a copy of the suspect machine, through VirtualBox. Agent Bahre will be analyzing the suspects Discord application.

To begin the analysis of the Discord application, Agent Bahre launches the .vdi file which was setup through virtual box done during the examination portion of the investigation.



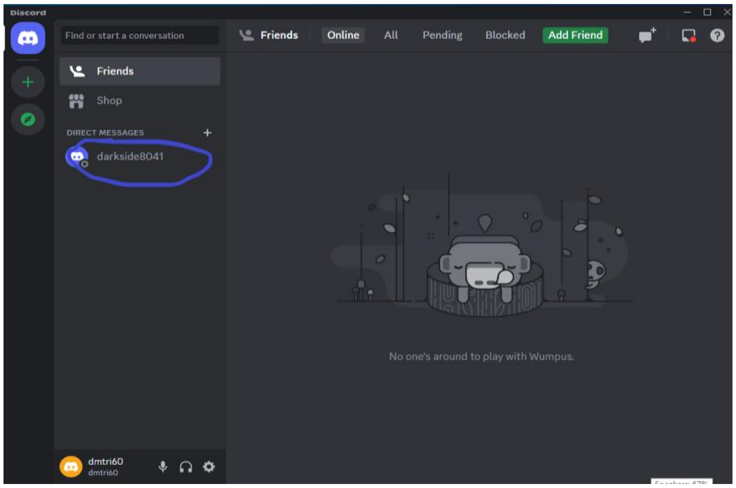
10/21/2023, 9:07AM, initial launch of copy of suspect image

An exact copy of the suspect image file has now been booted, and agent Bahre is on the machine exactly at the point where Michael Smirnov left off. To Agent Bahre's surprise, the Discord application automatically launches.



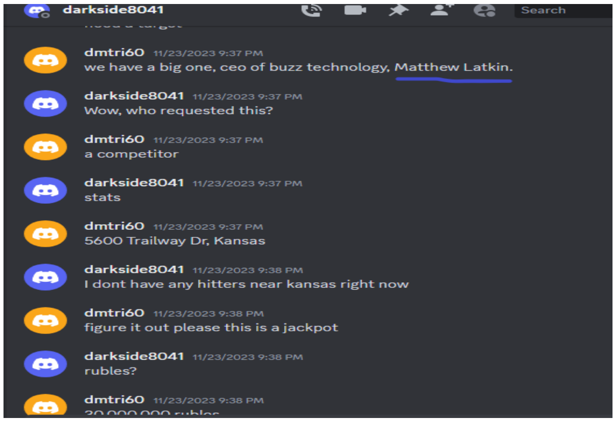
10/21/2023, 9:08AM, discord application auto launch on startup

At this point, it seems that Discord is configured as an application that boots upon startup of the machine. This leads Agent Bahre straight into Michael's Discord application, with direct access to messages.



10/21/2023, 9:12AM, discord application fully launches

Once the application is done loading, Agent Bahre notices there is only one user Michael has direct messages with. This user is named "darkside8041". Agent Bahre opens the direct message, and finds messages exchanged between the two that are discussing exact details of the victims, methods to kill them, and details of pay in rubles.



need a target

dmtri60 11/23/2023 9:37 PM
we have a big one, ceo of buzz technology, Matthew Latkin.

darkside8041 11/23/2023 9:37 PM
Wow, who requested this?

dmtri60 11/23/2023 9:37 PM
a competitor

darkside8041 11/23/2023 9:37 PM
stats

dmtri60 11/23/2023 9:37 PM
5600 Trailway Dr, Kansas

darkside8041 11/23/2023 9:38 PM
I dont have any hitters near kansas right now

dmtri60 11/23/2023 9:38 PM
figure it out please this is a jackpot

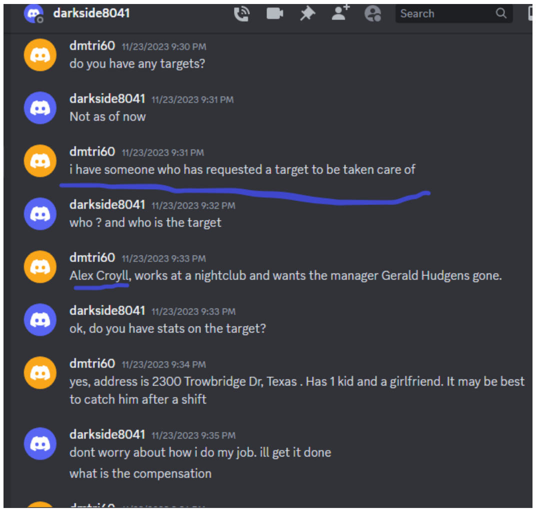
darkside8041 11/23/2023 9:38 PM
rubles?

dmtri60 11/23/2023 9:38 PM
30,000,000 rubles

10/21/2023, 9:18AM, messages discussing Matthew Latkin

In this specific portion, Michael, whose user account is named "dmtri60", is talking with "darkside8041", about the prime victim Matthew Latkin, telling his address, and discussing the pay, according to be

30,000,000 rubles, which translates to $333,000 USD. Agent Bahre continues to look through the messages and finds information related to another victim. Alex Croyll. The two suspects discuss the "target", his profession at a nightclub, and the method recommended to kill Croyll, as well as the compensation for the job.



dmtri60 11/23/2023 9:30 PM
do you have any targets?

darkside8041 11/23/2023 9:31 PM
Not as of now

dmtri60 11/23/2023 9:31 PM
i have someone who has requested a target to be taken care of

darkside8041 11/23/2023 9:32 PM
who ? and who is the target

dmtri60 11/23/2023 9:33 PM
Alex Croyll, works at a nightclub and wants the manager Gerald Hudgens gone.

darkside8041 11/23/2023 9:33 PM
ok, do you have stats on the target?

dmtri60 11/23/2023 9:34 PM
yes, address is 2300 Trowbridge Dr, Texas . Has 1 kid and a girlfriend. It may be best to catch him after a shift

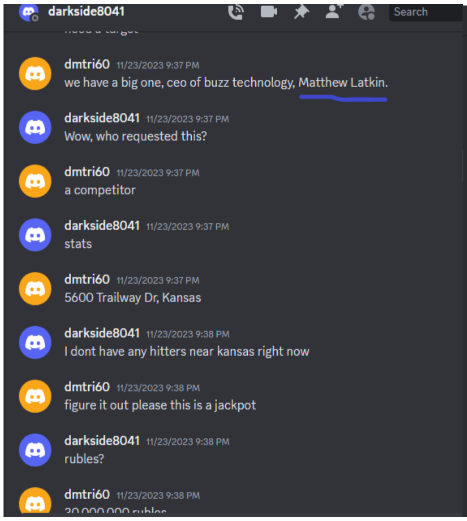
darkside8041 11/23/2023 9:35 PM
dont worry about how i do my job. ill get it done
what is the compensation

10/21/2023, 9:30AM, messages discussing Alex Croyll

At this point, Agent Bahre has discovered direct evidence on the suspect's machine, in which he discusses the murders of the victims in the case.

Forensic Evidence

Commented [SJ9]: Legal Analyst Marcus Harmon, 10/30/2023, 3:00PM, Austin PD Headquarters



need a target

dmtri60 11/23/2023 9:37 PM
we have a big one, ceo of buzz technology, Matthew Latkin.

darkside8041 11/23/2023 9:37 PM
Wow, who requested this?

dmtri60 11/23/2023 9:37 PM
a competitor

darkside8041 11/23/2023 9:37 PM
stats

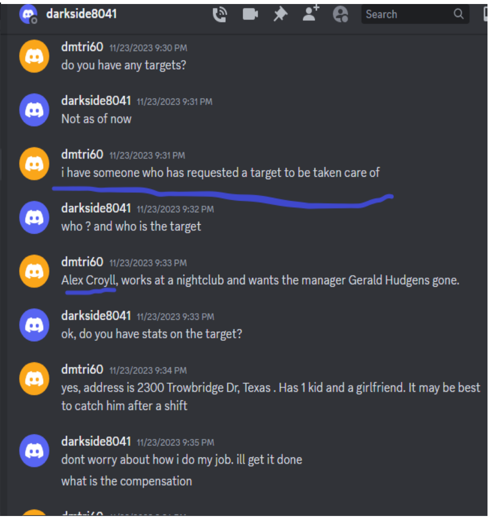
dmtri60 11/23/2023 9:37 PM
5600 Trailway Dr, Kansas

darkside8041 11/23/2023 9:38 PM
I dont have any hitters near kansas right now

dmtri60 11/23/2023 9:38 PM
figure it out please this is a jackpot

darkside8041 11/23/2023 9:38 PM
rubles?

dmtri60 11/23/2023 9:38 PM
30,000,000 rubles



dmtri60 11/23/2023 9:30 PM
do you have any targets?

darkside8041 11/23/2023 9:31 PM
Not as of now

dmtri60 11/23/2023 9:31 PM
i have someone who has requested a target to be taken care of

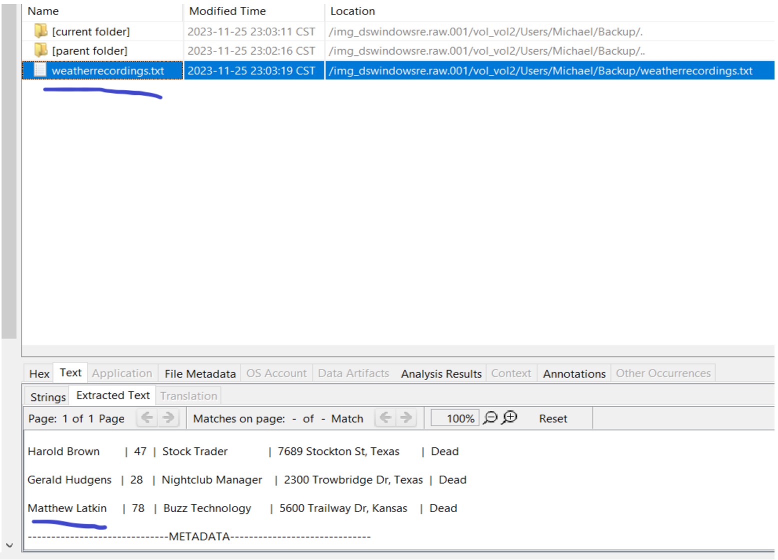
darkside8041 11/23/2023 9:32 PM
who ? and who is the target

dmtri60 11/23/2023 9:33 PM
Alex Croyll, works at a nightclub and wants the manager Gerald Hudgens gone.

darkside8041 11/23/2023 9:33 PM
ok, do you have stats on the target?

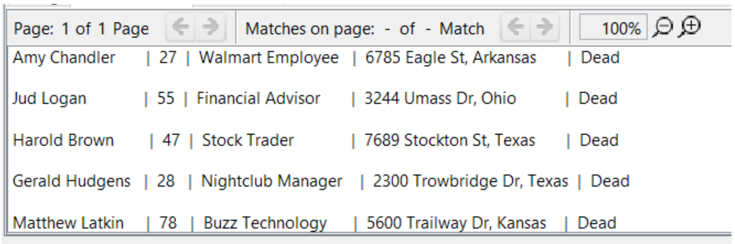
dmtri60 11/23/2023 9:34 PM
yes, address is 2300 Trowbridge Dr, Texas . Has 1 kid and a girlfriend. It may be best to catch him after a shift

darkside8041 11/23/2023 9:35 PM
dont worry about how i do my job. ill get it done
what is the compensation



Name	Modified Time	Location
[current folder]	2023-11-25 23:03:11 CST	/img_dswindowsre.raw.001/vol_vol2/Users/Michael/Backup/.
[parent folder]	2023-11-25 23:02:16 CST	/img_dswindowsre.raw.001/vol_vol2/Users/Michael/Backup/..
weatherrecordings.txt	2023-11-25 23:03:19 CST	/img_dswindowsre.raw.001/vol_vol2/Users/Michael/Backup/weatherrecordings.txt

```
Harold Brown     | 47 | Stock Trader       | 7689 Stockton St, Texas     | Dead

Gerald Hudgens  | 28  | Nightclub Manager  | 2300 Trowbridge Dr, Texas | Dead

Matthew Latkin   | 78  | Buzz Technology    | 5600 Trailway Dr, Kansas   | Dead

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



```
Amy Chandler     | 27 | Walmart Employee   | 6785 Eagle St, Arkansas      | Dead
Jud Logan        | 55 | Financial Advisor  | 3244 Umass Dr, Ohio          | Dead
Harold Brown     | 47 | Stock Trader       | 7689 Stockton St, Texas      | Dead
Gerald Hudgens   | 28 | Nightclub Manager  | 2300 Trowbridge Dr, Texas | Dead
Matthew Latkin   | 78 | Buzz Technology    | 5600 Trailway Dr, Kansas    | Dead
```

These messages show that Michael can be charged with a decent number of crimes, not only has he broken regular laws, but he has also broken cyber laws. The main laws that he will be counted on are being an accomplice to a murder, solicitation to commit murder, criminal attempt, concealing a crime. The cyber laws that Michael committed go as follows; conspiracy to commit a cybercrime, use of electronic information for criminal activity, and evidence of criminal intent. Our forensics team worked diligently on this case, and we believe that we have the right evidence to prove that Michael Smirnov is guilty on all these counts, that is not our job though.

References

https://www.google.com/imgres?imgurl=https%3A%2F%2Fnewschannel20.com%2Fresources%2Fmedia%2F675aed3a-84fb-4642-9152-0f62a2e16539-medium16x9_IMG_2390.jpg%3F1647044567166&tbnid=qmObkevdVouNpM&vet=12ahUKEwih3sii3_eCAxWDx8kDHXnhDn4QMyg1egUIARCmAQ..i&imgrefurl=https%3A%2F%2Fnewschannel20.com%2Fnews%2Flocal%2Fspringfield-police-using-forensic-database-to-link-crimes-find-leads&docid=EL3jl69gCnxXNM&w=648&h=365&q=police%20handling%20evidence%20of%20a%20computer&ved=2ahUKEwih3sii3_eCAxWDx8kDHXnhDn4QMyg1egUIARCmAQ

https://www.google.com/url?sa=i&url=https%3A%2F%2Fdigital.library.unt.edu%2Fark%3A%2F67531%2Fmetadc949124%2Fm1%2F253%2F&psig=AOvVaw2OLPg4goq5ZJ0Dswt1Yiye&ust=1701846789270000&source=images&cd=vfe&opi=89978449&ved=0CBIQjRxqFwoTCNj42bzf94IDFQAAAAAdAAAAABAE