LONE WOLF SCENARIO

ABOUT THIS DOCUMENT

The document presents a methodology to process the **Lone Wolfe** digital forensics scenario using **Forensic Explorer**. Whilst it provides a structured framework, it is not presented as the sole comprehensive solution.

ABOUT THIS SCENARIO

The 2018 Lone Wolf scenario is a set of materials from a fictional seizure of a laptop of a fictional individual who was planning a mass shooting. In the scenario, the individual's brother alerted the police regarding the increasingly concerning behaviour of his brother. As a result of the alert, the police seized the brother's laptop. The laptop was then imaged with the FTK Imager program.

*This scenario was created by **Thomas Moore**, a student at **George Mason University**, as his final project for CRFS 780: Cloud Forensics, taught in Spring 2018 by Simson Garfinkel. The purpose of the scenario is to give students the chance to work with a dataset that contains cloud artifacts left on clients, and to provide a scenario with a realistic size.*

(Source: *https://digitalcorpora.org/corpora/scenarios/2018-lone-wolf-scenario/*)

FORENSIC IMAGE SOURCE

The forensic image, **LoneWolf.E01** (consisting of 9 segments) can be download from Digital Corpa: https://digitalcorpora.org/corpora/scenarios/2018-lone-wolf-scenario/

Copyright statement:
https://digitalcorpora.s3.amazonaws.com/corpora/scenarios/2018-lonewolf/Lone%20Wolf%20Scenario%20Copyright.pdf

OTHER ONLINE SOLUTIONS

Other online solutions and a teaching guide are available at:
https://digitalcorpora.org/corpora/scenarios/2018-lone-wolf-scenario/

THE SCENARIO

Jim Cloudy is a resident of Alexandria, VA. He is unhappy with the media's coverage of gun violence and what he perceived as an attack on the 2nd Amendment. Prior to the start of the scenario, Jim gets into a heated online argument with his brother, Paul Cloudy. During this argument Jim destroys his laptop by throwing it on the floor. Jim disposes of this laptop using his Apartment's trash chute, which is collected daily. Paul gives Jim one of his old laptops with the promise that he wouldn't break it. Paul wiped the laptop's drive prior to giving it to Jim. Jim does not encrypt any data and takes no overt steps to obfuscate data.

Jim is currently unemployed and has trouble sleeping, so he sometimes spends odd hours on the computer. While officially unemployed, the scenario briefly alludes to his marihuana growing activities, and an amassed savings of $325,000. Jim becomes increasingly irate concerning the growing support for "gun-control". Jim starts writing about his personal views and begins planning a "Lone Wolf" style attack. Jim wants to ensure his views are saved for posterity and his documents and plans can be accessed from anywhere; therefore, he uploads documents to a variety of cloud storage services. Prior to the planned date of the attack Jim gives Paul access to his cloud storage accounts. Paul is suspicious based on Jim's sudden decision to go on vacation and not come back. When Paul reads some of the documents he notifies police, and a Search Warrant of Jim's apartment is executed, and he is apprehended while talking to Paul online.

On 6 Apr 18, Special Agent Dickhaus requested a Digital Forensic Examination of a laptop computer to recover any and all information pertaining to allegations Mr. Jim Cloudy was planning to attack a town hall meeting held to discuss gun violence.

A Search Warrant was approved by Not A. REALJUDGE, United States Magistrate Judge, Eastern District of Virginia authorizing the search of Mr. Cloudy's residence, and the seizure and subsequent Digital Forensic Examination of digital media found within. Computer Forensic Analyst {your name here}, {your address here}, concurred the Search Warrant was legally sufficient to conduct the examination as requested within the Laboratory Examination Request.

THE QUESTIONS

1	***What is the Operating System and edition installed on the computer?***
2	***What is the computer name?***
3	***Who is the operating system registered owner and organization?***
4	***What time zone was the computer set to when it was imaged?***
5	***Was the system clock manually or automatically updated and how was this established?***
6	***Which user account logged on at 30 Mar 2018 at 03:27 UTC or 29 Mar 2018 at 23:27 local time)?***
7	***When was the computer last shutdown (date and time)?***
8	***Is a password required for the user account with a RID (Relative Identifier) of interest and how do you know this?***
9	***What is the Password Hint for the jcloudy user account?***
10	***What is the SSID of the wireless network that this computer was connected to?***

11	***True or false: There was an externally connected USB device attached to this computer?***
12	***What is the serial number, vendor and product identifier for any USB drive(s), identified within the Lone Wolf evidence file?***
13	***What file system does the volume that contains the operating system use?***
14	***Prior to being deleted, what was the original filename now referenced as $RYRY5PT.jpg?***
15	***When was the Chrome browser first used? Is this the same date as when the browser was installed and how do you know this?***

Create a forensic report that contains:

- Relevant documents (Word, PowerPoint, pictures, etc).
- Cloud storage services being used to store and synchronize documents in the cloud.
- Internet searches.
- Chats.
- Other items that you deem important.

PREPARING THE CASE IN FORENSIC EXPLORER

The following initial Forensic Explorer processing steps are recommended.

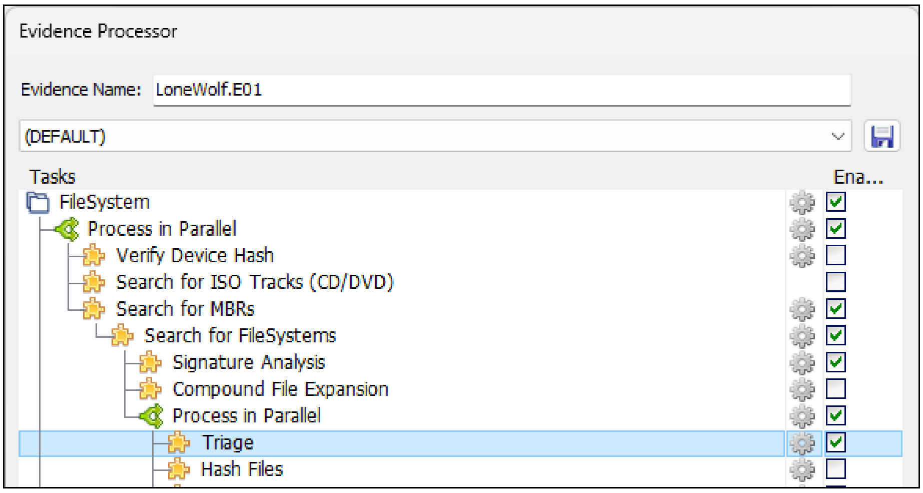
PREP: ADD EVIDENCE - LONEWOLF.E01

In the Forensic Explorer **Evidence module**:

1. Select the **New Case**.
2. Enter **investigator details** (if required) and a **case name**.
3. Click **Add Image**.
4. Add the evidence file **LoneWolf.E01**.

In the **Evidence Processor** window, add **Triage** to processing options. [Optional - See Triage below].

Figure 1: Running Triage from the Evidence Processor window.



Evidence Processor

Evidence Name: LoneWolf.E01

(DEFAULT)

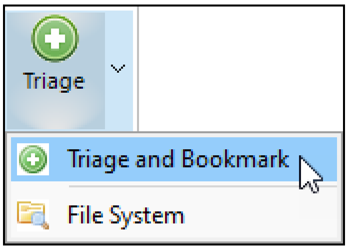
Tasks	Ena...
FileSystem	☑
Process in Parallel	☑
Verify Device Hash	□
Search for ISO Tracks (CD/DVD)	□
Search for MBRs	☑
Search for FileSystems	☑
Signature Analysis	☑
Compound File Expansion	□
Process in Parallel	☑
Triage	☑
Hash Files	□

PREP: TRIAGE AND BOOKMARK

Triage is a fast process that extracts and bookmarks common files and artifacts. These bookmarks are used to produce a **Triage Report** in the **Reports** module**.**

Triage can either be run when evidence is added, by selecting the Triage checkbox in the Evidence Processor window, or at any later time by selecting the **File System module > Toolbar > Triage > Triage and Bookmark.**

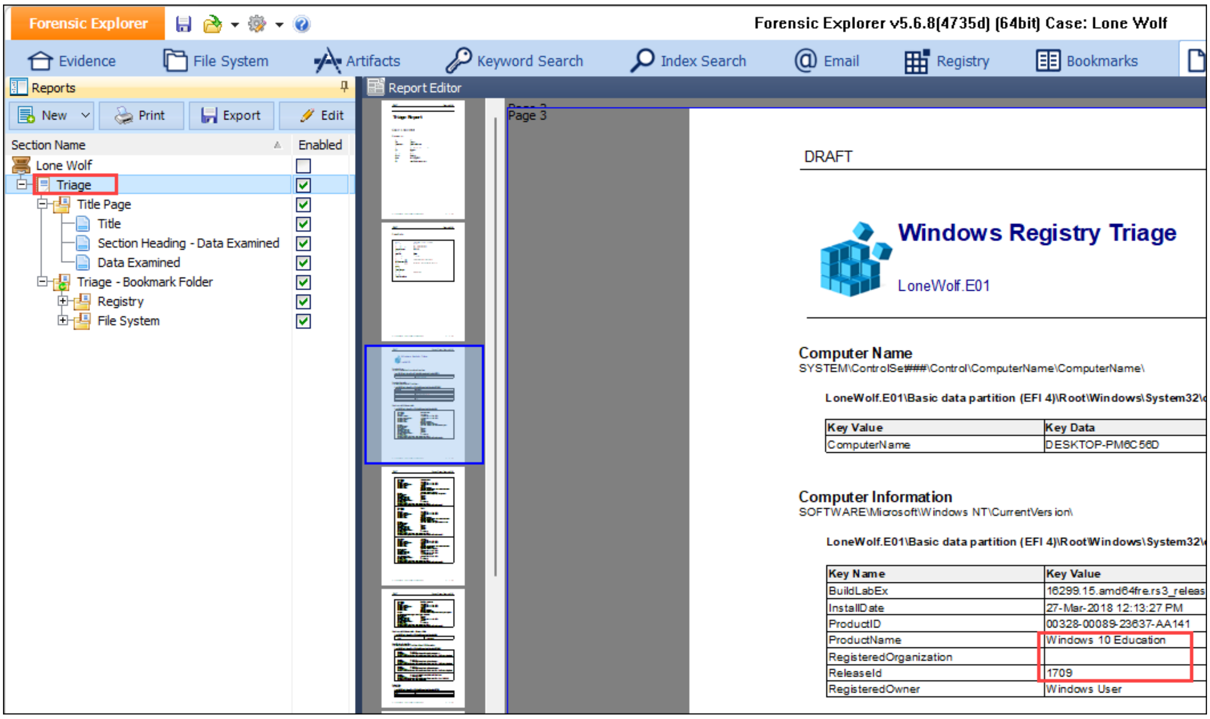
Figure 2: Launch Triage from File System module.



Reports module **Triage Report**:

1. Triage is the default report in the **Reports** Module. If the Triage report is not displayed, select **New > Triage (Default)** and it will be added to the tree.

Figure 3: Reports > Triage > Computer Information



Section Name	Enabled
Lone Wolf	□
Triage	☑
Title Page	☑
Title	☑
Section Heading - Data Examined	☑
Data Examined	☑
Triage - Bookmark Folder	☑
Registry	☑
File System	☑

DRAFT

Windows Registry Triage

LoneWolf.E01

Computer Name
SYSTEM\ControlSet###\Control\ComputerName\ComputerName\

LoneWolf.E01\Basic data partition (EFI 4)\Root\Windows\System32\

Key Value	Key Data
ComputerName	DESKTOP-PM6C56D

Computer Information
SOFTWARE\Microsoft\Windows NT\CurrentVersion\

LoneWolf.E01\Basic data partition (EFI 4)\Root\Windows\System32\

Key Name	Key Value
BuildLabEx	16299.15.amd64fre.rs3_releas
InstallDate	27-Mar-2018 12:13:27 PM
ProductID	00328-00089-23637-AA141
ProductName	Windows 10 Education
RegisteredOrganization	
ReleaseId	1709
RegisteredOwner	Windows User

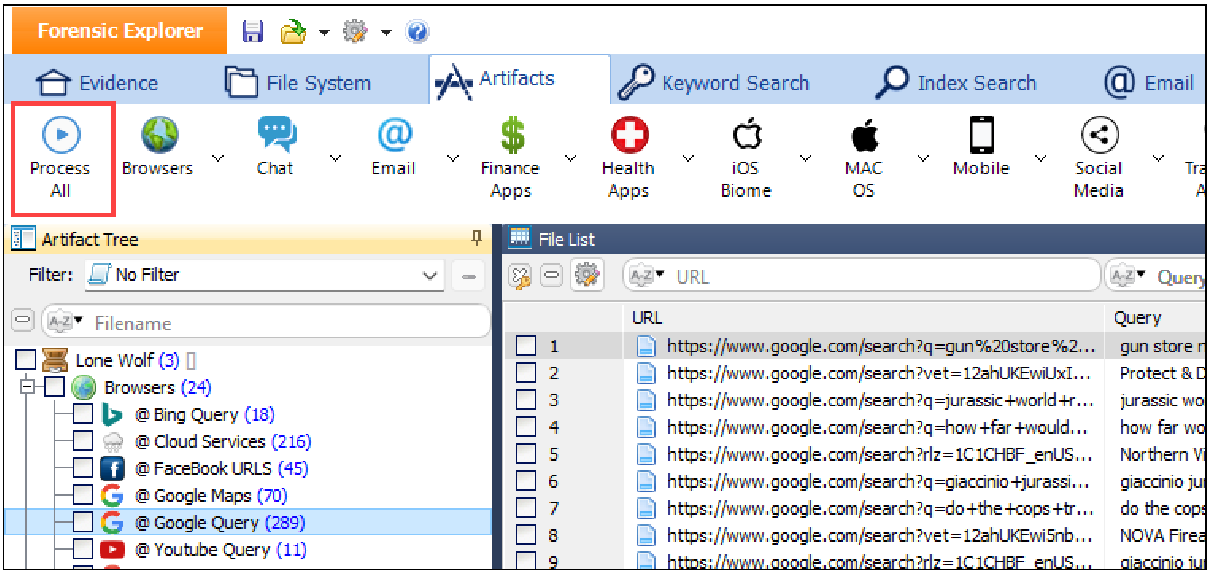
PREP: ARTIFACTS MODULE - POPULATE

The Artifacts module in Forensic Explorer is designed to make artifact records easily accessible by the forensic examiner.

To populate the Artifacts module:

1. In the **Artifacts** module, select the **Process All** button.

Figure 4: Artifacts > Process All



Filter: No Filter

- □ Lone Wolf (3)
  - □ Browsers (24)
    - □ @ Bing Query (18)
    - □ @ Cloud Services (216)
    - □ @ FaceBook URLS (45)
    - □ @ Google Maps (70)
    - □ @ Google Query (289)
    - □ @ Youtube Query (11)

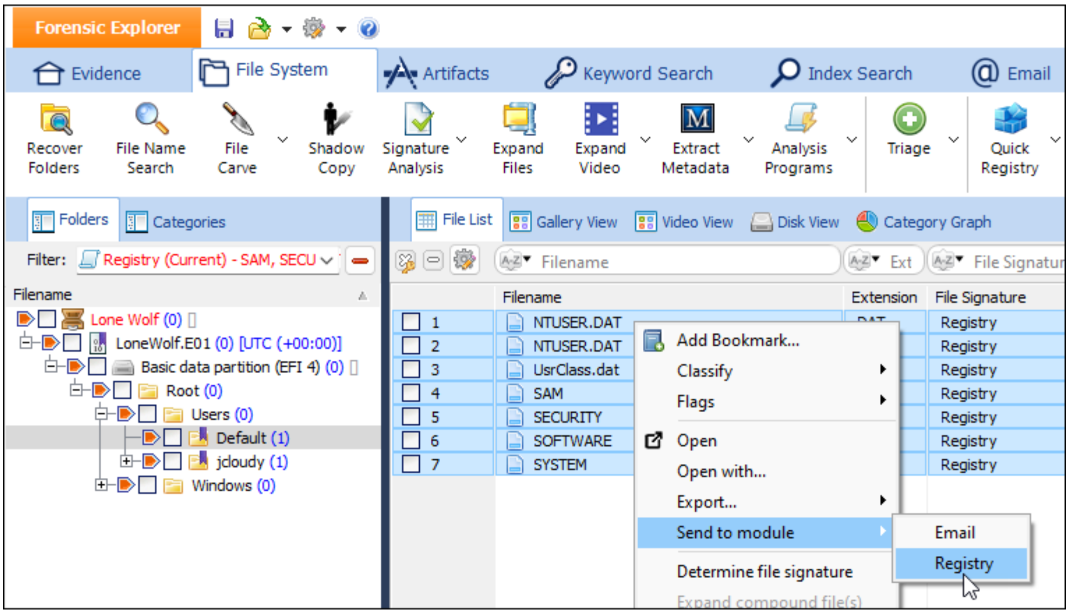
	URL	Query
□ 1	https://www.google.com/search?q=gun%20store%2...	gun store n
□ 2	https://www.google.com/search?vet=12ahUKEwiUxI...	Protect & D
□ 3	https://www.google.com/search?q=jurassic+world+r...	jurassic wo
□ 4	https://www.google.com/search?q=how+far+would...	how far wo
□ 5	https://www.google.com/search?rlz=1C1CHBF_enUS...	Northern Vi
□ 6	https://www.google.com/search?q=giaccinio+jurassi...	giaccinio ju
□ 7	https://www.google.com/search?q=do+the+cops+tr...	do the cops
□ 8	https://www.google.com/search?vet=12ahUKEwi5nb...	NOVA Firea
□ 9	https://www.google.com/search?rlz=1C1CHBF_enUS...	giaccinio ju

PREP: REGISTRY MODULE - POPULATE

To populate the Registry module:

1. In the **File System** module, **branch plate** [▶] the entire case.
2. Run a Registry folders filter.
3. Click in the **File List**, and then press **CTRL-A**, to highlight the filtered registry files.
4. Right-click and select **Send to module** > **Registry**.

Figure 5: File System Registry folders filter, Send to module > Registry.



Filter: Registry (Current) - SAM, SECU

	Filename	Extension	File Signature
1	NTUSER.DAT	DAT	Registry
2	NTUSER.DAT		Registry
3	UsrClass.dat		Registry
4	SAM		Registry
5	SECURITY		Registry
6	SOFTWARE		Registry
7	SYSTEM		Registry

PREP: LIVE BOOT - VIRTUALIZATION

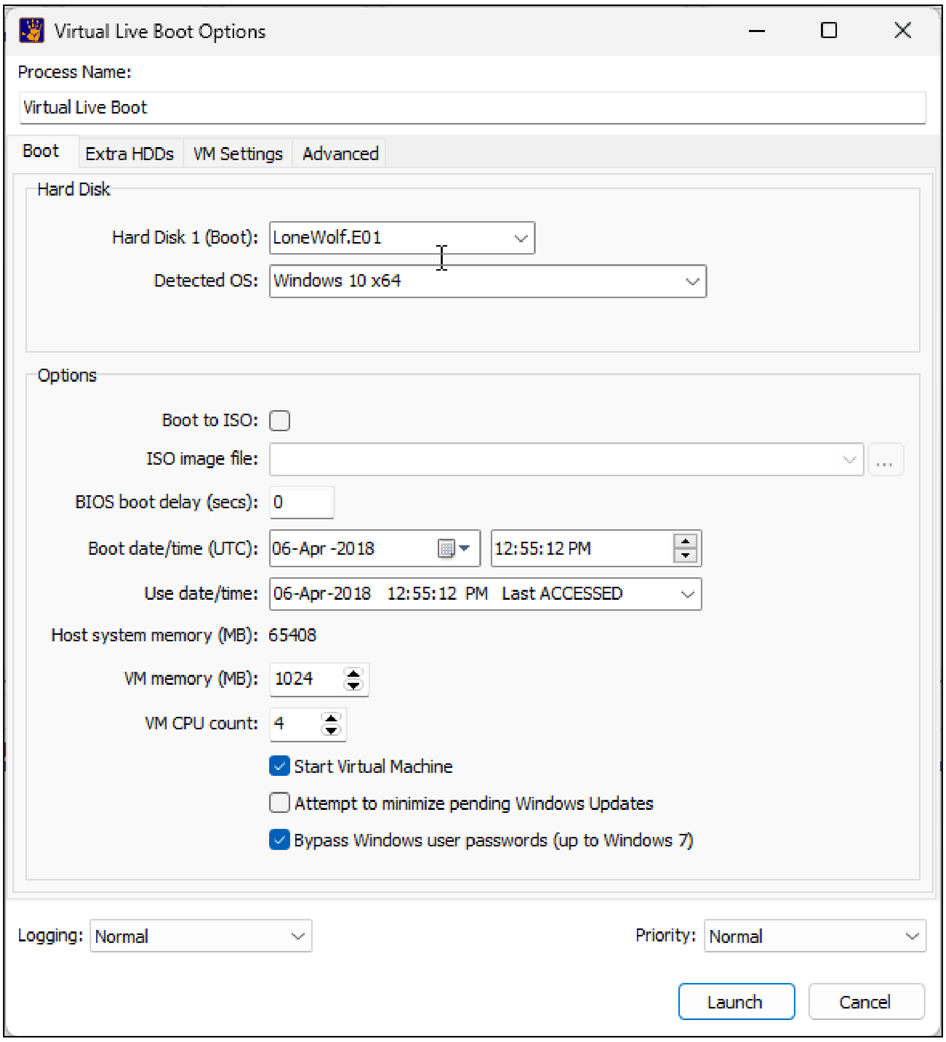
Live Boot is a component of Forensic Explorer that enables an investigator to boot a forensic image. The investigator can then operate the computer in a real time virtual environment. The boot process is achieved through and integration of Forensic Explorer, Mount Image Pro, and VMWare or VirtualBox.

To Live Boot the Lone Wolf forensic image:

1. Click on the **Virtual Live Boot** button in the **Evidence** or **File System** modules.

2. The following Virtual Live Boot Options window will display. Launch the Live Boot with the default settings.

Figure 6: Live Boot Virtualization



Virtual Live Boot Options

Process Name: Virtual Live Boot

Hard Disk

Hard Disk 1 (Boot): LoneWolf.E01

Detected OS: Windows 10 x64

Options

Boot to ISO: □

ISO image file:

BIOS boot delay (secs): 0

Boot date/time (UTC): 06-Apr -2018 12:55:12 PM

Use date/time: 06-Apr-2018 12:55:12 PM Last ACCESSED

Host system memory (MB): 65408

VM memory (MB): 1024

VM CPU count: 4

☑ Start Virtual Machine

□ Attempt to minimize pending Windows Updates

☑ Bypass Windows user passwords (up to Windows 7)

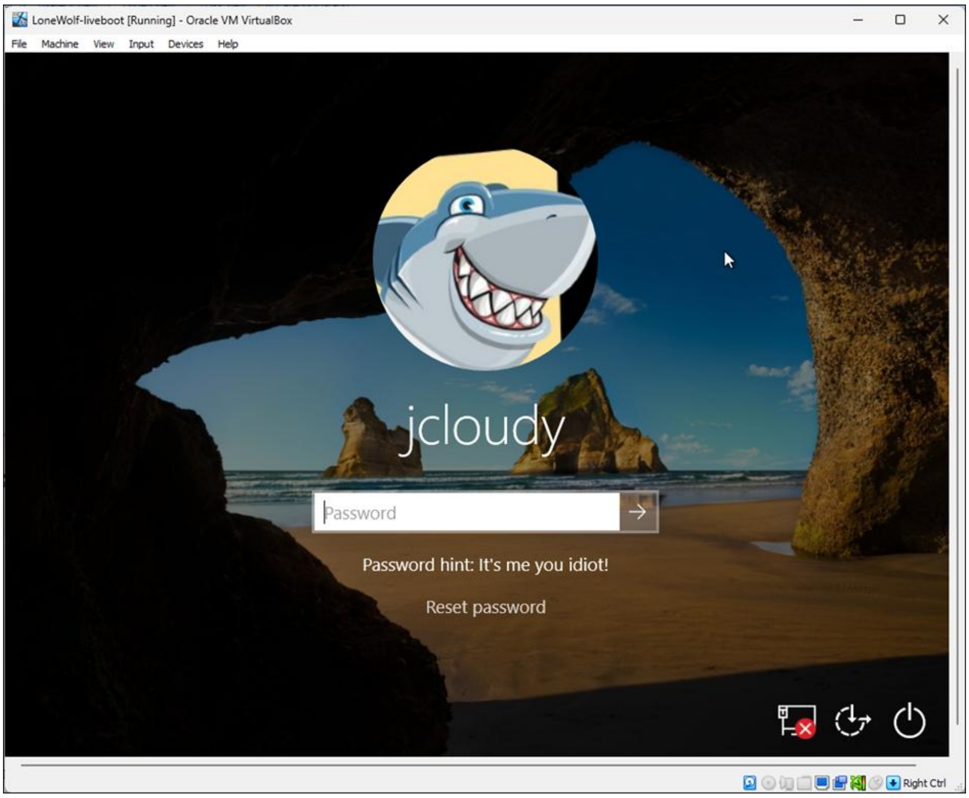
Logging: Normal

Priority: Normal

3. The virtual machine will boot to the **jcloudy** password protected Windows login screen.

Note: Use the right CTRL key to exit the cursor from the Virtual Box window.

Figure 7: Windows Shutdown in VirtualBox



Password hint: It's me you idiot!

PASSWORD BYPASS OF A UEFI SYSTEM USING VIRTUAL BOX

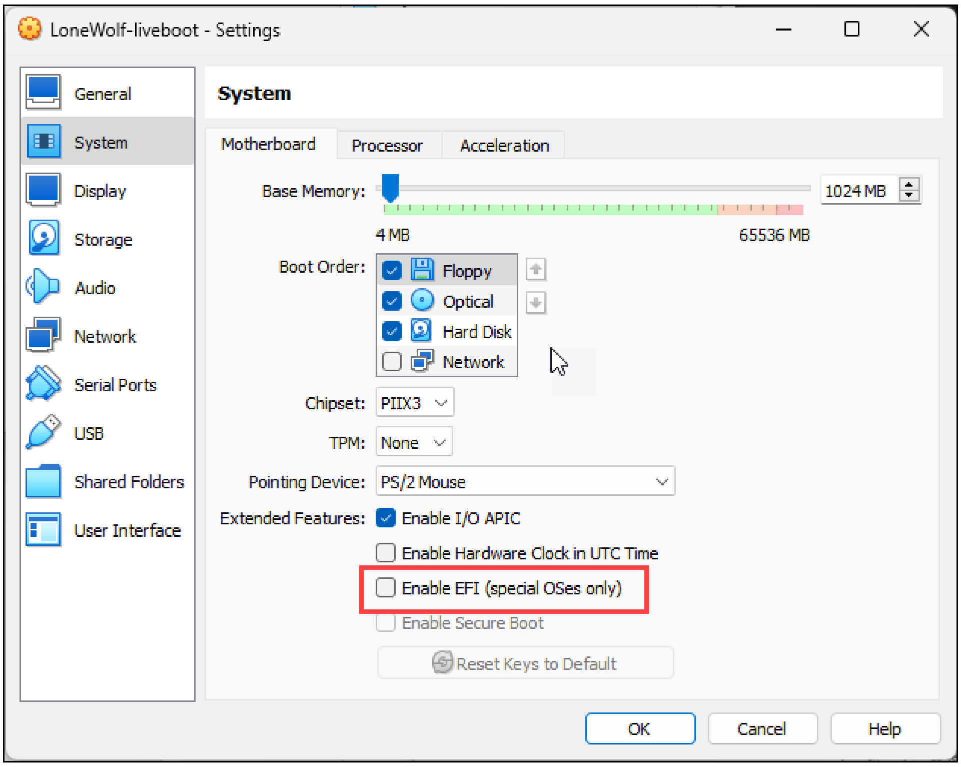
Note: In question 8, the password to the **jcloudy** account was determined from the NTLM hash to be **Jcloudy2018!!**. This password can be used to log into the jcloudy account without the need to bypass.

The original Lone Wolf PC had a UEFI (Unified Extensible Firmware Interface) BIOS. To bypass Windows user passwords on an UEFI partition using VirtualBox and PCUnlocker it is necessary to disable UEFI during the password bypass process:

1. At the Windows login screen, **shutdown** the machine using the standard Windows shutdown procedure (Windows must be shutdown correctly to obtain access to system boot settings in VirtualBox).
2. Run **Oracle VM VirtualBox** from the **desktop icon**. From the VirtualBox menu, select **Machine > Settings > System** to display the window shown in Figure 8 below. **Uncheck** the

Enable EFI (special OSes only) box:

Figure 8: VirtualBox System Settings - Disable EFI



LoneWolf-liveboot - Settings

System

Base Memory: 1024 MB

Boot Order: ☑ Floppy, ☑ Optical, ☑ Hard Disk, □ Network

Chipset: PIIX3

TPM: None

Pointing Device: PS/2 Mouse

Extended Features: ☑ Enable I/O APIC

□ Enable Hardware Clock in UTC Time

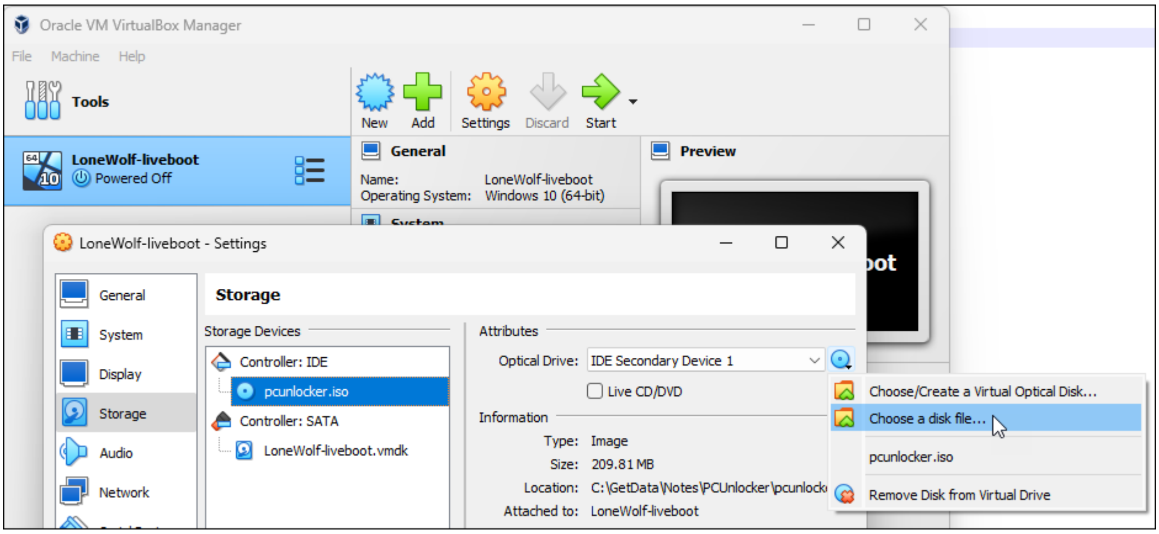
□ Enable EFI (special OSes only)

□ Enable Secure Boot

Important: If the Enable EFI (special OSes only) is greyed out, it means that the Virtual Machine is running, or Windows has not shutdown correctly (i.e., the running state of the virtual machine has been saved). Restart the virtual machine and power down using the Windows shutdown procedure.

3. With the virtual machine shutdown, in the virtual machine **Settings** > **Storage** > **Storage Devices** window, click on the **Optical Drive** and select the **pcunlocker.iso** file:

Figure 9: Select the PCUnlocker ISO from the VirtualBox settings window.


Oracle VM VirtualBox Manager
File Machine Help
Tools
New Add Settings Discard Start
LoneWolf-liveboot
Powered Off
General
Preview
LoneWolf-liveboot - Settings
General
System
Display
Storage
Audio
Network
Choose/Create a Virtual Optical Disk…
Choose a disk file…
pcunlocker.iso
Remove Disk from Virtual Drive

Name: LoneWolf-liveboot
Operating System: Windows 10 (64-bit)

Storage

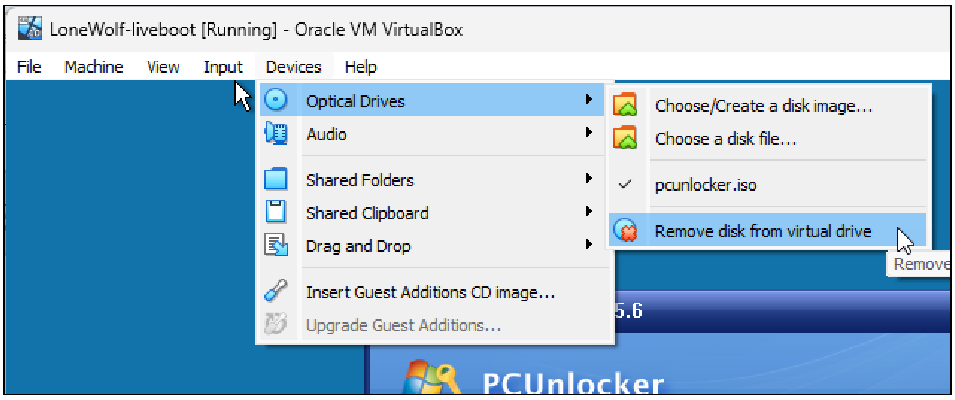
Storage Devices
Controller: IDE
pcunlocker.iso
Controller: SATA
LoneWolf-liveboot.vmdk

Attributes
Optical Drive: IDE Secondary Device 1
□ Live CD/DVD

Information
Type: Image
Size: 209.81 MB
Location: C:\GetData\Notes\PCUnlocker\pcunlock
Attached to: LoneWolf-liveboot

4. Click **Start** to launch the virtual machine and **boot with PCUnlocker**. Follow the PCUnlocker instructions to reset the jcloudy user password. Once the passwords have been reset, eject the virtual CD containing the pcunlocker.iso by selecting **Devices > Optical Drives > Remove disk from virtual drive:**

Figure 10: VirtualBox > Devices > Optical Drives > Remove disk from virtual drive.


LoneWolf-liveboot [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Optical Drives
Audio
Shared Folders
Shared Clipboard
Drag and Drop
Insert Guest Additions CD image…
Upgrade Guest Additions…
Choose/Create a disk image…
Choose a disk file…
✓ pcunlocker.iso
Remove disk from virtual drive
Remove
5.6
PCUnlocker

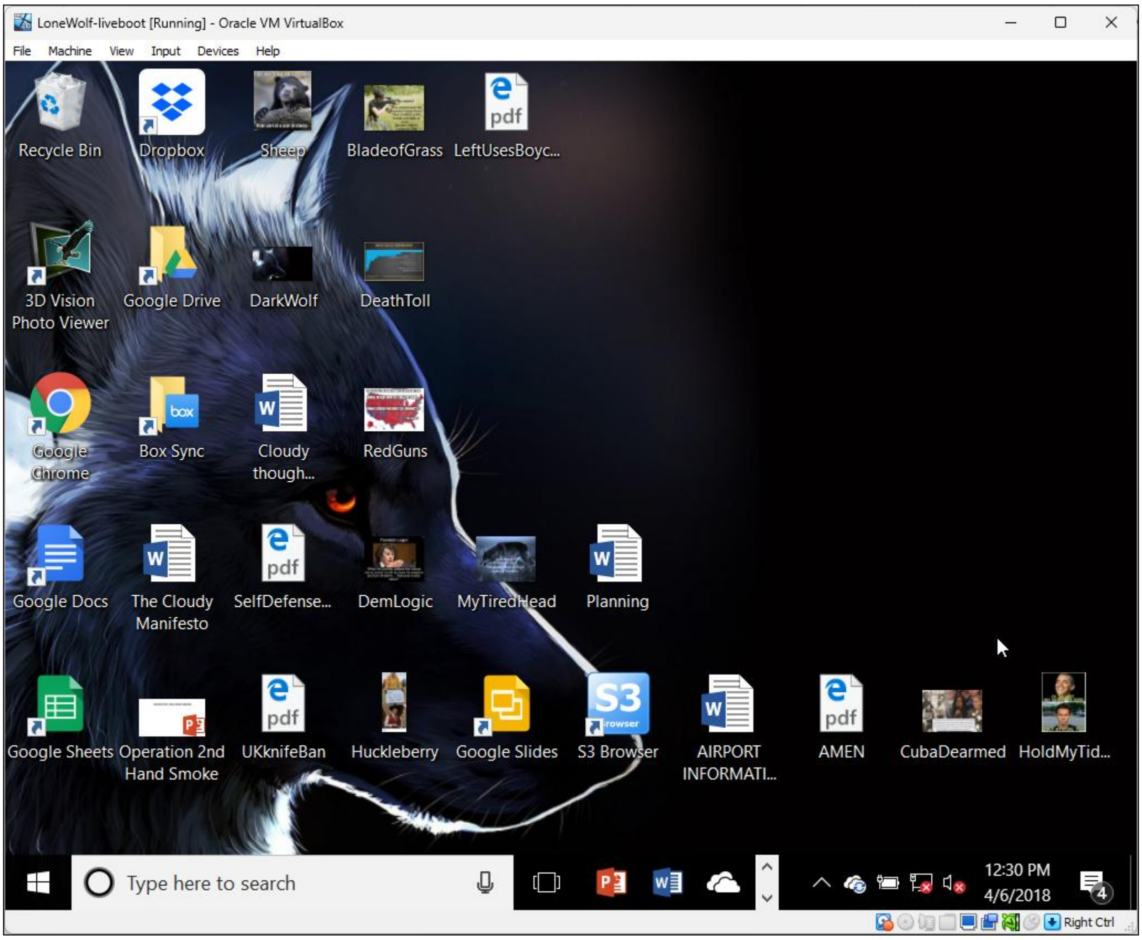
4. Power off the machine by selecting the **X** button in the top right corner of VirtualBox and select **Power off the machine**.

5. Once the machine is powered down go back to the **Machine > Settings > System** settings and re-check **Enable EFI (special OSes only)**.

6. Ensure that in the virtual machine settings window that the **optical drive** is **empty** (eject the pcunlocker.iso if it is still present).

7. Click **Start** to launch the virtual machine. The machine should now boot to the Windows Desktop with passwords bypassed.

Figure 11: Live Boot > jcloudy desktop.



An examination of the Windows desktop identifies the use of the following programs:

- Box Sync
- Dropbox
- Google Docs
- MS PowerPoint
- MS Word
- S3 Browser

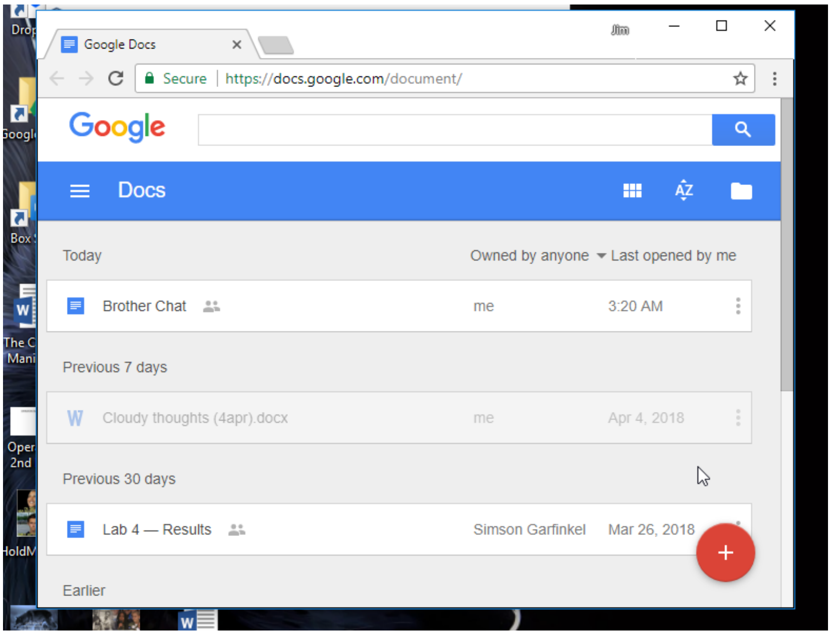
An examination of the Windows desktop identifies the following key documents:

- AIRPORT INFORMATION.docx
- Brother Chat
- Cloudy thoughts (4apr).docx
- Operation 2nd Hand Smoke.pptx
- Planning.docx
- The Cloudy Manifesto.docx

RUNNING LIVE BOOT VIRTUALIZATION

Live Boot presents the opportunity to launch and examine installed programs as the suspect would have done.

Figure 12: Live Boot - Navigating installed applications.



Today — Owned by anyone — Last opened by me

Brother Chat	me	3:20 AM

Previous 7 days

Cloudy thoughts (4apr).docx	me	Apr 4, 2018

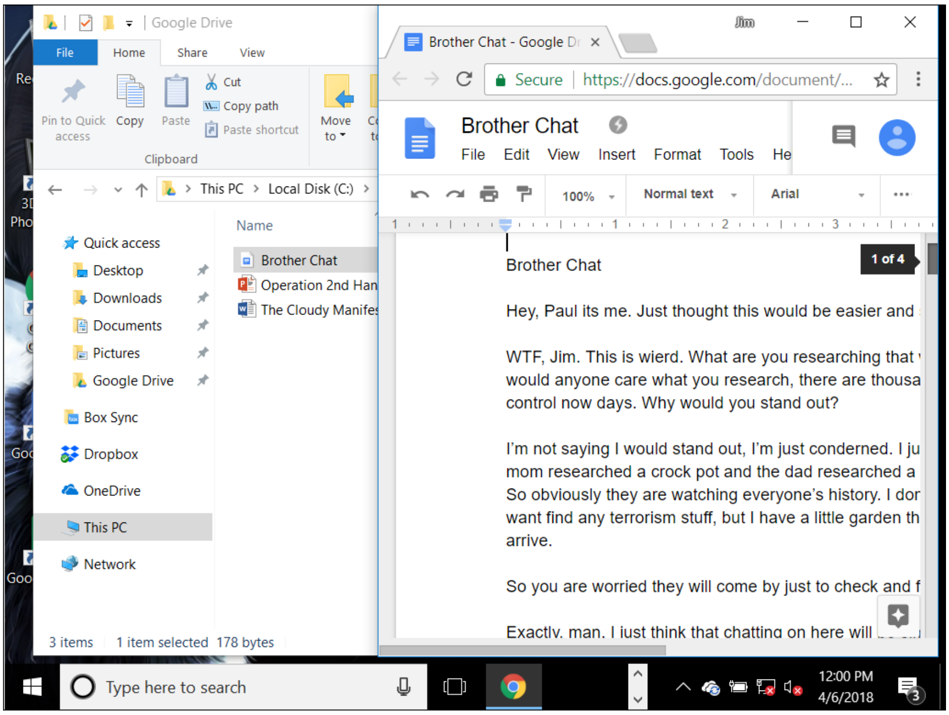
Previous 30 days

Lab 4 — Results	Simson Garfinkel	Mar 26, 2018

Earlier

In some instances, this can give access to documents that can prove more difficult to examine through forensic software. For example, **Brother Chat.gdoc** shown below:

Figure 13: Live Boot - Navigating installed applications.



Brother Chat

Hey, Paul its me. Just thought this would be easier and

WTF, Jim. This is wierd. What are you researching that
would anyone care what you research, there are thousa
control now days. Why would you stand out?

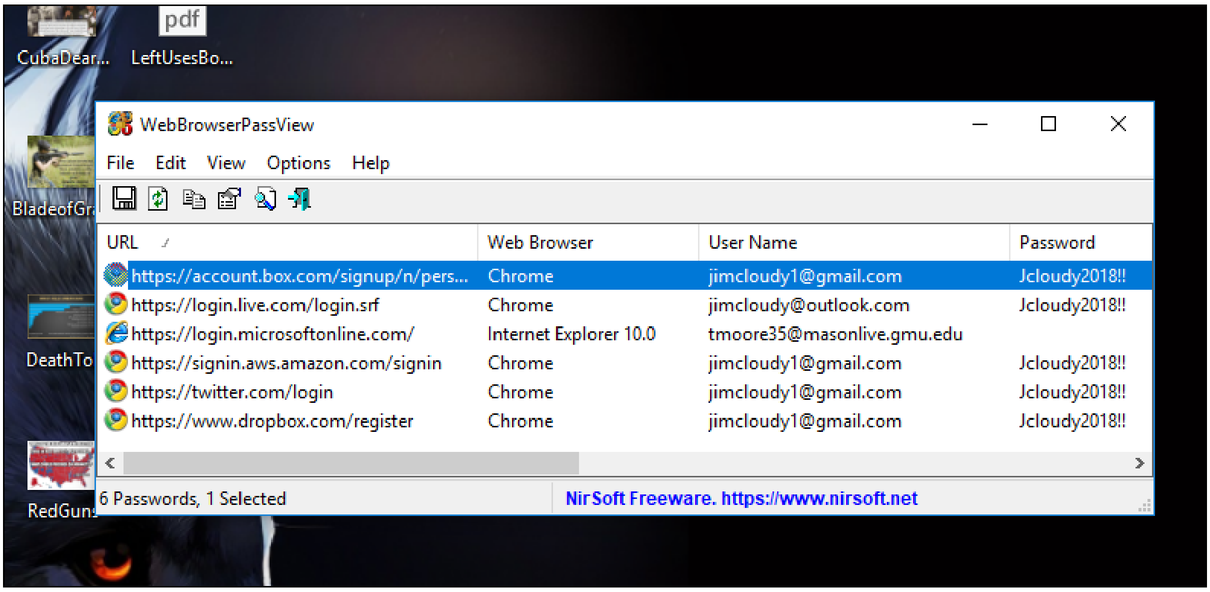
I'm not saying I would stand out, I'm just conderned. I ju
mom researched a crock pot and the dad researched a
So obviously they are watching everyone's history. I dor
want find any terrorism stuff, but I have a little garden th
arrive.

So you are worried they will come by just to check and f

Exactly, man. I just think that chatting on here will

Live Boot also presents the opportunity to run external programs on the target computer. This is achieved by installing **Oracle VM VirtualBox Guest Additions**, which provides the ability to drag and drop applications from the host computer to the virtual machine desktop (search YouTube for detailed installation instructions). NirSoft WebBrowserPassView is shown below:

Figure 14: Running tools inside the virtual machine (NirSoft WebBrowserPassView shown).



URL	Web Browser	User Name	Password
https://account.box.com/signup/n/pers...	Chrome	jimcloudy1@gmail.com	Jcloudy2018!!
https://login.live.com/login.srf	Chrome	jimcloudy@outlook.com	Jcloudy2018!!
https://login.microsoftonline.com/	Internet Explorer 10.0	tmoore35@masonlive.gmu.edu	
https://signin.aws.amazon.com/signin	Chrome	jimcloudy1@gmail.com	Jcloudy2018!!
https://twitter.com/login	Chrome	jimcloudy1@gmail.com	Jcloudy2018!!
https://www.dropbox.com/register	Chrome	jimcloudy1@gmail.com	Jcloudy2018!!

6 Passwords, 1 Selected

NirSoft Freeware. https://www.nirsoft.net

PREP: KEYWORD LIST

The following keywords were collected:

[General Scenario Words]
$325
2nd Amendment
Gun control
Gun violence
gun-control
Jim cloudy
Marihuana
town hall
town hall meeting

[Artifacts - Google Searches]
9mm rifles
Bali airport
ApMsgfwd
strap cash
hotels in Bali
gun free zones
police response

[Live Boot General Keywords]
Denpasar
Korean Air
Manifesto
Sea Breeze Candidasa

[Live Boot Cloud Services]
Drop Box
Box Sync
OneDrive
Amazon S3

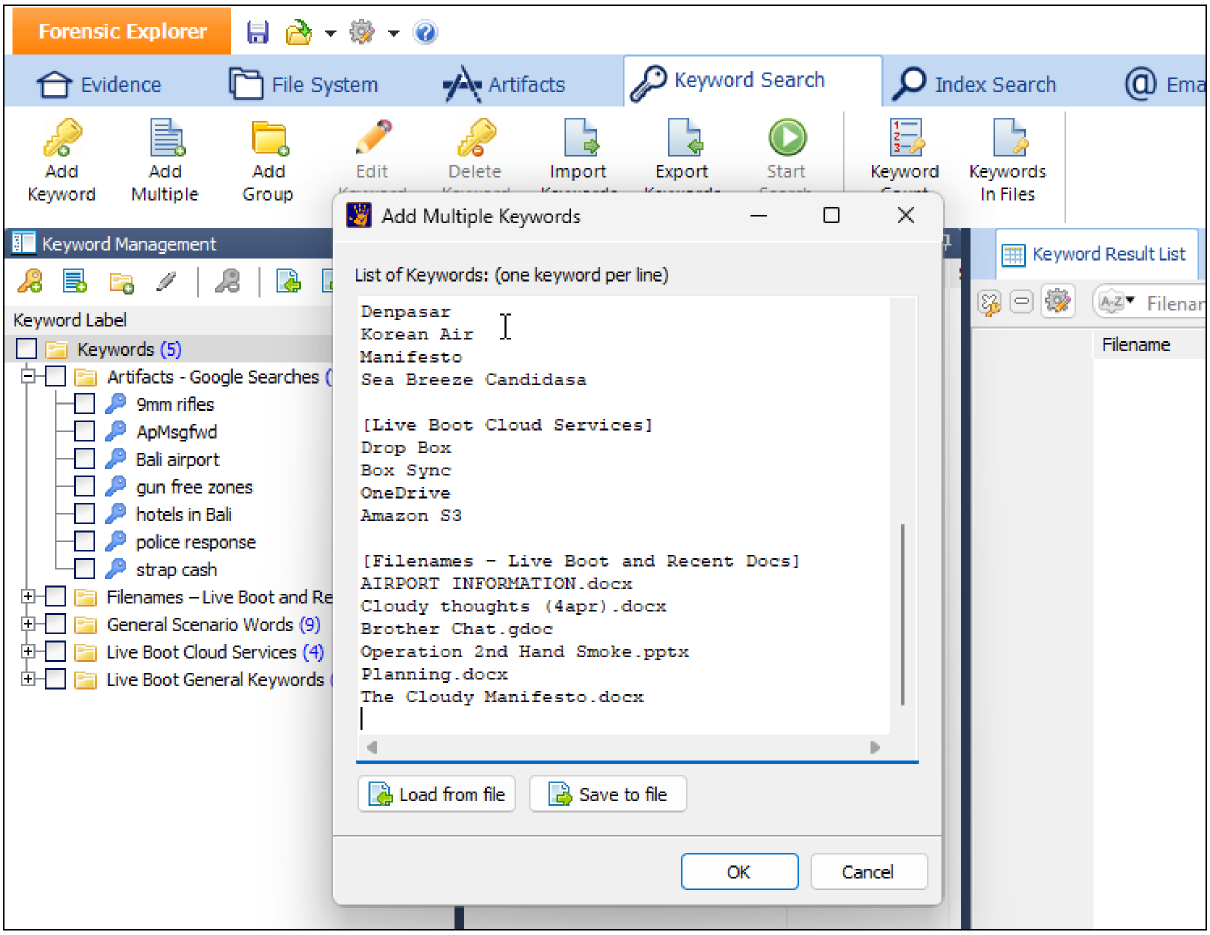
[Filenames – Live Boot and Recent Docs]
AIRPORT INFORMATION.docx
Cloudy thoughts \(4apr\).docx
Brother Chat.gdoc
Operation 2nd Hand Smoke.pptx
Planning.docx
The Cloudy Manifesto.docx

PREP: KEYWORD SEARCH

Note: Keyword Search

A Keyword Search is a sequential sector search of the evidence. The duration of the search will depend on the size of the evidence and the number of keywords used. For this reason, it can be more practical to run a Keyword Search after other faster processing options have been run and reviewed.

Figure 15: Keyword Search Module > Add Multiple Keywords



List of Keywords: (one keyword per line)

```
Denpasar
Korean Air
Manifesto
Sea Breeze Candidasa

[Live Boot Cloud Services]
Drop Box
Box Sync
OneDrive
Amazon S3

[Filenames - Live Boot and Recent Docs]
AIRPORT INFORMATION.docx
Cloudy thoughts (4apr).docx
Brother Chat.gdoc
Operation 2nd Hand Smoke.pptx
Planning.docx
The Cloudy Manifesto.docx
```

In the Keyword Management tree:

1. Check the keywords to search.
2. Click the **Start Search** button.

Examine the search results in the **Keyword Result List**.

PREP: INDEX SEARCH

Note: Index Search

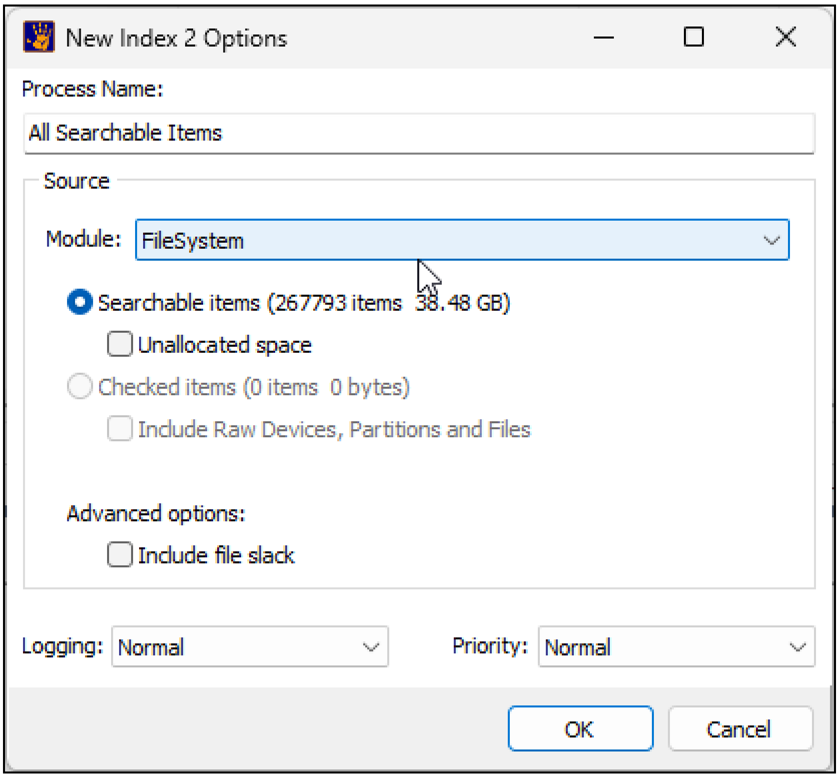
The Index Search module uses DTSearch to create index of words. The time taken to create the index will be determined by the size of the evidence. For this reason, it can be practical to create an index after other faster processing options have been run and reviewed.

The advantage of an Index Search is that it will natively support compound documents like Microsoft Word (.docx) and Microsoft Email (.pst, .mbox, etc.). See https://support.dtsearch.com/faq/index.html for more DTSearch information.

To create and index:

1. Click the **New Index** button.
2. Select the required data to index and press **OK**.

Figure 16: Index Search



New Index 2 Options

Process Name: All Searchable Items

Source

Module: FileSystem

● Searchable items (267793 items 38.48 GB)

□ Unallocated space

○ Checked items (0 items 0 bytes)

□ Include Raw Devices, Partitions and Files

Advanced options:

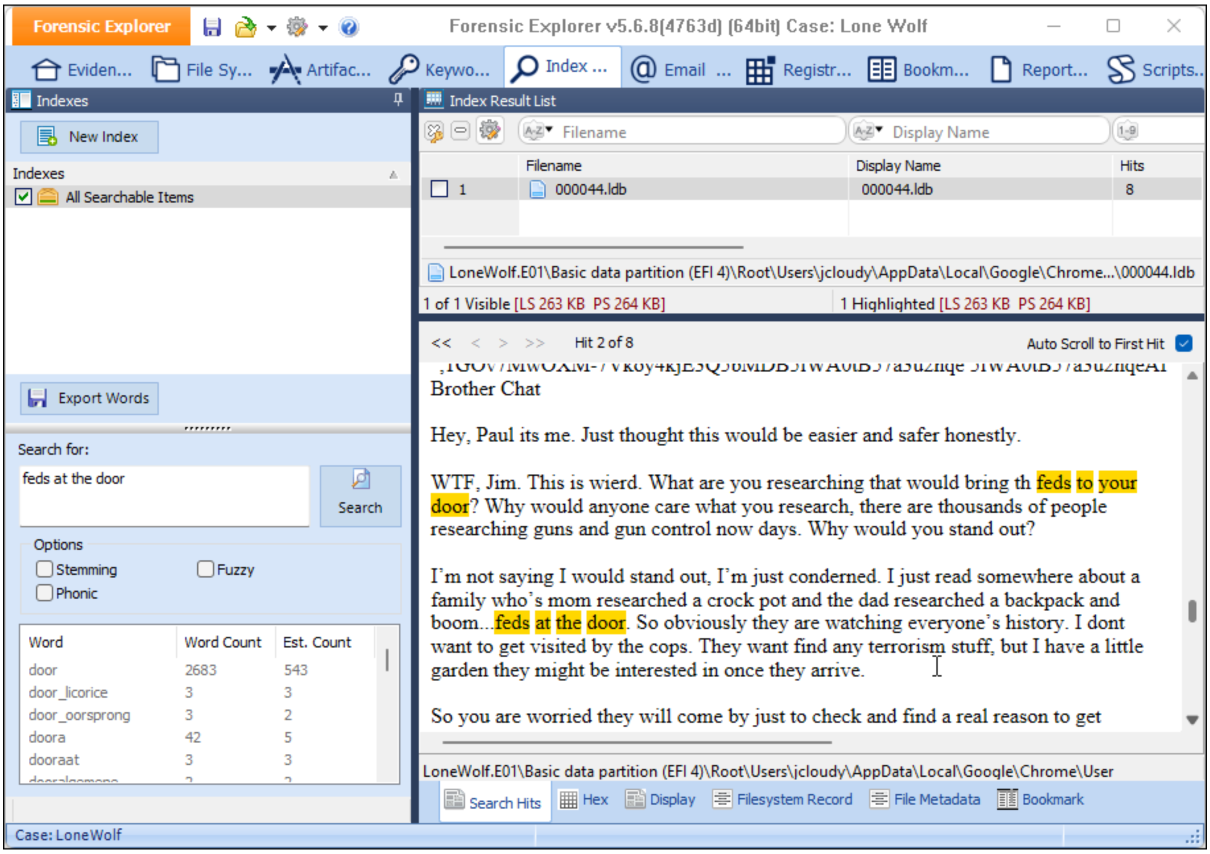
□ Include file slack

Logging: Normal

Priority: Normal

3. Enter the search criteria in the **Search for** box and press the **Search** button.

Figure 17: Index Search



Indexes

☑ All Searchable Items

Search for: feds at the door

Options

☐ Stemming ☐ Fuzzy

☐ Phonic

Word	Word Count	Est. Count
door	2683	543
door_licorice	3	3
door_oorsprong	3	2
doora	42	5
dooraat	3	3

	Filename	Display Name	Hits
☐ 1	000044.ldb	000044.ldb	8

LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome...\000044.ldb

1 of 1 Visible [LS 263 KB PS 264 KB] 1 Highlighted [LS 263 KB PS 264 KB]

<< < > >> Hit 2 of 8 Auto Scroll to First Hit ☑

Brother Chat

Hey, Paul its me. Just thought this would be easier and safer honestly.

WTF, Jim. This is wierd. What are you researching that would bring th feds to your door? Why would anyone care what you research, there are thousands of people researching guns and gun control now days. Why would you stand out?

I'm not saying I would stand out, I'm just conderned. I just read somewhere about a family who's mom researched a crock pot and the dad researched a backpack and boom...feds at the door. So obviously they are watching everyone's history. I dont want to get visited by the cops. They want find any terrorism stuff, but I have a little garden they might be interested in once they arrive.

So you are worried they will come by just to check and find a real reason to get

LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User

QUESTION 1 - OPERATING SYSTEM

What is the Operating System and edition installed on the computer?

Q1. ANSWER

Windows 10 Education (1709).

Q1. FORENSIC EXPLORER METHODOLOGY

Operating System information is stored in the following **Registry** locations:

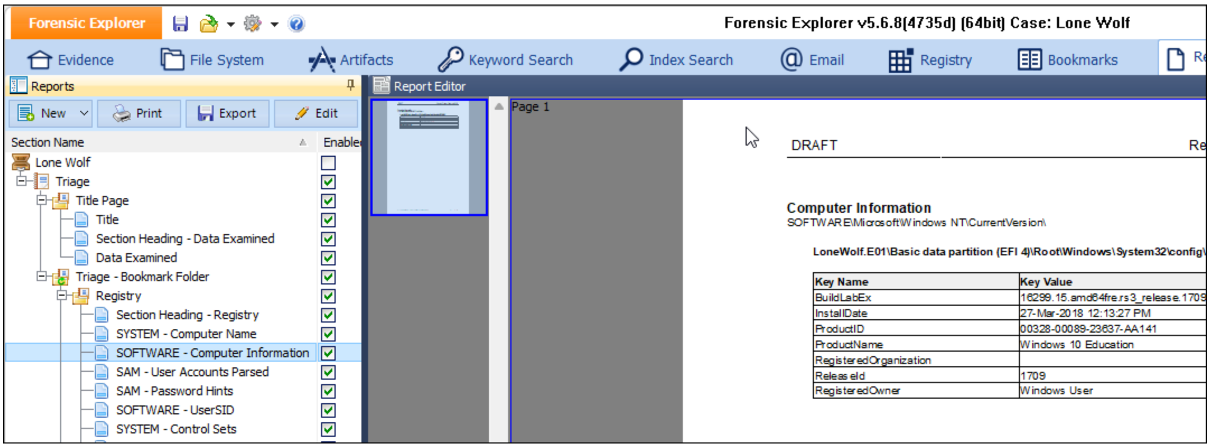
- **SOFTWARE\Microsoft\Windows NT\CurrentVersion\**
- **SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\**

Q1. TRIAGE REPORT

Select **Reports** module > **Triage** report:

1. In the report tree, select **SOFTWARE - Computer Information** (If the Triage report is not populated see Triage on page 8 above).

Figure 18: Reports > Triage > SOFTWARE - Computer Information



Computer Information
SOFTWARE\Microsoft\Windows NT\CurrentVersion\

LoneWolf.E01\Basic data partition (EFI 4)\Root\Windows\System32\config\

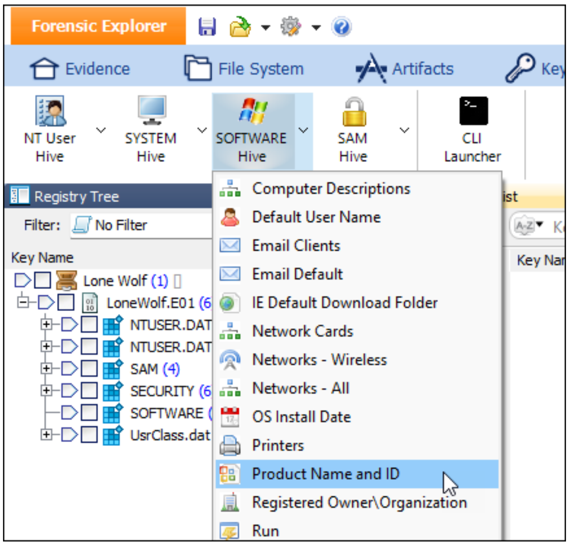
Key Name	Key Value
BuildLabEx	16299.15.amd64fre.rs3_release.1709
InstallDate	27-Mar-2018 12:13:27 PM
ProductID	00328-00089-23637-AA141
ProductName	Windows 10 Education
RegisteredOrganization	
ReleaseId	1709
RegisteredOwner	Windows User

Q1. REGISTRY MODULE - TOOLBAR

To examine registry data (see page 10 above to populate the Registry module):

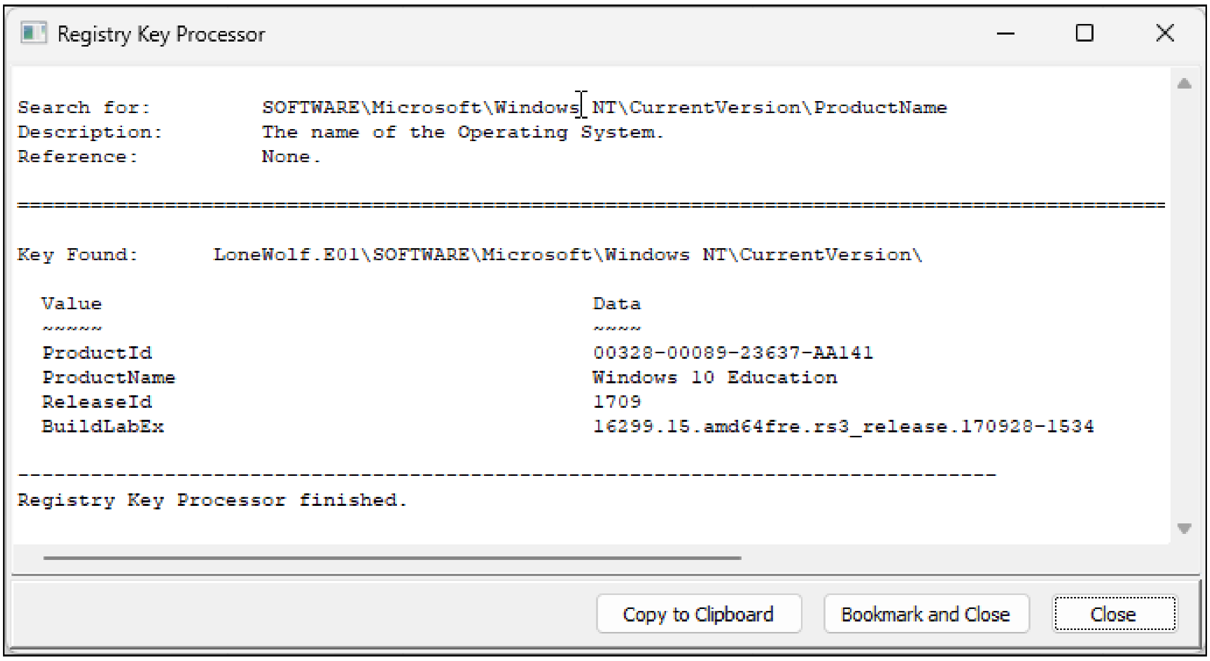
1. In the **Registry module toolbar**, select **SOFTWARE Hive** > **Product Name and ID**.

Figure 19: Registry > SOFTWARE Hive > Product Name and ID



2. The following summary report will appear:

Figure 20: Registry module toolbar > SOFTWARE Hive > Product name and ID result.



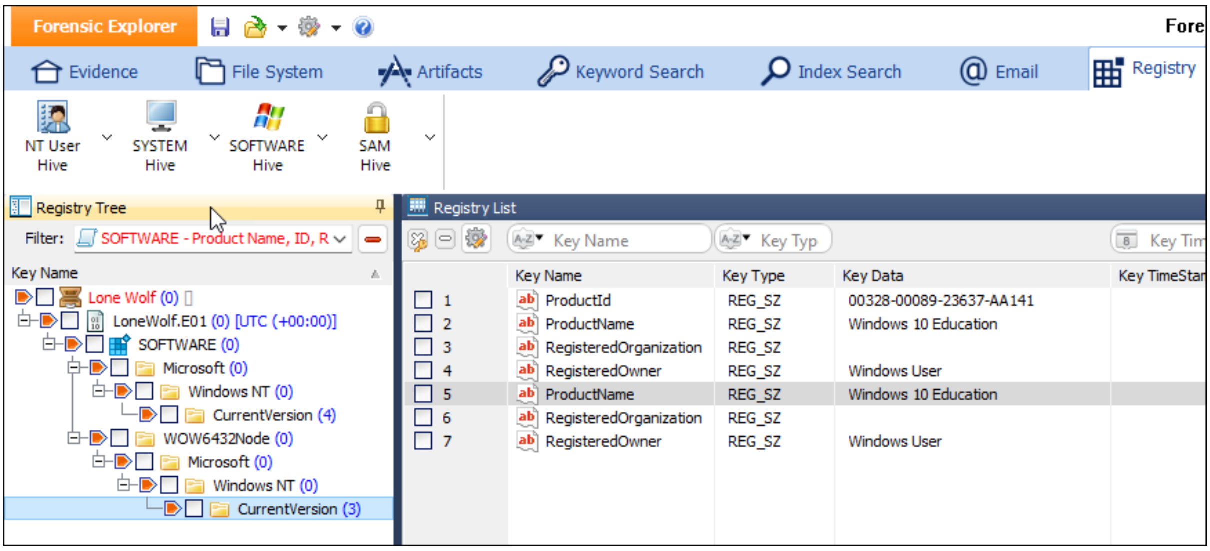
```
Search for:         SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName
Description:        The name of the Operating System.
Reference:          None.

==============================================================================================

Key Found:      LoneWolf.E01\SOFTWARE\Microsoft\Windows NT\CurrentVersion\

  Value                                          Data
  ~~~~~                                          ~~~~
  ProductId                                      00328-00089-23637-AA141
  ProductName                                    Windows 10 Education
  ReleaseId                                      1709
  BuildLabEx                                     16299.15.amd64fre.rs3_release.170928-1534

--------------------------------------------------------------------------------
Registry Key Processor finished.
```

Q1. REGISTRY MODULE - SOURCE DATA

To examine the source registry keys:

1. **Branch plate** [▶] the entire **Registry** module.
2. Apply the folders filter: **Registry Keys** > **SOFTWARE - Product Name, ID, Registered Organization and Owner.**

Figure 21: Registry module > Folders Filter > SOFTWARE - Product Name…



Filter: SOFTWARE - Product Name, ID, R

Key Name
- Lone Wolf (0)
  - LoneWolf.E01 (0) [UTC (+00:00)]
    - SOFTWARE (0)
      - Microsoft (0)
        - Windows NT (0)
          - CurrentVersion (4)
      - WOW6432Node (0)
        - Microsoft (0)
          - Windows NT (0)
            - CurrentVersion (3)

	Key Name	Key Type	Key Data	Key TimeStar
□ 1	ProductId	REG_SZ	00328-00089-23637-AA141	
□ 2	ProductName	REG_SZ	Windows 10 Education	
□ 3	RegisteredOrganization	REG_SZ		
□ 4	RegisteredOwner	REG_SZ	Windows User	
□ 5	ProductName	REG_SZ	Windows 10 Education	
□ 6	RegisteredOrganization	REG_SZ		
□ 7	RegisteredOwner	REG_SZ	Windows User	

QUESTION 2 - COMPUTER NAME

What is the computer name?

Q2. ANSWER

DESKTOP-PM6C56D.

Q2. FORENSIC EXPLORER METHODOLOGY

Computer Name information is stored in the following Registry location:

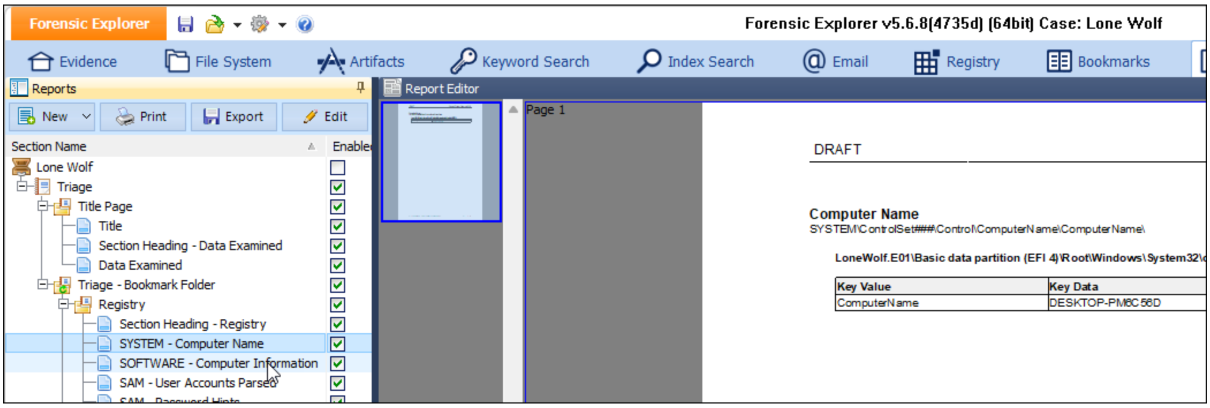
- **SYSTEM\ControlSet001\Control\ComputerName\ComputerName\ComputerName**

Q2. TRIAGE REPORT

Select **Reports** module > **Triage** report:

1. In the report tree, select **Registry** > **SOFTWARE - Computer Name** (If the Triage report is not populated see Triage on page 8 above).

Figure 22: Reports > Triage > SOFTWARE - Computer Name



DRAFT

Computer Name
SYSTEM\ControlSet####\Control\ComputerName\ComputerName\

LoneWolf.E01\Basic data partition (EFI 4)\Root\Windows\System32\c

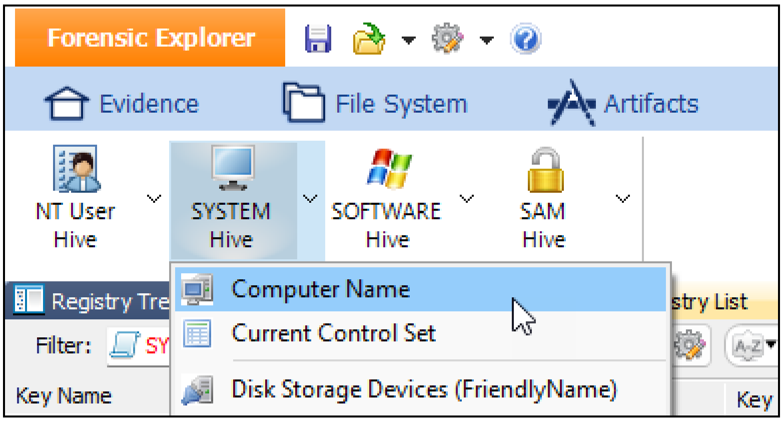
Key Value	Key Data
ComputerName	DESKTOP-PM6C56D

Q2. REGISTRY MODULE - TOOLBAR

To examine registry data (see page 10 above to populate the Registry module):

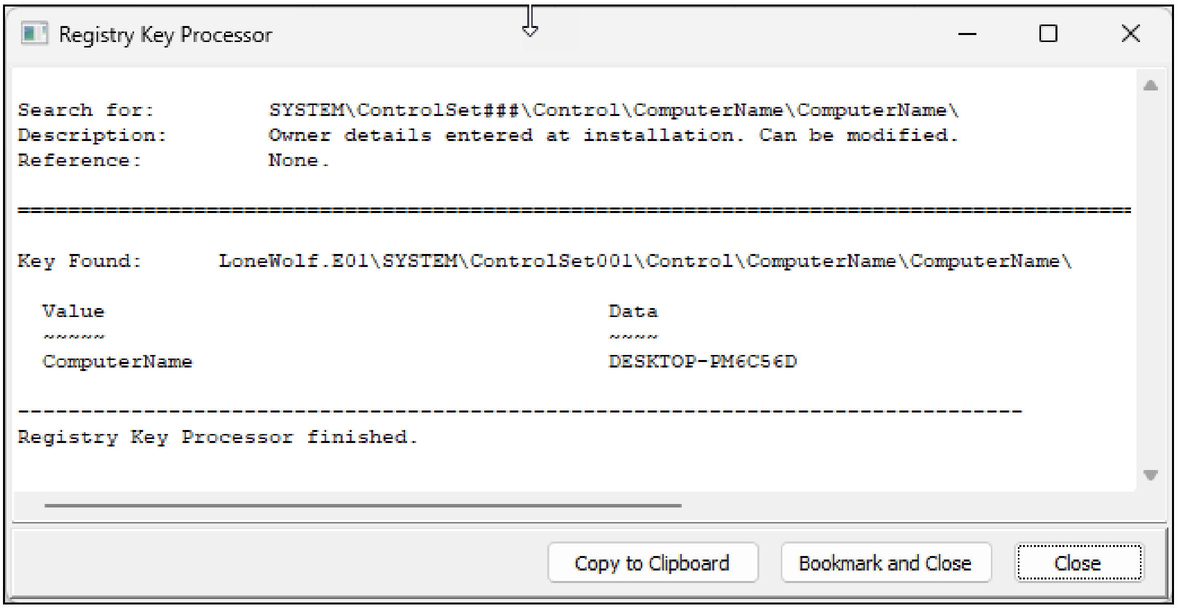
1. In the **Registry module toolbar**, select **SYSTEM Hive** > **Computer Name**.

Figure 23: Registry module > Toolbar > SYSTEM Hive > Computer Name



2. The following summary report will appear:

Figure 24: : Registry module toolbar > SYSTEM Hive > Computer Name



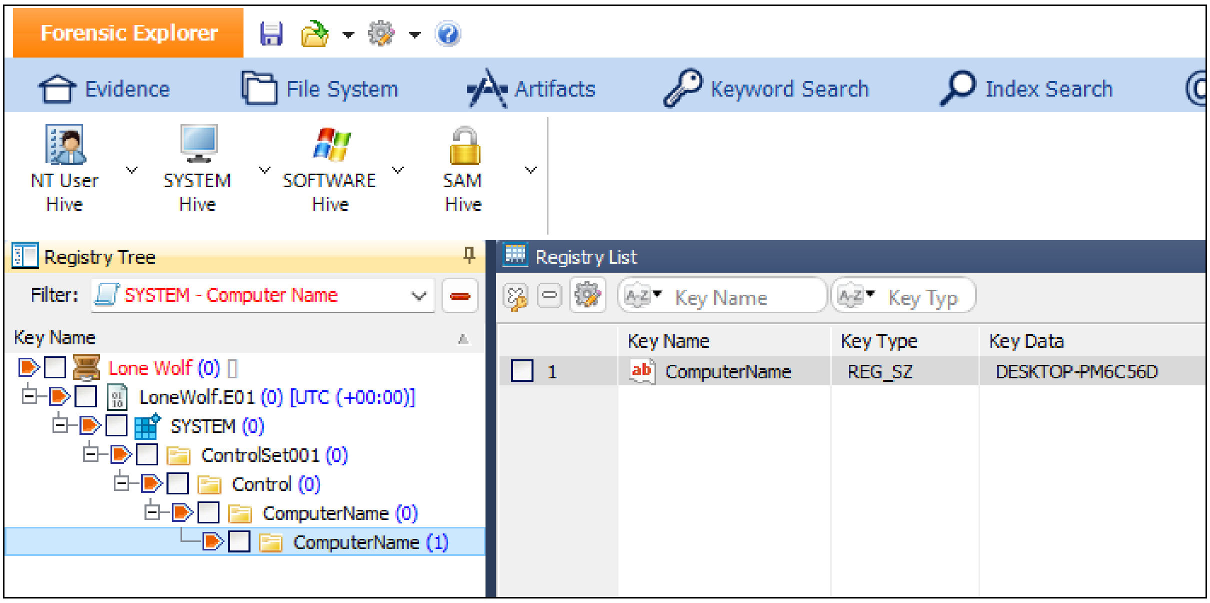
```
Search for:         SYSTEM\ControlSet###\Control\ComputerName\ComputerName\
Description:        Owner details entered at installation. Can be modified.
Reference:          None.

==========================================================================================

Key Found:      LoneWolf.E01\SYSTEM\ControlSet001\Control\ComputerName\ComputerName\

  Value                                          Data
  ~~~~~                                          ~~~~
  ComputerName                                   DESKTOP-PM6C56D

--------------------------------------------------------------------------------
Registry Key Processor finished.
```

Q2. REGISTRY MODULE - SOURCE DATA

To examine the source registry keys:

1. **Branch plate** [▶] the entire **Registry** module.
2. Apply the folders filter: **Registry Keys** > **SYSTEM - Computer Name**.

Figure 25: Registry module > Folders Filter > SOFTWARE - Product Name...



Filter: SYSTEM - Computer Name

Key Name
- Lone Wolf (0)
  - LoneWolf.E01 (0) [UTC (+00:00)]
    - SYSTEM (0)
      - ControlSet001 (0)
        - Control (0)
          - ComputerName (0)
            - ComputerName (1)

	Key Name	Key Type	Key Data
□ 1	ComputerName	REG_SZ	DESKTOP-PM6C56D

QUESTION 3 - REGISTERED OWNER AND ORGANIZATION

Who is the operating system registered owner and organization?

Q3. ANSWER

Registered owner is **Windows User.** No registered organization is listed.

Q3. FORENSIC EXPLORER METHODOLOGY

Registered owner and organization information is stored in the following Registry location:

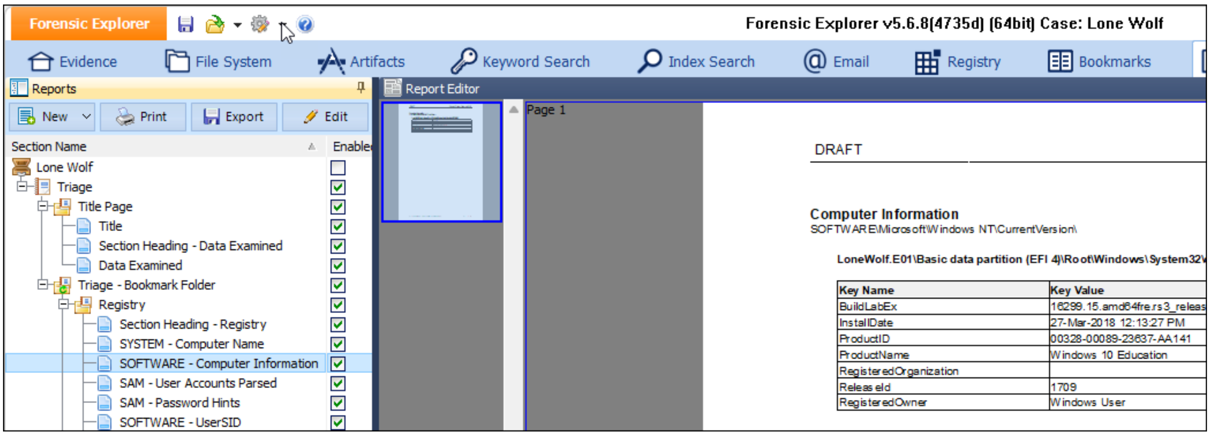
- **SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOwner**
- **SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOrganization**
- **SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\RegisteredOwner**
- **SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\RegisteredOrganization**

Q3. TRIAGE REPORT

Select **Reports** module > **Triage** report:

1. In the report tree, select **Registry** > **SOFTWARE - Computer Information** (If the Triage report is not populated see Triage on page 8 above).

Figure 26: Reports > Triage > SOFTWARE - Computer Information



DRAFT

Computer Information
SOFTWARE\Microsoft\Windows NT\CurrentVersion\

LoneWolf.E01\Basic data partition (EFI 4)\Root\Windows\System32\

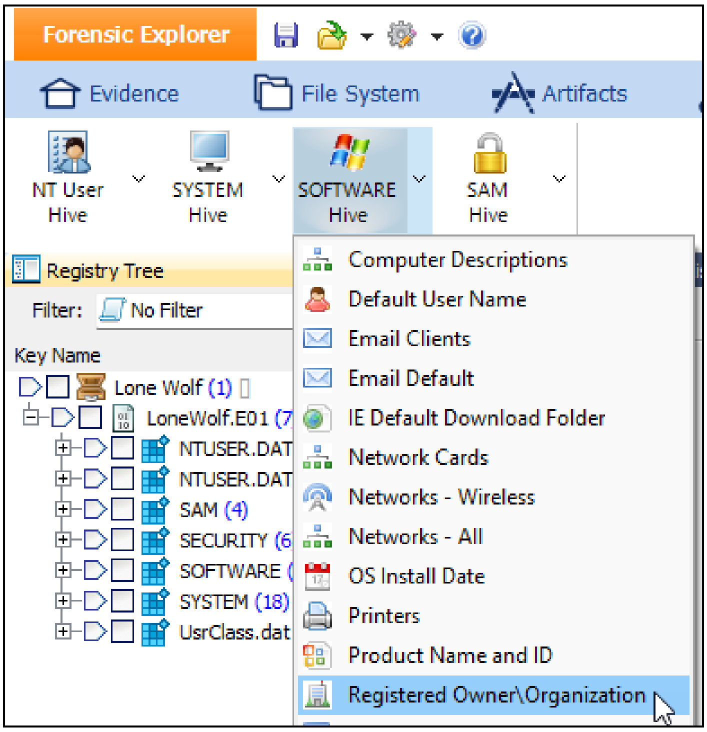
Key Name	Key Value
BuildLabEx	16299.15.amd64fre.rs3_releas
InstallDate	27-Mar-2018 12:13:27 PM
ProductID	00328-00089-23637-AA141
ProductName	Windows 10 Education
RegisteredOrganization	
ReleaseId	1709
RegisteredOwner	Windows User

Q3. REGISTRY MODULE - TOOLBAR

To examine registry data (see page 10 above to populate the Registry module):

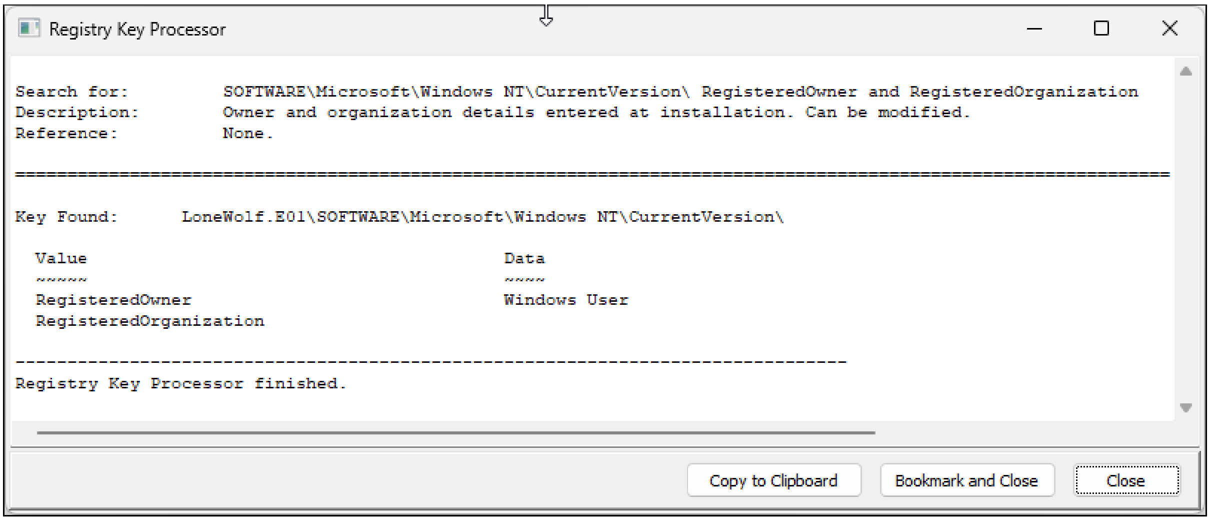
1. In the **Registry module toolbar**, select **SOFTWARE Hive** > **Registered Owner\Organization**.

Figure 27: Registry > SOFTWAR Hive > Registered Owner\Organization



3. The following summary report will appear:

Figure 28: Registry > SOFTWAR Hive > Registered Owner\Organization result.



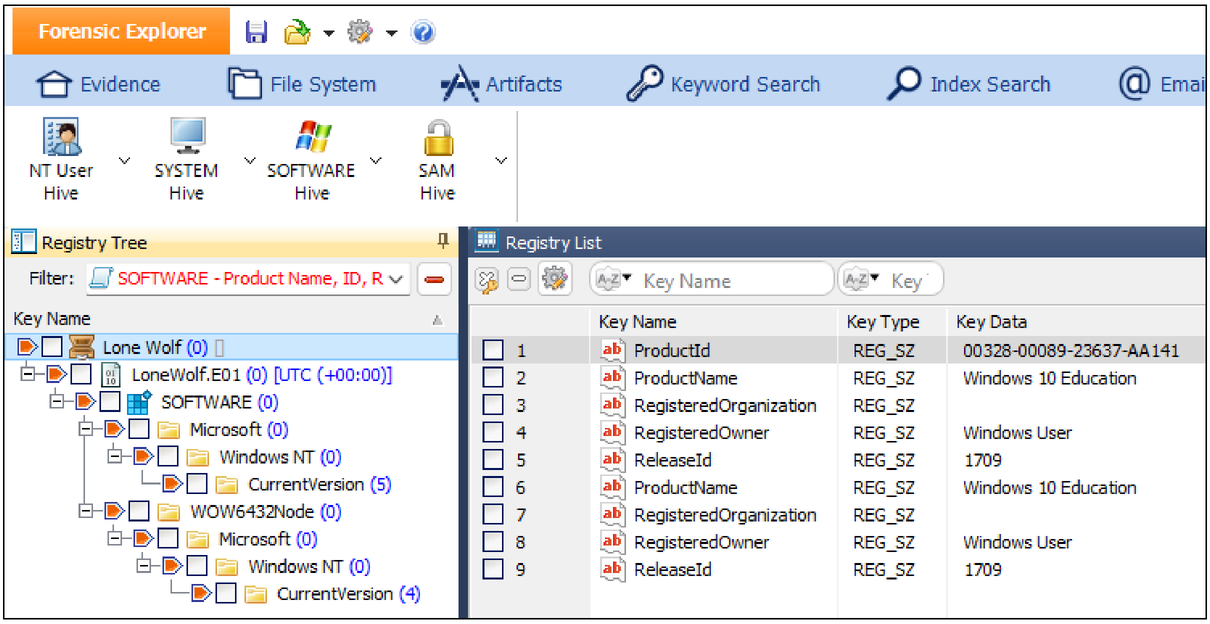
```
Search for:        SOFTWARE\Microsoft\Windows NT\CurrentVersion\ RegisteredOwner and RegisteredOrganization
Description:       Owner and organization details entered at installation. Can be modified.
Reference:         None.

==============================================================================================================

Key Found:     LoneWolf.E01\SOFTWARE\Microsoft\Windows NT\CurrentVersion\

  Value                                         Data
  ~~~~~                                         ~~~~
  RegisteredOwner                               Windows User
  RegisteredOrganization

--------------------------------------------------------------------------------
Registry Key Processor finished.
```

Q3. REGISTRY MODULE - SOURCE DATA

To examine the source registry keys:

1. **Branch plate** [▶] the entire **Registry** module.
2. Apply the folders filter: **SOFTWARE - Product Name, ID, Registered Organization and Owner.**

Figure 29: Registry > Folders filter > Software – Product Name, ID, Registered Organization and Owner



	Key Name	Key Type	Key Data
□ 1	ProductId	REG_SZ	00328-00089-23637-AA141
□ 2	ProductName	REG_SZ	Windows 10 Education
□ 3	RegisteredOrganization	REG_SZ	
□ 4	RegisteredOwner	REG_SZ	Windows User
□ 5	ReleaseId	REG_SZ	1709
□ 6	ProductName	REG_SZ	Windows 10 Education
□ 7	RegisteredOrganization	REG_SZ	
□ 8	RegisteredOwner	REG_SZ	Windows User
□ 9	ReleaseId	REG_SZ	1709

QUESTION 4 - TIME ZONE

What time zone was the computer set to when it was imaged?

Q4. ANSWER

Eastern Daylight time (-5 from UTC)

Q4. FORENSIC EXPLORER METHODOLOGY

Registered owner and organization information is stored in the following Registry location:

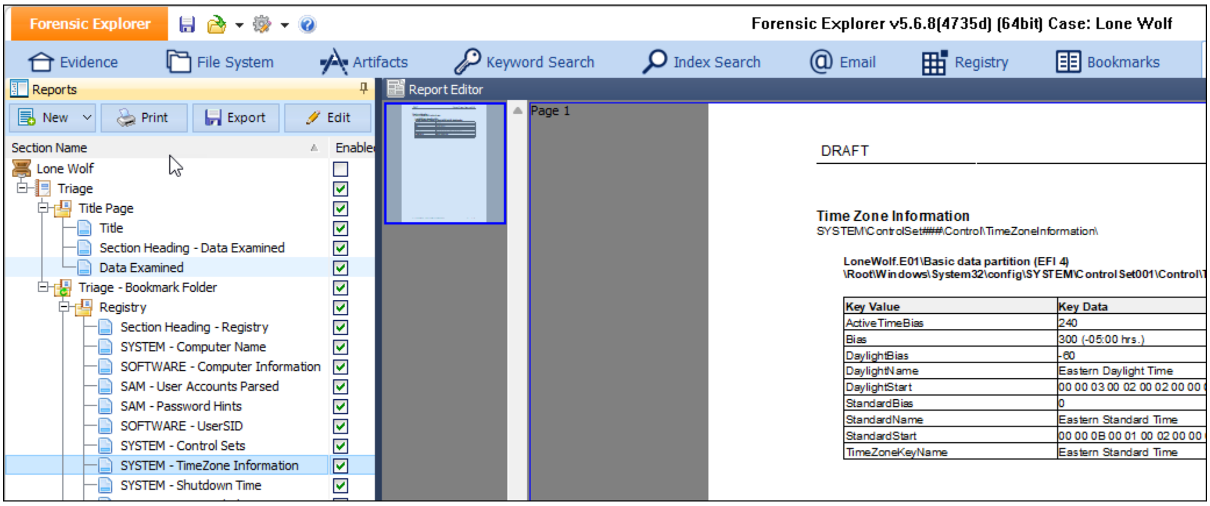
- **SYSTEM\ControlSet001\Control\TimeZoneInformation\TimeZoneKeyName**

Q4. TRIAGE REPORT

Select **Reports** module > **Triage** report:

1. In the report tree, select **Registry** > **SYSTEM - TimeZone Information** (If the Triage report is not populated see Triage on page 8 above).

Figure 30: Reports > Triage > SYSTEM: TimeZone Information



DRAFT

Time Zone Information
SYSTEM\ControlSet###\Control\TimeZoneInformation\

LoneWolf.E01\Basic data partition (EFI 4)
\Root\Windows\System32\config\SYSTEM\ControlSet001\Control\T

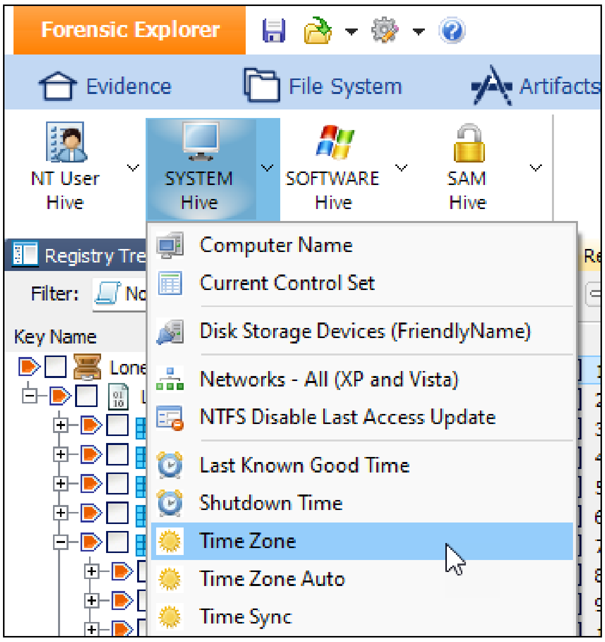
Key Value	Key Data
ActiveTimeBias	240
Bias	300 (-05:00 hrs.)
DaylightBias	-60
DaylightName	Eastern Daylight Time
DaylightStart	00 00 03 00 02 00 02 00 00
StandardBias	0
StandardName	Eastern Standard Time
StandardStart	00 00 0B 00 01 00 02 00 00
TimeZoneKeyName	Eastern Standard Time

Q4. REGISTRY MODULE - TOOLBAR

To examine registry data (see page 10 above to populate the Registry module):

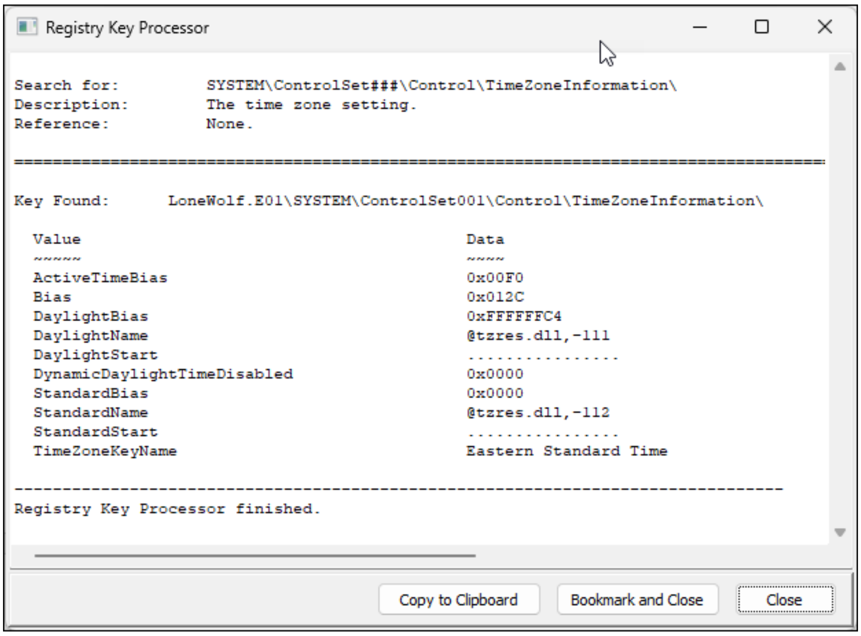
1. In the **Registry module toolbar**, select **Registry** > **SYSTEM Hive** > **Time Zone**.

Figure 31: Registry module > Toolbar > SYSTEM Hive > Time Zone



2. The following summary report will appear:

Figure 32: : Registry module toolbar > SYSTEM Hive > Time Zone



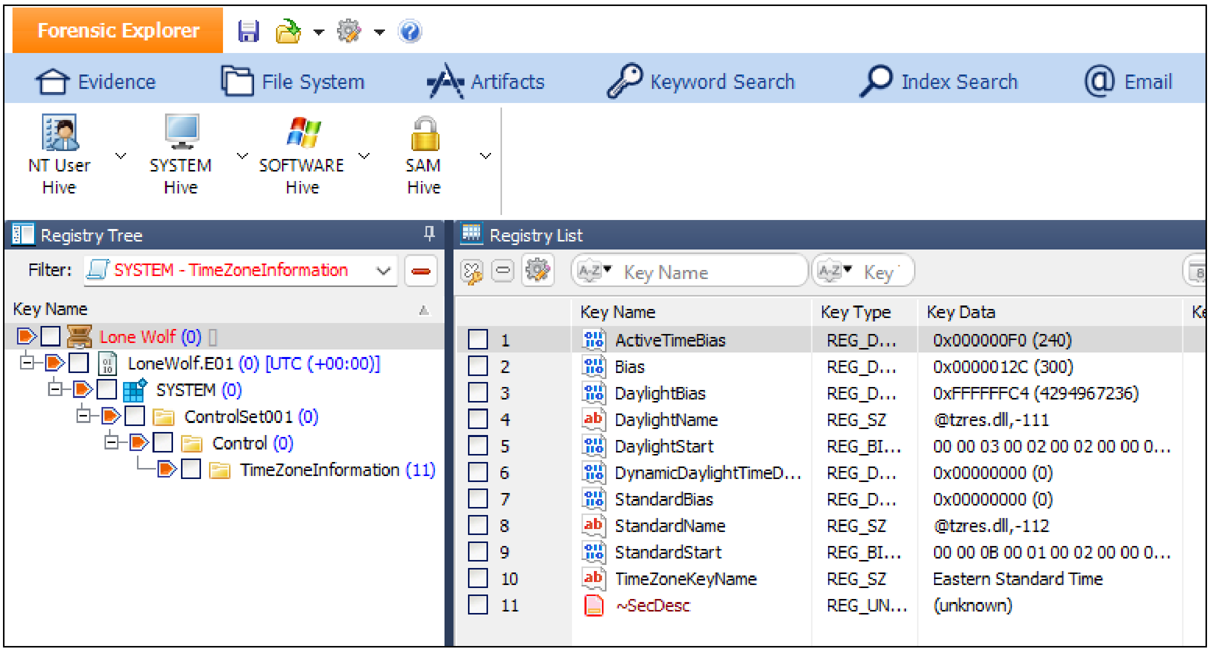
```
Search for:          SYSTEM\ControlSet###\Control\TimeZoneInformation\
Description:         The time zone setting.
Reference:           None.

=====================================================================================

Key Found:      LoneWolf.E01\SYSTEM\ControlSet001\Control\TimeZoneInformation\

  Value                                         Data
  ~~~~~                                         ~~~~
  ActiveTimeBias                                0x00F0
  Bias                                          0x012C
  DaylightBias                                  0xFFFFFFC4
  DaylightName                                  @tzres.dll,-111
  DaylightStart                                 ................
  DynamicDaylightTimeDisabled                   0x0000
  StandardBias                                  0x0000
  StandardName                                  @tzres.dll,-112
  StandardStart                                 ................
  TimeZoneKeyName                               Eastern Standard Time

--------------------------------------------------------------------------------
Registry Key Processor finished.
```

Q4. REGISTRY MODULE - SOURCE DATA

To examine the source registry keys:

1. **Branch plate** [▷] the entire **Registry** module.
2. Apply the folders filter: **SOFTWARE - Product Name, ID, Registered Organization and Owner.**

Figure 33: Registry > SYSTEM - TimeZoneInformation folders filter.



Filter: SYSTEM - TimeZoneInformation

Key Name

- Lone Wolf (0)
  - LoneWolf.E01 (0) [UTC (+00:00)]
    - SYSTEM (0)
      - ControlSet001 (0)
        - Control (0)
          - TimeZoneInformation (11)

	Key Name	Key Type	Key Data
□ 1	ActiveTimeBias	REG_D...	0x000000F0 (240)
□ 2	Bias	REG_D...	0x0000012C (300)
□ 3	DaylightBias	REG_D...	0xFFFFFFC4 (4294967236)
□ 4	DaylightName	REG_SZ	@tzres.dll,-111
□ 5	DaylightStart	REG_BI...	00 00 03 00 02 00 02 00 00 0...
□ 6	DynamicDaylightTimeD...	REG_D...	0x00000000 (0)
□ 7	StandardBias	REG_D...	0x00000000 (0)
□ 8	StandardName	REG_SZ	@tzres.dll,-112
□ 9	StandardStart	REG_BI...	00 00 0B 00 01 00 02 00 00 0...
□ 10	TimeZoneKeyName	REG_SZ	Eastern Standard Time
□ 11	~SecDesc	REG_UN...	(unknown)

QUESTION 5 - SYSTEM CLOCK

Was the system clock manually or automatically updated and how was this established?

Q5. ANSWER

Automatic.

Q5. FORENSIC EXPLORER METHODOLOGY

System time configuration settings are stored in the registry key:

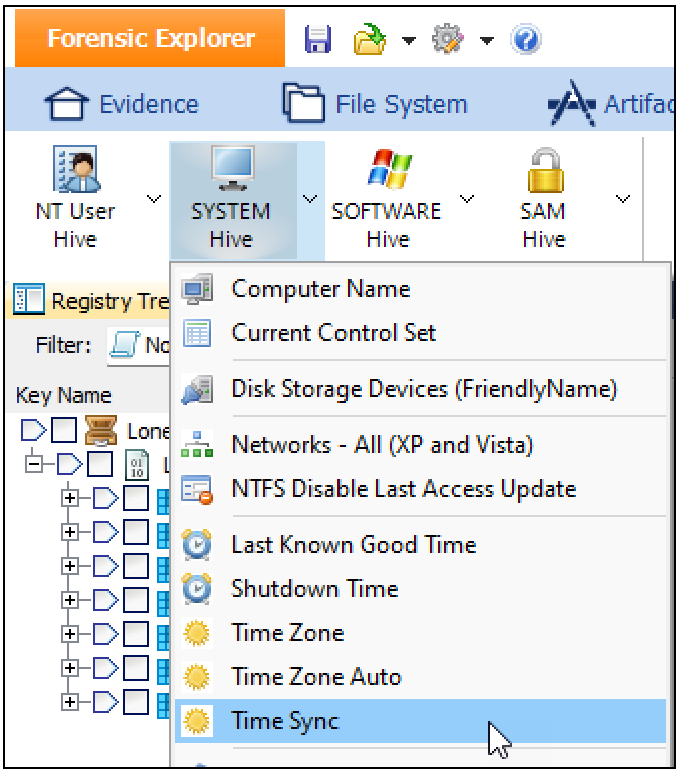
- **SYSTEM\ControlSet001\Services\W32Time\Parameters\Type**

Q5. REGISTRY MODULE - TOOLBAR

To examine registry data (see page 10 above to populate the Registry module):

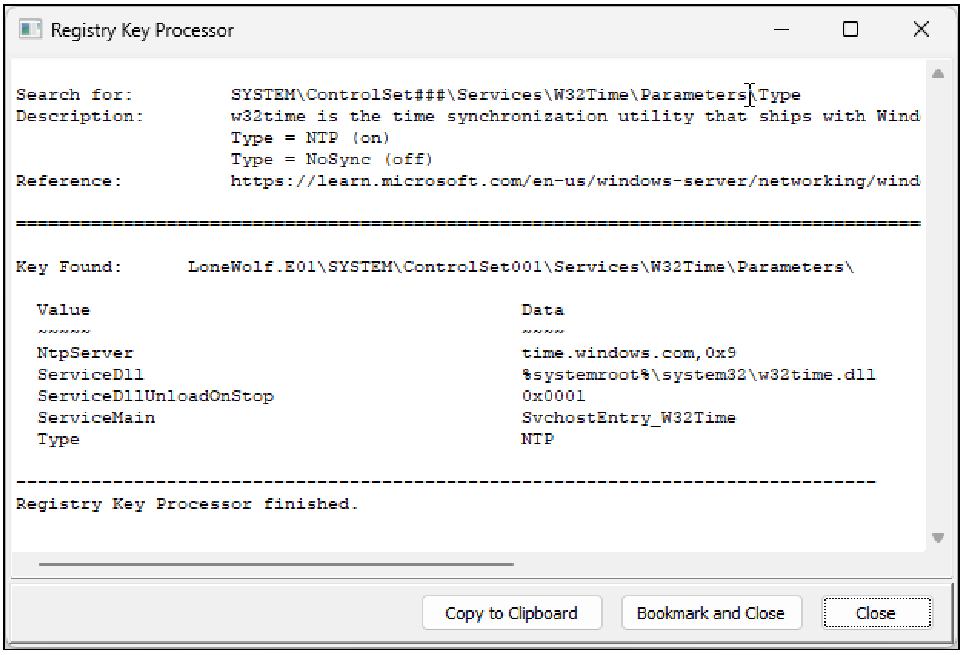
1. In the **Registry module toolbar**, select **SYSTEM Hive** > **Time Sync**.

Figure 34: Registry toolbar > SYSTEM Hive > Time Sync



3. The following summary report will appear:

Figure 35: Registry toolbar > Time Sync



```
Search for:         SYSTEM\ControlSet###\Services\W32Time\Parameters\Type
Description:        w32time is the time synchronization utility that ships with Wind
                    Type = NTP (on)
                    Type = NoSync (off)
Reference:          https://learn.microsoft.com/en-us/windows-server/networking/wind

==================================================================================

Key Found:      LoneWolf.E01\SYSTEM\ControlSet001\Services\W32Time\Parameters\

  Value                                         Data
  ~~~~~                                         ~~~~
  NtpServer                                     time.windows.com,0x9
  ServiceDll                                    %systemroot%\system32\w32time.dll
  ServiceDllUnloadOnStop                        0x0001
  ServiceMain                                   SvchostEntry_W32Time
  Type                                          NTP

--------------------------------------------------------------------------------
Registry Key Processor finished.
```

A Type value of **NTP** stands for Network Time Protocol, a protocol used for clock synchronization between computer systems over a network. When the Type registry key is set to NTP it means that the Windows Time service is configured to synchronize its clock with an NTP server.

When the Type registry key is set to **NoSync**, it means that the Windows Time service is not actively synchronizing its clock with an external time source such as a network time server (NTP). Instead, the system may rely on its internal clock without adjustment from external time sources.

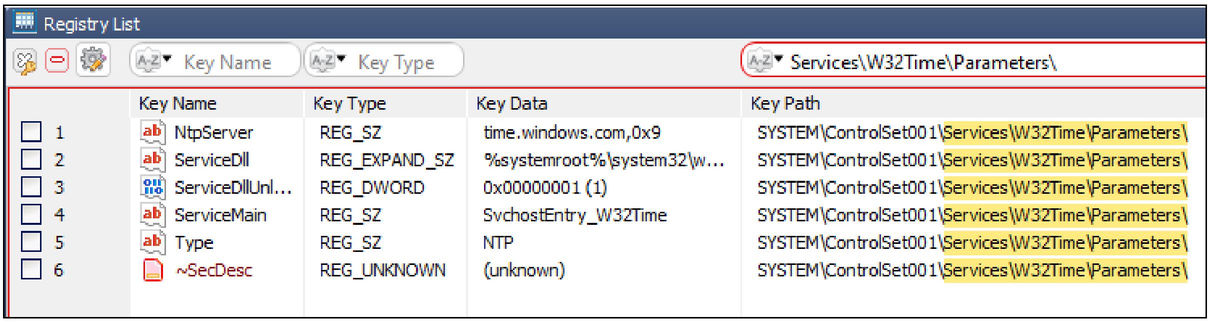
See https://learn.microsoft.com/en-us/windows-server/networking/windows-time-service/windows-time-service-tools-and-settings?tabs=config for more information.

Q5. REGISTRY MODULE - SOURCE DATA

To examine the source registry keys:

1. **Branch plate** [ ] the entire **Registry** module.
2. Filter the **Key Path** column for the path **Services\W32Time\Parameters\Type** and examine the **Type** value.

Figure 36: Registry > Key path filter for Services\W32Time\Parameters\.

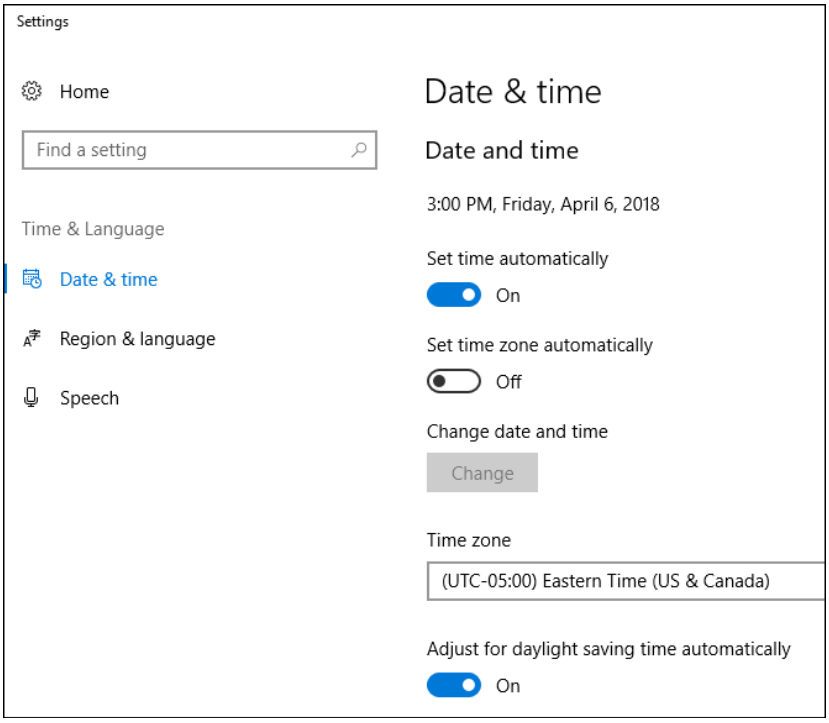


	Key Name	Key Type	Key Data	Key Path
□ 1	NtpServer	REG_SZ	time.windows.com,0x9	SYSTEM\ControlSet001\Services\W32Time\Parameters\
□ 2	ServiceDll	REG_EXPAND_SZ	%systemroot%\system32\w…	SYSTEM\ControlSet001\Services\W32Time\Parameters\
□ 3	ServiceDllUnl…	REG_DWORD	0x00000001 (1)	SYSTEM\ControlSet001\Services\W32Time\Parameters\
□ 4	ServiceMain	REG_SZ	SvchostEntry_W32Time	SYSTEM\ControlSet001\Services\W32Time\Parameters\
□ 5	Type	REG_SZ	NTP	SYSTEM\ControlSet001\Services\W32Time\Parameters\
□ 6	~SecDesc	REG_UNKNOWN	(unknown)	SYSTEM\ControlSet001\Services\W32Time\Parameters\

Q5. LIVE BOOT

Launch Live Boot (see Live Boot - Virtualization on page 11 above) and navigate in the jcloudy account to Windows **Date & Time Settings**. **Set time automatically** is in the **on** position.

Figure 37: Live Boot > jcloudy > Settings > Date & Time



Date & time

Date and time

3:00 PM, Friday, April 6, 2018

Set time automatically
On

Set time zone automatically
Off

Change date and time

Time zone
(UTC-05:00) Eastern Time (US & Canada)

Adjust for daylight saving time automatically
On

QUESTION 6 - USER ACCOUNT LOG

Which user account logged on at 30 Mar 2018 at 03:27 UTC or 29 Mar 2018 at 23:27 local time)?

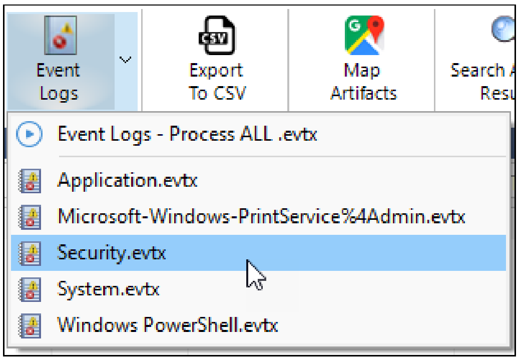
Q6. ANSWER

Jcloudy.

Q6. FORENSIC EXPLORER METHODOLOGY

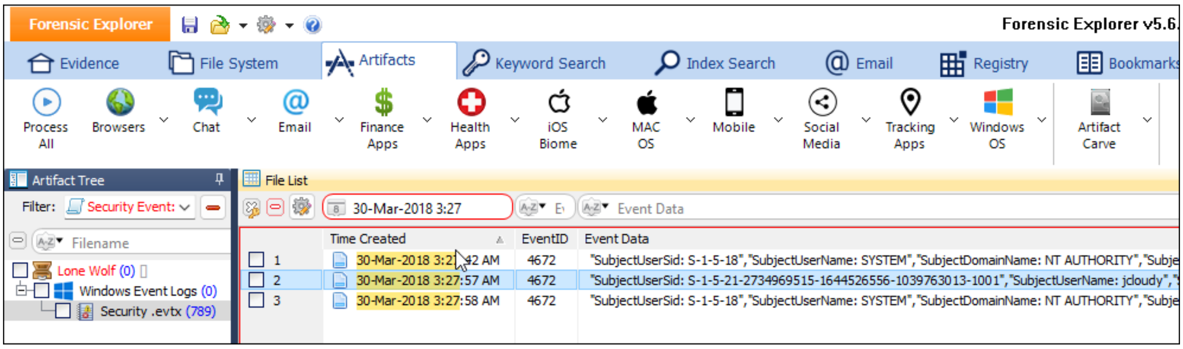
In the **Artifacts** module select **Event Logs** > **Security.evtx**.

Figure 38: Artifacts > Event Logs > Security.evtx



1. Select the folders filter Security Event: 4672 Account logon with superuser rights (Administrator).
2. Double click on the **Time Created** column to sort.
3. In the **Time Created** column, filter for the value **30 Mar 2018 at 03:27**.

Figure 39: Artifacts > Event Logs > Security.evtx > Time Created column filter.



30-Mar-2018 3:27

	Time Created	EventID	Event Data
1	30-Mar-2018 3:2?:42 AM	4672	"SubjectUserSid: S-1-5-18","SubjectUserName: SYSTEM","SubjectDomainName: NT AUTHORITY","Subje
2	30-Mar-2018 3:27:57 AM	4672	"SubjectUserSid: S-1-5-21-2734969515-1644526556-1039763013-1001","SubjectUserName: jcloudy","
3	30-Mar-2018 3:27:58 AM	4672	"SubjectUserSid: S-1-5-18","SubjectUserName: SYSTEM","SubjectDomainName: NT AUTHORITY","Subje

Examine the **Event Data** column to locate the following text:

"SubjectUserSid: S-1-5-21-2734969515-1644526556-1039763013-1001","SubjectUserName: jcloudy","SubjectDomainName: DESKTOP-PM6C56D","SubjectLogonId: 0x0000000003AD0561"

QUESTION 7 - LAST SHUTDOWN

When was the computer last shutdown (date and time)?

Q7. ANSWER

27 Mar 2018 at 21:45 (UTC or 17:45 local time)

Q7. FORENSIC EXPLORER METHODOLOGY

Shutdown Time is stored in the following Registry location:

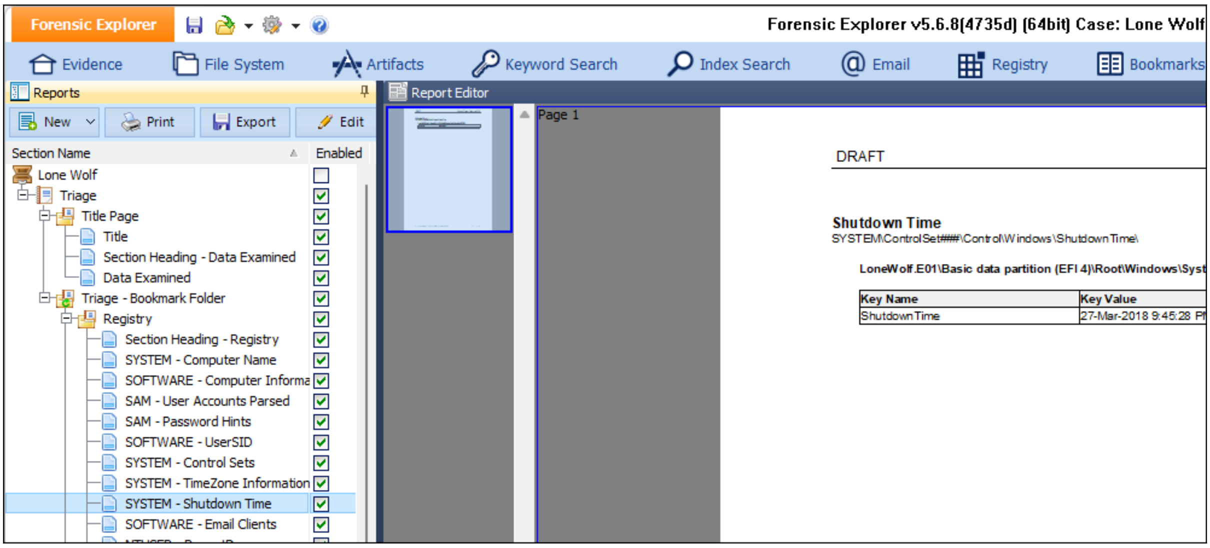
- **SYSTEM\ControlSet001\Control\Windows\ShutdownTime**

Q7. TRIAGE REPORT

Select **Reports** module > **Triage** report:

1. In the report tree, select **Registry** > **SYSTEM - Shutdown Time** (If the Triage report is not populated see Triage on page 8 above).

Figure 40: Reports > Triage > Registry > SYSTEM - Shutdown Time



DRAFT

Shutdown Time
SYSTEM\ControlSet####\Control\Windows\ShutdownTime\

LoneWolf.E01\Basic data partition (EFI 4)\Root\Windows\Syst

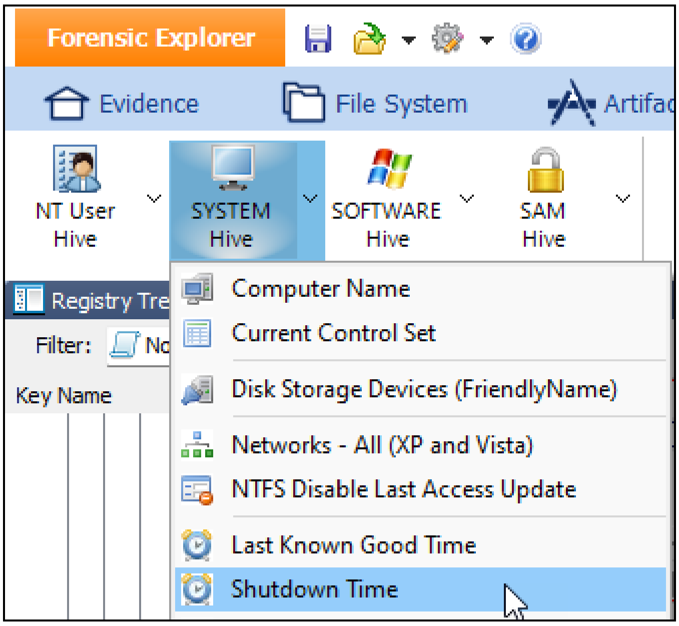
Key Name	Key Value
ShutdownTime	27-Mar-2018 9:45:28 P

Q7. REGISTRY MODULE - TOOLBAR

To examine registry data (see page 10 above to populate the Registry module):

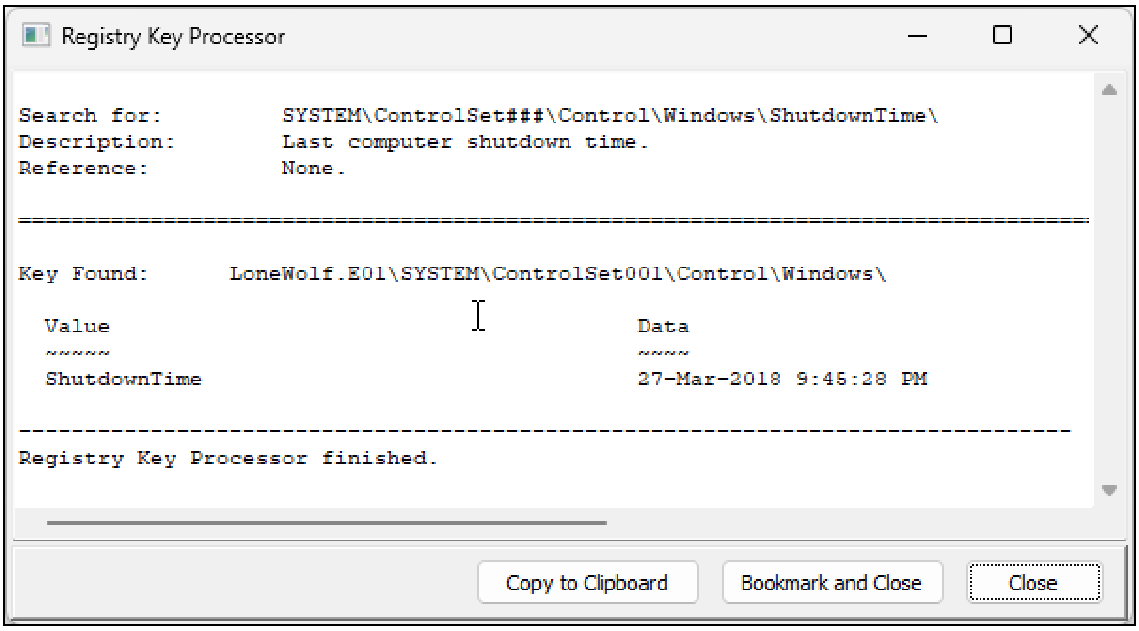
1. In the **Registry module toolbar**, select **System Hive** > **Shutdown Time**.

Figure 41: Registry > Toolbar > SYSTEM Hive > Shutdown Time



2. The following summary report with appear:

Figure 42: Registry > Toolbar > SYSTEM Hive > Shutdown Time > Results.



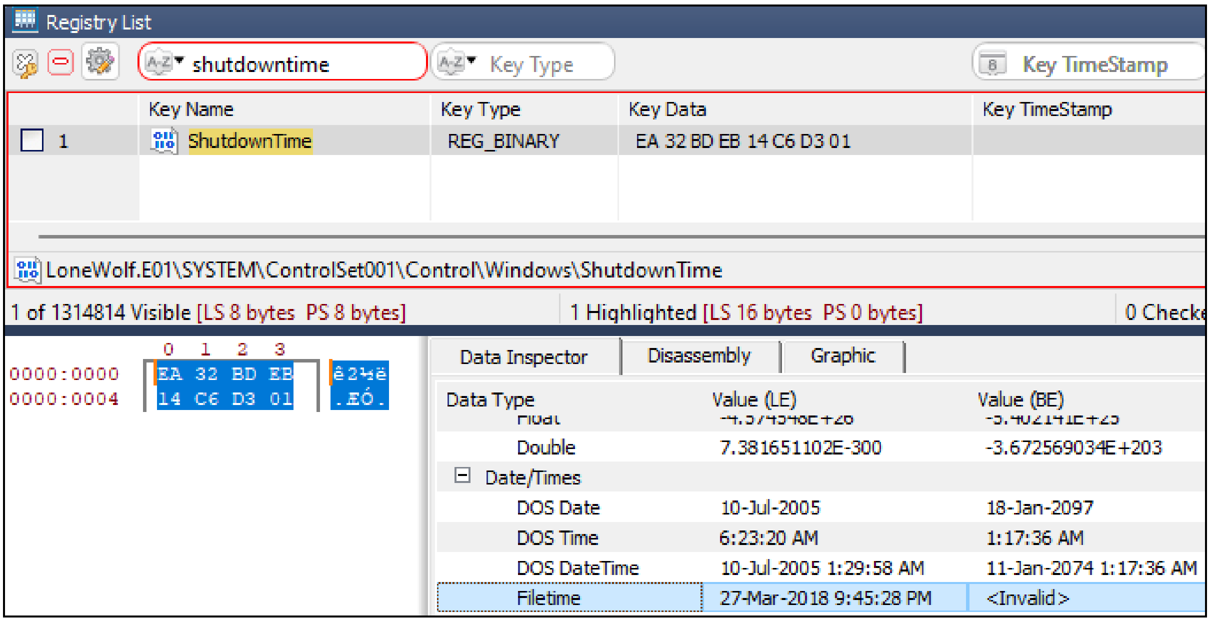
```
Search for:         SYSTEM\ControlSet###\Control\Windows\ShutdownTime\
Description:        Last computer shutdown time.
Reference:          None.

==================================================================================

Key Found:      LoneWolf.E01\SYSTEM\ControlSet001\Control\Windows\

  Value                                          Data
  ~~~~~                                          ~~~~
  ShutdownTime                                   27-Mar-2018 9:45:28 PM

--------------------------------------------------------------------------------
Registry Key Processor finished.
```

Q7. REGISTRY MODULE - SOURCE DATA

To examine the source registry data:

1. **Branch plate** [ ] the entire **Registry** module.
2. Apply the folders filter: **Registry Keys** > **SYSTEM - Shutdown Time**.
3. Highlight the **Key Data** in the **Hex** view. The 8 bytes will be decoded as **Filetime**.

Figure 43: Registry > Key Name filter > Shutdown Time > Hex > Filetime.



	Key Name	Key Type	Key Data	Key TimeStamp
□ 1	ShutdownTime	REG_BINARY	EA 32 BD EB 14 C6 D3 01	

LoneWolf.E01\SYSTEM\ControlSet001\Control\Windows\ShutdownTime

1 of 1314814 Visible [LS 8 bytes PS 8 bytes] 1 Highlighted [LS 16 bytes PS 0 bytes] 0 Checke

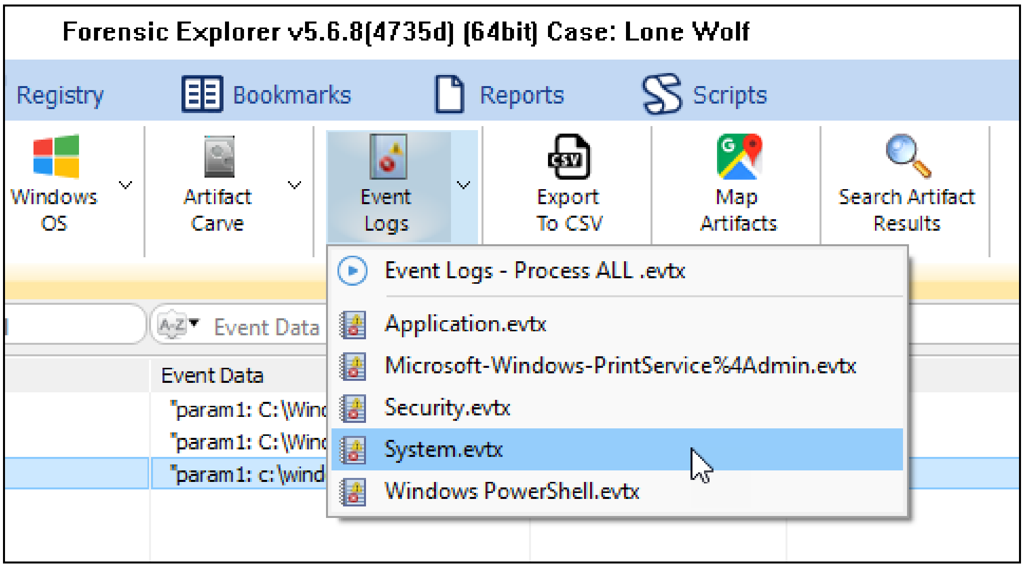
```
           0  1  2  3
0000:0000  EA 32 BD EB   ê2½ë
0000:0004  14 C6 D3 01   .ÆÓ.
```

Data Type	Value (LE)	Value (BE)
Float	[illegible]	[illegible]
Double	7.381651102E-300	-3.672569034E+203
⊟ Date/Times		
DOS Date	10-Jul-2005	18-Jan-2097
DOS Time	6:23:20 AM	1:17:36 AM
DOS DateTime	10-Jul-2005 1:29:58 AM	11-Jan-2074 1:17:36 AM
Filetime	27-Mar-2018 9:45:28 PM	<Invalid>

Q7. ARTIFACTS MODULE - WINDOWS EVENT LOGS (.EVTX)

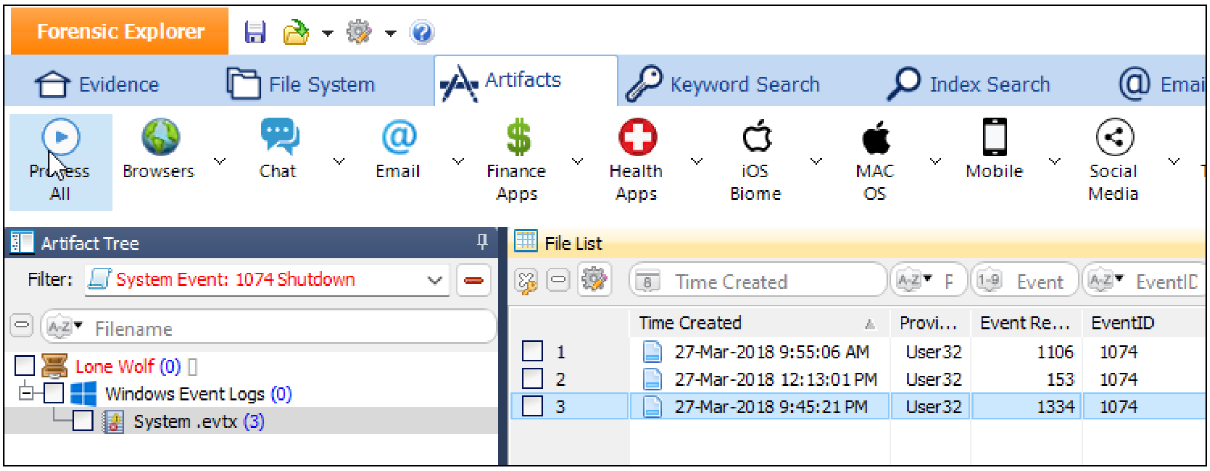
In the **Artifacts** module select Event Logs > System.evtx.

Figure 44: Artifacts > Event Logs > System.evtx



1. Once System event logs are populated in the Artifacts module, select the folders filter **System Event: 1074 Shutdown**.
2. Double click on the **Time Created** column to sort the filtered logs.
3. Locate the last shutdown event **Time Created** value.

Figure 45: Artifacts > System Event: 1074 Shutdown



Filter: System Event: 1074 Shutdown

	Time Created	Provi...	Event Re...	EventID
1	27-Mar-2018 9:55:06 AM	User32	1106	1074
2	27-Mar-2018 12:13:01 PM	User32	153	1074
3	27-Mar-2018 9:45:21 PM	User32	1334	1074

QUESTION 8 - PASSWORD RELATIVE ID

Is a password required for the user account with a RID (Relative Identifier) of interest and how do you know this?

Q8. ANSWER

The password for the **jcloudy** user account is: Jcloudy2018!!

Q8. FORENSIC EXPLORER METHODOLOGY

The Live Boot process (described in Live Boot - Virtualization on page 11 above) identified that the **jcloudy** account was protected by a Windows user password.

A Relative Identifier (RID) is a unique number assigned to each security principal (user, group, or computer) in a Windows environment. The RID of interest is taken to be the one assigned to the jcloudy user account.

Windows uses a cryptographic hash function to convert the plain-text password into a fixed-length string of characters, which is the hashed password. The hashed password, known as a NTLM hash, is then stored in the Windows Security Accounts Manager (SAM) database.

To extract **NTLM** hashes:

1. In the **File System module** toolbar, select **Analysis Programs > NTLM Hash Extract**.

Figure 46: NTLM Hash Extract.

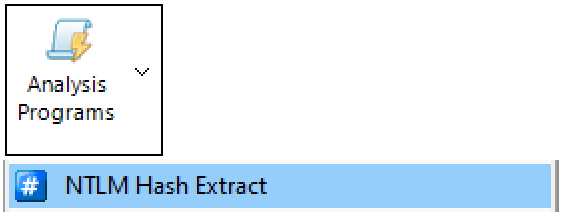
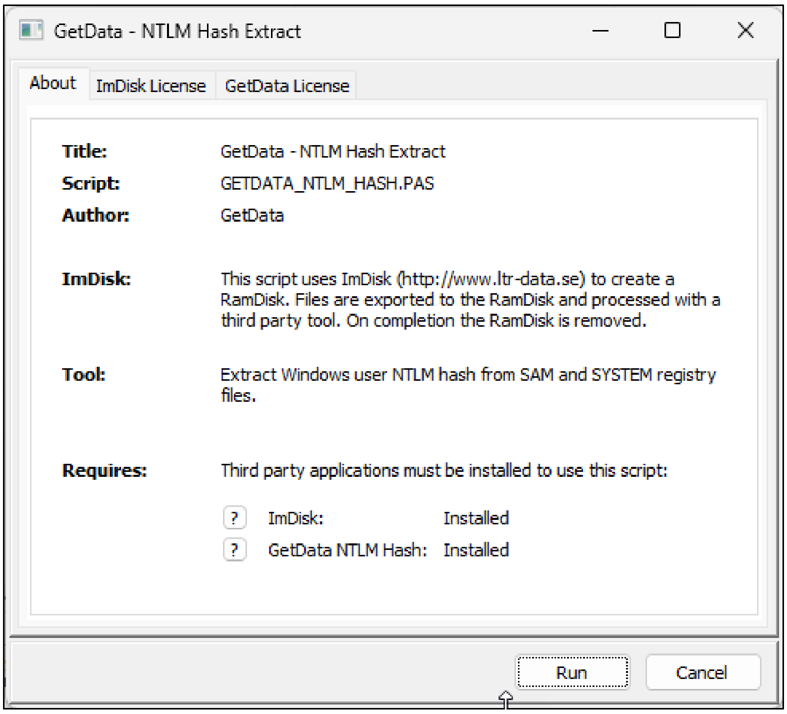


Figure 47: : GetData NTLM Hash Extract



Title: GetData - NTLM Hash Extract
Script: GETDATA_NTLM_HASH.PAS
Author: GetData

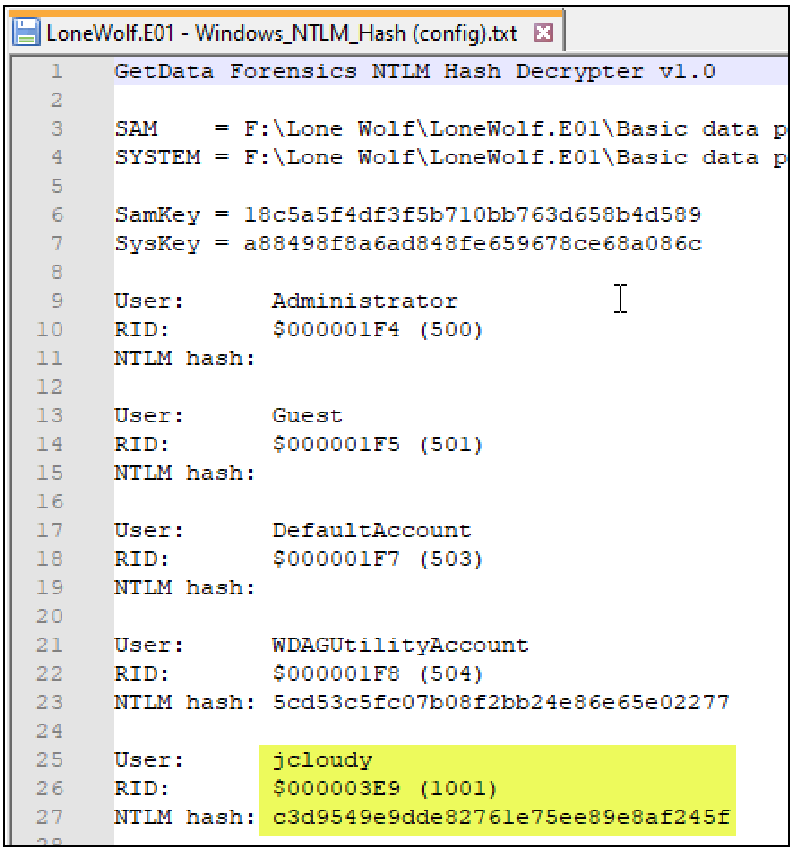
ImDisk: This script uses ImDisk (http://www.ltr-data.se) to create a RamDisk. Files are exported to the RamDisk and processed with a third party tool. On completion the RamDisk is removed.

Tool: Extract Windows user NTLM hash from SAM and SYSTEM registry files.

Requires: Third party applications must be installed to use this script:

?	ImDisk:	Installed
?	GetData NTLM Hash:	Installed

Figure 48: GetData NTLM Hash Extract > Output.



```
GetData Forensics NTLM Hash Decrypter v1.0

SAM    = F:\Lone Wolf\LoneWolf.E01\Basic data p
SYSTEM = F:\Lone Wolf\LoneWolf.E01\Basic data p

SamKey = 18c5a5f4df3f5b710bb763d658b4d589
SysKey = a88498f8a6ad848fe659678ce68a086c

User:      Administrator
RID:       $000001F4 (500)
NTLM hash:

User:      Guest
RID:       $000001F5 (501)
NTLM hash:

User:      DefaultAccount
RID:       $000001F7 (503)
NTLM hash:

User:      WDAGUtilityAccount
RID:       $000001F8 (504)
NTLM hash: 5cd53c5fc07b08f2bb24e86e65e02277

User:      jcloudy
RID:       $000003E9 (1001)
NTLM hash: c3d9549e9dde82761e75ee89e8af245f
```

There are a number of online NTM decryption websites, such as https://md5decrypt.net/en/Ntlm/ which decode known hash values. The jcloudy has decodes to be: **Jcloudy2018!!**

QUESTION 9 - PASSWORD HINT

What is the Password Hint for the jcloudy user account?

Q9. ANSWER

It’s me you idiot!

Q9. FORENSIC EXPLORER METHODOLOGY

Password hint data is stored in the following **Registry** location:

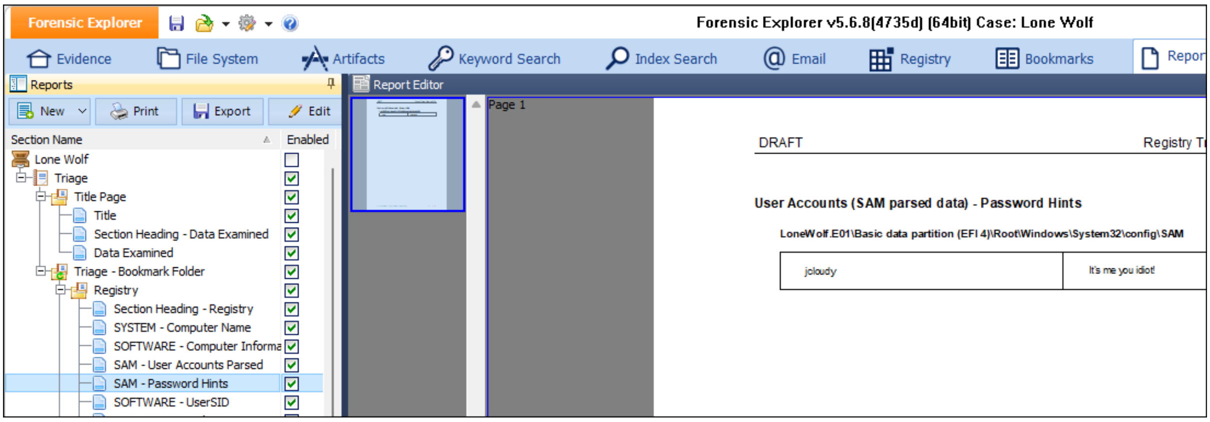
- **SAM\SAM\Domains\Account\Users\000003E9\UserPasswordHint**

Q9. TRIAGE REPORT

Select **Reports** module > **Triage** report:

1. In the report tree, select **SAM - Password Hints** (If the Triage report is not populated see Triage on page 8 above).

Figure 49: Reports > Triage > Registry > SAM - Password Hints



DRAFT — Registry T

User Accounts (SAM parsed data) - Password Hints

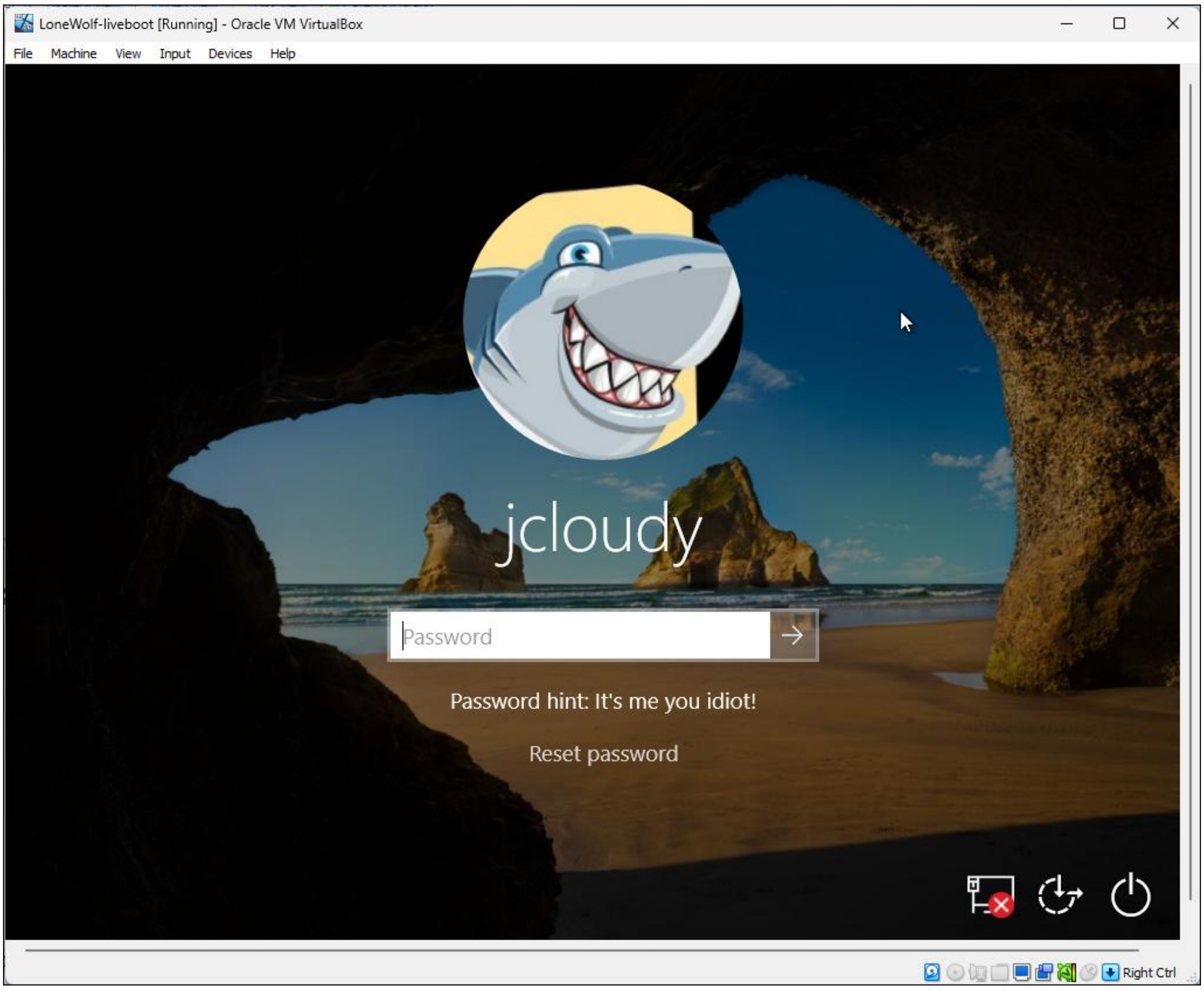
LoneWolf.E01\Basic data partition (EFI 4)\Root\Windows\System32\config\SAM

jcloudy	It's me you idiot!

Q9. LIVE BOOT - VIRTUALIZATION

Launch Live Boot (see Live Boot - Virtualization on page 11 above). At the jcloudy login screen, cycle through an incorrect password to display the password hint.

Figure 50: Live Boot > jcloudy > Password Hint



jcloudy

Password

Password hint: It's me you idiot!

Reset password

QUESTION 10 - SSID

What is the SSID of the wireless network that this computer was connected to?

Q10. ANSWER

Net 2.4.

Q10. FORENSIC EXPLORER METHODOLOGY

SSID stands for **Service Set Identifier**, and it is the name of a wireless network. SSID information is stored in the following Registry location:

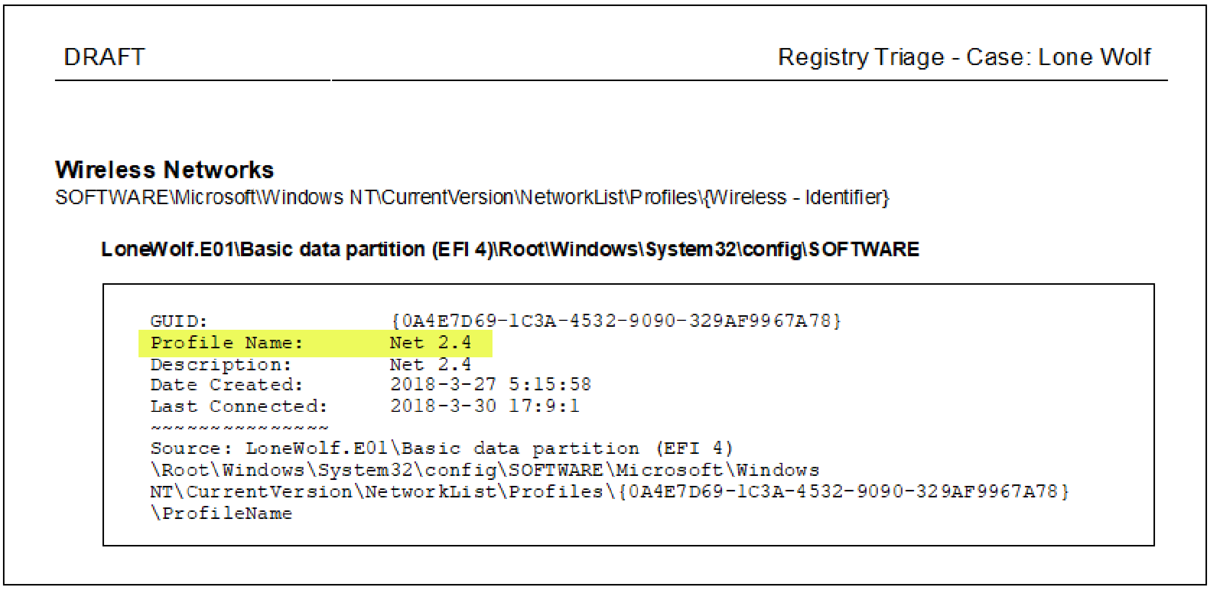
- **SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{GUID}\ProfileName**

Q10. TRIAGE REPORT

Select **Reports** module > **Triage** report:

1. In the report tree, select **Registry** > **SOFTWARE - Wireless Networks** (If the Triage report is not populated see Triage on page 8 above).

Figure 51: Reports > Triage > Registry > SOFTWARE - Wireless Networks



DRAFT   Registry Triage - Case: Lone Wolf

Wireless Networks

SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{Wireless - Identifier}

LoneWolf.E01\Basic data partition (EFI 4)\Root\Windows\System32\config\SOFTWARE

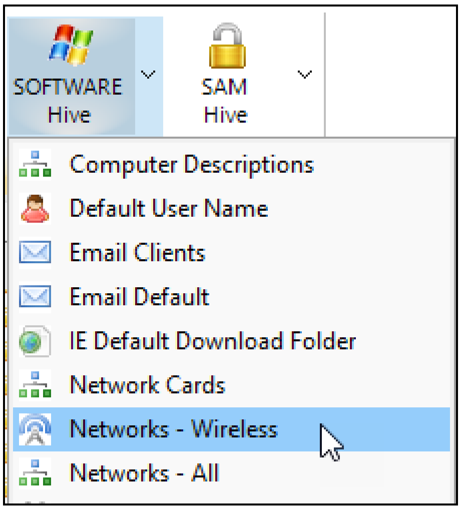
```
GUID:                   {0A4E7D69-1C3A-4532-9090-329AF9967A78}
Profile Name:           Net 2.4
Description:            Net 2.4
Date Created:           2018-3-27 5:15:58
Last Connected:         2018-3-30 17:9:1
~~~~~~~~~~~~~~~
Source: LoneWolf.E01\Basic data partition (EFI 4)
\Root\Windows\System32\config\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\NetworkList\Profiles\{0A4E7D69-1C3A-4532-9090-329AF9967A78}
\ProfileName
```

Q10. REGISTRY MODULE - TOOLBAR

To examine registry hive data: (see page 10 above to populate the Registry module).

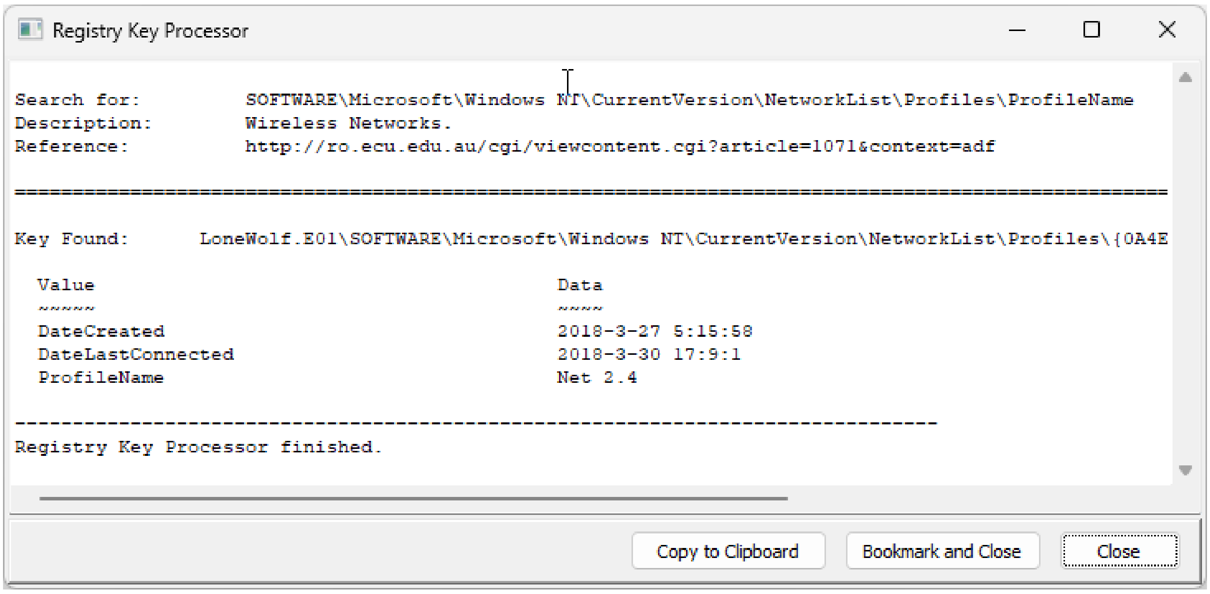
1. In the **Registry module toolbar**, select **SOFTWARE Hive** > **Networks - Wireless**.

Figure 52: Registry > Software HIVE > Networks - Wireless



2. The following summary report with appear:

Figure 53: Registry > SOFTWARE Hive > Networks – Wireless > Output.



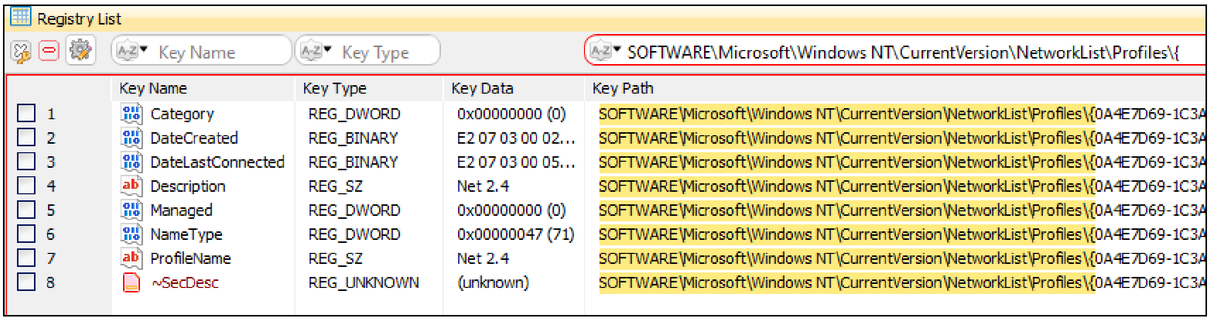
```
Search for:         SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\ProfileName
Description:        Wireless Networks.
Reference:          http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1071&context=adf

====================================================================================================

Key Found:      LoneWolf.E01\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{0A4E

  Value                                        Data
  ~~~~~                                        ~~~~
  DateCreated                                  2018-3-27 5:15:58
  DateLastConnected                            2018-3-30 17:9:1
  ProfileName                                  Net 2.4

--------------------------------------------------------------------------------
Registry Key Processor finished.
```

Q10. REGISTRY MODULE - SOURCE DATA

To examine the source registry keys:

1. **Branch plate** [▶] the entire **Registry** module.
2. Apply a **Key** Path column filter: **SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{**

Figure 54: Registry > Key Path filter > NetworkList\Profiles

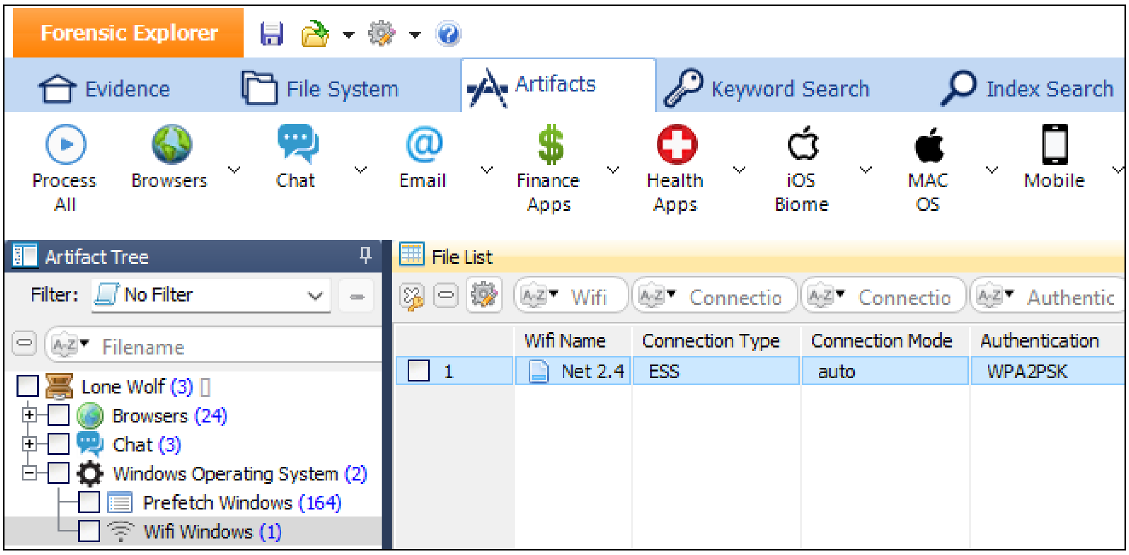

Registry List
Key Name
Key Type
SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{

		Key Name	Key Type	Key Data	Key Path
□	1	Category	REG_DWORD	0x00000000 (0)	SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{0A4E7D69-1C3A
□	2	DateCreated	REG_BINARY	E2 07 03 00 02…	SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{0A4E7D69-1C3A
□	3	DateLastConnected	REG_BINARY	E2 07 03 00 05…	SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{0A4E7D69-1C3A
□	4	Description	REG_SZ	Net 2.4	SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{0A4E7D69-1C3A
□	5	Managed	REG_DWORD	0x00000000 (0)	SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{0A4E7D69-1C3A
□	6	NameType	REG_DWORD	0x00000047 (71)	SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{0A4E7D69-1C3A
□	7	ProfileName	REG_SZ	Net 2.4	SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{0A4E7D69-1C3A
□	8	~SecDesc	REG_UNKNOWN	(unknown)	SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{0A4E7D69-1C3A

Q10. ARTIFACTS MODULE

In the Artifacts module the Wifi Windows name is collected from a different source.

Figure 55: Artifacts > Windows Operating System > Wifi Windows



Filter: No Filter

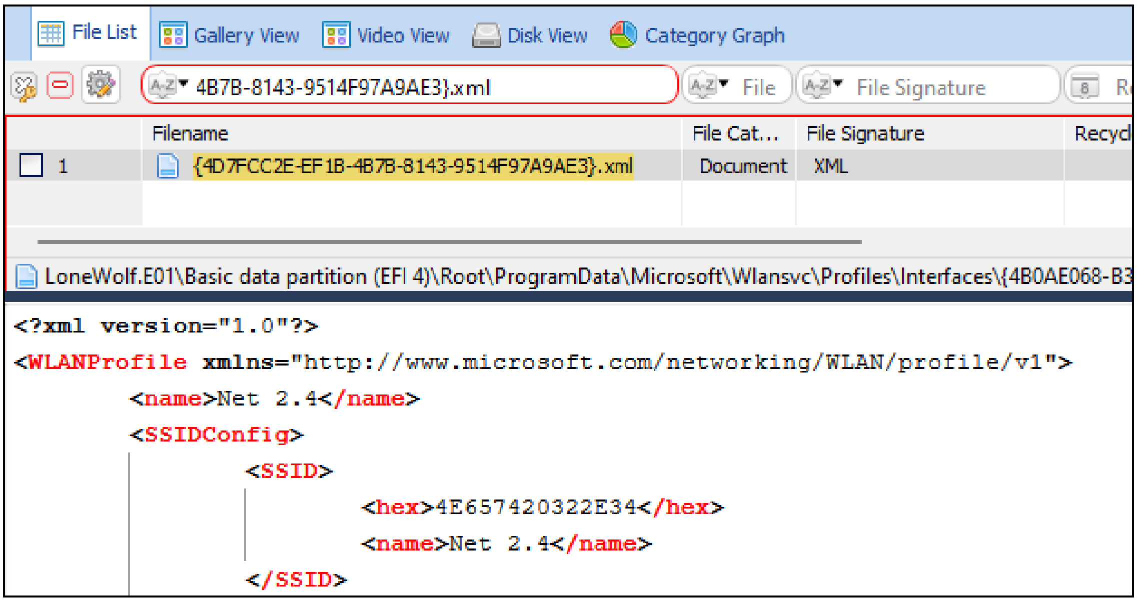
- □ Lone Wolf (3)
  - □ Browsers (24)
  - □ Chat (3)
  - □ Windows Operating System (2)
    - □ Prefetch Windows (164)
    - □ Wifi Windows (1)

	Wifi Name	Connection Type	Connection Mode	Authentication
□ 1	Net 2.4	ESS	auto	WPA2PSK

Use the **Source Name** and **Source Path** columns to locate the source file:

1. **Branch plate** [▶] the entire **File System** module.
2. Apply a **Filename** column filter for the source name: {4D7FCC2E-EF1B-4B7B-8143-9514F97A9AE3}.xml.
3. Switch to **Display** view to view the xml content of the file.

Figure 56: File System > Filename filter.



4B7B-8143-9514F97A9AE3}.xml

	Filename	File Cat...	File Signature	Recycl
□ 1	{4D7FCC2E-EF1B-4B7B-8143-9514F97A9AE3}.xml	Document	XML	

LoneWolf.E01\Basic data partition (EFI 4)\Root\ProgramData\Microsoft\Wlansvc\Profiles\Interfaces\{4B0AE068-B3

```
<?xml version="1.0"?>
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
        <name>Net 2.4</name>
        <SSIDConfig>
                <SSID>
                        <hex>4E657420322E34</hex>
                        <name>Net 2.4</name>
                </SSID>
```

QUESTION 11 - TRUE OR FALSE

True or false: There was an externally connected USB device attached to this computer?

Q11. ANSWER

True - SanDisk Extreme.

Q11. FORENSIC EXPLORER METHODOLOGY

See Question 12 below.

QUESTION 12 - USB DRIVES

What is the serial number, vendor and product identifier for any USB drive(s), identified within the Lone Wolf evidence file?

Q12. ANSWER

Serial #: AA010215170355310594, Vendor ID: 0781, Product ID: 5580 (SanDisk Extreme)

Serial #: AA010603160707470215, Vendor ID: 0781, Product ID: 5580 (SanDisk Extreme)

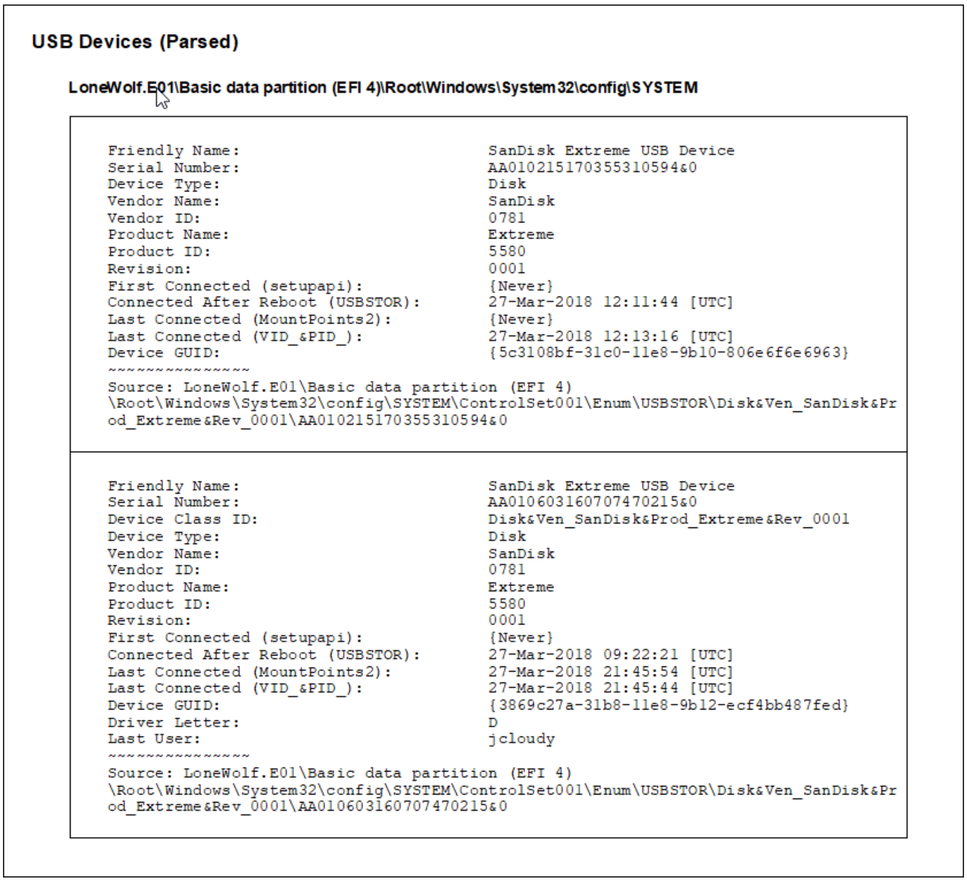
Q12. FORENSIC EXPLORER METHODOLOGY

Q12. TRIAGE REPORT

Select **Reports** module > **Triage** report:

1. In the report tree, select **SYSTEM - USBStor Parsed** (If the Triage report is not populated see Triage on page 8 above).

Figure 57: Reports > Triage > Registry > SYSTEM - USBStor Parsed



USB Devices (Parsed)

LoneWolf.E01\Basic data partition (EFI 4)\Root\Windows\System32\config\SYSTEM

```
Friendly Name:                         SanDisk Extreme USB Device
Serial Number:                         AA010215170355310594&0
Device Type:                           Disk
Vendor Name:                           SanDisk
Vendor ID:                             0781
Product Name:                          Extreme
Product ID:                            5580
Revision:                              0001
First Connected (setupapi):            {Never}
Connected After Reboot (USBSTOR):      27-Mar-2018 12:11:44 [UTC]
Last Connected (MountPoints2):         {Never}
Last Connected (VID_&PID_):            27-Mar-2018 12:13:16 [UTC]
Device GUID:                           {5c3108bf-31c0-11e8-9b10-806e6f6e6963}
~~~~~~~~~~~~~~~
Source: LoneWolf.E01\Basic data partition (EFI 4)
\Root\Windows\System32\config\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_SanDisk&Pr
od_Extreme&Rev_0001\AA010215170355310594&0
```

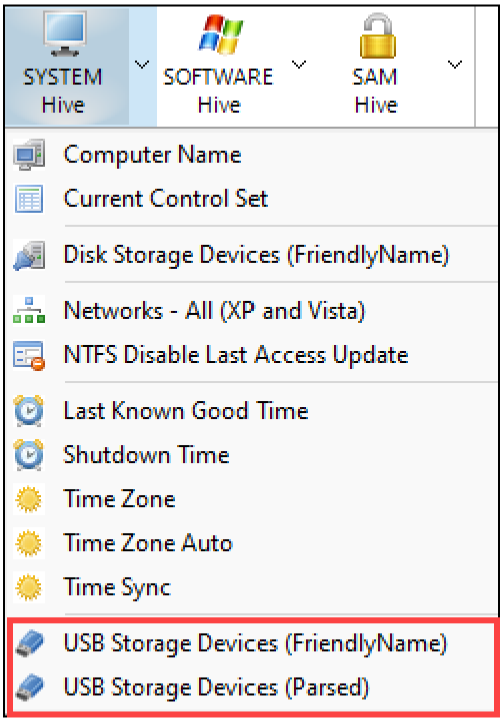
```
Friendly Name:                         SanDisk Extreme USB Device
Serial Number:                         AA010603160707470215&0
Device Class ID:                       Disk&Ven_SanDisk&Prod_Extreme&Rev_0001
Device Type:                           Disk
Vendor Name:                           SanDisk
Vendor ID:                             0781
Product Name:                          Extreme
Product ID:                            5580
Revision:                              0001
First Connected (setupapi):            {Never}
Connected After Reboot (USBSTOR):      27-Mar-2018 09:22:21 [UTC]
Last Connected (MountPoints2):         27-Mar-2018 21:45:54 [UTC]
Last Connected (VID_&PID_):            27-Mar-2018 21:45:44 [UTC]
Device GUID:                           {3869c27a-31b8-11e8-9b12-ecf4bb487fed}
Driver Letter:                         D
Last User:                             jcloudy
~~~~~~~~~~~~~~~
Source: LoneWolf.E01\Basic data partition (EFI 4)
\Root\Windows\System32\config\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_SanDisk&Pr
od_Extreme&Rev_0001\AA010603160707470215&0
```

Q12. REGISTRY MODULE - TOOLBAR

To examine registry data (see page 10 above to populate the Registry module):

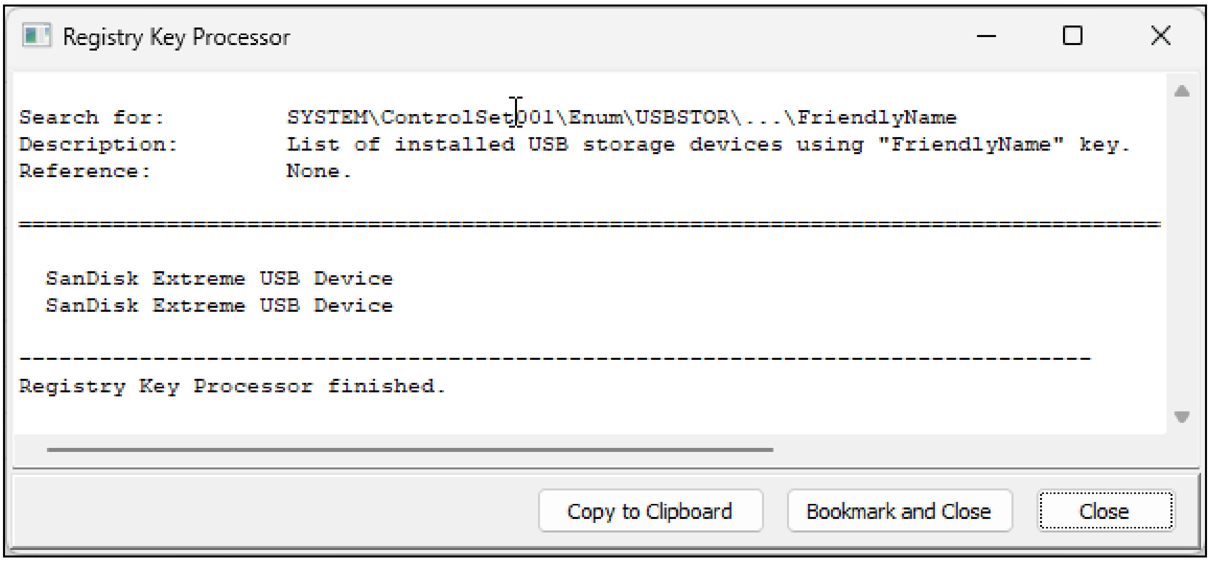
1. In the **Registry module toolbar**, select **SYSTEM Hive** > **USB Storage Devices (FriendlyName)**.

Figure 58: Registry > SYSTEM **Hive >** USB Storage Devices (FriendlyName)


SYSTEM Hive
SOFTWARE Hive
SAM Hive
Computer Name
Current Control Set
Disk Storage Devices (FriendlyName)
Networks - All (XP and Vista)
NTFS Disable Last Access Update
Last Known Good Time
Shutdown Time
Time Zone
Time Zone Auto
Time Sync
USB Storage Devices (FriendlyName)
USB Storage Devices (Parsed)

2. The following summary report will appear:

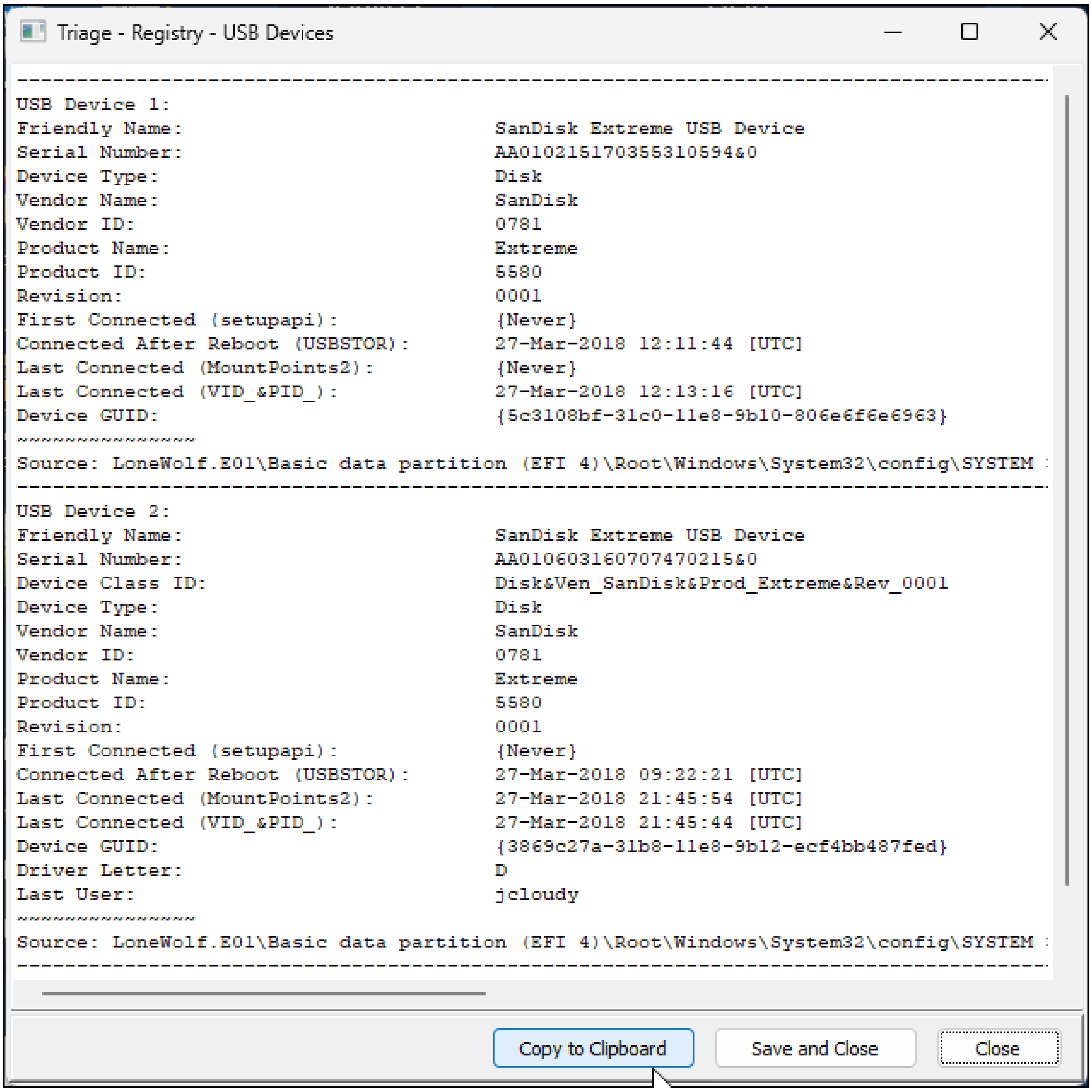
Figure 59: Registry > SYSTEM **Hive >** USB Storage Devices (FriendlyName)



```
Search for:         SYSTEM\ControlSet001\Enum\USBSTOR\...\FriendlyName
Description:        List of installed USB storage devices using "FriendlyName" key.
Reference:          None.

=====================================================================================

  SanDisk Extreme USB Device
  SanDisk Extreme USB Device

--------------------------------------------------------------------------------
Registry Key Processor finished.
```

3. In the **Registry module toolbar**, select **SYSTEM Hive** > **USB Storage Devices (Parsed)**. The following summary report will appear:

Figure 60: Registry > SYSTEM Hive > USB Storage Devices (Parsed).

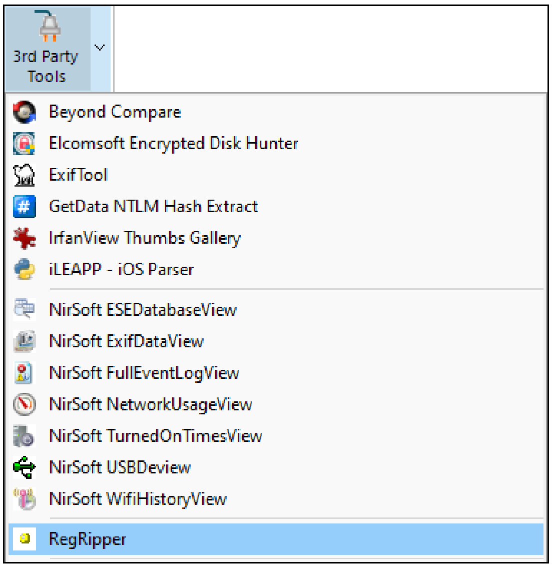


```
-------------------------------------------------------------------------------------
USB Device 1:
Friendly Name:                          SanDisk Extreme USB Device
Serial Number:                          AA010215170355310594&0
Device Type:                            Disk
Vendor Name:                            SanDisk
Vendor ID:                              0781
Product Name:                           Extreme
Product ID:                             5580
Revision:                               0001
First Connected (setupapi):             {Never}
Connected After Reboot (USBSTOR):       27-Mar-2018 12:11:44 [UTC]
Last Connected (MountPoints2):          {Never}
Last Connected (VID_&PID_):             27-Mar-2018 12:13:16 [UTC]
Device GUID:                            {5c3108bf-31c0-11e8-9b10-806e6f6e6963}
~~~~~~~~~~~~~~~
Source: LoneWolf.E01\Basic data partition (EFI 4)\Root\Windows\System32\config\SYSTEM :
-------------------------------------------------------------------------------------
USB Device 2:
Friendly Name:                          SanDisk Extreme USB Device
Serial Number:                          AA010603160707470215&0
Device Class ID:                        Disk&Ven_SanDisk&Prod_Extreme&Rev_0001
Device Type:                            Disk
Vendor Name:                            SanDisk
Vendor ID:                              0781
Product Name:                           Extreme
Product ID:                             5580
Revision:                               0001
First Connected (setupapi):             {Never}
Connected After Reboot (USBSTOR):       27-Mar-2018 09:22:21 [UTC]
Last Connected (MountPoints2):          27-Mar-2018 21:45:54 [UTC]
Last Connected (VID_&PID_):             27-Mar-2018 21:45:44 [UTC]
Device GUID:                            {3869c27a-31b8-11e8-9b12-ecf4bb487fed}
Driver Letter:                          D
Last User:                              jcloudy
~~~~~~~~~~~~~~~
Source: LoneWolf.E01\Basic data partition (EFI 4)\Root\Windows\System32\config\SYSTEM :
-------------------------------------------------------------------------------------
```

Q12. 3RD PARTY TOOLS - REGRIPPER

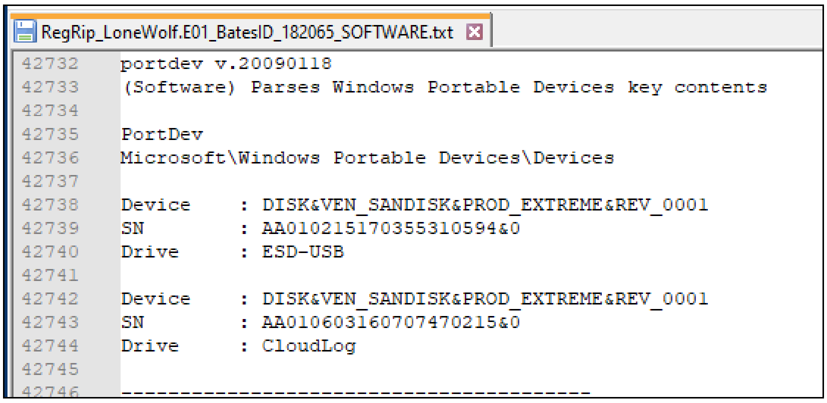
As a validation technique, In the File System module select **Tools > Add Remove 3rd Party Tools > RegRipper** (follow the onscreen installation instructions if RegRipper is not previously installed):

Figure 61: 3rd Party Tools > RegRipper.



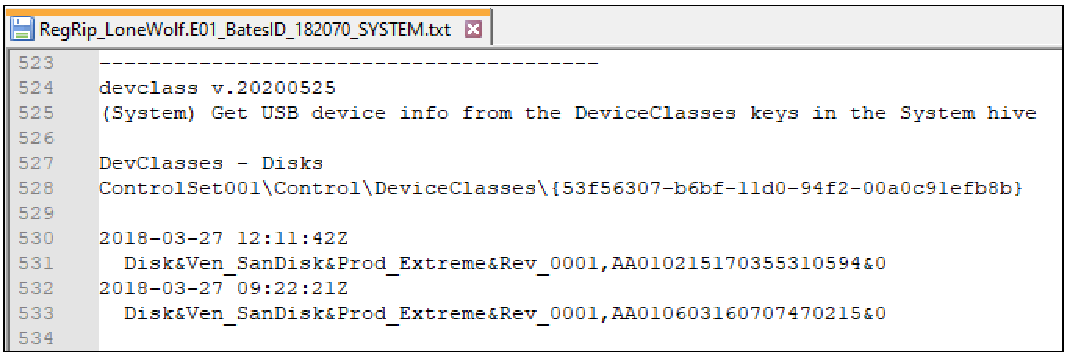
RegRipper produces the following output:

Figure 62: RegRipper Output



```
portdev v.20090118
(Software) Parses Windows Portable Devices key contents

PortDev
Microsoft\Windows Portable Devices\Devices

Device     : DISK&VEN_SANDISK&PROD_EXTREME&REV_0001
SN         : AA010215170355310594&0
Drive      : ESD-USB

Device     : DISK&VEN_SANDISK&PROD_EXTREME&REV_0001
SN         : AA010603160707470215&0
Drive      : CloudLog

----------------------------------------
```

Figure 63: RegRipper Output

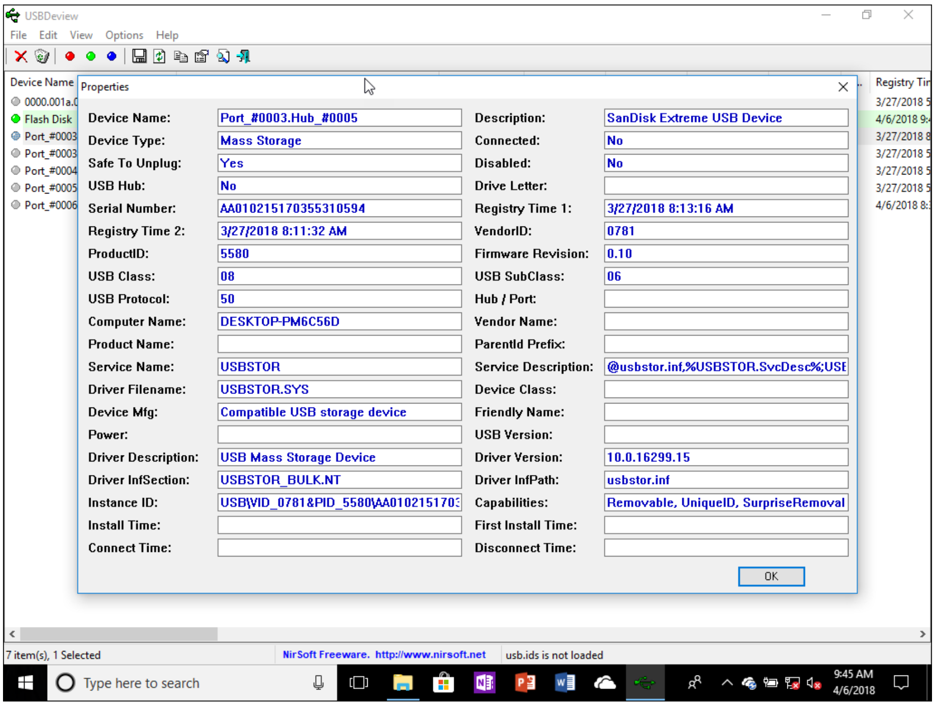


```
----------------------------------------
devclass v.20200525
(System) Get USB device info from the DeviceClasses keys in the System hive

DevClasses - Disks
ControlSet001\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

2018-03-27 12:11:42Z
  Disk&Ven_SanDisk&Prod_Extreme&Rev_0001,AA010215170355310594&0
2018-03-27 09:22:21Z
  Disk&Ven_SanDisk&Prod_Extreme&Rev_0001,AA010603160707470215&0

```

Q12. LIVE BOOT – NIRSOFT USBDEVIEW

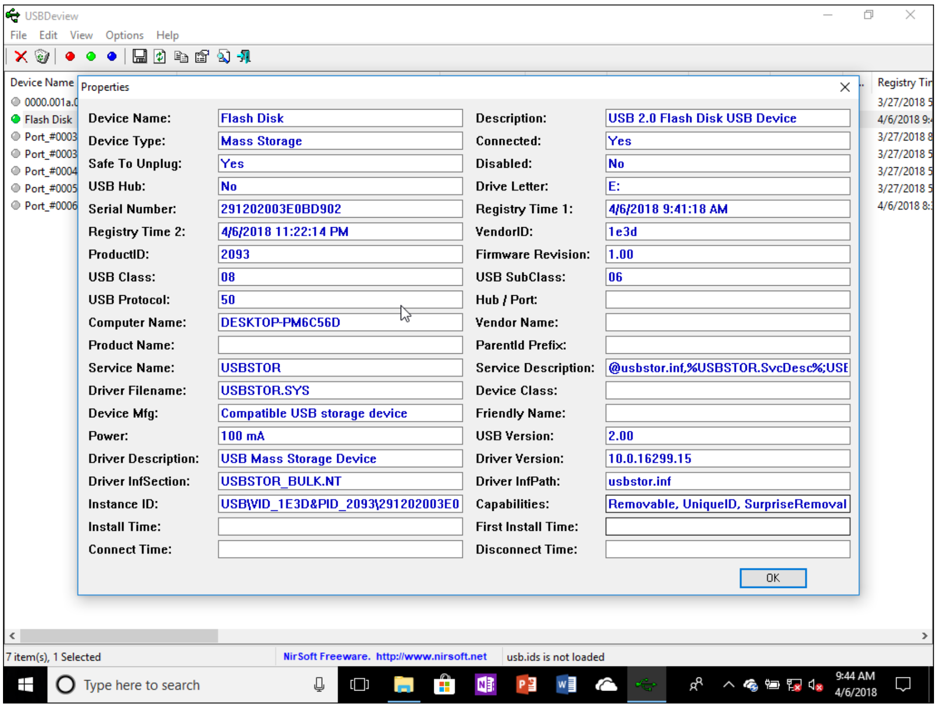
As a validation technique, install and run NirSoft USBDeview (https://www.nirsoft.net/utils/usb_devices_view.html) on the running Live Boot virtual machine:

Figure 64: USBDeview



Device Name:	Port_#0003.Hub_#0005	Description:	SanDisk Extreme USB Device
Device Type:	Mass Storage	Connected:	No
Safe To Unplug:	Yes	Disabled:	No
USB Hub:	No	Drive Letter:	
Serial Number:	AA010215170355310594	Registry Time 1:	3/27/2018 8:13:16 AM
Registry Time 2:	3/27/2018 8:11:32 AM	VendorID:	0781
ProductID:	5580	Firmware Revision:	0.10
USB Class:	08	USB SubClass:	06
USB Protocol:	50	Hub / Port:	
Computer Name:	DESKTOP-PM6C56D	Vendor Name:	
Product Name:		ParentId Prefix:	
Service Name:	USBSTOR	Service Description:	@usbstor.inf,%USBSTOR.SvcDesc%;USE
Driver Filename:	USBSTOR.SYS	Device Class:	
Device Mfg:	Compatible USB storage device	Friendly Name:	
Power:		USB Version:	
Driver Description:	USB Mass Storage Device	Driver Version:	10.0.16299.15
Driver InfSection:	USBSTOR_BULK.NT	Driver InfPath:	usbstor.inf
Instance ID:	USB\VID_0781&PID_5580\AA01021517035	Capabilities:	Removable, UniqueID, SurpriseRemoval
Install Time:		First Install Time:	
Connect Time:		Disconnect Time:	

Figure 65: USBDeview



Device Name:	Flash Disk	Description:	USB 2.0 Flash Disk USB Device
Device Type:	Mass Storage	Connected:	Yes
Safe To Unplug:	Yes	Disabled:	No
USB Hub:	No	Drive Letter:	E:
Serial Number:	291202003E0BD902	Registry Time 1:	4/6/2018 9:41:18 AM
Registry Time 2:	4/6/2018 11:22:14 PM	VendorID:	1e3d
ProductID:	2093	Firmware Revision:	1.00
USB Class:	08	USB SubClass:	06
USB Protocol:	50	Hub / Port:	
Computer Name:	DESKTOP-PM6C56D	Vendor Name:	
Product Name:		ParentId Prefix:	
Service Name:	USBSTOR	Service Description:	@usbstor.inf,%USBSTOR.SvcDesc%;USE
Driver Filename:	USBSTOR.SYS	Device Class:	
Device Mfg:	Compatible USB storage device	Friendly Name:	
Power:	100 mA	USB Version:	2.00
Driver Description:	USB Mass Storage Device	Driver Version:	10.0.16299.15
Driver InfSection:	USBSTOR_BULK.NT	Driver InfPath:	usbstor.inf
Instance ID:	USB\VID_1E3D&PID_2093\291202003E0	Capabilities:	Removable, UniqueID, SurpriseRemoval
Install Time:		First Install Time:	
Connect Time:		Disconnect Time:	

QUESTION 13 - VOLUME

What file system does the volume that contains the operating system use?

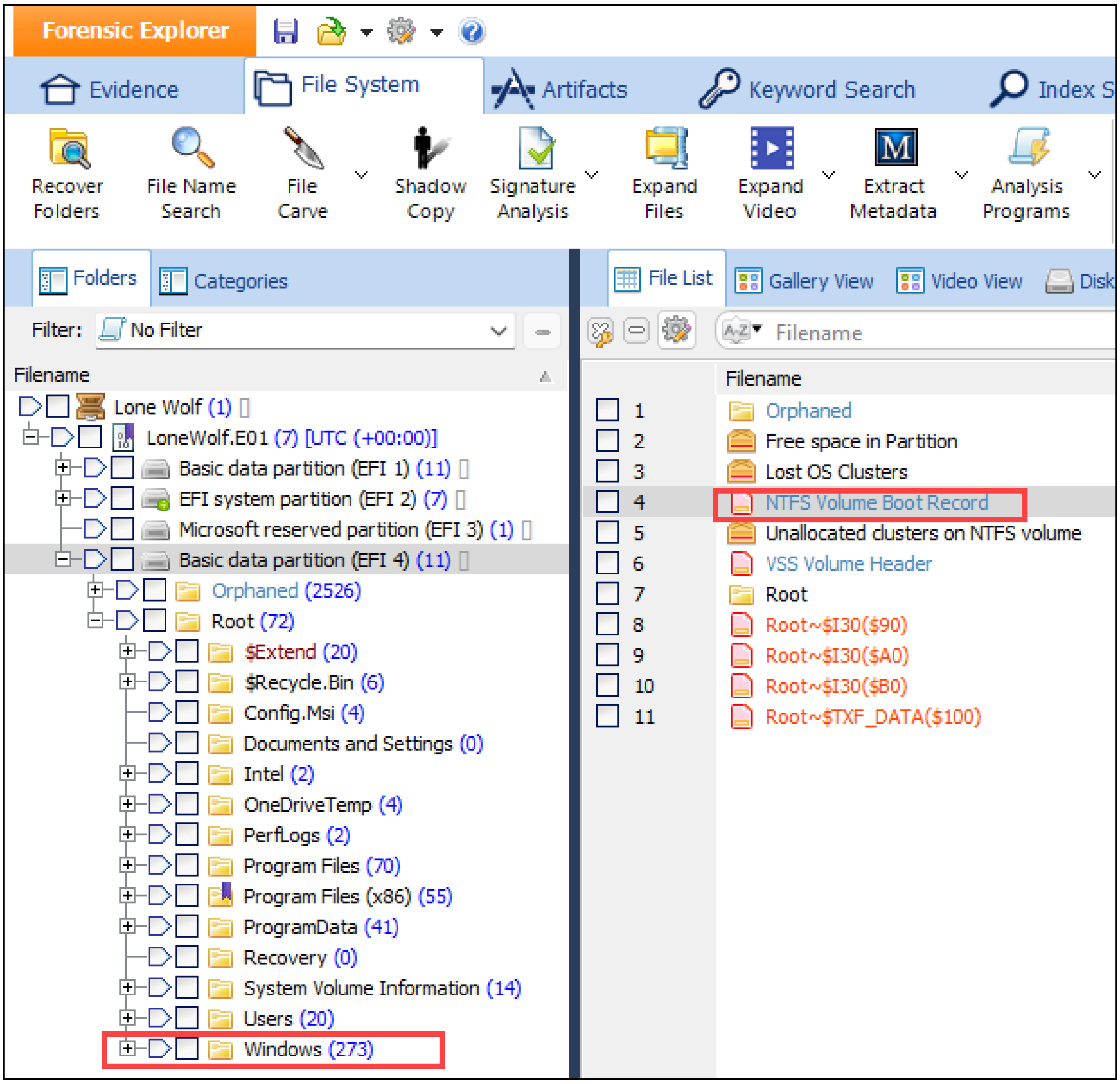
Q13. ANSWER

NTFS.

Q13. FORENSIC EXPLORER METHODOLOGY

The File System folder tree shows the Windows Operating System to be installed on the **Basic data partition (EFI 4)**. The partition has an **NTFS Volume Boot Record**.

Figure 66: File System module.

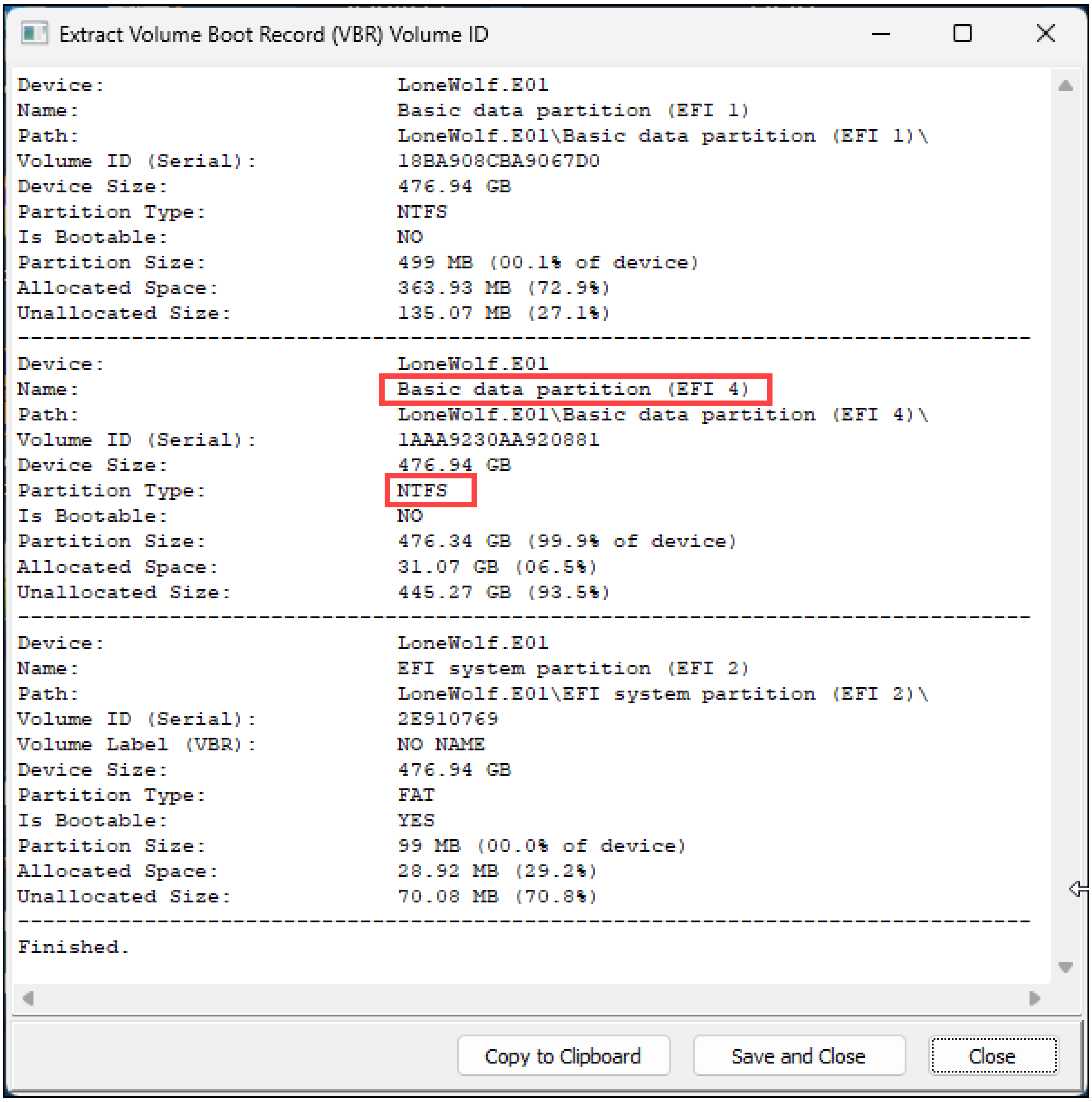


Filter: No Filter

```
Filename
Lone Wolf (1)
  LoneWolf.E01 (7) [UTC (+00:00)]
    Basic data partition (EFI 1) (11)
    EFI system partition (EFI 2) (7)
    Microsoft reserved partition (EFI 3) (1)
    Basic data partition (EFI 4) (11)
      Orphaned (2526)
      Root (72)
        $Extend (20)
        $Recycle.Bin (6)
        Config.Msi (4)
        Documents and Settings (0)
        Intel (2)
        OneDriveTemp (4)
        PerfLogs (2)
        Program Files (70)
        Program Files (x86) (55)
        ProgramData (41)
        Recovery (0)
        System Volume Information (14)
        Users (20)
        Windows (273)
```

	Filename
1	Orphaned
2	Free space in Partition
3	Lost OS Clusters
4	NTFS Volume Boot Record
5	Unallocated clusters on NTFS volume
6	VSS Volume Header
7	Root
8	Root~$I30($90)
9	Root~$I30($A0)
10	Root~$I30($B0)
11	Root~$TXF_DATA($100)

In the **File System** module toolbar, select **Analysis Programs** > **Volume ID and Partition Information**. The following summary report will display:



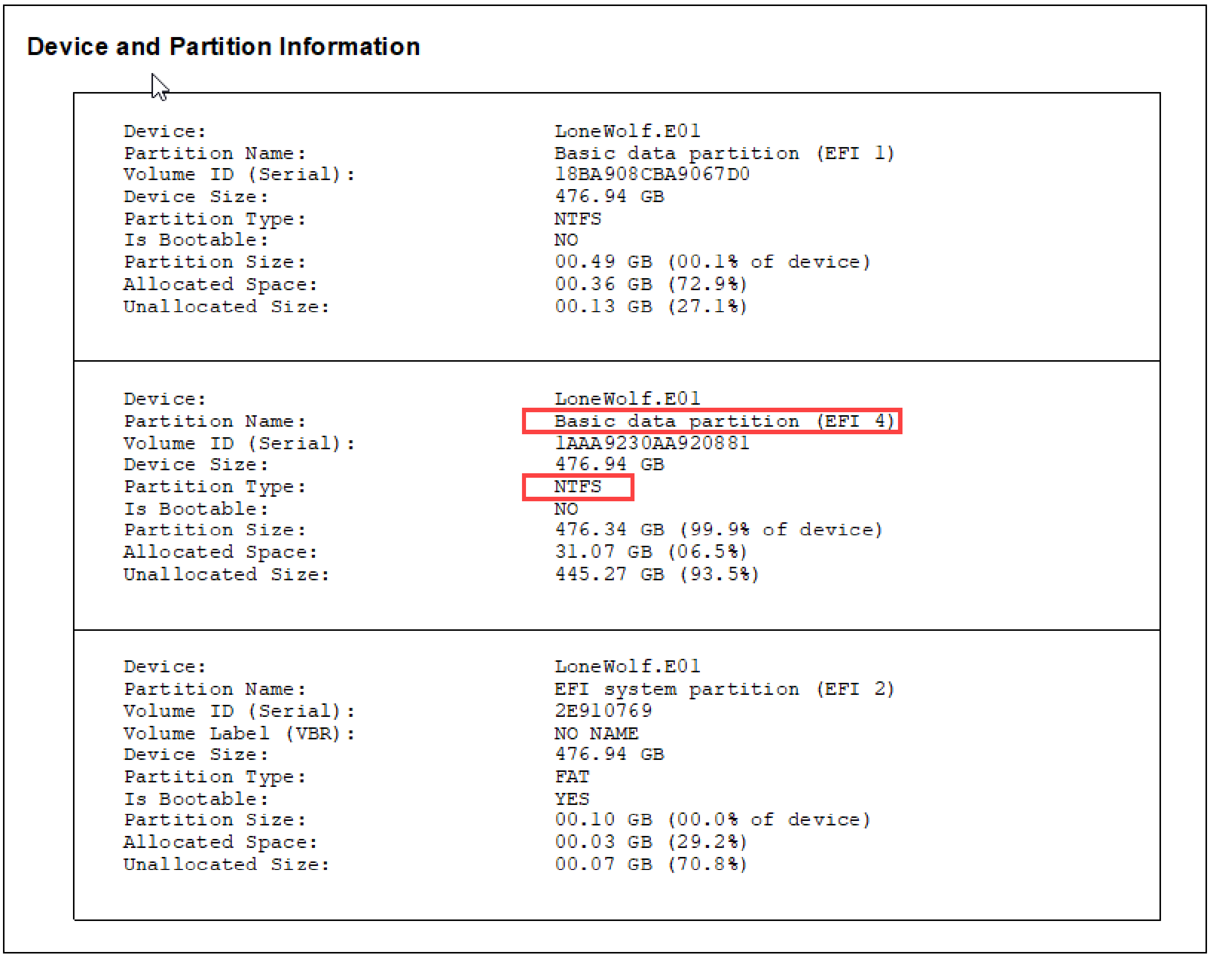
```
Device:                       LoneWolf.E01
Name:                         Basic data partition (EFI 1)
Path:                         LoneWolf.E01\Basic data partition (EFI 1)\
Volume ID (Serial):           18BA908CBA9067D0
Device Size:                  476.94 GB
Partition Type:               NTFS
Is Bootable:                  NO
Partition Size:               499 MB (00.1% of device)
Allocated Space:              363.93 MB (72.9%)
Unallocated Size:             135.07 MB (27.1%)
--------------------------------------------------------------------------------
Device:                       LoneWolf.E01
Name:                         Basic data partition (EFI 4)
Path:                         LoneWolf.E01\Basic data partition (EFI 4)\
Volume ID (Serial):           1AAA9230AA920881
Device Size:                  476.94 GB
Partition Type:               NTFS
Is Bootable:                  NO
Partition Size:               476.34 GB (99.9% of device)
Allocated Space:              31.07 GB (06.5%)
Unallocated Size:             445.27 GB (93.5%)
--------------------------------------------------------------------------------
Device:                       LoneWolf.E01
Name:                         EFI system partition (EFI 2)
Path:                         LoneWolf.E01\EFI system partition (EFI 2)\
Volume ID (Serial):           2E910769
Volume Label (VBR):           NO NAME
Device Size:                  476.94 GB
Partition Type:               FAT
Is Bootable:                  YES
Partition Size:               99 MB (00.0% of device)
Allocated Space:              28.92 MB (29.2%)
Unallocated Size:             70.08 MB (70.8%)
--------------------------------------------------------------------------------
Finished.
```

Q13. TRIAGE REPORT

Select **Reports** module > **Triage** report:

1. **Triage > File System > Device and Partitions** report.

Figure 67: Triage module > Triage > File System > Device and Partitions



Device and Partition Information

```
Device:                               LoneWolf.E01
Partition Name:                       Basic data partition (EFI 1)
Volume ID (Serial):                   18BA908CBA9067D0
Device Size:                          476.94 GB
Partition Type:                       NTFS
Is Bootable:                          NO
Partition Size:                       00.49 GB (00.1% of device)
Allocated Space:                      00.36 GB (72.9%)
Unallocated Size:                     00.13 GB (27.1%)
```

```
Device:                               LoneWolf.E01
Partition Name:                       Basic data partition (EFI 4)
Volume ID (Serial):                   1AAA9230AA920881
Device Size:                          476.94 GB
Partition Type:                       NTFS
Is Bootable:                          NO
Partition Size:                       476.34 GB (99.9% of device)
Allocated Space:                      31.07 GB (06.5%)
Unallocated Size:                     445.27 GB (93.5%)
```

```
Device:                               LoneWolf.E01
Partition Name:                       EFI system partition (EFI 2)
Volume ID (Serial):                   2E910769
Volume Label (VBR):                   NO NAME
Device Size:                          476.94 GB
Partition Type:                       FAT
Is Bootable:                          YES
Partition Size:                       00.10 GB (00.0% of device)
Allocated Space:                      00.03 GB (29.2%)
Unallocated Size:                     00.07 GB (70.8%)
```

QUESTION 14 - ORIGINAL FILENAME

Prior to being deleted, what was the original filename now referenced as $RYRY5PT.jpg?

Q14. ANSWER

DemGun.jpg.

Q14. FORENSIC EXPLORER METHODOLOGY

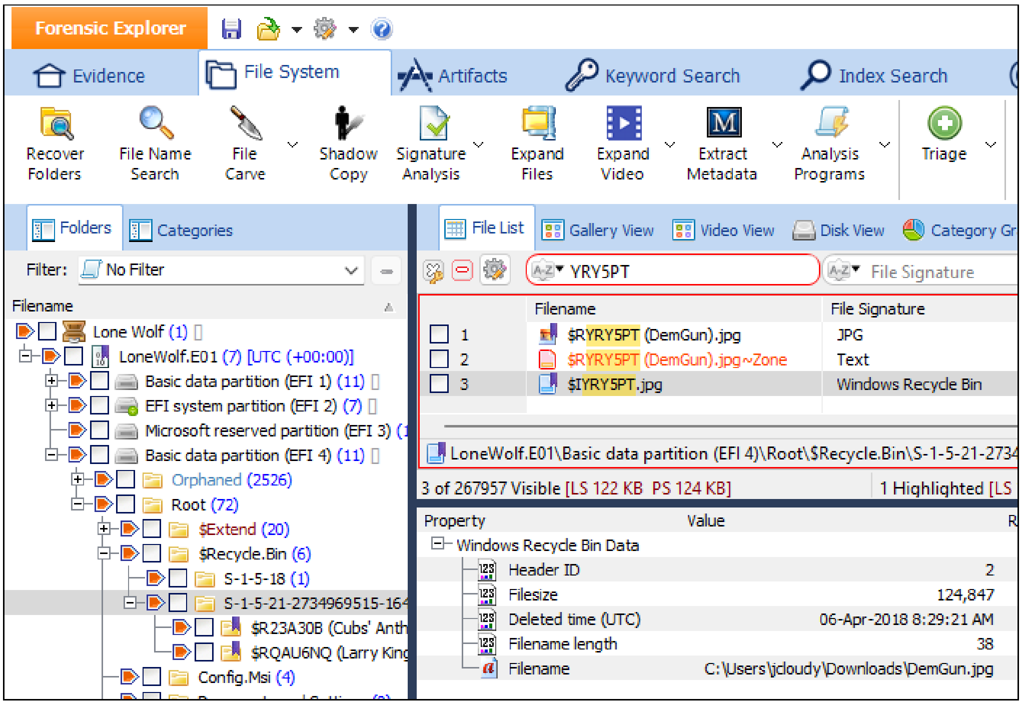
A Windows 10 OS holds two artifacts for a Recycle Bin deleted file:

1. A "$R" followed by a random string and contains the actual contents of the recycled file.
2. The second file begins with "$I", ends in the same string as the "$R" file and contains the metadata for that specific file.

In the **File System** module:

1. **Branch plate** [▶] the entire case.
2. Apply a Filename column filter for the name **YRY5PT.**
3. This identifies both the $I and $R files. The metadata tab for the $I show the original path and filename to be: **C:\Users\jcloudy\Downloads\DemGun.jpg**

Figure 68: File System > Filename filter for YRY5PT.



Filter: No Filter

Filename
- Lone Wolf (1)
- LoneWolf.E01 (7) [UTC (+00:00)]
  - Basic data partition (EFI 1) (11)
  - EFI system partition (EFI 2) (7)
  - Microsoft reserved partition (EFI 3) (1
  - Basic data partition (EFI 4) (11)
    - Orphaned (2526)
    - Root (72)
      - $Extend (20)
      - $Recycle.Bin (6)
        - S-1-5-18 (1)
        - S-1-5-21-2734969515-164
          - $R23A30B (Cubs' Anth
          - $RQAU6NQ (Larry King
      - Config.Msi (4)

YRY5PT | File Signature

	Filename	File Signature
□ 1	$RYRY5PT (DemGun).jpg	JPG
□ 2	$RYRY5PT (DemGun).jpg~Zone	Text
□ 3	$IYRY5PT.jpg	Windows Recycle Bin

LoneWolf.E01\Basic data partition (EFI 4)\Root\$Recycle.Bin\S-1-5-21-2734

3 of 267957 Visible [LS 122 KB PS 124 KB] | 1 Highlighted [LS

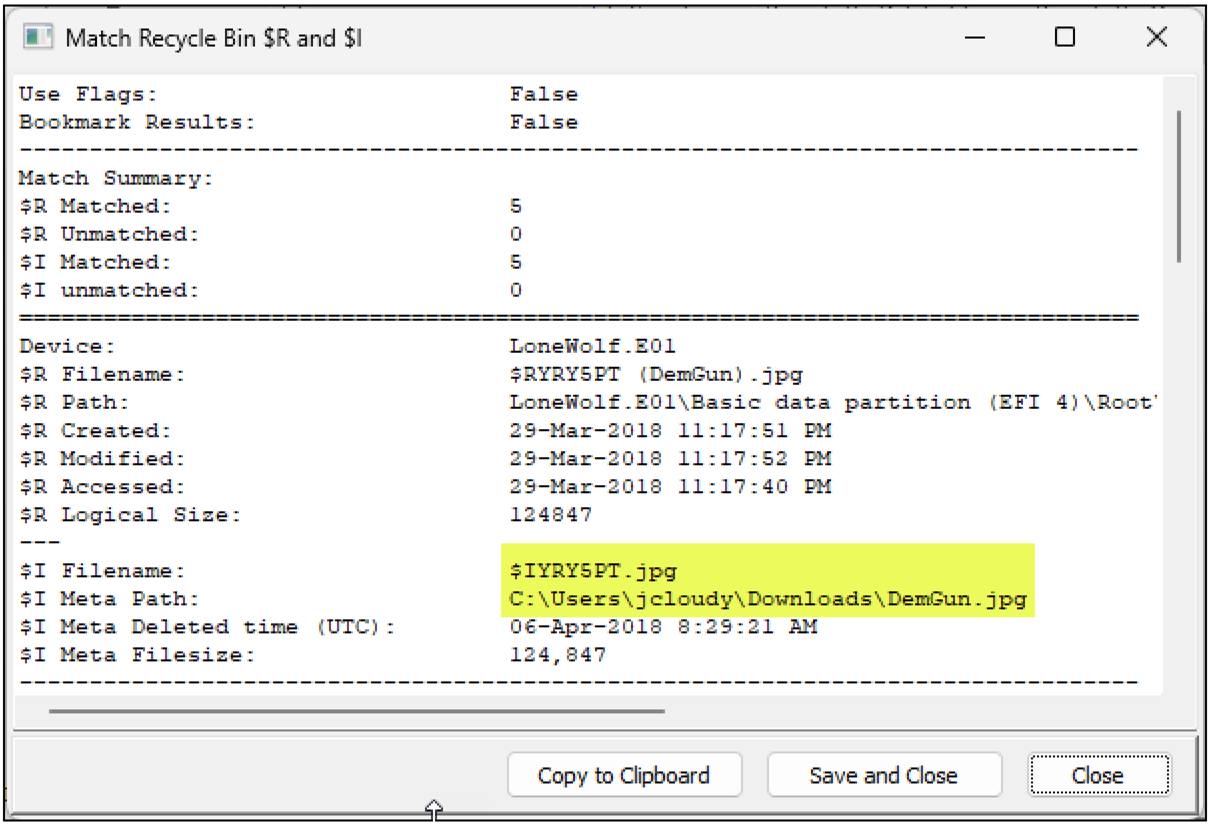
Property	Value
Windows Recycle Bin Data	
Header ID	2
Filesize	124,847
Deleted time (UTC)	06-Apr-2018 8:29:21 AM
Filename length	38
Filename	C:\Users\jcloudy\Downloads\DemGun.jpg

In the **File System** module toolbar:

1. Click on the **Analysis Programs** toolbar button.
2. Select **Recycle Bin - Match $I with $R** from the drop-down menu.

A script will run and produce the following result:

Figure 69: File System > Analysis Programs > Recycle Bin - Match $I with $R > Results.



Match Recycle Bin $R and $I

```
Use Flags:                         False
Bookmark Results:                  False
-------------------------------------------------------------------------------
Match Summary:
$R Matched:                        5
$R Unmatched:                      0
$I Matched:                        5
$I unmatched:                      0
===============================================================================
Device:                            LoneWolf.E01
$R Filename:                       $RYRY5PT (DemGun).jpg
$R Path:                           LoneWolf.E01\Basic data partition (EFI 4)\Root'
$R Created:                        29-Mar-2018 11:17:51 PM
$R Modified:                       29-Mar-2018 11:17:52 PM
$R Accessed:                       29-Mar-2018 11:17:40 PM
$R Logical Size:                   124847
---
$I Filename:                       $IYRY5PT.jpg
$I Meta Path:                      C:\Users\jcloudy\Downloads\DemGun.jpg
$I Meta Deleted time (UTC):        06-Apr-2018 8:29:21 AM
$I Meta Filesize:                  124,847
-------------------------------------------------------------------------------
```

QUESTION 15 - BROWSER

When was the Chrome browser first used? Is this the same date as when the browser was installed and how do you know this?

Q15. ANSWER

Chrome was installed and first used on 27-Mar-2018 09:32:50 hours (UTC).

Q15. FORENSIC EXPLORER METHODOLOGY

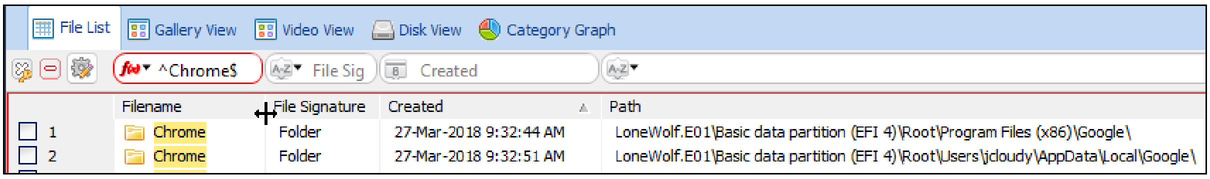
Q15. APPLICATION FOLDER CREATION DATE

The creation date of the application folder can provide an indication of when the software was installed.

In the **File System** module:

1. **Branch plate** [▷] the entire case.
2. Change the **Filename** column filter to **RegEx** and filter for **^Chrome$** (^ = starting with, $ = ending with).
3. Look for the Chrome folder creation time in the **Program Files** path.

Figure 70: File System > Chrome > Application folder Created.

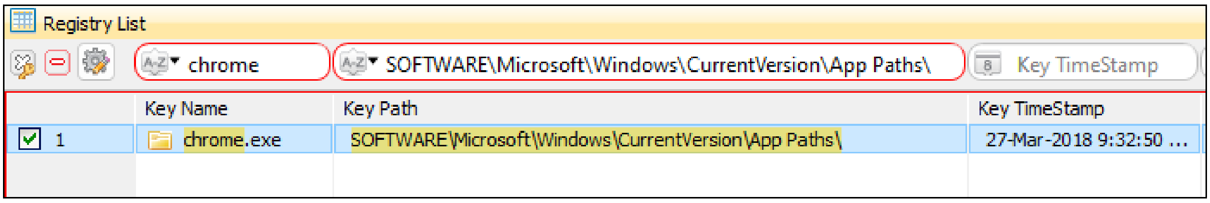


	Filename	File Signature	Created	Path
□ 1	Chrome	Folder	27-Mar-2018 9:32:44 AM	LoneWolf.E01\Basic data partition (EFI 4)\Root\Program Files (x86)\Google\
□ 2	Chrome	Folder	27-Mar-2018 9:32:51 AM	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\

In the **Registry** module:

1. **Branch plate** [▷] the entire case.
2. Apply a Key Name filter of **chrome**.
3. Apply a Key Path filter of: **SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths**
4. Look for the registry folder creation date.

Figure 71: Registry > chrome.exe folder.



Filters: chrome | SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\ | Key TimeStamp

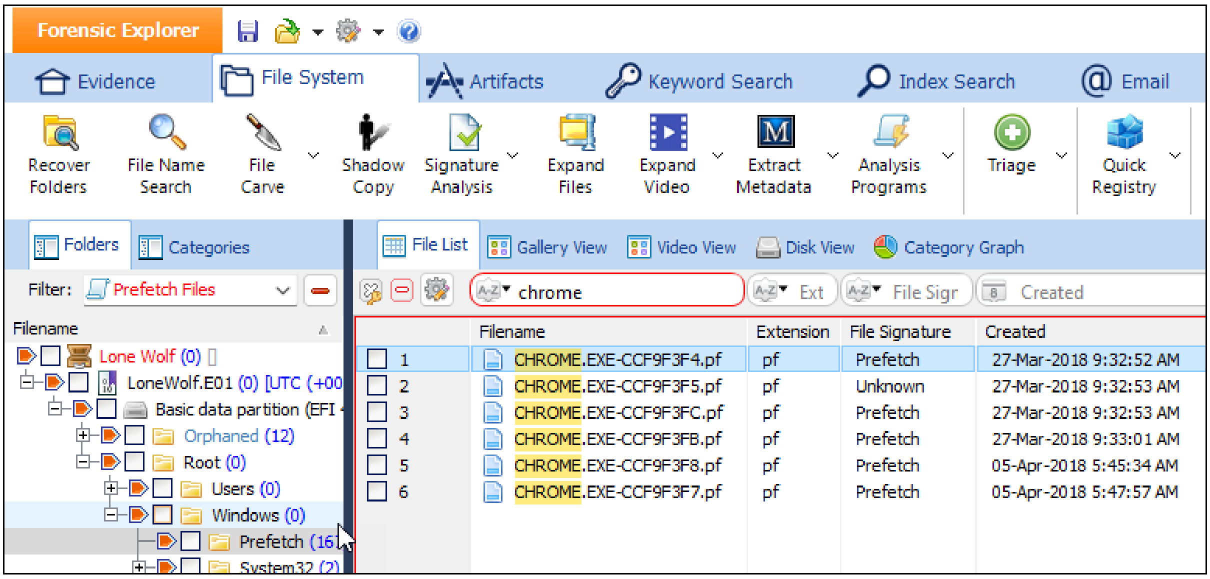
	Key Name	Key Path	Key TimeStamp
☑ 1	chrome.exe	SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\	27-Mar-2018 9:32:50 ...

Q15. PREFETCH FILE CREATION

Windows creates a prefetch file when an application is run from a particular location for the first time. In the **File System** module:

1. **Branch plate** [▶] the entire case.
2. Apply a folders filter for **Prefetch Files**.
3. Apply a **Filename** column filter of **Chrome**.
4. Double-click the **Created** column header to sort by created date.

Figure 72: File System > Chrome > CHROME.EXE-CCF9F3F4.pf > Created.



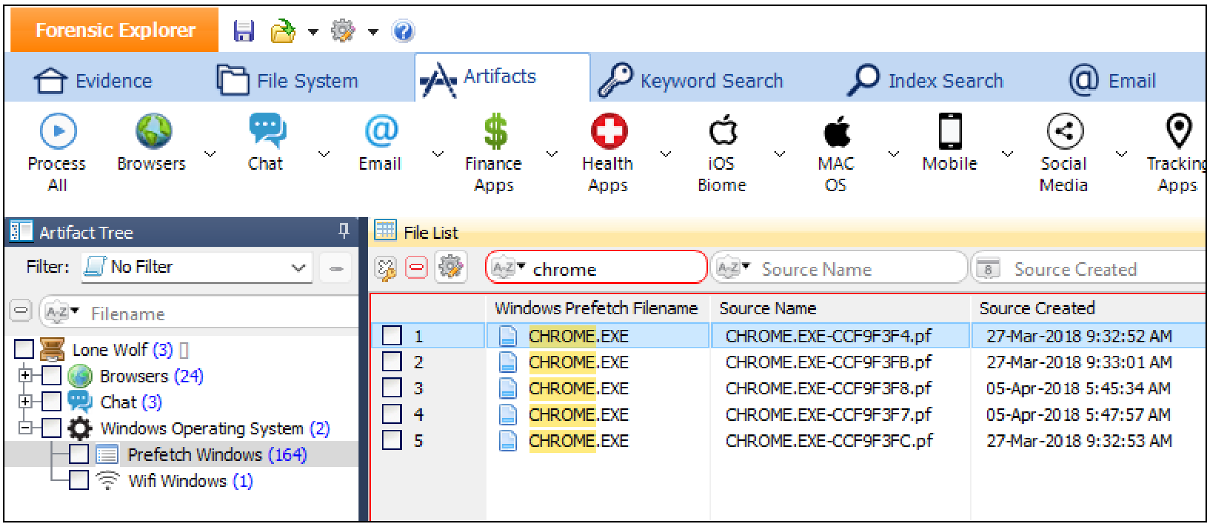
Filter: Prefetch Files

Filters: chrome | Ext | File Sigr | Created

	Filename	Extension	File Signature	Created
□ 1	CHROME.EXE-CCF9F3F4.pf	pf	Prefetch	27-Mar-2018 9:32:52 AM
□ 2	CHROME.EXE-CCF9F3F5.pf	pf	Unknown	27-Mar-2018 9:32:53 AM
□ 3	CHROME.EXE-CCF9F3FC.pf	pf	Prefetch	27-Mar-2018 9:32:53 AM
□ 4	CHROME.EXE-CCF9F3FB.pf	pf	Prefetch	27-Mar-2018 9:33:01 AM
□ 5	CHROME.EXE-CCF9F3F8.pf	pf	Prefetch	05-Apr-2018 5:45:34 AM
□ 6	CHROME.EXE-CCF9F3F7.pf	pf	Prefetch	05-Apr-2018 5:47:57 AM

These files are also listed in the **Artifacts** module under **Windows Operating System** > **Prefetch Windows**. Filter the **Windows Prefetch Filename** by **chrome**.

Figure 73: Artifacts > CHROME.EXE-CCF9F3F4.pf > Source Created



Filter: No Filter

Filename

- Lone Wolf (3)
  - Browsers (24)
  - Chat (3)
  - Windows Operating System (2)
    - Prefetch Windows (164)
    - Wifi Windows (1)

chrome

	Windows Prefetch Filename	Source Name	Source Created
□ 1	CHROME.EXE	CHROME.EXE-CCF9F3F4.pf	27-Mar-2018 9:32:52 AM
□ 2	CHROME.EXE	CHROME.EXE-CCF9F3FB.pf	27-Mar-2018 9:33:01 AM
□ 3	CHROME.EXE	CHROME.EXE-CCF9F3F8.pf	05-Apr-2018 5:45:34 AM
□ 4	CHROME.EXE	CHROME.EXE-CCF9F3F7.pf	05-Apr-2018 5:47:57 AM
□ 5	CHROME.EXE	CHROME.EXE-CCF9F3FC.pf	27-Mar-2018 9:32:53 AM

CREATING A REPORT OF KEY FILES AND ARTIFACTS

A Forensic Explorer report is created from **bookmarked files**. For a **well structed automated report**, bookmark files in their categories, i.e.:

- Artifacts
- Documents
- Email
- Graphics
- Registry

Use the **Bookmark module Create Folders button** to create relevant sub-folders (2 sub-folder level maximum is recommended):

Figure 74: Bookmarks > Create Folders

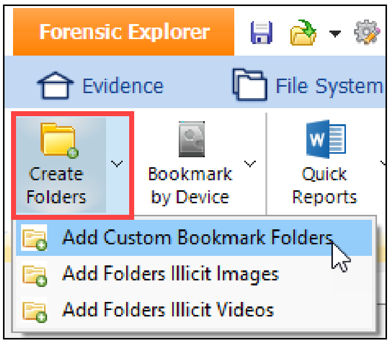
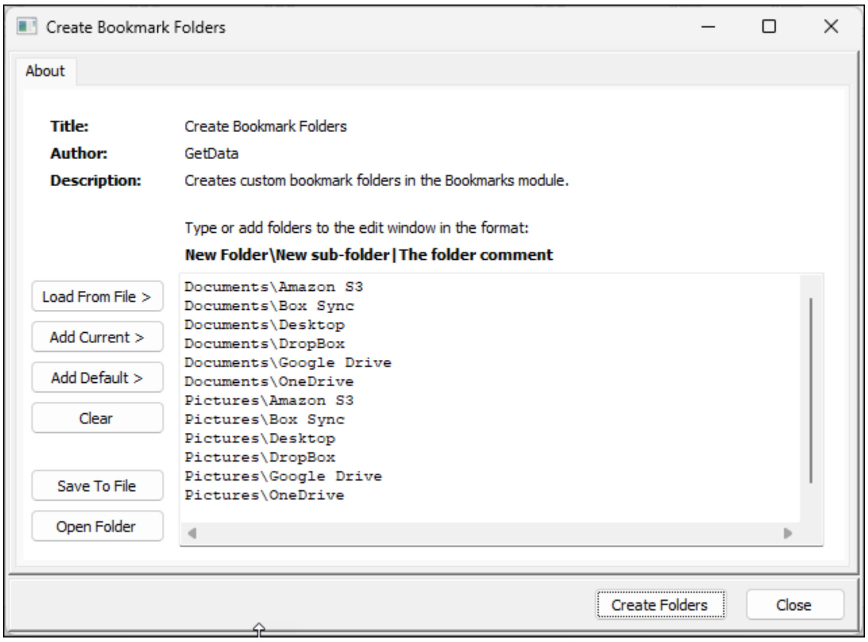


Figure 75: Bookmarks > Create Folders



Title: Create Bookmark Folders
Author: GetData
Description: Creates custom bookmark folders in the Bookmarks module.

Type or add folders to the edit window in the format:
New Folder\New sub-folder|The folder comment

```
Documents\Amazon S3
Documents\Box Sync
Documents\Desktop
Documents\DropBox
Documents\Google Drive
Documents\OneDrive
Pictures\Amazon S3
Pictures\Box Sync
Pictures\Desktop
Pictures\DropBox
Pictures\Google Drive
Pictures\OneDrive
```

BOOKMARK DOCUMENTS

To locate and bookmark relevant **Documents**:

1. Using the filename keywords identified above, run a **File System** > **File Name Search**:

Figure 76: File System > Toolbar.

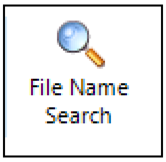
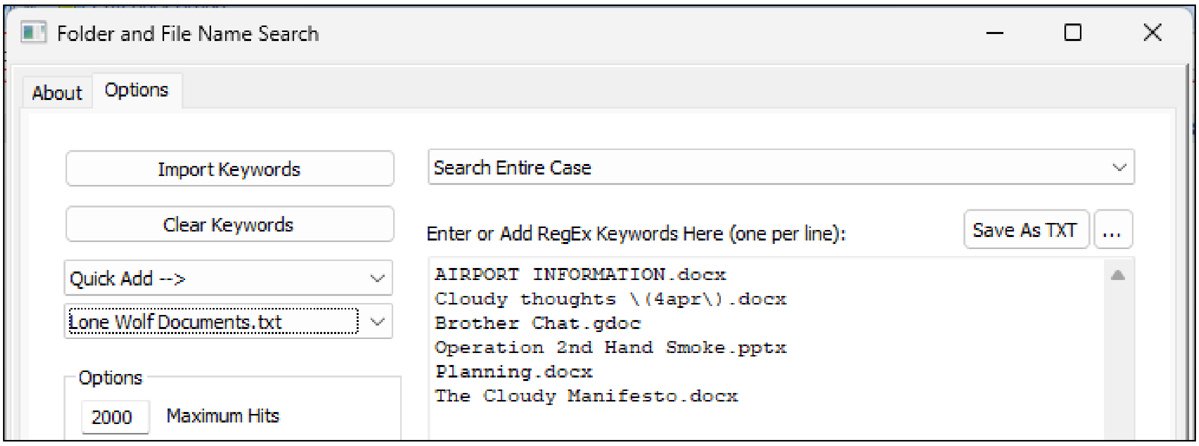


Figure 77: Folder and File Name Search



Search Entire Case

Lone Wolf Documents.txt

Options

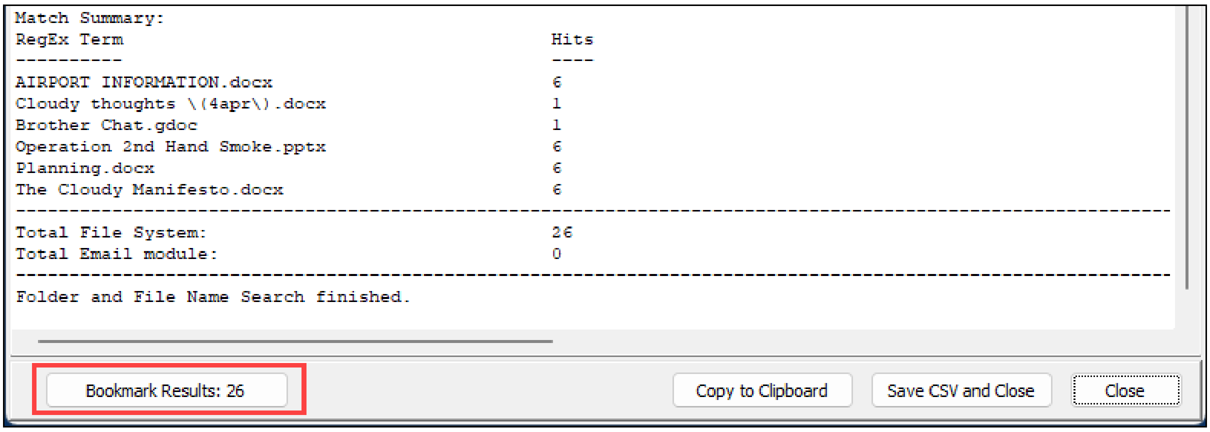
2000 Maximum Hits

Enter or Add RegEx Keywords Here (one per line):

```
AIRPORT INFORMATION.docx
Cloudy thoughts \(4apr\).docx
Brother Chat.gdoc
Operation 2nd Hand Smoke.pptx
Planning.docx
The Cloudy Manifesto.docx
```

2. Click the **Bookmark Results** button to bookmark the files found. Bookmarks are created under the **Script Output** folder.

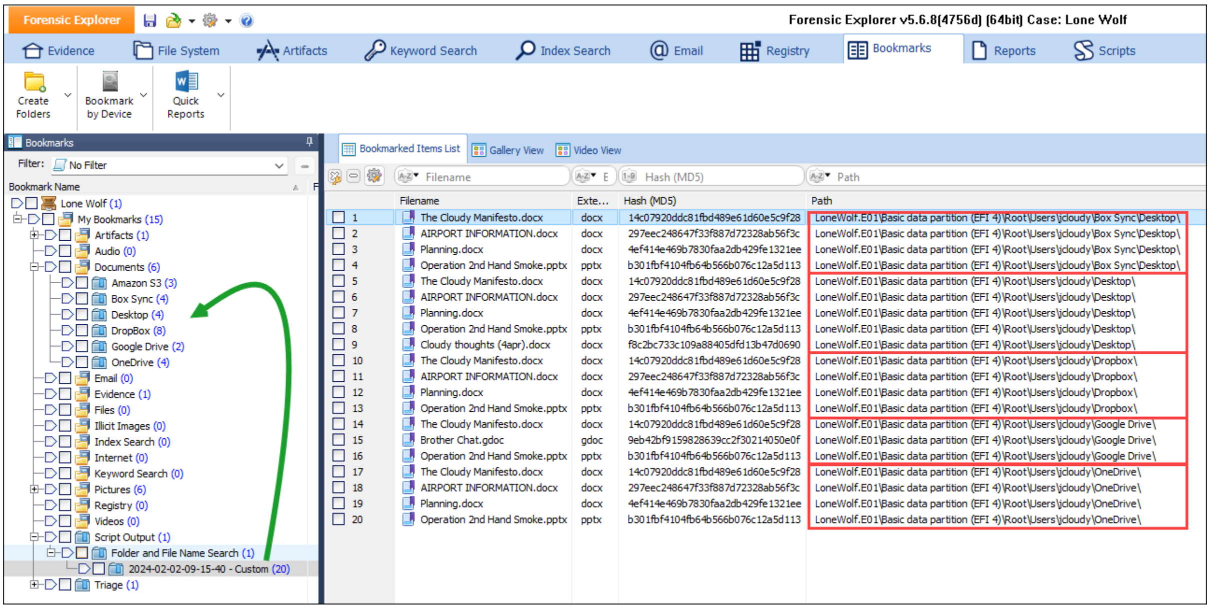
Figure 78: Folder and File Name Search > Bookmark Results



```
Match Summary:
RegEx Term                                        Hits
----------                                        ----
AIRPORT INFORMATION.docx                          6
Cloudy thoughts \(4apr\).docx                     1
Brother Chat.gdoc                                 1
Operation 2nd Hand Smoke.pptx                     6
Planning.docx                                     6
The Cloudy Manifesto.docx                         6
------------------------------------------------------------------------------------------------------------
Total File System:                                26
Total Email module:                               0
------------------------------------------------------------------------------------------------------------
Folder and File Name Search finished.
```

3. Drag and drop **Script Output** bookmarks into their **relevant sub-folder**.

Figure 79: Move documents of relevance to My Bookmarks\Documents sub-folders.



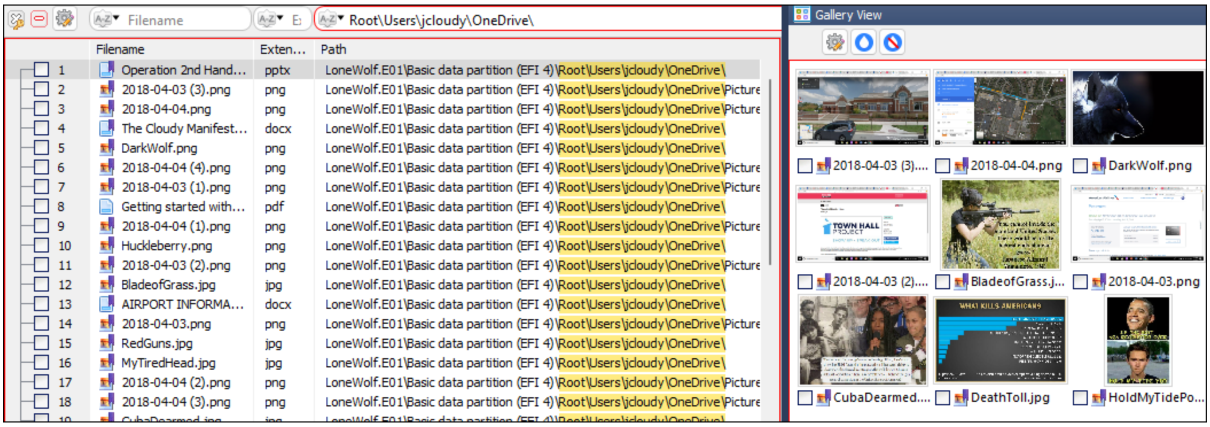
	Filename	Exte...	Hash (MD5)	Path
□ 1	The Cloudy Manifesto.docx	docx	14c07920ddc81fbd489e61d60e5c9f28	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Box Sync\Desktop\
□ 2	AIRPORT INFORMATION.docx	docx	297eec248647f33f887d72328ab56f3c	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Box Sync\Desktop\
□ 3	Planning.docx	docx	4ef414e469b7830faa2db429fe1321ee	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Box Sync\Desktop\
□ 4	Operation 2nd Hand Smoke.pptx	pptx	b301fbf4104fb64b566b076c12a5d113	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Box Sync\Desktop\
□ 5	The Cloudy Manifesto.docx	docx	14c07920ddc81fbd489e61d60e5c9f28	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Desktop\
□ 6	AIRPORT INFORMATION.docx	docx	297eec248647f33f887d72328ab56f3c	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Desktop\
□ 7	Planning.docx	docx	4ef414e469b7830faa2db429fe1321ee	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Desktop\
□ 8	Operation 2nd Hand Smoke.pptx	pptx	b301fbf4104fb64b566b076c12a5d113	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Desktop\
□ 9	Cloudy thoughts (4apr).docx	docx	f8c2bc733c109a88405dfd13b47d0690	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Desktop\
□ 10	The Cloudy Manifesto.docx	docx	14c07920ddc81fbd489e61d60e5c9f28	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Dropbox\
□ 11	AIRPORT INFORMATION.docx	docx	297eec248647f33f887d72328ab56f3c	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Dropbox\
□ 12	Planning.docx	docx	4ef414e469b7830faa2db429fe1321ee	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Dropbox\
□ 13	Operation 2nd Hand Smoke.pptx	pptx	b301fbf4104fb64b566b076c12a5d113	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Dropbox\
□ 14	The Cloudy Manifesto.docx	docx	14c07920ddc81fbd489e61d60e5c9f28	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Google Drive\
□ 15	Brother Chat.gdoc	gdoc	9eb42bf9159828639cc2f30214050e0f	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Google Drive\
□ 16	Operation 2nd Hand Smoke.pptx	pptx	b301fbf4104fb64b566b076c12a5d113	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Google Drive\
□ 17	The Cloudy Manifesto.docx	docx	14c07920ddc81fbd489e61d60e5c9f28	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\
□ 18	AIRPORT INFORMATION.docx	docx	297eec248647f33f887d72328ab56f3c	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\
□ 19	Planning.docx	docx	4ef414e469b7830faa2db429fe1321ee	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\
□ 20	Operation 2nd Hand Smoke.pptx	pptx	b301fbf4104fb64b566b076c12a5d113	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\

BOOKMARKS GRAPHICS

To **bookmark graphics**:

1. In the **File System** module, use the **Path** column filter and the **Gallery View** to locate pictures of relevance.
2. Select relevant pictures in the Gallery View (use CTRL, or SHIFT, or CTRL A to select multiple).
3. **Right-Click** and **bookmark** the **graphics** to their relevant sub-folders under the **Pictures** bookmark folder:

Figure 80: Bookmark relevant graphics.



Filename | E: | Root\Users\jcloudy\OneDrive\

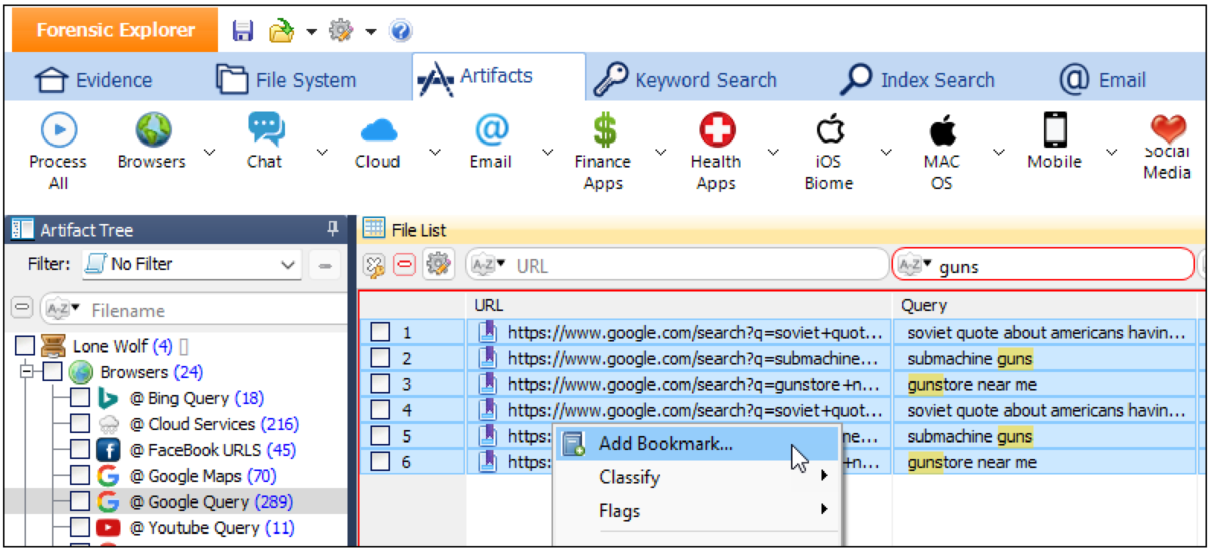
	Filename	Exten…	Path
□ 1	Operation 2nd Hand…	pptx	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\
□ 2	2018-04-03 (3).png	png	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\Picture
□ 3	2018-04-04.png	png	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\Picture
□ 4	The Cloudy Manifest…	docx	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\
□ 5	DarkWolf.png	png	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\
□ 6	2018-04-04 (4).png	png	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\Picture
□ 7	2018-04-03 (1).png	png	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\Picture
□ 8	Getting started with…	pdf	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\
□ 9	2018-04-04 (1).png	png	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\Picture
□ 10	Huckleberry.png	png	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\
□ 11	2018-04-03 (2).png	png	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\Picture
□ 12	BladeofGrass.jpg	jpg	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\
□ 13	AIRPORT INFORMA…	docx	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\
□ 14	2018-04-03.png	png	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\Picture
□ 15	RedGuns.jpg	jpg	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\
□ 16	MyTiredHead.jpg	jpg	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\
□ 17	2018-04-04 (2).png	png	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\Picture
□ 18	2018-04-04 (3).png	png	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\Picture
□ 19	CubaDearmed.jpg	jpg	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\

ARTIFACT BOOKMARKS

To bookmark artifacts:

1. In the Artifacts module, use the various filtering techniques to locate items of interest.
2. Highlight the items in the **File List**, right-click and **Add Bookmark.**

Figure 81.: Artifacts > Google Query > "guns".

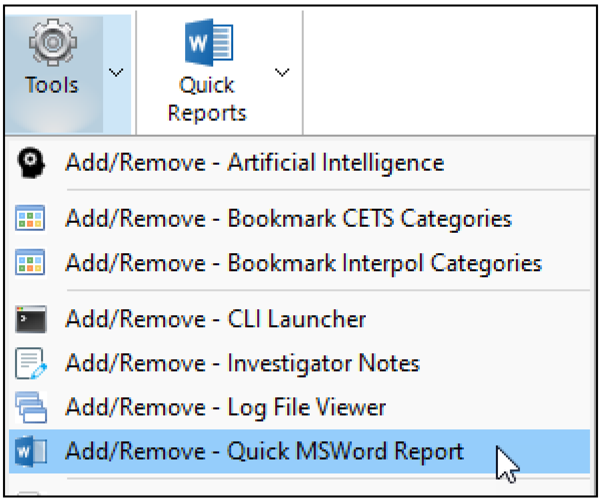


	URL	Query
□ 1	https://www.google.com/search?q=soviet+quot…	soviet quote about americans havin…
□ 2	https://www.google.com/search?q=submachine…	submachine guns
□ 3	https://www.google.com/search?q=gunstore+n…	gunstore near me
□ 4	https://www.google.com/search?q=soviet+quot…	soviet quote about americans havin…
□ 5	https: ne…	submachine guns
□ 6	https: +n…	gunstore near me

QUICK MS WORD REPORT

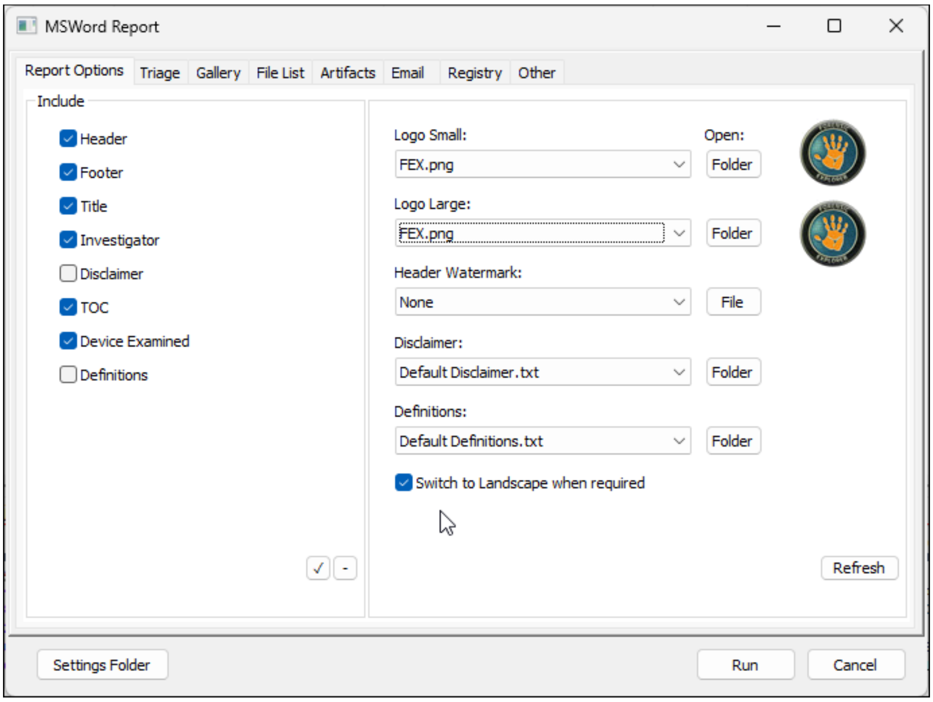
Quick Reports is a methodology to quickly generate a **Microsoft Word report** on **bookmarked items**. Quick Reports is launched from module toolbar icons. It can be added and removed from modules from the File System module by selecting **Tools** > **Add/Remove MSWord Report**.

Figure 82: File System > Tools > Add/Remove Quick MSWord Report


Tools
Quick Reports
Add/Remove - Artificial Intelligence
Add/Remove - Bookmark CETS Categories
Add/Remove - Bookmark Interpol Categories
Add/Remove - CLI Launcher
Add/Remove - Investigator Notes
Add/Remove - Log File Viewer
Add/Remove - Quick MSWord Report

Launching Quick Reports for the first time opens the Report Options window. Select the required options or customize report sections by saving logos and text.

Figure 83: Quick Reports > Report Options tab.



Include

- ☑ Header
- ☑ Footer
- ☑ Title
- ☑ Investigator
- ☐ Disclaimer
- ☑ TOC
- ☑ Device Examined
- ☐ Definitions

Logo Small: FEX.png

Logo Large: FEX.png

Header Watermark: None

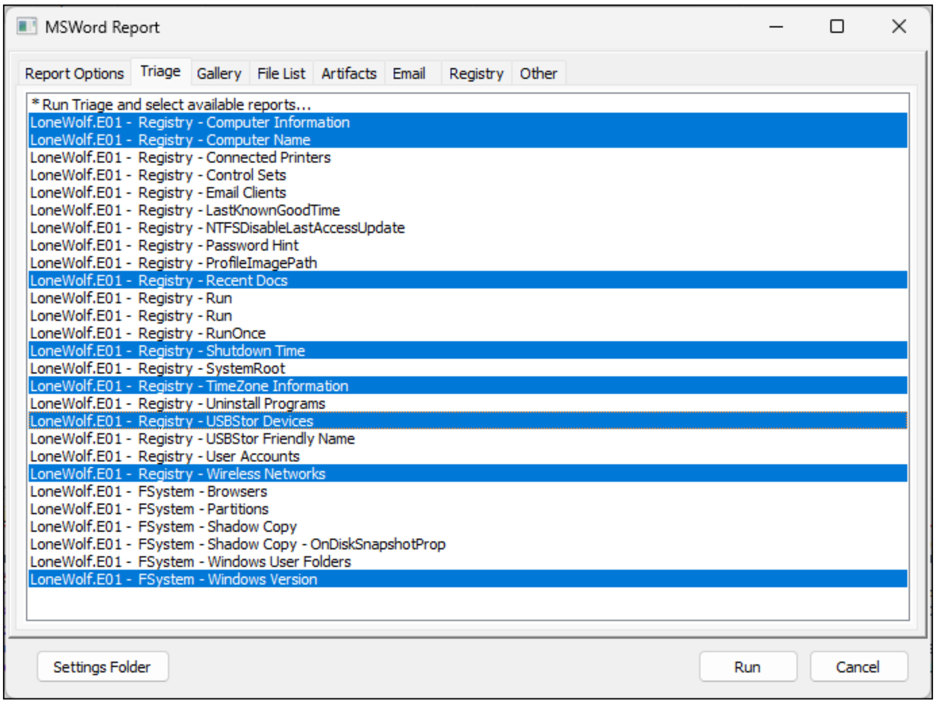
Disclaimer: Default Disclaimer.txt

Definitions: Default Definitions.txt

☑ Switch to Landscape when required

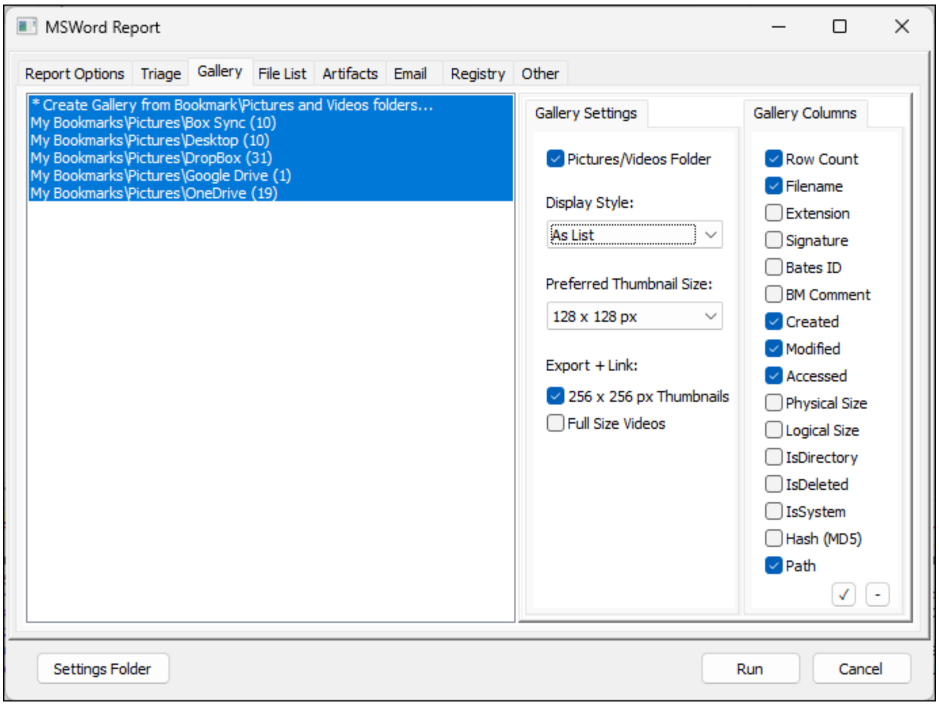
Navigate through the Quick Reports tabs selecting the require items for inclusion.

Figure 84: Quick Reports > Triage.



* Run Triage and select available reports…
LoneWolf.E01 - Registry - Computer Information
LoneWolf.E01 - Registry - Computer Name
LoneWolf.E01 - Registry - Connected Printers
LoneWolf.E01 - Registry - Control Sets
LoneWolf.E01 - Registry - Email Clients
LoneWolf.E01 - Registry - LastKnownGoodTime
LoneWolf.E01 - Registry - NTFSDisableLastAccessUpdate
LoneWolf.E01 - Registry - Password Hint
LoneWolf.E01 - Registry - ProfileImagePath
LoneWolf.E01 - Registry - Recent Docs
LoneWolf.E01 - Registry - Run
LoneWolf.E01 - Registry - Run
LoneWolf.E01 - Registry - RunOnce
LoneWolf.E01 - Registry - Shutdown Time
LoneWolf.E01 - Registry - SystemRoot
LoneWolf.E01 - Registry - TimeZone Information
LoneWolf.E01 - Registry - Uninstall Programs
LoneWolf.E01 - Registry - USBStor Devices
LoneWolf.E01 - Registry - USBStor Friendly Name
LoneWolf.E01 - Registry - User Accounts
LoneWolf.E01 - Registry - Wireless Networks
LoneWolf.E01 - FSystem - Browsers
LoneWolf.E01 - FSystem - Partitions
LoneWolf.E01 - FSystem - Shadow Copy
LoneWolf.E01 - FSystem - Shadow Copy - OnDiskSnapshotProp
LoneWolf.E01 - FSystem - Windows User Folders
LoneWolf.E01 - FSystem - Windows Version

Figure 85: Quick Reports > Gallery.

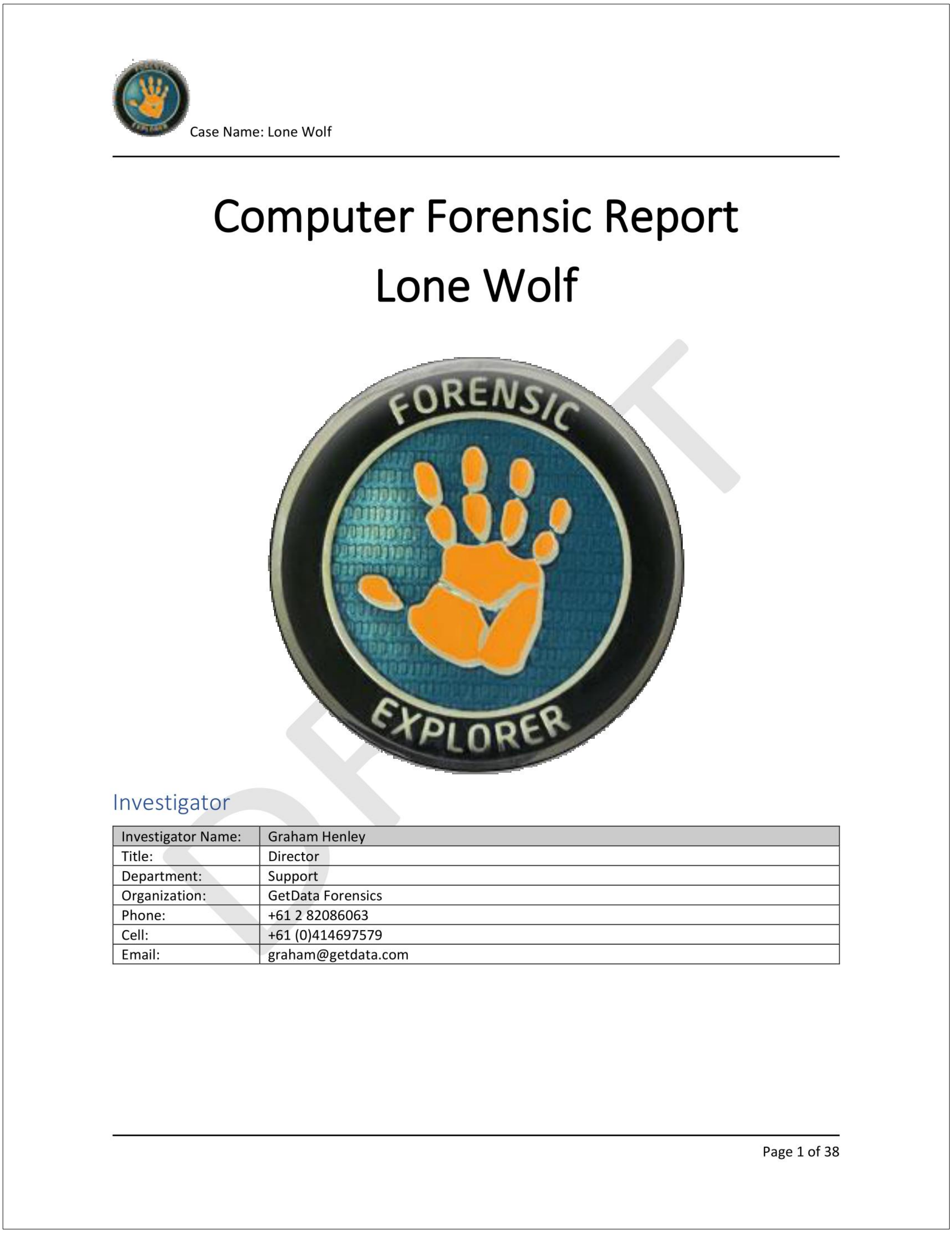


* Create Gallery from Bookmark\Pictures and Videos folders…
My Bookmarks\Pictures\Box Sync (10)
My Bookmarks\Pictures\Desktop (10)
My Bookmarks\Pictures\DropBox (31)
My Bookmarks\Pictures\Google Drive (1)
My Bookmarks\Pictures\OneDrive (19)

☑ Pictures/Videos Folder
Display Style: As List
Preferred Thumbnail Size: 128 x 128 px
Export + Link:
☑ 256 x 256 px Thumbnails
☐ Full Size Videos

☑ Row Count
☑ Filename
☐ Extension
☐ Signature
☐ Bates ID
☐ BM Comment
☑ Created
☑ Modified
☑ Accessed
☐ Physical Size
☐ Logical Size
☐ IsDirectory
☐ IsDeleted
☐ IsSystem
☐ Hash (MD5)
☑ Path

Then press the **Run** button to launch Microsoft Word.



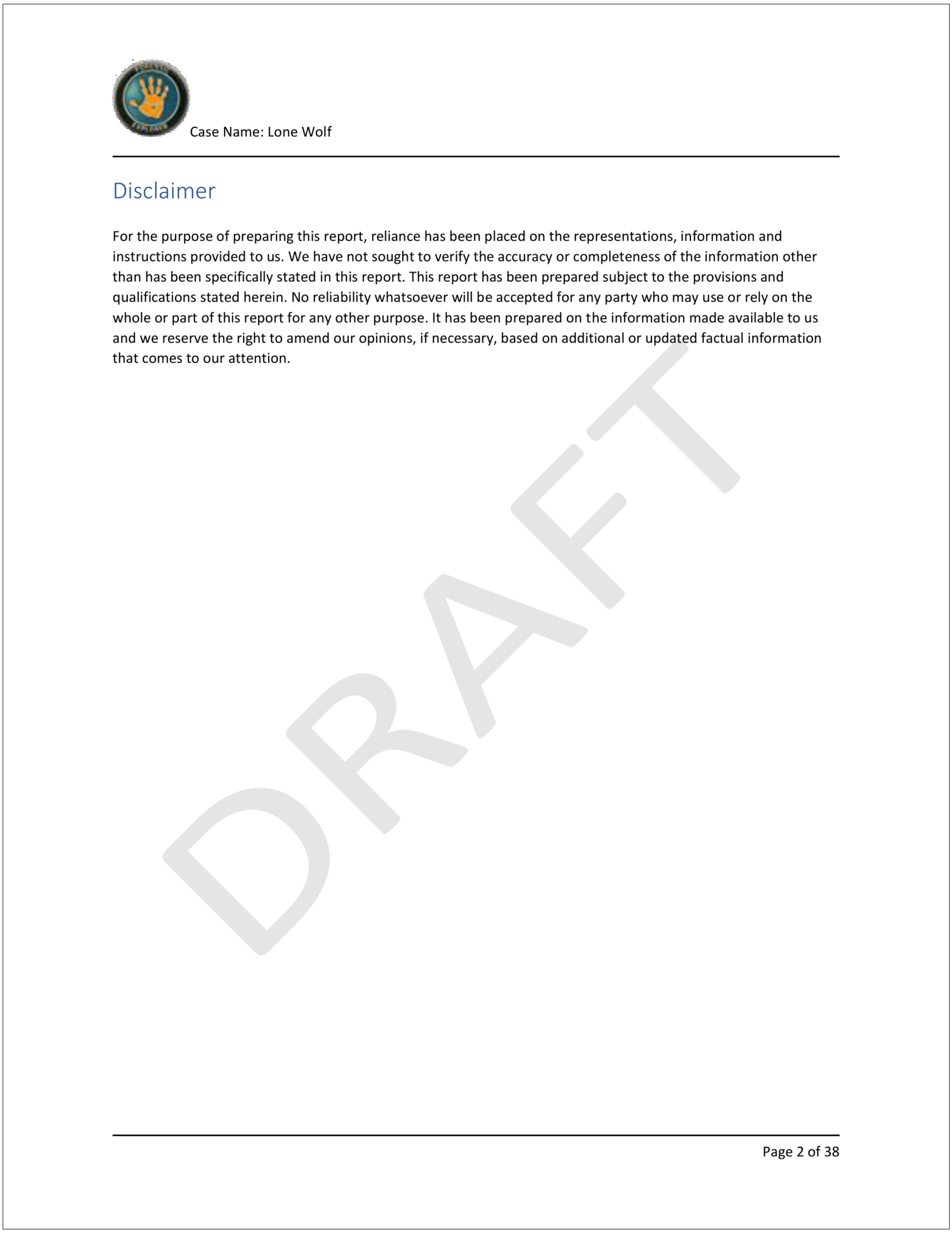
Case Name: Lone Wolf

Computer Forensic Report
Lone Wolf

Investigator

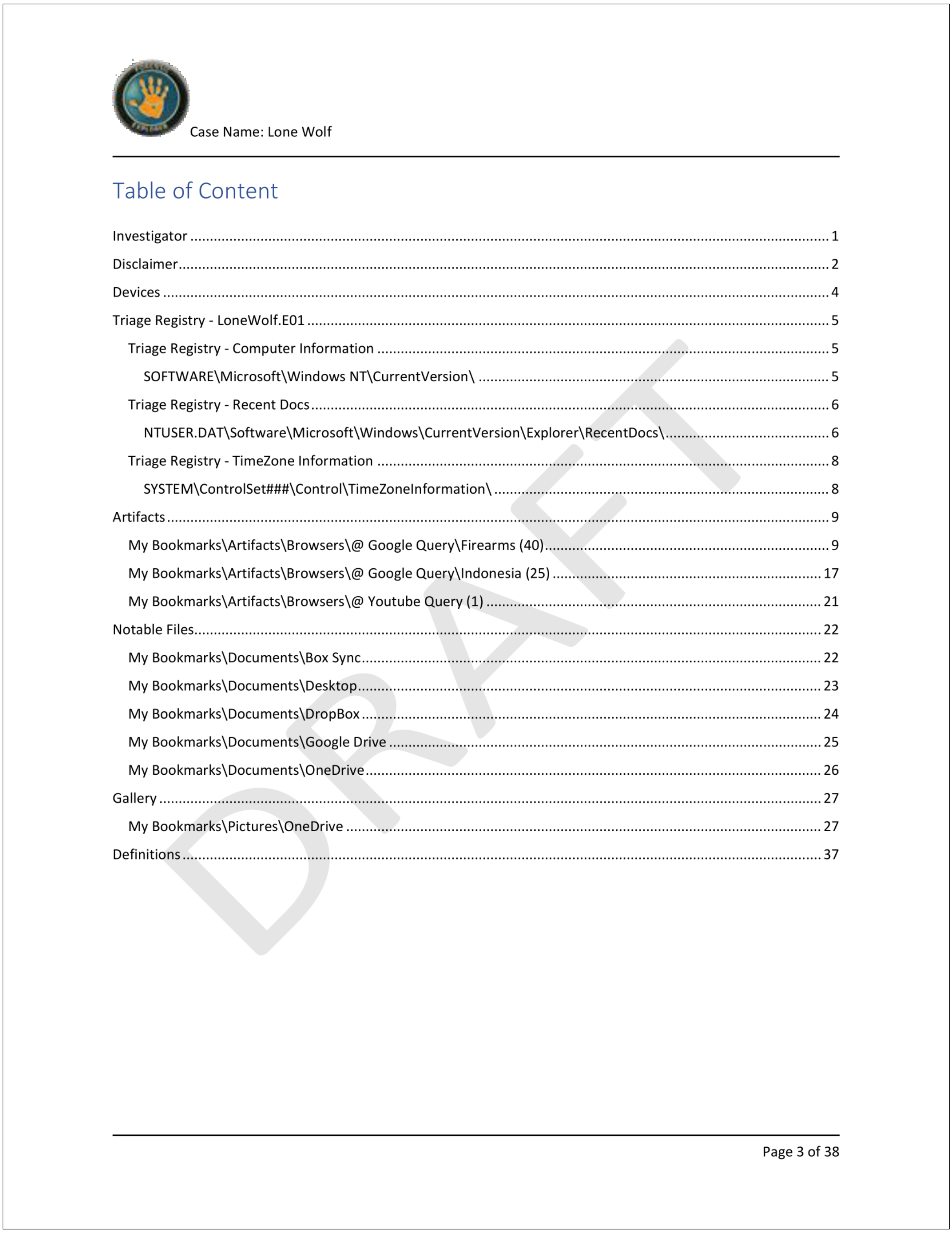
Investigator Name:	Graham Henley
Title:	Director
Department:	Support
Organization:	GetData Forensics
Phone:	+61 2 82086063
Cell:	+61 (0)414697579
Email:	graham@getdata.com

Page 1 of 38



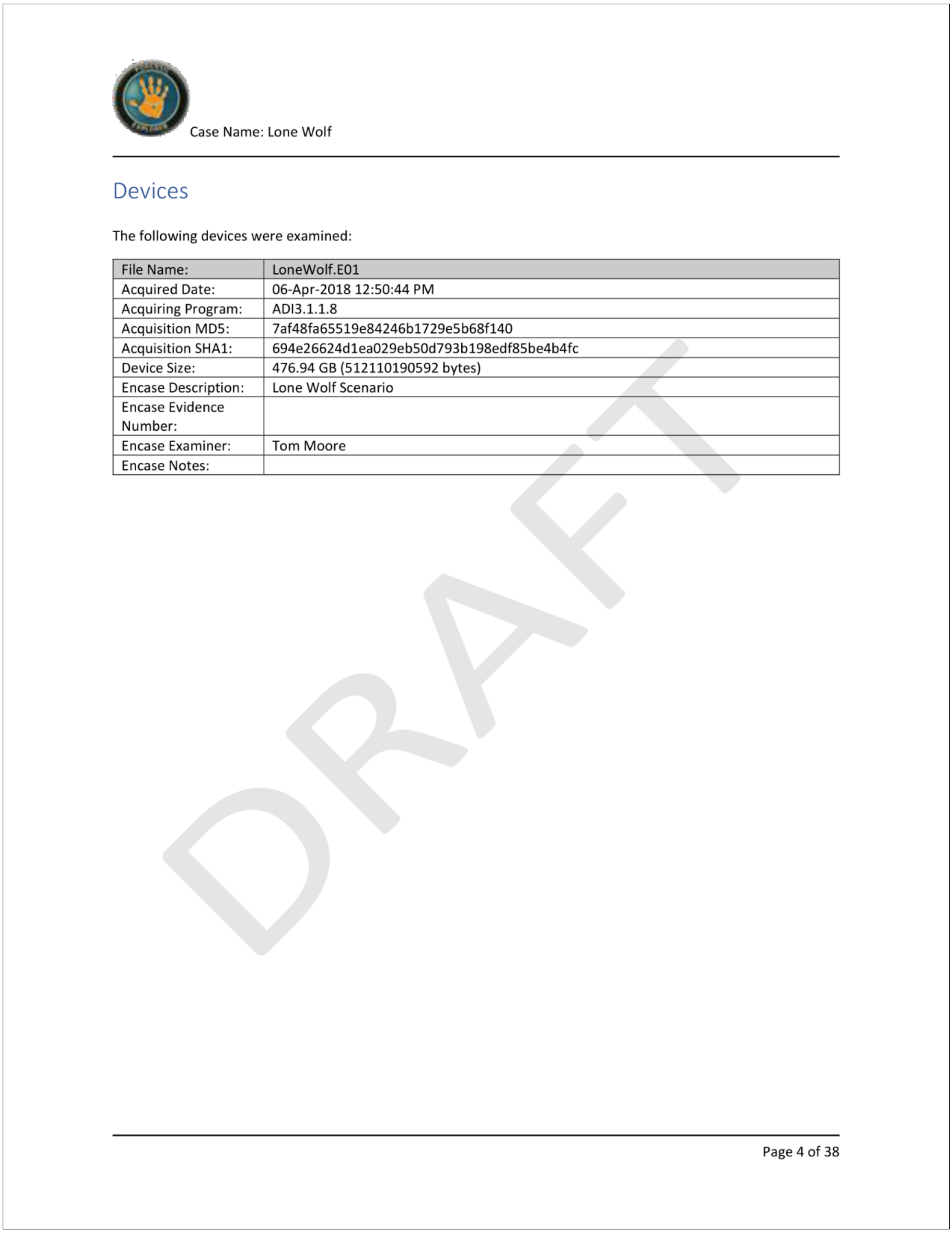
Disclaimer

For the purpose of preparing this report, reliance has been placed on the representations, information and instructions provided to us. We have not sought to verify the accuracy or completeness of the information other than has been specifically stated in this report. This report has been prepared subject to the provisions and qualifications stated herein. No reliability whatsoever will be accepted for any party who may use or rely on the whole or part of this report for any other purpose. It has been prepared on the information made available to us and we reserve the right to amend our opinions, if necessary, based on additional or updated factual information that comes to our attention.



Case Name: Lone Wolf

Table of Content



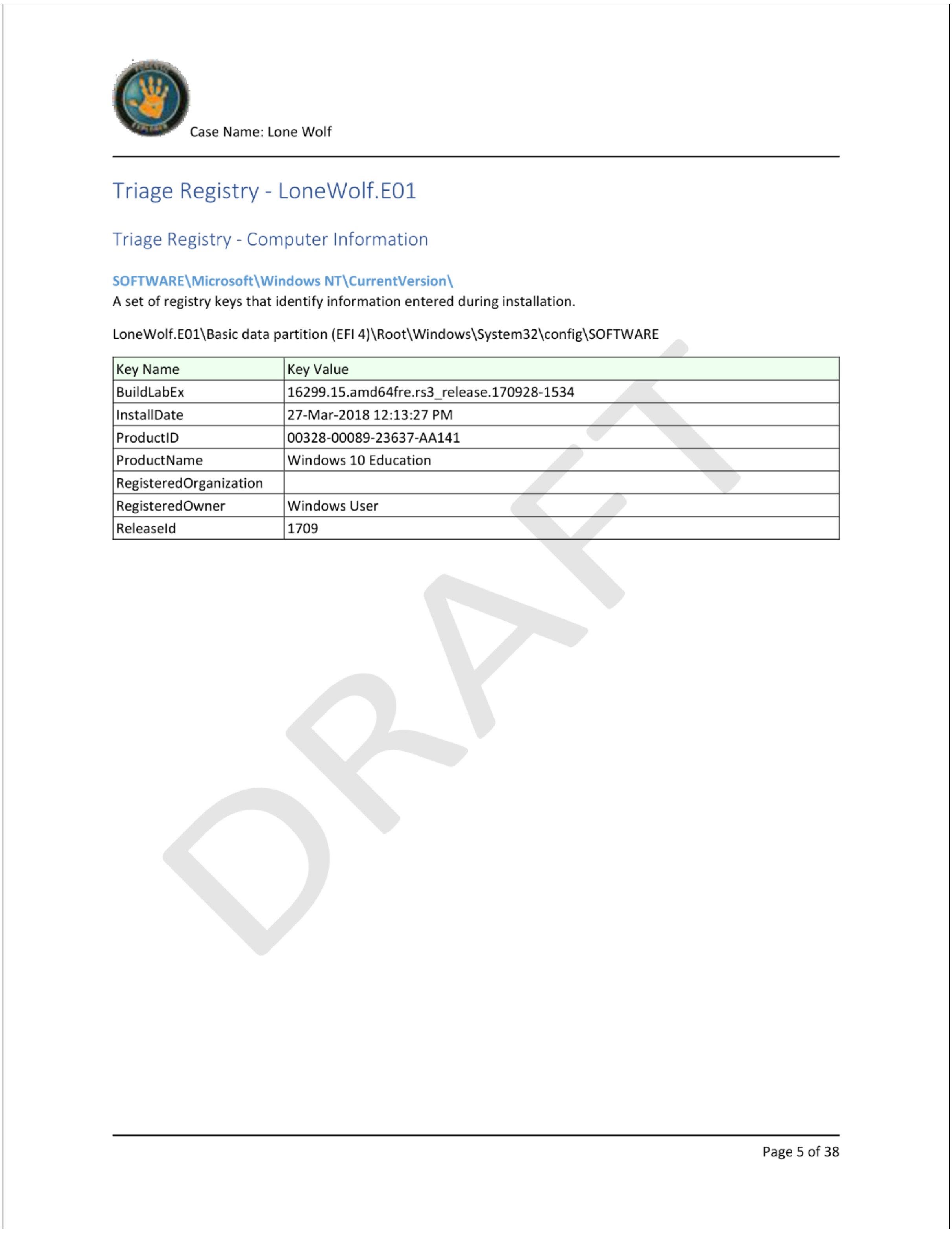
Case Name: Lone Wolf

Devices

The following devices were examined:

File Name:	LoneWolf.E01
Acquired Date:	06-Apr-2018 12:50:44 PM
Acquiring Program:	ADI3.1.1.8
Acquisition MD5:	7af48fa65519e84246b1729e5b68f140
Acquisition SHA1:	694e26624d1ea029eb50d793b198edf85be4b4fc
Device Size:	476.94 GB (512110190592 bytes)
Encase Description:	Lone Wolf Scenario
Encase Evidence Number:	
Encase Examiner:	Tom Moore
Encase Notes:	

Page 4 of 38



Case Name: Lone Wolf

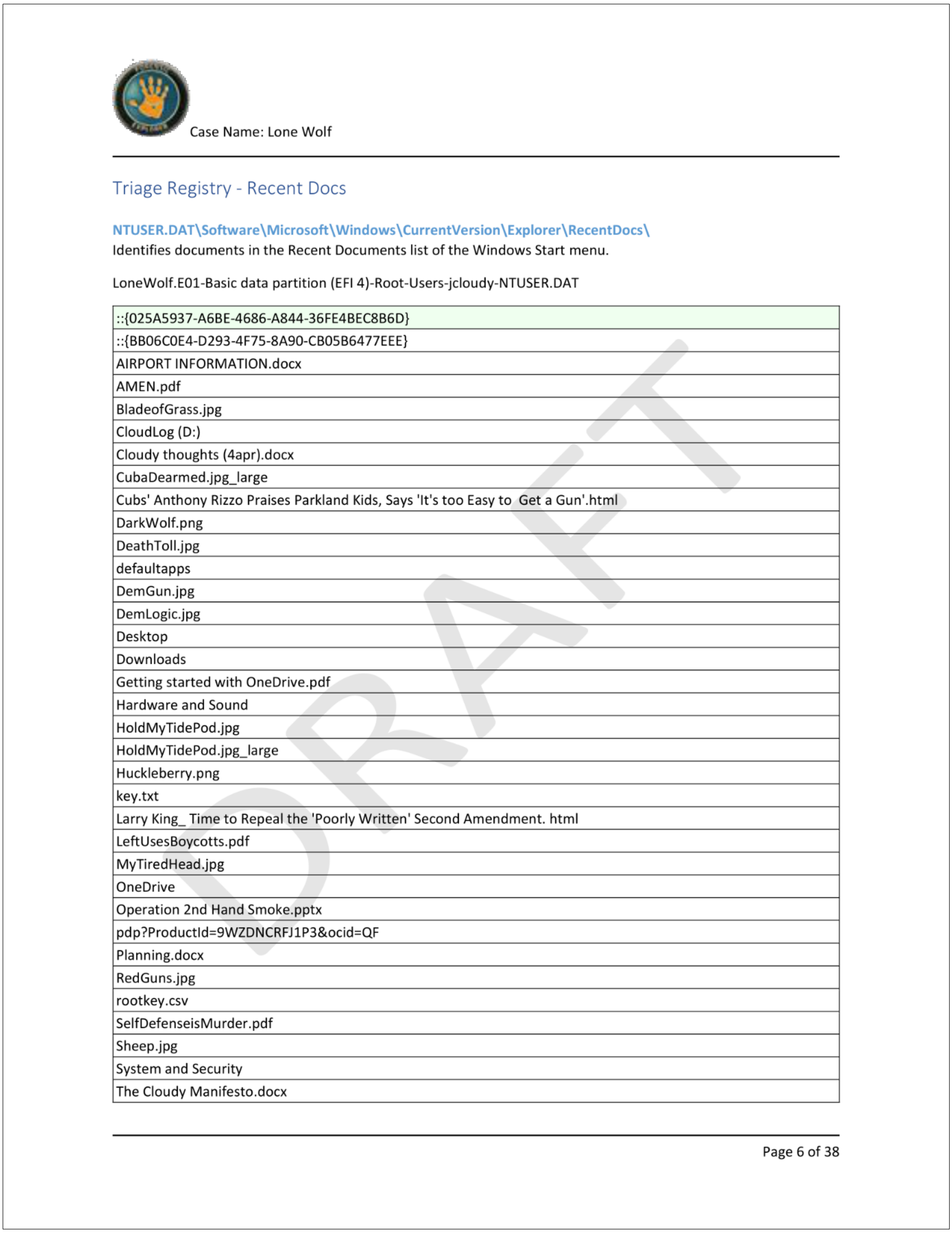
Triage Registry - LoneWolf.E01

Triage Registry - Computer Information

SOFTWARE\Microsoft\Windows NT\CurrentVersion\
A set of registry keys that identify information entered during installation.

LoneWolf.E01\Basic data partition (EFI 4)\Root\Windows\System32\config\SOFTWARE

Key Name	Key Value
BuildLabEx	16299.15.amd64fre.rs3_release.170928-1534
InstallDate	27-Mar-2018 12:13:27 PM
ProductID	00328-00089-23637-AA141
ProductName	Windows 10 Education
RegisteredOrganization	
RegisteredOwner	Windows User
ReleaseId	1709



Case Name: Lone Wolf

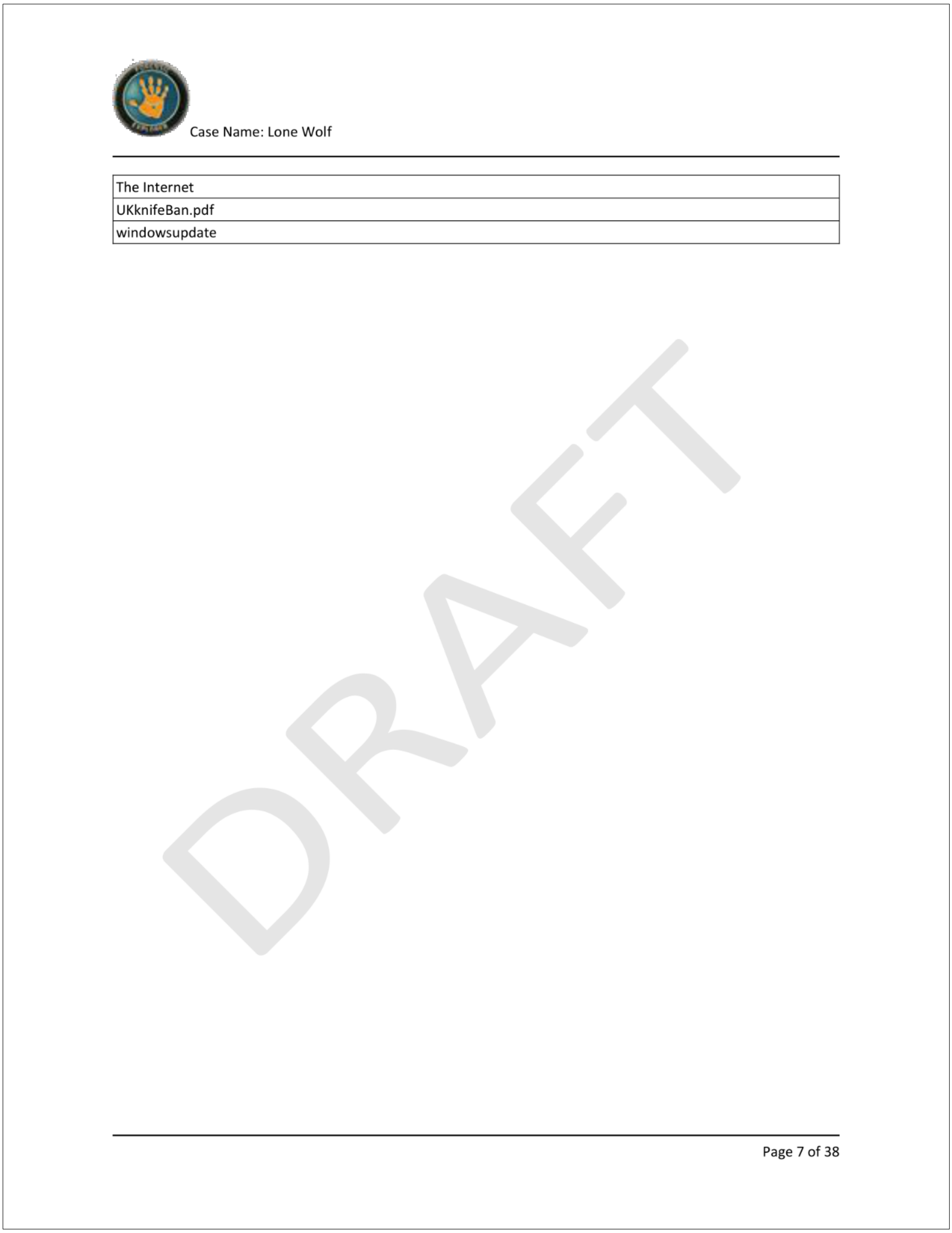
Triage Registry - Recent Docs

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\
Identifies documents in the Recent Documents list of the Windows Start menu.

LoneWolf.E01-Basic data partition (EFI 4)-Root-Users-jcloudy-NTUSER.DAT

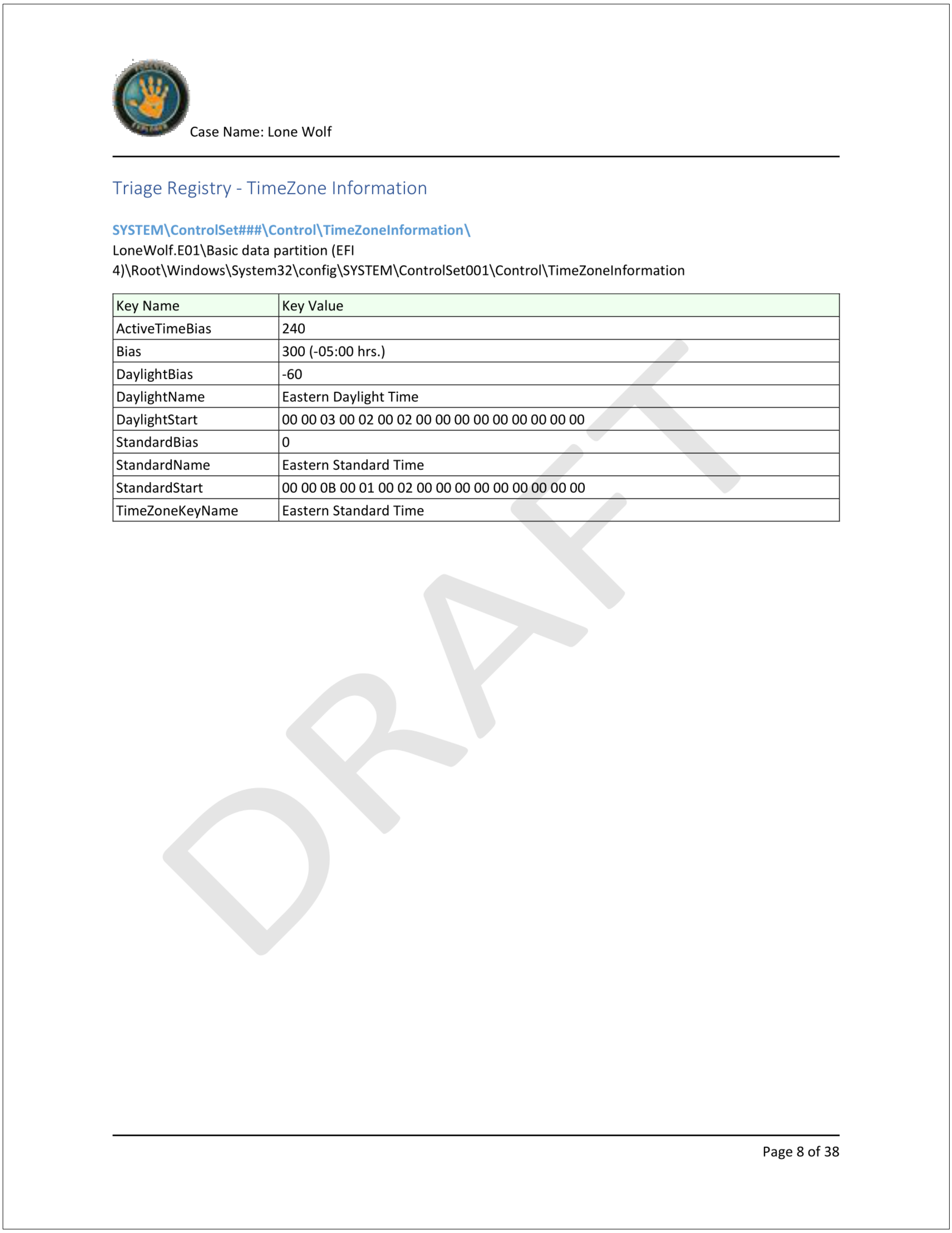
::{025A5937-A6BE-4686-A844-36FE4BEC8B6D}
::{BB06C0E4-D293-4F75-8A90-CB05B6477EEE}
AIRPORT INFORMATION.docx
AMEN.pdf
BladeofGrass.jpg
CloudLog (D:)
Cloudy thoughts (4apr).docx
CubaDearmed.jpg_large
Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's too Easy to Get a Gun'.html
DarkWolf.png
DeathToll.jpg
defaultapps
DemGun.jpg
DemLogic.jpg
Desktop
Downloads
Getting started with OneDrive.pdf
Hardware and Sound
HoldMyTidePod.jpg
HoldMyTidePod.jpg_large
Huckleberry.png
key.txt
Larry King_ Time to Repeal the 'Poorly Written' Second Amendment. html
LeftUsesBoycotts.pdf
MyTiredHead.jpg
OneDrive
Operation 2nd Hand Smoke.pptx
pdp?ProductId=9WZDNCRFJ1P3&ocid=QF
Planning.docx
RedGuns.jpg
rootkey.csv
SelfDefenseisMurder.pdf
Sheep.jpg
System and Security
The Cloudy Manifesto.docx

Page 6 of 38



Case Name: Lone Wolf

The Internet
UKknifeBan.pdf
windowsupdate



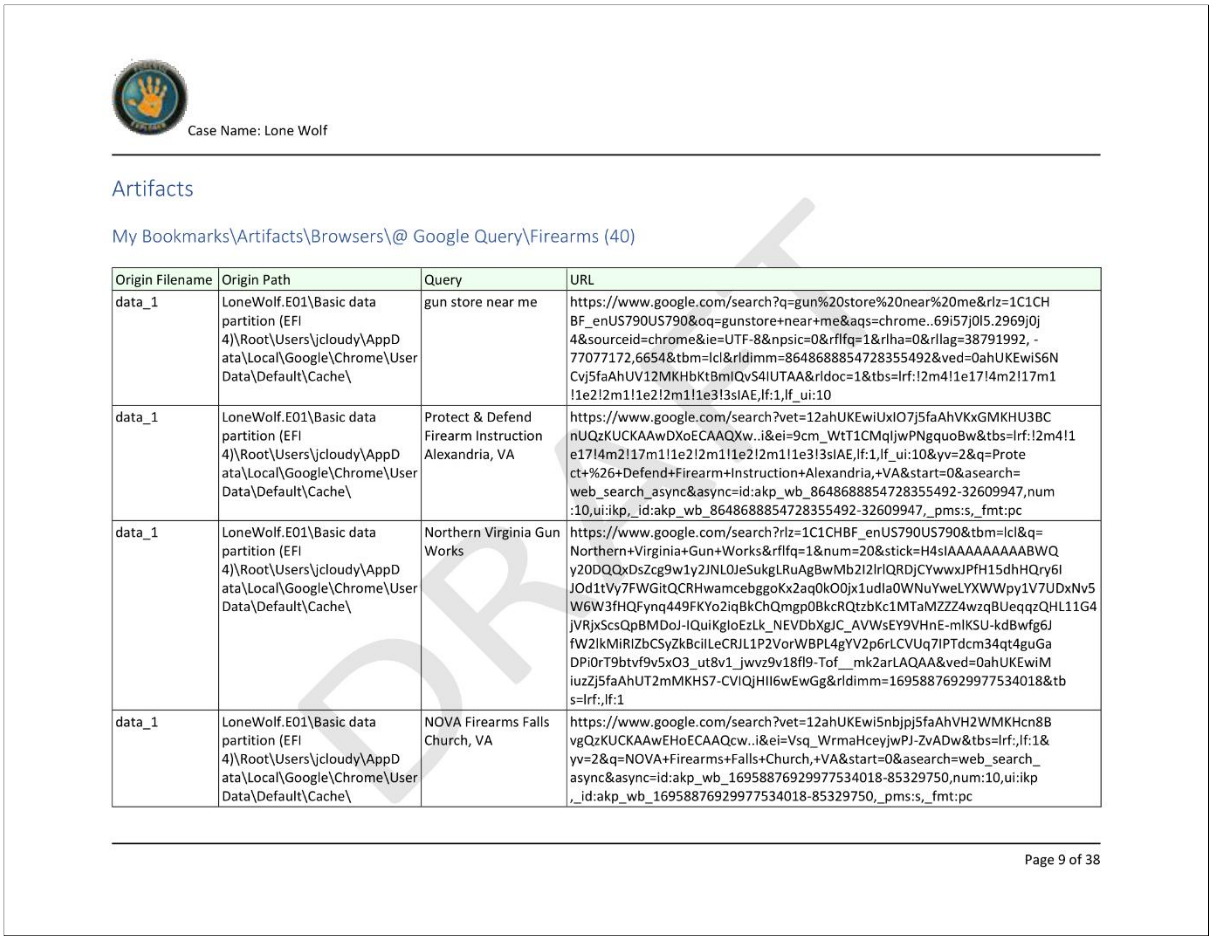
Case Name: Lone Wolf

Triage Registry - TimeZone Information

SYSTEM\ControlSet###\Control\TimeZoneInformation\

LoneWolf.E01\Basic data partition (EFI 4)\Root\Windows\System32\config\SYSTEM\ControlSet001\Control\TimeZoneInformation

Key Name	Key Value
ActiveTimeBias	240
Bias	300 (-05:00 hrs.)
DaylightBias	-60
DaylightName	Eastern Daylight Time
DaylightStart	00 00 03 00 02 00 02 00 00 00 00 00 00 00 00 00
StandardBias	0
StandardName	Eastern Standard Time
StandardStart	00 00 0B 00 01 00 02 00 00 00 00 00 00 00 00 00
TimeZoneKeyName	Eastern Standard Time



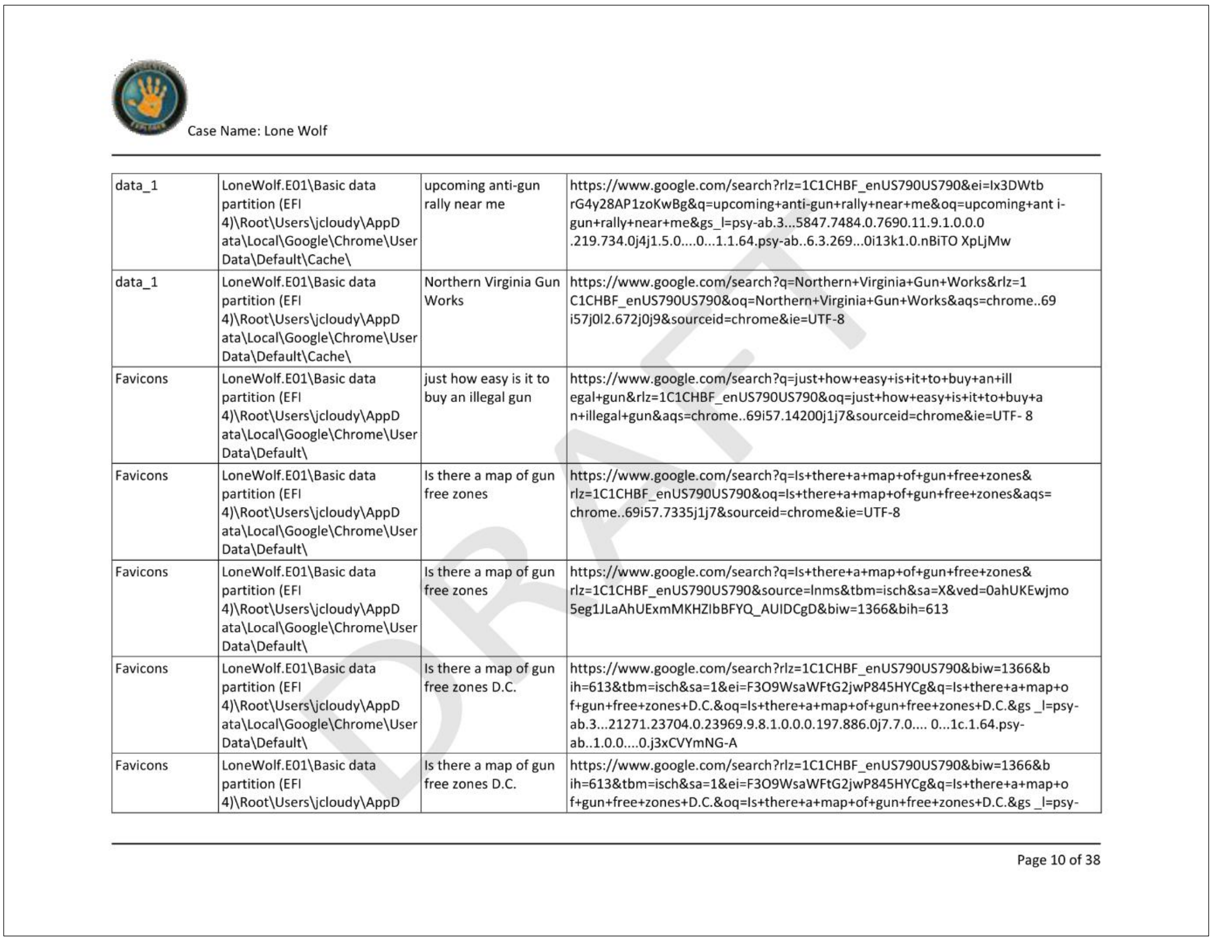
Case Name: Lone Wolf

Artifacts

My Bookmarks\Artifacts\Browsers\@ Google Query\Firearms (40)

Origin Filename	Origin Path	Query	URL
data_1	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\Cache\	gun store near me	https://www.google.com/search?q=gun%20store%20near%20me&rlz=1C1CHBF_enUS790US790&oq=gunstore+near+me&aqs=chrome..69i57j0l5.2969j0j4&sourceid=chrome&ie=UTF-8&npsic=0&rflfq=1&rlha=0&rllag=38791992, -77077172,6654&tbm=lcl&rldimm=8648688854728355492&ved=0ahUKEwiS6NCvj5faAhUV12MKHbKtBmIQvS4IUTAA&rldoc=1&tbs=lrf:!2m4!1e17!4m2!17m1!1e2!2m1!1e2!2m1!1e3!3sIAE,lf:1,lf_ui:10
data_1	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\Cache\	Protect & Defend Firearm Instruction Alexandria, VA	https://www.google.com/search?vet=12ahUKEwiUxIO7j5faAhVKxGMKHU3BCnUQzKUCKAAwDXoECAAQXw..i&ei=9cm_WtT1CMqIjwPNgquoBw&tbs=lrf:!2m4!1e17!4m2!17m1!1e2!2m1!1e2!2m1!1e3!3sIAE,lf:1,lf_ui:10&yv=2&q=Protect+%26+Defend+Firearm+Instruction+Alexandria,+VA&start=0&asearch=web_search_async&async=id:akp_wb_8648688854728355492-32609947,num:10,ui:ikp,_id:akp_wb_8648688854728355492-32609947,_pms:s,_fmt:pc
data_1	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\Cache\	Northern Virginia Gun Works	https://www.google.com/search?rlz=1C1CHBF_enUS790US790&tbm=lcl&q=Northern+Virginia+Gun+Works&rflfq=1&num=20&stick=H4sIAAAAAAAAABWQy20DQQxDsZcg9w1y2JNL0JeSukgLRuAgBwMb2I2lrlQRDjCYwwxJPfH15dhHQry6IJOd1tVy7FWGitQCRHwamcebggoKx2aq0kO0jx1udIa0WNuYweLYXWWpy1V7UDxNv5W6W3fHQFynq449FKYo2iqBkChQmgp0BkcRQtzbKc1MTaMZZZ4wzqBUeqqzQHL11G4jVRjxScsQpBMDoJ-IQuiKgIoEzLk_NEVDbXgJC_AVWsEY9VHnE-mlKSU-kdBwfg6JfW2lkMiRIZbCSyZkBciILeCRJL1P2VorWBPL4gYV2p6rLCVUq7IPTdcm34qt4guGaDPi0rT9btvf9v5xO3_ut8v1_jwvz9v18fl9-Tof__mk2arLAQAA&ved=0ahUKEwiMiuzZj5faAhUT2mMKHS7-CVIQjHII6wEwGg&rldimm=16958876929977534018&tbs=lrf:,lf:1
data_1	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\Cache\	NOVA Firearms Falls Church, VA	https://www.google.com/search?vet=12ahUKEwi5nbjpj5faAhVH2WMKHcn8BvgQzKUCKAAwEHoECAAQcw..i&ei=Vsq_WrmaHceyjwPJ-ZvADw&tbs=lrf:,lf:1&yv=2&q=NOVA+Firearms+Falls+Church,+VA&start=0&asearch=web_search_async&async=id:akp_wb_16958876929977534018-85329750,num:10,ui:ikp,_id:akp_wb_16958876929977534018-85329750,_pms:s,_fmt:pc

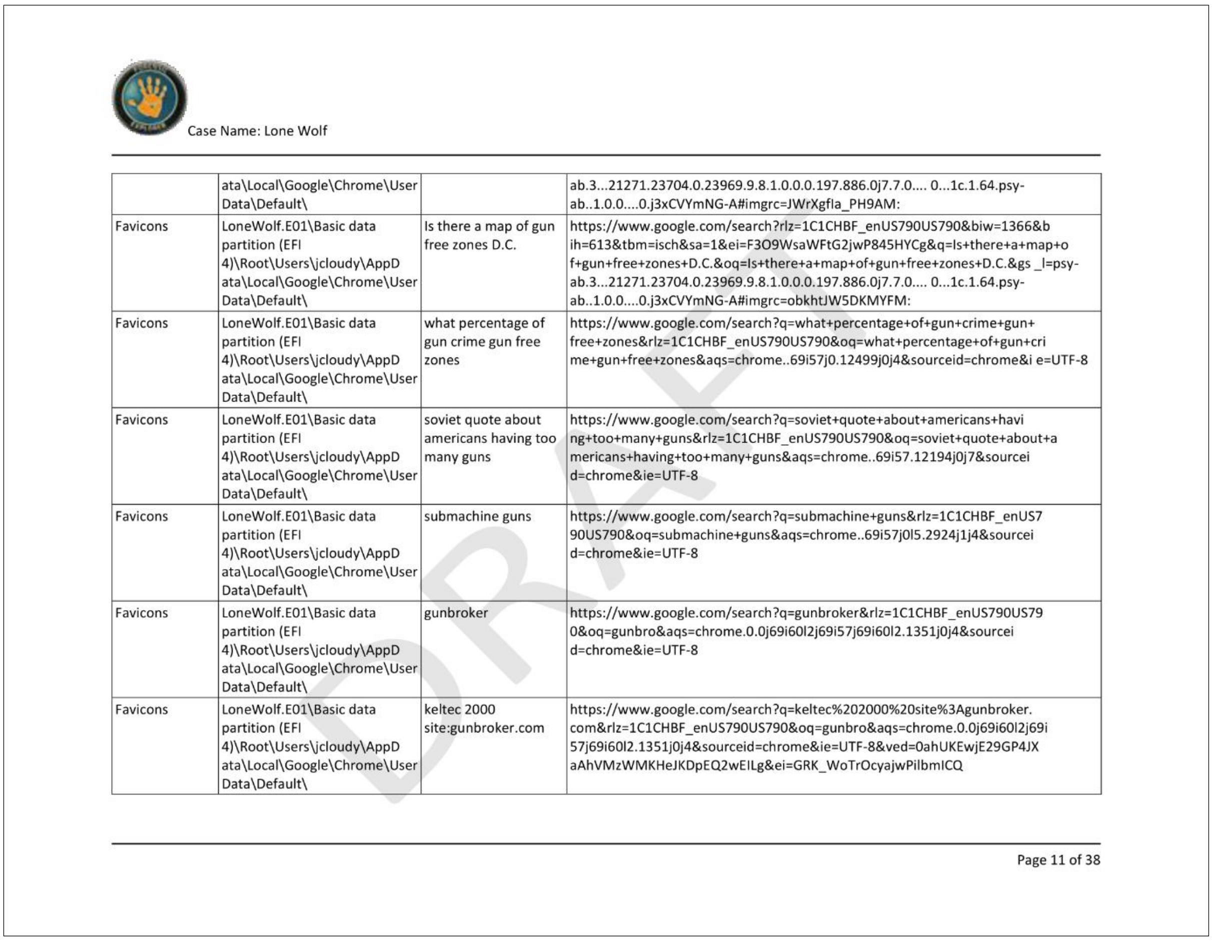
Page 9 of 38



Case Name: Lone Wolf

data_1	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\Cache\	upcoming anti-gun rally near me	https://www.google.com/search?rlz=1C1CHBF_enUS790US790&ei=Ix3DWtbrG4y28AP1zoKwBg&q=upcoming+anti-gun+rally+near+me&oq=upcoming+ant i-gun+rally+near+me&gs_l=psy-ab.3...5847.7484.0.7690.11.9.1.0.0.0.219.734.0j4j1.5.0....0...1.1.64.psy-ab..6.3.269...0i13k1.0.nBiTO XpLjMw
data_1	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\Cache\	Northern Virginia Gun Works	https://www.google.com/search?q=Northern+Virginia+Gun+Works&rlz=1C1CHBF_enUS790US790&oq=Northern+Virginia+Gun+Works&aqs=chrome..69i57j0l2.672j0j9&sourceid=chrome&ie=UTF-8
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	just how easy is it to buy an illegal gun	https://www.google.com/search?q=just+how+easy+is+it+to+buy+an+illegal+gun&rlz=1C1CHBF_enUS790US790&oq=just+how+easy+is+it+to+buy+an+illegal+gun&aqs=chrome..69i57.14200j1j7&sourceid=chrome&ie=UTF- 8
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	Is there a map of gun free zones	https://www.google.com/search?q=Is+there+a+map+of+gun+free+zones&rlz=1C1CHBF_enUS790US790&oq=Is+there+a+map+of+gun+free+zones&aqs=chrome..69i57.7335j1j7&sourceid=chrome&ie=UTF-8
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	Is there a map of gun free zones	https://www.google.com/search?q=Is+there+a+map+of+gun+free+zones&rlz=1C1CHBF_enUS790US790&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjmo5eg1JLaAhUExmMKHZIbBFYQ_AUIDCgD&biw=1366&bih=613
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	Is there a map of gun free zones D.C.	https://www.google.com/search?rlz=1C1CHBF_enUS790US790&biw=1366&bih=613&tbm=isch&sa=1&ei=F3O9WsaWFtG2jwP845HYCg&q=Is+there+a+map+of+gun+free+zones+D.C.&oq=Is+there+a+map+of+gun+free+zones+D.C.&gs _l=psy-ab.3...21271.23704.0.23969.9.8.1.0.0.0.197.886.0j7.7.0.... 0...1c.1.64.psy-ab..1.0.0....0.j3xCVYmNG-A
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppD	Is there a map of gun free zones D.C.	https://www.google.com/search?rlz=1C1CHBF_enUS790US790&biw=1366&bih=613&tbm=isch&sa=1&ei=F3O9WsaWFtG2jwP845HYCg&q=Is+there+a+map+of+gun+free+zones+D.C.&oq=Is+there+a+map+of+gun+free+zones+D.C.&gs _l=psy-

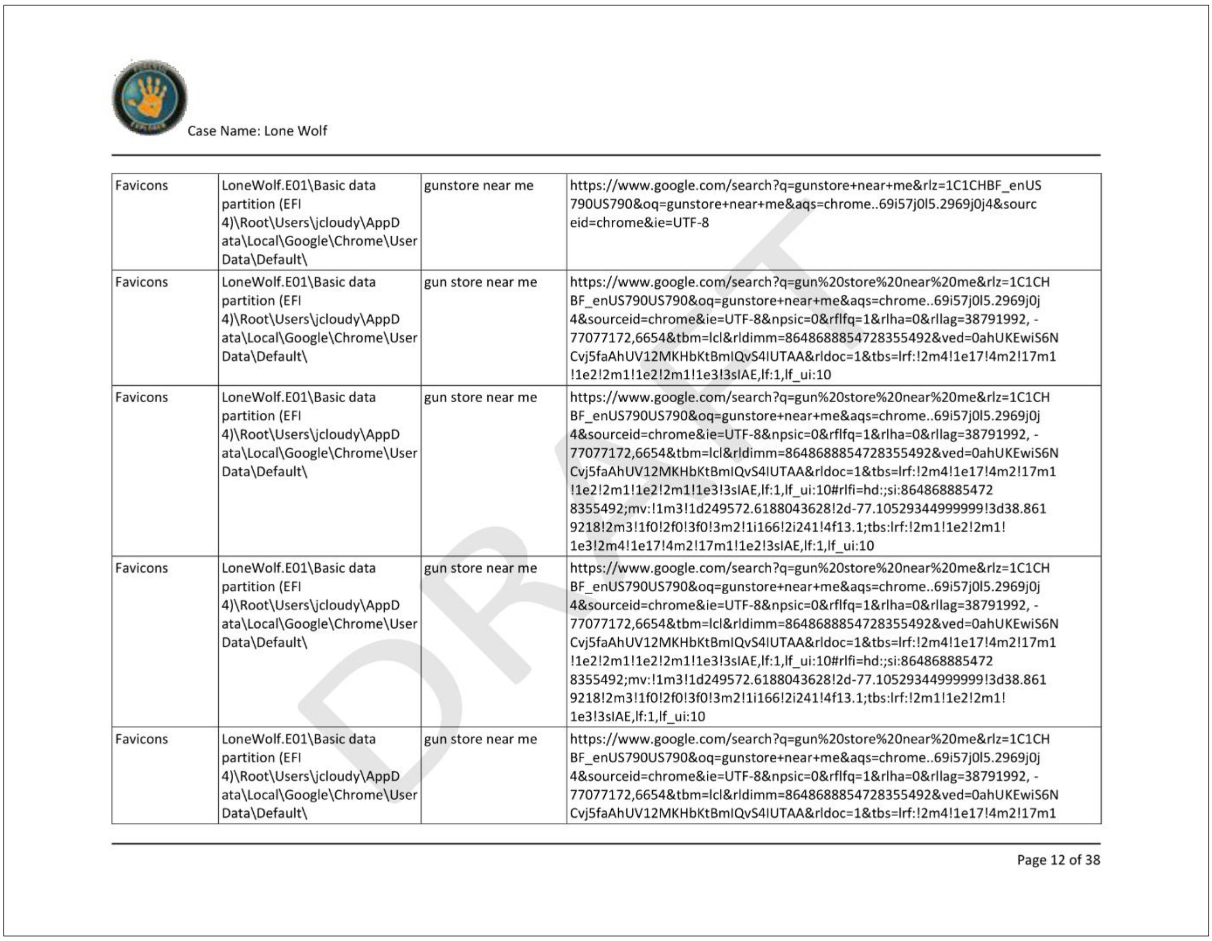
Page 10 of 38



Case Name: Lone Wolf

	ata\Local\Google\Chrome\User Data\Default\		ab.3...21271.23704.0.23969.9.8.1.0.0.0.197.886.0j7.7.0.... 0...1c.1.64.psy-ab..1.0.0....0.j3xCVYmNG-A#imgrc=JWrXgfla_PH9AM:
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	Is there a map of gun free zones D.C.	https://www.google.com/search?rlz=1C1CHBF_enUS790US790&biw=1366&bih=613&tbm=isch&sa=1&ei=F3O9WsaWFtG2jwP845HYCg&q=Is+there+a+map+of+gun+free+zones+D.C.&oq=Is+there+a+map+of+gun+free+zones+D.C.&gs _l=psy-ab.3...21271.23704.0.23969.9.8.1.0.0.0.197.886.0j7.7.0.... 0...1c.1.64.psy-ab..1.0.0....0.j3xCVYmNG-A#imgrc=obkhtJW5DKMYFM:
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	what percentage of gun crime gun free zones	https://www.google.com/search?q=what+percentage+of+gun+crime+gun+free+zones&rlz=1C1CHBF_enUS790US790&oq=what+percentage+of+gun+crime+gun+free+zones&aqs=chrome..69i57j0.12499j0j4&sourceid=chrome&i e=UTF-8
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	soviet quote about americans having too many guns	https://www.google.com/search?q=soviet+quote+about+americans+having+too+many+guns&rlz=1C1CHBF_enUS790US790&oq=soviet+quote+about+americans+having+too+many+guns&aqs=chrome..69i57.12194j0j7&sourceid=chrome&ie=UTF-8
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	submachine guns	https://www.google.com/search?q=submachine+guns&rlz=1C1CHBF_enUS790US790&oq=submachine+guns&aqs=chrome..69i57j0l5.2924j1j4&sourceid=chrome&ie=UTF-8
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	gunbroker	https://www.google.com/search?q=gunbroker&rlz=1C1CHBF_enUS790US790&oq=gunbro&aqs=chrome.0.0j69i60l2j69i57j69i60l2.1351j0j4&sourceid=chrome&ie=UTF-8
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	keltec 2000 site:gunbroker.com	https://www.google.com/search?q=keltec%202000%20site%3Agunbroker.com&rlz=1C1CHBF_enUS790US790&oq=gunbro&aqs=chrome.0.0j69i60l2j69i57j69i60l2.1351j0j4&sourceid=chrome&ie=UTF-8&ved=0ahUKEwjE29GP4JXaAhVMzWMKHeJKDpEQ2wEILg&ei=GRK_WoTrOcyajwPilbmICQ

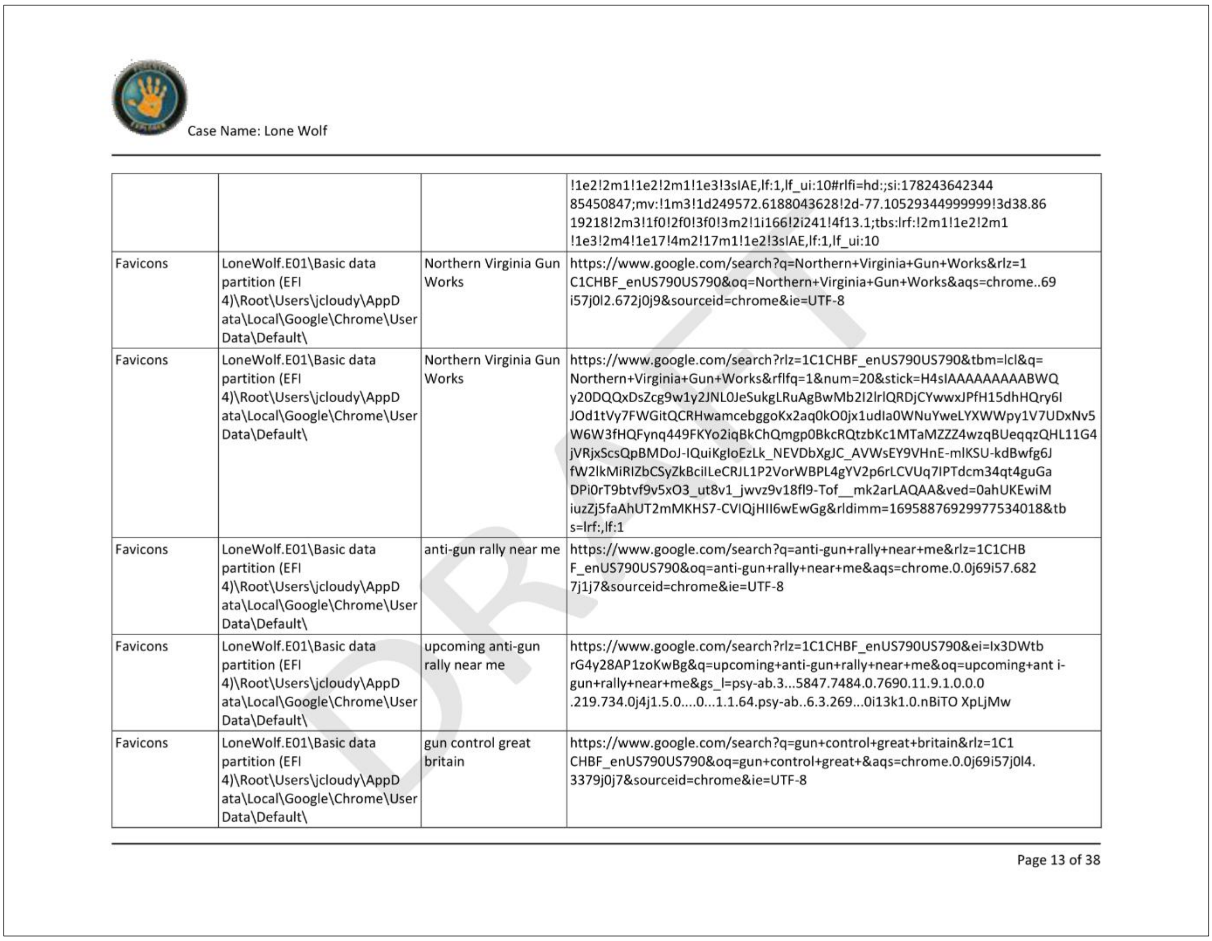
Page 11 of 38



Case Name: Lone Wolf

Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	gunstore near me	https://www.google.com/search?q=gunstore+near+me&rlz=1C1CHBF_enUS790US790&oq=gunstore+near+me&aqs=chrome..69i57j0l5.2969j0j4&sourceid=chrome&ie=UTF-8
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	gun store near me	https://www.google.com/search?q=gun%20store%20near%20me&rlz=1C1CHBF_enUS790US790&oq=gunstore+near+me&aqs=chrome..69i57j0l5.2969j0j4&sourceid=chrome&ie=UTF-8&npsic=0&rflfq=1&rlha=0&rllag=38791992, -77077172,6654&tbm=lcl&rldimm=8648688854728355492&ved=0ahUKEwiS6NCvj5faAhUV12MKHbKtBmIQvS4IUTAA&rldoc=1&tbs=lrf:!2m4!1e17!4m2!17m1!1e2!2m1!1e2!2m1!1e3!3sIAE,lf:1,lf_ui:10
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	gun store near me	https://www.google.com/search?q=gun%20store%20near%20me&rlz=1C1CHBF_enUS790US790&oq=gunstore+near+me&aqs=chrome..69i57j0l5.2969j0j4&sourceid=chrome&ie=UTF-8&npsic=0&rflfq=1&rlha=0&rllag=38791992, -77077172,6654&tbm=lcl&rldimm=8648688854728355492&ved=0ahUKEwiS6NCvj5faAhUV12MKHbKtBmIQvS4IUTAA&rldoc=1&tbs=lrf:!2m4!1e17!4m2!17m1!1e2!2m1!1e2!2m1!1e3!3sIAE,lf:1,lf_ui:10#rlfi=hd:;si:8648688854728355492;mv:!1m3!1d249572.6188043628!2d-77.10529344999999!3d38.8619218!2m3!1f0!2f0!3f0!3m2!1i166!2i241!4f13.1;tbs:lrf:!2m1!1e2!2m1!1e3!2m4!1e17!4m2!17m1!1e2!3sIAE,lf:1,lf_ui:10
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	gun store near me	https://www.google.com/search?q=gun%20store%20near%20me&rlz=1C1CHBF_enUS790US790&oq=gunstore+near+me&aqs=chrome..69i57j0l5.2969j0j4&sourceid=chrome&ie=UTF-8&npsic=0&rflfq=1&rlha=0&rllag=38791992, -77077172,6654&tbm=lcl&rldimm=8648688854728355492&ved=0ahUKEwiS6NCvj5faAhUV12MKHbKtBmIQvS4IUTAA&rldoc=1&tbs=lrf:!2m4!1e17!4m2!17m1!1e2!2m1!1e2!2m1!1e3!3sIAE,lf:1,lf_ui:10#rlfi=hd:;si:8648688854728355492;mv:!1m3!1d249572.6188043628!2d-77.10529344999999!3d38.8619218!2m3!1f0!2f0!3f0!3m2!1i166!2i241!4f13.1;tbs:lrf:!2m1!1e2!2m1!1e3!3sIAE,lf:1,lf_ui:10
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	gun store near me	https://www.google.com/search?q=gun%20store%20near%20me&rlz=1C1CHBF_enUS790US790&oq=gunstore+near+me&aqs=chrome..69i57j0l5.2969j0j4&sourceid=chrome&ie=UTF-8&npsic=0&rflfq=1&rlha=0&rllag=38791992, -77077172,6654&tbm=lcl&rldimm=8648688854728355492&ved=0ahUKEwiS6NCvj5faAhUV12MKHbKtBmIQvS4IUTAA&rldoc=1&tbs=lrf:!2m4!1e17!4m2!17m1

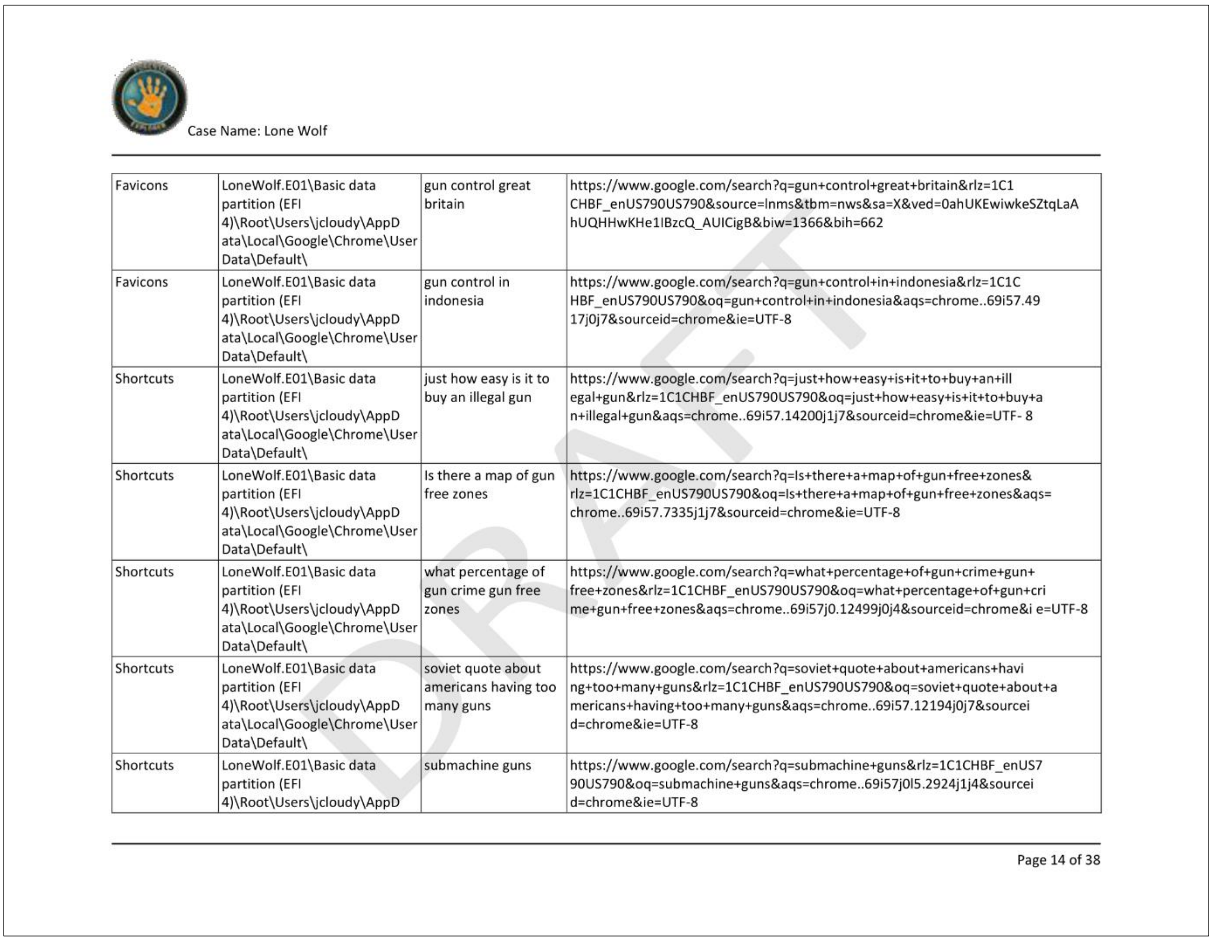
Page 12 of 38



Case Name: Lone Wolf

			!1e2!2m1!1e2!2m1!1e3!3sIAE,lf:1,lf_ui:10#rlfi=hd:;si:17824364234485450847;mv:!1m3!1d249572.6188043628!2d-77.10529344999999!3d38.8619218!2m3!1f0!2f0!3f0!3m2!1i166!2i241!4f13.1;tbs:lrf:!2m1!1e2!2m1!1e3!2m4!1e17!4m2!17m1!1e2!3sIAE,lf:1,lf_ui:10
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	Northern Virginia Gun Works	https://www.google.com/search?q=Northern+Virginia+Gun+Works&rlz=1C1CHBF_enUS790US790&oq=Northern+Virginia+Gun+Works&aqs=chrome..69i57j0l2.672j0j9&sourceid=chrome&ie=UTF-8
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	Northern Virginia Gun Works	https://www.google.com/search?rlz=1C1CHBF_enUS790US790&tbm=lcl&q=Northern+Virginia+Gun+Works&rflfq=1&num=20&stick=H4sIAAAAAAAAABWQy20DQQxDsZcg9w1y2JNL0JeSukgLRuAgBwMb2I2lrlQRDjCYwwxJPfH15dhHQry6IJOd1tVy7FWGitQCRHwamcebggoKx2aq0kO0jx1udIa0WNuYweLYXWWpy1V7UDxNv5W6W3fHQFynq449FKYo2iqBkChQmgp0BkcRQtzbKc1MTaMZZZ4wzqBUeqqzQHL11G4jVRjxScsQpBMDoJ-IQuiKgIoEzLk_NEVDbXgJC_AVWsEY9VHnE-mlKSU-kdBwfg6JfW2lkMiRIZbCSyZkBciILeCRJL1P2VorWBPL4gYV2p6rLCVUq7IPTdcm34qt4guGaDPi0rT9btvf9v5xO3_ut8v1_jwvz9v18fl9-Tof__mk2arLAQAA&ved=0ahUKEwiMiuzZj5faAhUT2mMKHS7-CVIQjHII6wEwGg&rldimm=16958876929977534018&tbs=lrf:,lf:1
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	anti-gun rally near me	https://www.google.com/search?q=anti-gun+rally+near+me&rlz=1C1CHBF_enUS790US790&oq=anti-gun+rally+near+me&aqs=chrome.0.0j69i57.6827j1j7&sourceid=chrome&ie=UTF-8
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	upcoming anti-gun rally near me	https://www.google.com/search?rlz=1C1CHBF_enUS790US790&ei=Ix3DWtbrG4y28AP1zoKwBg&q=upcoming+anti-gun+rally+near+me&oq=upcoming+ant i-gun+rally+near+me&gs_l=psy-ab.3...5847.7484.0.7690.11.9.1.0.0.0.219.734.0j4j1.5.0....0...1.1.64.psy-ab..6.3.269...0i13k1.0.nBiTO XpLjMw
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	gun control great britain	https://www.google.com/search?q=gun+control+great+britain&rlz=1C1CHBF_enUS790US790&oq=gun+control+great+&aqs=chrome.0.0j69i57j0l4.3379j0j7&sourceid=chrome&ie=UTF-8

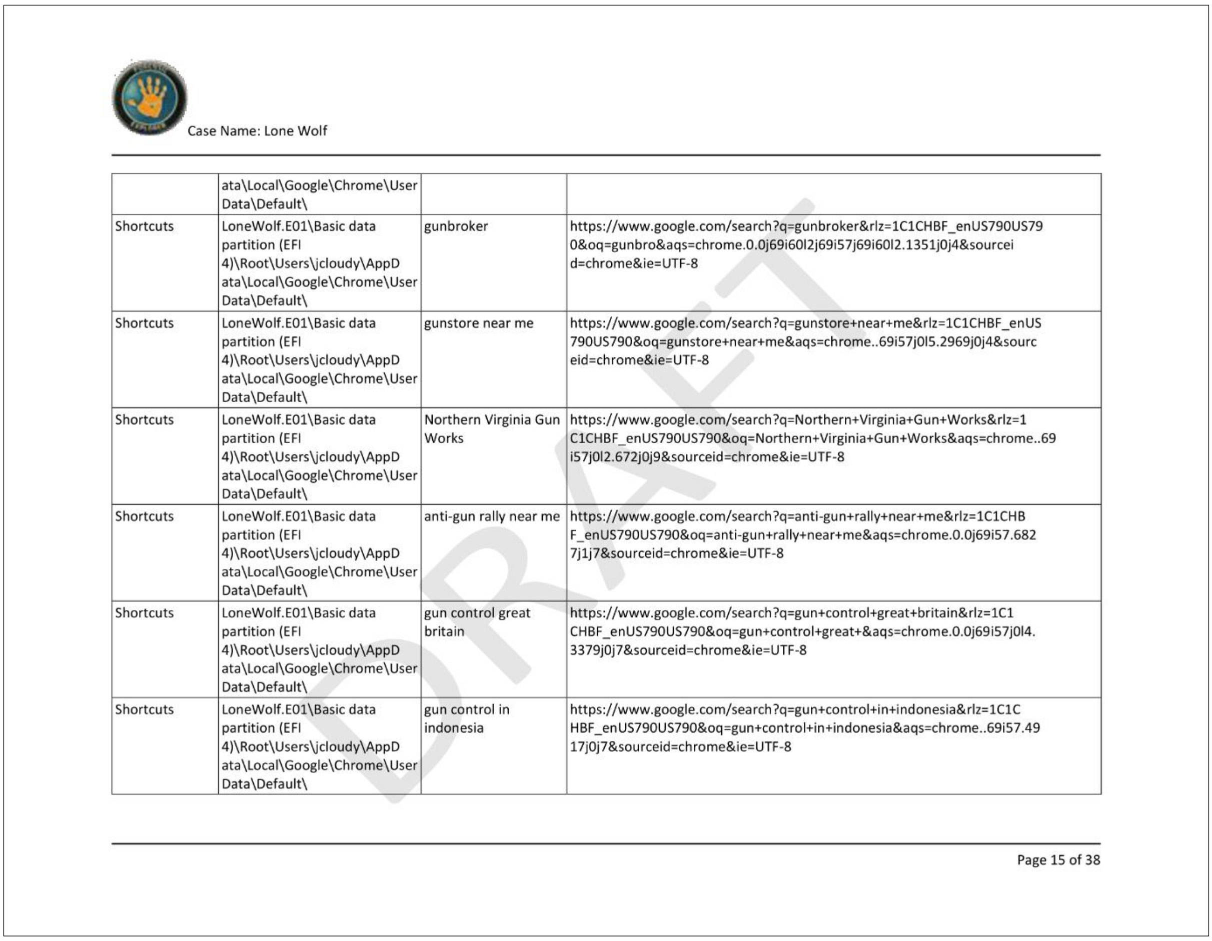
Page 13 of 38



Case Name: Lone Wolf

Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	gun control great britain	https://www.google.com/search?q=gun+control+great+britain&rlz=1C1CHBF_enUS790US790&source=lnms&tbm=nws&sa=X&ved=0ahUKEwiwkeSZtqLaAhUQHHwKHe1lBzcQ_AUICigB&biw=1366&bih=662
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	gun control in indonesia	https://www.google.com/search?q=gun+control+in+indonesia&rlz=1C1CHBF_enUS790US790&oq=gun+control+in+indonesia&aqs=chrome..69i57.4917j0j7&sourceid=chrome&ie=UTF-8
Shortcuts	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	just how easy is it to buy an illegal gun	https://www.google.com/search?q=just+how+easy+is+it+to+buy+an+illegal+gun&rlz=1C1CHBF_enUS790US790&oq=just+how+easy+is+it+to+buy+an+illegal+gun&aqs=chrome..69i57.14200j1j7&sourceid=chrome&ie=UTF- 8
Shortcuts	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	Is there a map of gun free zones	https://www.google.com/search?q=Is+there+a+map+of+gun+free+zones&rlz=1C1CHBF_enUS790US790&oq=Is+there+a+map+of+gun+free+zones&aqs=chrome..69i57.7335j1j7&sourceid=chrome&ie=UTF-8
Shortcuts	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	what percentage of gun crime gun free zones	https://www.google.com/search?q=what+percentage+of+gun+crime+gun+free+zones&rlz=1C1CHBF_enUS790US790&oq=what+percentage+of+gun+crime+gun+free+zones&aqs=chrome..69i57j0.12499j0j4&sourceid=chrome&i e=UTF-8
Shortcuts	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	soviet quote about americans having too many guns	https://www.google.com/search?q=soviet+quote+about+americans+having+too+many+guns&rlz=1C1CHBF_enUS790US790&oq=soviet+quote+about+americans+having+too+many+guns&aqs=chrome..69i57.12194j0j7&sourceid=chrome&ie=UTF-8
Shortcuts	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppD	submachine guns	https://www.google.com/search?q=submachine+guns&rlz=1C1CHBF_enUS790US790&oq=submachine+guns&aqs=chrome..69i57j0l5.2924j1j4&sourceid=chrome&ie=UTF-8

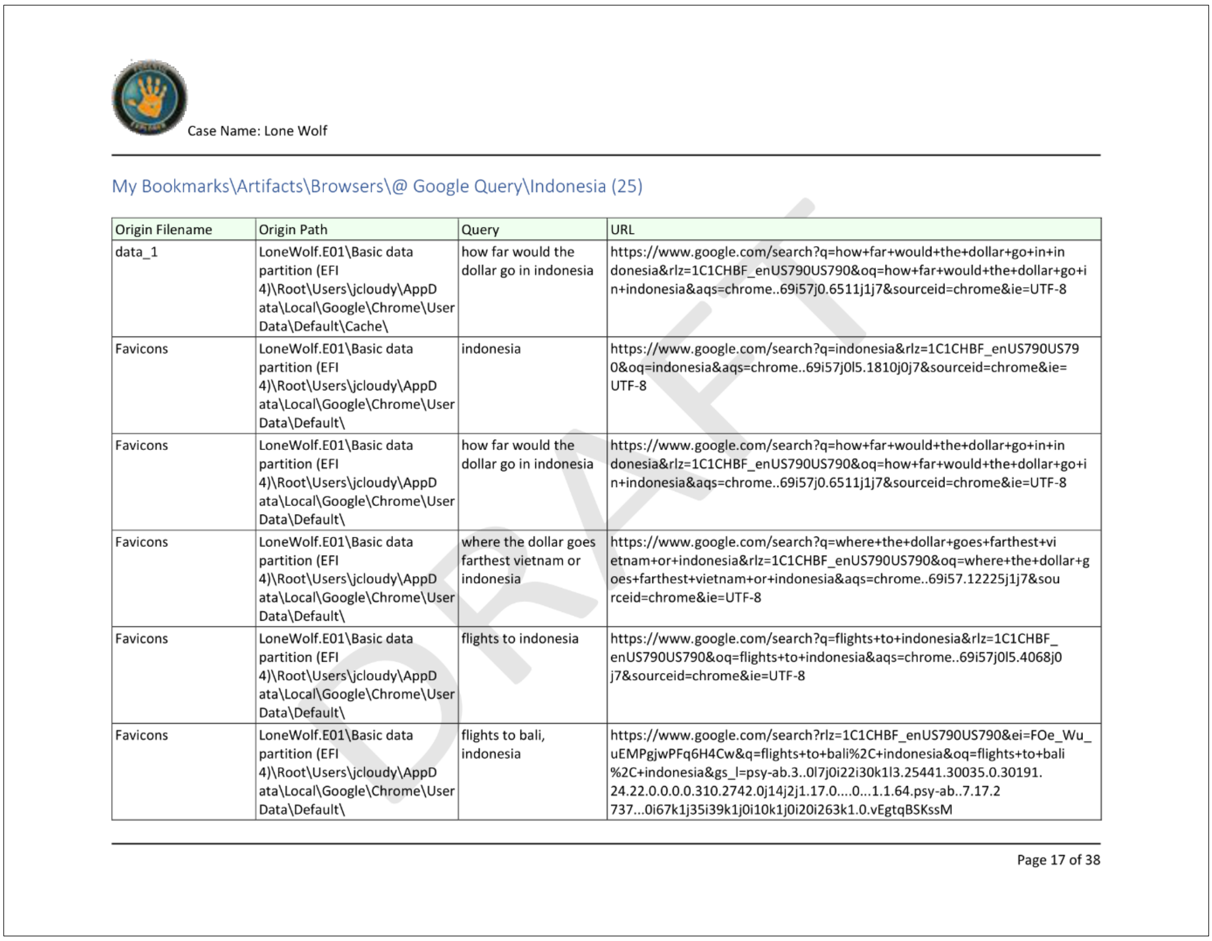
Page 14 of 38



Case Name: Lone Wolf

	ata\Local\Google\Chrome\User Data\Default\		
Shortcuts	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	gunbroker	https://www.google.com/search?q=gunbroker&rlz=1C1CHBF_enUS790US790&oq=gunbro&aqs=chrome.0.0j69i60l2j69i57j69i60l2.1351j0j4&sourceid=chrome&ie=UTF-8
Shortcuts	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	gunstore near me	https://www.google.com/search?q=gunstore+near+me&rlz=1C1CHBF_enUS790US790&oq=gunstore+near+me&aqs=chrome..69i57j0l5.2969j0j4&sourceid=chrome&ie=UTF-8
Shortcuts	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	Northern Virginia Gun Works	https://www.google.com/search?q=Northern+Virginia+Gun+Works&rlz=1C1CHBF_enUS790US790&oq=Northern+Virginia+Gun+Works&aqs=chrome..69i57j0l2.672j0j9&sourceid=chrome&ie=UTF-8
Shortcuts	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	anti-gun rally near me	https://www.google.com/search?q=anti-gun+rally+near+me&rlz=1C1CHBF_enUS790US790&oq=anti-gun+rally+near+me&aqs=chrome.0.0j69i57.6827j1j7&sourceid=chrome&ie=UTF-8
Shortcuts	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	gun control great britain	https://www.google.com/search?q=gun+control+great+britain&rlz=1C1CHBF_enUS790US790&oq=gun+control+great+&aqs=chrome.0.0j69i57j0l4.3379j0j7&sourceid=chrome&ie=UTF-8
Shortcuts	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	gun control in indonesia	https://www.google.com/search?q=gun+control+in+indonesia&rlz=1C1CHBF_enUS790US790&oq=gun+control+in+indonesia&aqs=chrome..69i57.4917j0j7&sourceid=chrome&ie=UTF-8

Page 15 of 38

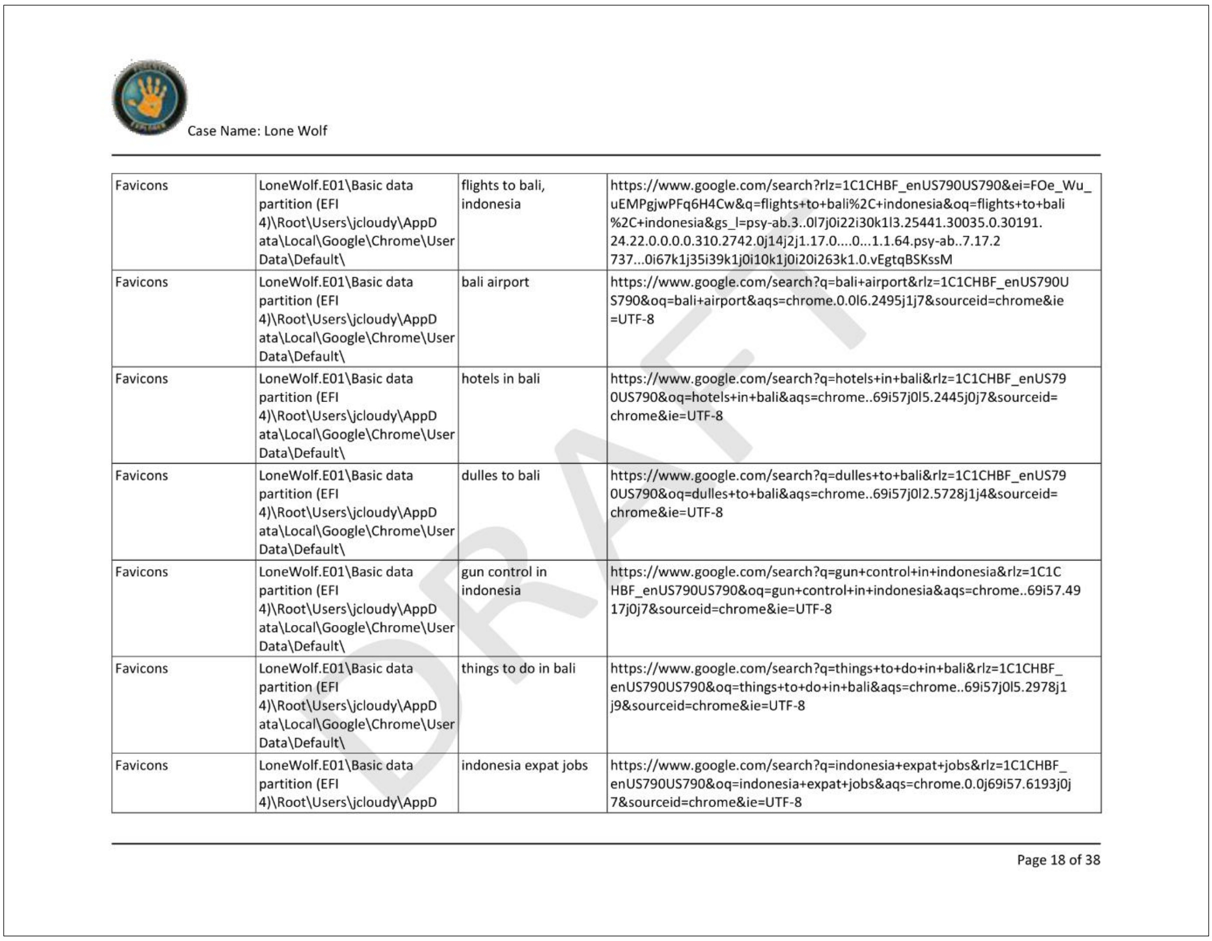


Case Name: Lone Wolf

My Bookmarks\Artifacts\Browsers\@ Google Query\Indonesia (25)

Origin Filename	Origin Path	Query	URL
data_1	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\Cache\	how far would the dollar go in indonesia	https://www.google.com/search?q=how+far+would+the+dollar+go+in+indonesia&rlz=1C1CHBF_enUS790US790&oq=how+far+would+the+dollar+go+in+indonesia&aqs=chrome..69i57j0.6511j1j7&sourceid=chrome&ie=UTF-8
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	indonesia	https://www.google.com/search?q=indonesia&rlz=1C1CHBF_enUS790US790&oq=indonesia&aqs=chrome..69i57j0l5.1810j0j7&sourceid=chrome&ie=UTF-8
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	how far would the dollar go in indonesia	https://www.google.com/search?q=how+far+would+the+dollar+go+in+indonesia&rlz=1C1CHBF_enUS790US790&oq=how+far+would+the+dollar+go+in+indonesia&aqs=chrome..69i57j0.6511j1j7&sourceid=chrome&ie=UTF-8
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	where the dollar goes farthest vietnam or indonesia	https://www.google.com/search?q=where+the+dollar+goes+farthest+vietnam+or+indonesia&rlz=1C1CHBF_enUS790US790&oq=where+the+dollar+goes+farthest+vietnam+or+indonesia&aqs=chrome..69i57.12225j1j7&sourceid=chrome&ie=UTF-8
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	flights to indonesia	https://www.google.com/search?q=flights+to+indonesia&rlz=1C1CHBF_enUS790US790&oq=flights+to+indonesia&aqs=chrome..69i57j0l5.4068j0j7&sourceid=chrome&ie=UTF-8
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	flights to bali, indonesia	https://www.google.com/search?rlz=1C1CHBF_enUS790US790&ei=FOe_Wu_uEMPgjwPFq6H4Cw&q=flights+to+bali%2C+indonesia&oq=flights+to+bali%2C+indonesia&gs_l=psy-ab.3..0l7j0i22i30k1l3.25441.30035.0.30191.24.22.0.0.0.0.310.2742.0j14j2j1.17.0....0...1.1.64.psy-ab..7.17.2737...0i67k1j35i39k1j0i10k1j0i20i263k1.0.vEgtqBSKssM

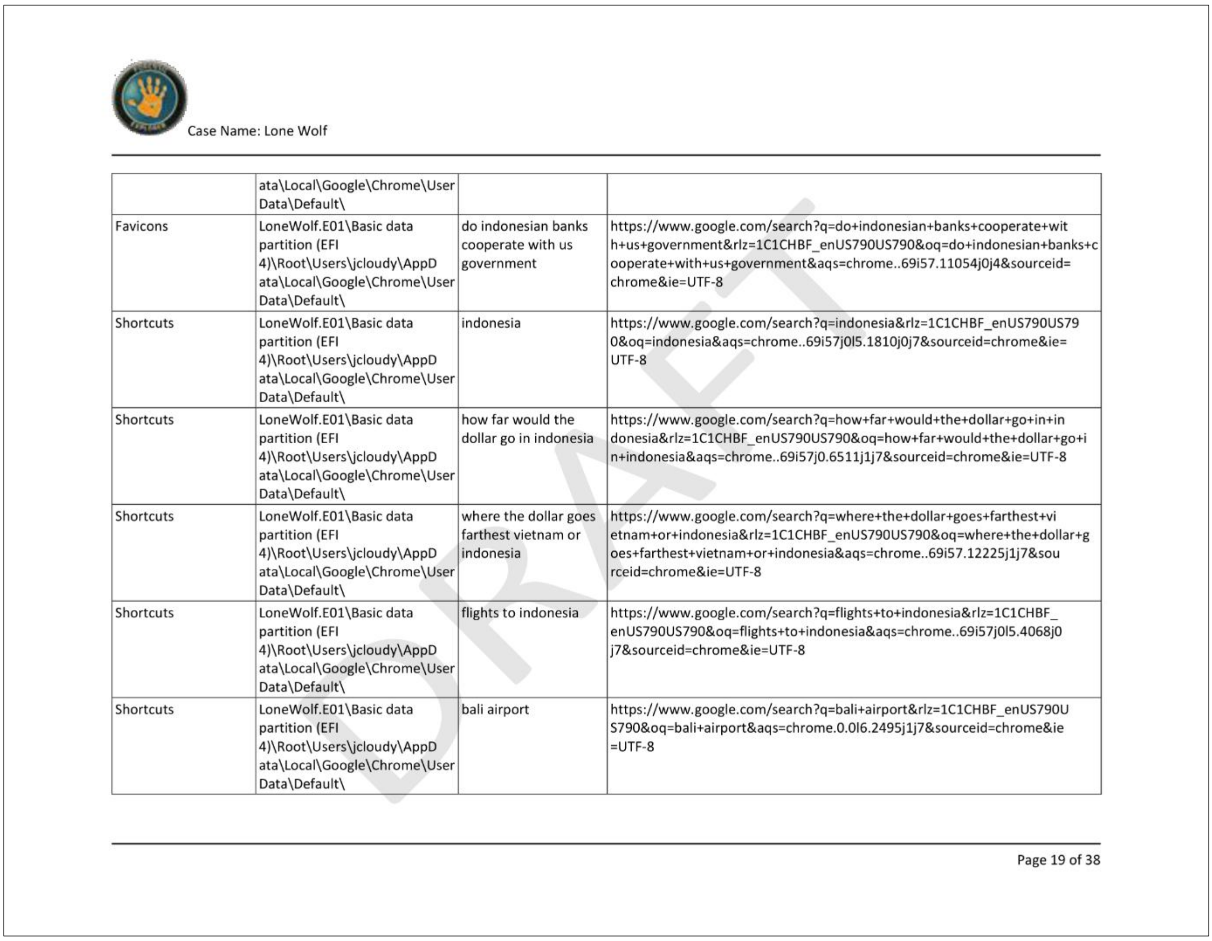
Page 17 of 38



Case Name: Lone Wolf

Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	flights to bali, indonesia	https://www.google.com/search?rlz=1C1CHBF_enUS790US790&ei=FOe_Wu_uEMPgjwPFq6H4Cw&q=flights+to+bali%2C+indonesia&oq=flights+to+bali%2C+indonesia&gs_l=psy-ab.3..0l7j0i22i30k1l3.25441.30035.0.30191.24.22.0.0.0.0.310.2742.0j14j2j1.17.0....0...1.1.64.psy-ab..7.17.2737...0i67k1j35i39k1j0i10k1j0i20i263k1.0.vEgtqBSKssM
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	bali airport	https://www.google.com/search?q=bali+airport&rlz=1C1CHBF_enUS790US790&oq=bali+airport&aqs=chrome.0.0l6.2495j1j7&sourceid=chrome&ie=UTF-8
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	hotels in bali	https://www.google.com/search?q=hotels+in+bali&rlz=1C1CHBF_enUS790US790&oq=hotels+in+bali&aqs=chrome..69i57j0l5.2445j0j7&sourceid=chrome&ie=UTF-8
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	dulles to bali	https://www.google.com/search?q=dulles+to+bali&rlz=1C1CHBF_enUS790US790&oq=dulles+to+bali&aqs=chrome..69i57j0l2.5728j1j4&sourceid=chrome&ie=UTF-8
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	gun control in indonesia	https://www.google.com/search?q=gun+control+in+indonesia&rlz=1C1CHBF_enUS790US790&oq=gun+control+in+indonesia&aqs=chrome..69i57.4917j0j7&sourceid=chrome&ie=UTF-8
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	things to do in bali	https://www.google.com/search?q=things+to+do+in+bali&rlz=1C1CHBF_enUS790US790&oq=things+to+do+in+bali&aqs=chrome..69i57j0l5.2978j1j9&sourceid=chrome&ie=UTF-8
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppD	indonesia expat jobs	https://www.google.com/search?q=indonesia+expat+jobs&rlz=1C1CHBF_enUS790US790&oq=indonesia+expat+jobs&aqs=chrome.0.0j69i57.6193j0j7&sourceid=chrome&ie=UTF-8

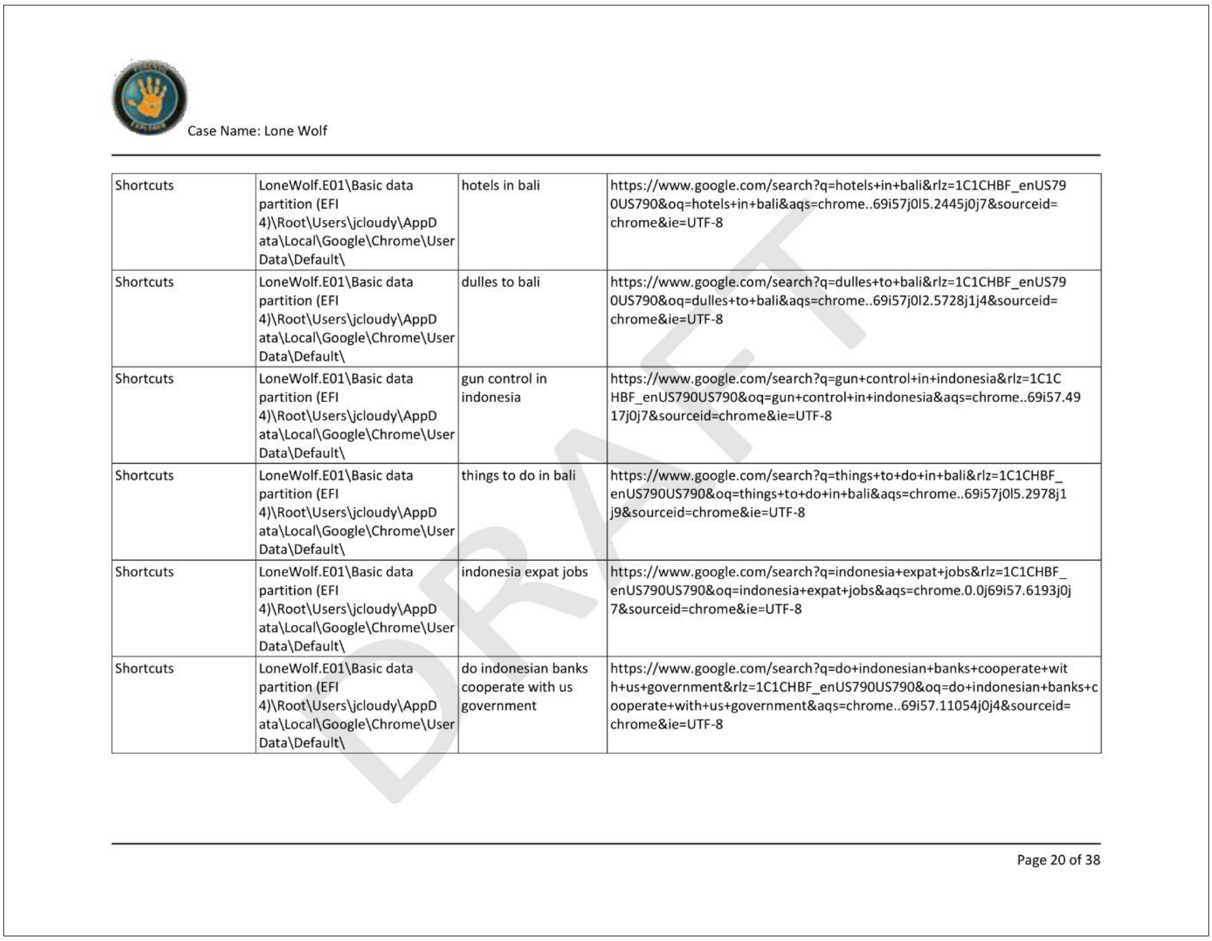
Page 18 of 38



Case Name: Lone Wolf

	ata\Local\Google\Chrome\User Data\Default\		
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	do indonesian banks cooperate with us government	https://www.google.com/search?q=do+indonesian+banks+cooperate+with+us+government&rlz=1C1CHBF_enUS790US790&oq=do+indonesian+banks+cooperate+with+us+government&aqs=chrome..69i57.11054j0j4&sourceid=chrome&ie=UTF-8
Shortcuts	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	indonesia	https://www.google.com/search?q=indonesia&rlz=1C1CHBF_enUS790US790&oq=indonesia&aqs=chrome..69i57j0l5.1810j0j7&sourceid=chrome&ie=UTF-8
Shortcuts	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	how far would the dollar go in indonesia	https://www.google.com/search?q=how+far+would+the+dollar+go+in+indonesia&rlz=1C1CHBF_enUS790US790&oq=how+far+would+the+dollar+go+in+indonesia&aqs=chrome..69i57j0.6511j1j7&sourceid=chrome&ie=UTF-8
Shortcuts	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	where the dollar goes farthest vietnam or indonesia	https://www.google.com/search?q=where+the+dollar+goes+farthest+vietnam+or+indonesia&rlz=1C1CHBF_enUS790US790&oq=where+the+dollar+goes+farthest+vietnam+or+indonesia&aqs=chrome..69i57.12225j1j7&sourceid=chrome&ie=UTF-8
Shortcuts	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	flights to indonesia	https://www.google.com/search?q=flights+to+indonesia&rlz=1C1CHBF_enUS790US790&oq=flights+to+indonesia&aqs=chrome..69i57j0l5.4068j0j7&sourceid=chrome&ie=UTF-8
Shortcuts	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	bali airport	https://www.google.com/search?q=bali+airport&rlz=1C1CHBF_enUS790US790&oq=bali+airport&aqs=chrome.0.0l6.2495j1j7&sourceid=chrome&ie=UTF-8

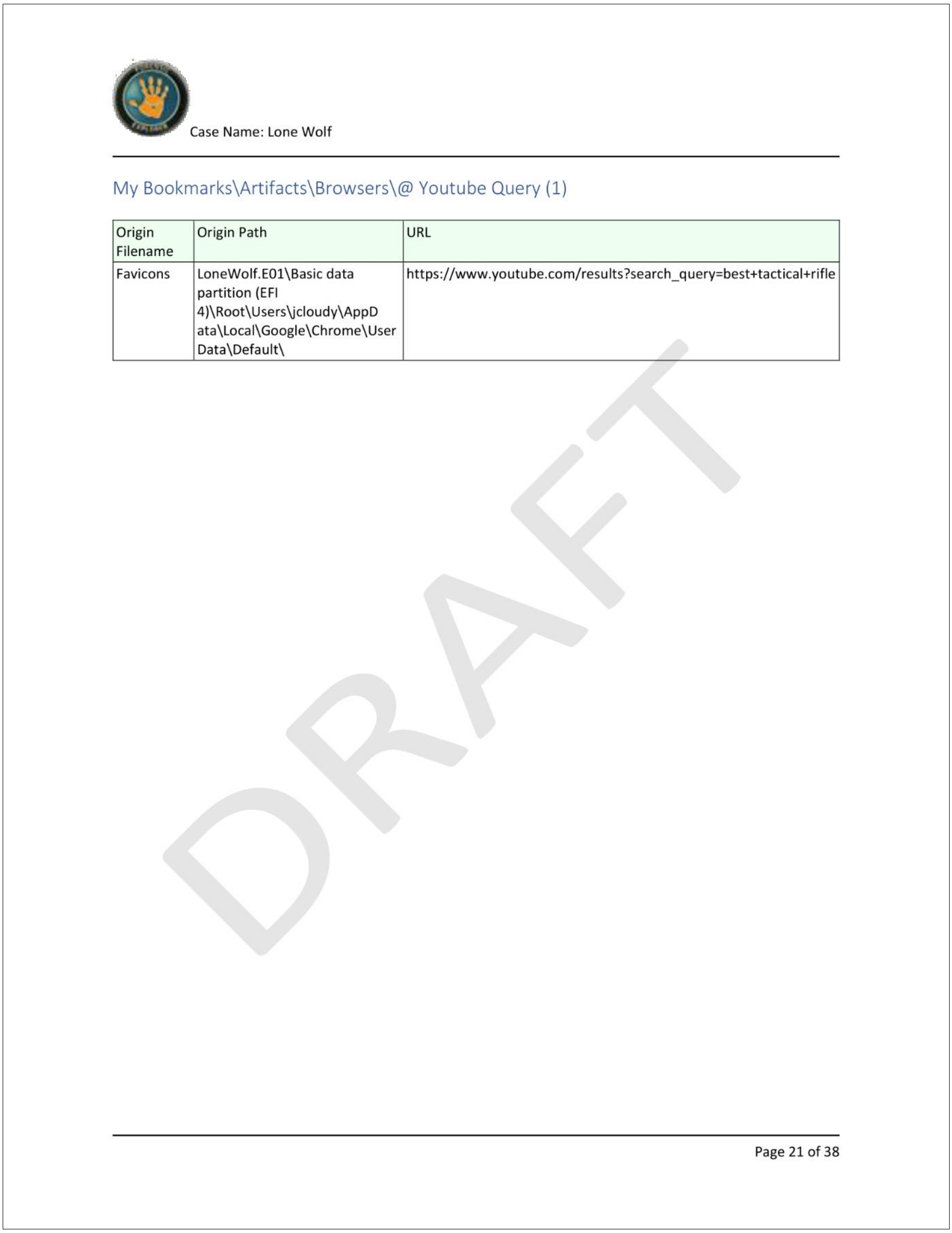
Page 19 of 38



Case Name: Lone Wolf

Shortcuts	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	hotels in bali	https://www.google.com/search?q=hotels+in+bali&rlz=1C1CHBF_enUS790US790&oq=hotels+in+bali&aqs=chrome..69i57j0l5.2445j0j7&sourceid=chrome&ie=UTF-8
Shortcuts	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	dulles to bali	https://www.google.com/search?q=dulles+to+bali&rlz=1C1CHBF_enUS790US790&oq=dulles+to+bali&aqs=chrome..69i57j0l2.5728j1j4&sourceid=chrome&ie=UTF-8
Shortcuts	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	gun control in indonesia	https://www.google.com/search?q=gun+control+in+indonesia&rlz=1C1CHBF_enUS790US790&oq=gun+control+in+indonesia&aqs=chrome..69i57.4917j0j7&sourceid=chrome&ie=UTF-8
Shortcuts	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	things to do in bali	https://www.google.com/search?q=things+to+do+in+bali&rlz=1C1CHBF_enUS790US790&oq=things+to+do+in+bali&aqs=chrome..69i57j0l5.2978j1j9&sourceid=chrome&ie=UTF-8
Shortcuts	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	indonesia expat jobs	https://www.google.com/search?q=indonesia+expat+jobs&rlz=1C1CHBF_enUS790US790&oq=indonesia+expat+jobs&aqs=chrome.0.0j69i57.6193j0j7&sourceid=chrome&ie=UTF-8
Shortcuts	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	do indonesian banks cooperate with us government	https://www.google.com/search?q=do+indonesian+banks+cooperate+with+us+government&rlz=1C1CHBF_enUS790US790&oq=do+indonesian+banks+cooperate+with+us+government&aqs=chrome..69i57.11054j0j4&sourceid=chrome&ie=UTF-8

Page 20 of 38

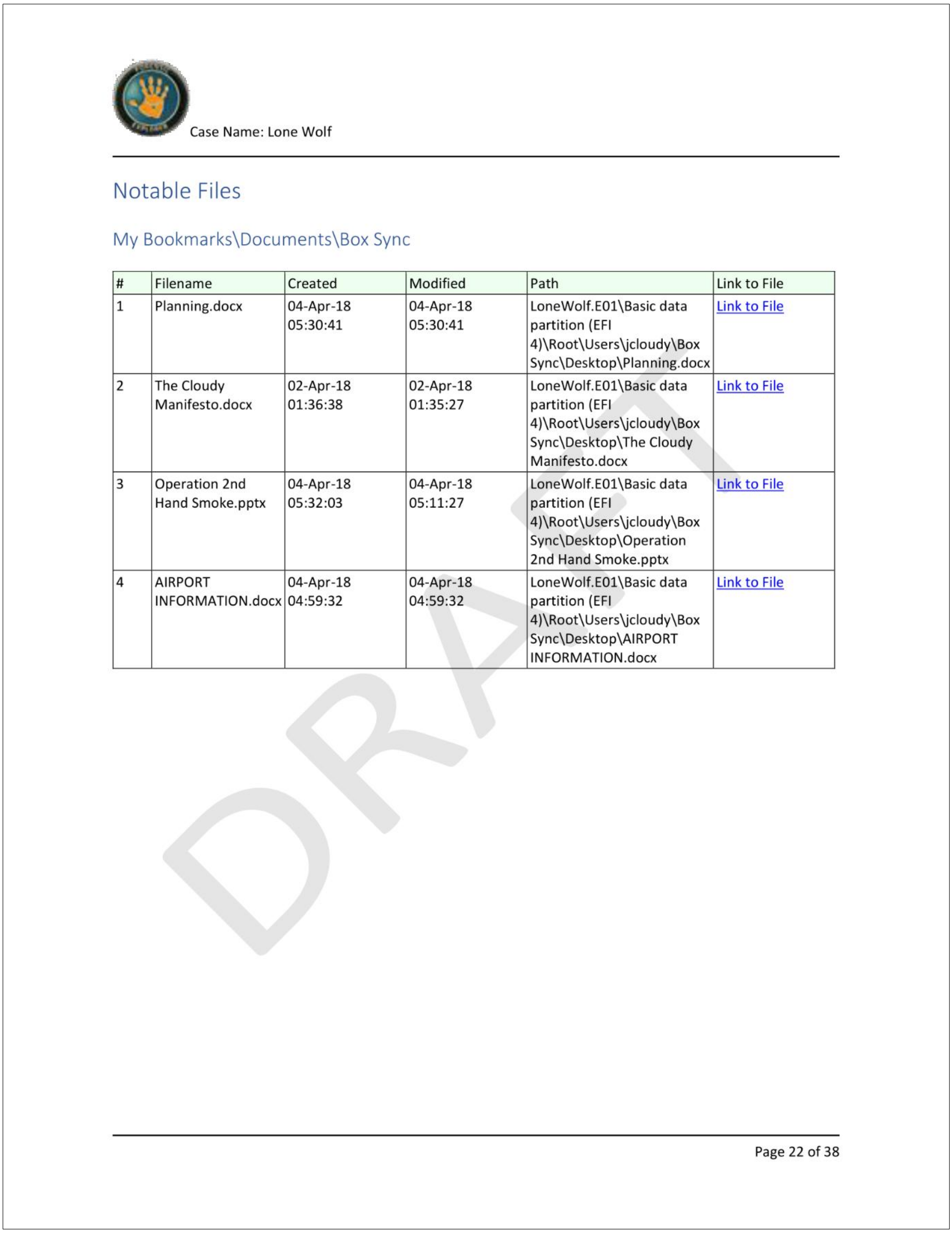


Case Name: Lone Wolf

My Bookmarks\Artifacts\Browsers\@ Youtube Query (1)

Origin Filename	Origin Path	URL
Favicons	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\	https://www.youtube.com/results?search_query=best+tactical+rifle

Page 21 of 38



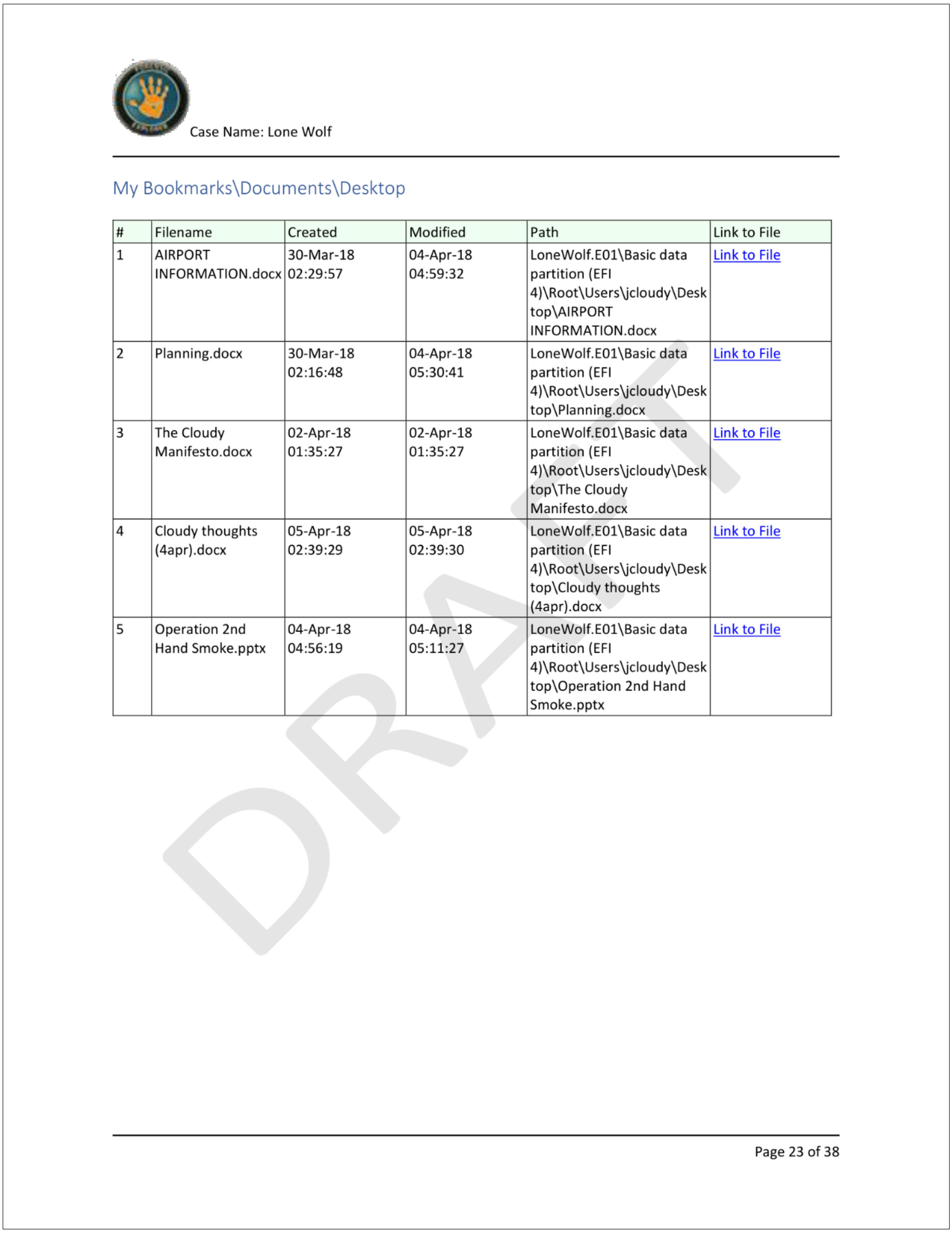
Case Name: Lone Wolf

Notable Files

My Bookmarks\Documents\Box Sync

#	Filename	Created	Modified	Path	Link to File
1	Planning.docx	04-Apr-18 05:30:41	04-Apr-18 05:30:41	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Box Sync\Desktop\Planning.docx	Link to File
2	The Cloudy Manifesto.docx	02-Apr-18 01:36:38	02-Apr-18 01:35:27	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Box Sync\Desktop\The Cloudy Manifesto.docx	Link to File
3	Operation 2nd Hand Smoke.pptx	04-Apr-18 05:32:03	04-Apr-18 05:11:27	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Box Sync\Desktop\Operation 2nd Hand Smoke.pptx	Link to File
4	AIRPORT INFORMATION.docx	04-Apr-18 04:59:32	04-Apr-18 04:59:32	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Box Sync\Desktop\AIRPORT INFORMATION.docx	Link to File

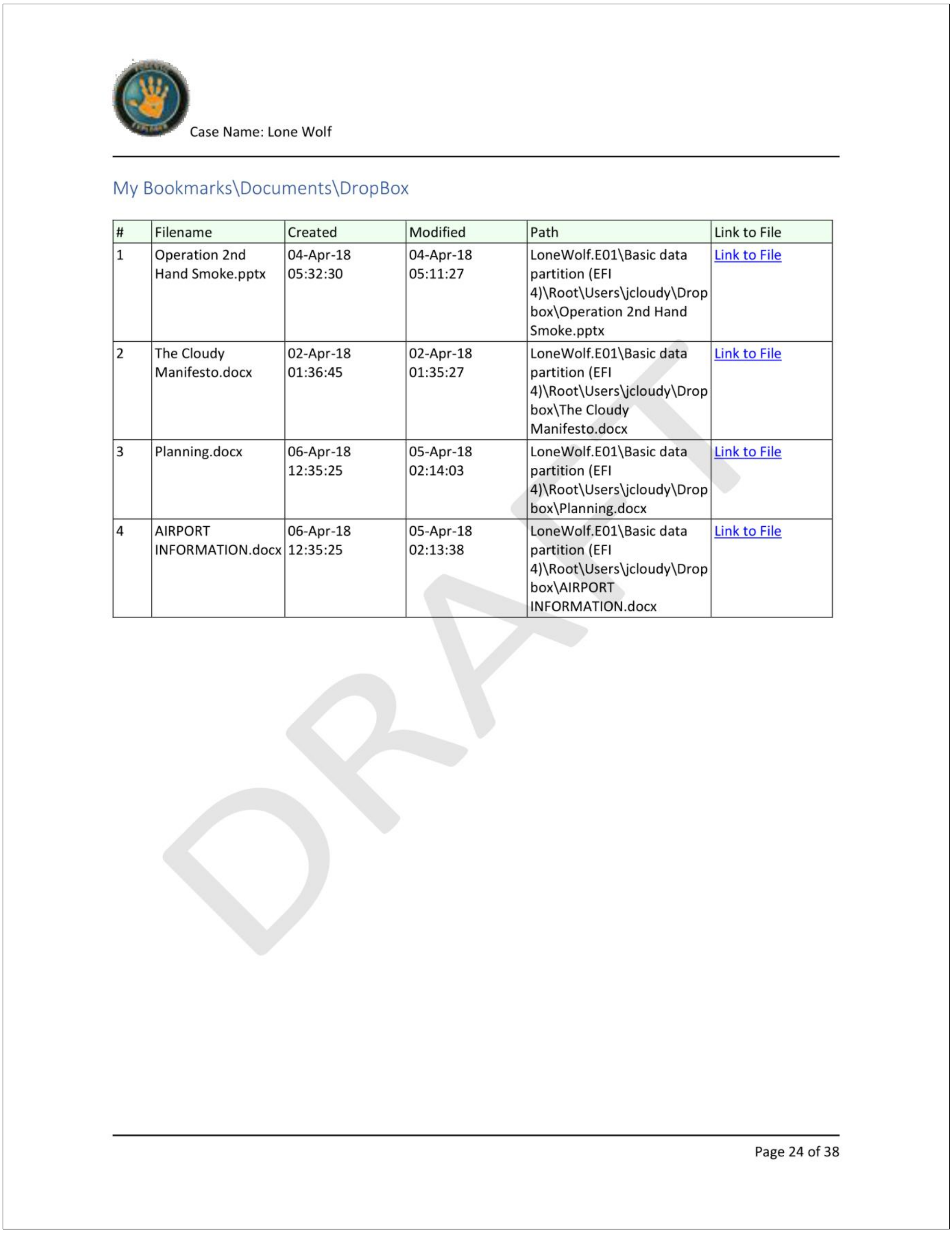
Page 22 of 38



Case Name: Lone Wolf

My Bookmarks\Documents\Desktop

#	Filename	Created	Modified	Path	Link to File
1	AIRPORT INFORMATION.docx	30-Mar-18 02:29:57	04-Apr-18 04:59:32	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Desktop\AIRPORT INFORMATION.docx	Link to File
2	Planning.docx	30-Mar-18 02:16:48	04-Apr-18 05:30:41	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Desktop\Planning.docx	Link to File
3	The Cloudy Manifesto.docx	02-Apr-18 01:35:27	02-Apr-18 01:35:27	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Desktop\The Cloudy Manifesto.docx	Link to File
4	Cloudy thoughts (4apr).docx	05-Apr-18 02:39:29	05-Apr-18 02:39:30	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Desktop\Cloudy thoughts (4apr).docx	Link to File
5	Operation 2nd Hand Smoke.pptx	04-Apr-18 04:56:19	04-Apr-18 05:11:27	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Desktop\Operation 2nd Hand Smoke.pptx	Link to File

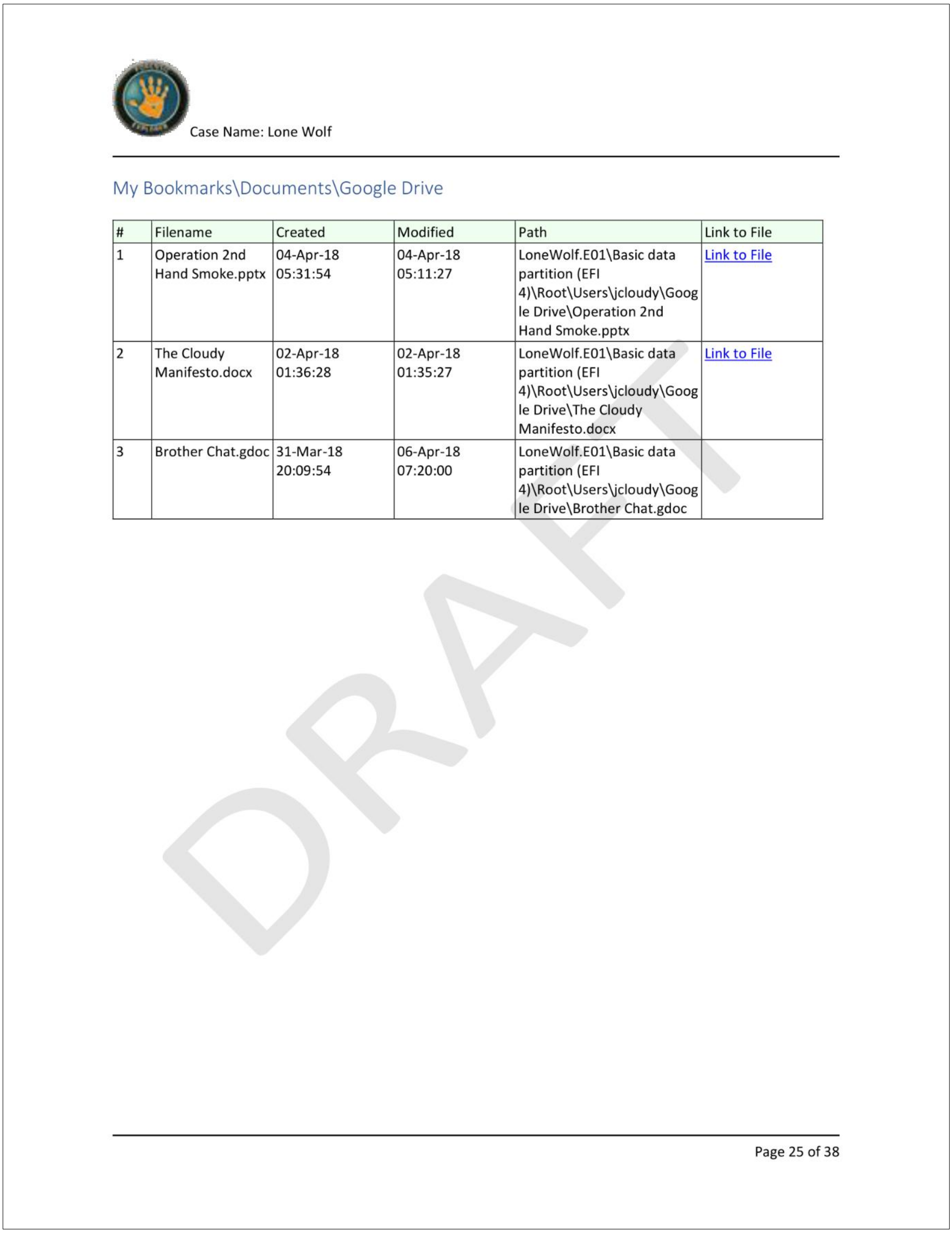


Case Name: Lone Wolf

My Bookmarks\Documents\DropBox

#	Filename	Created	Modified	Path	Link to File
1	Operation 2nd Hand Smoke.pptx	04-Apr-18 05:32:30	04-Apr-18 05:11:27	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Dropbox\Operation 2nd Hand Smoke.pptx	Link to File
2	The Cloudy Manifesto.docx	02-Apr-18 01:36:45	02-Apr-18 01:35:27	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Dropbox\The Cloudy Manifesto.docx	Link to File
3	Planning.docx	06-Apr-18 12:35:25	05-Apr-18 02:14:03	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Dropbox\Planning.docx	Link to File
4	AIRPORT INFORMATION.docx	06-Apr-18 12:35:25	05-Apr-18 02:13:38	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Dropbox\AIRPORT INFORMATION.docx	Link to File

Page 24 of 38

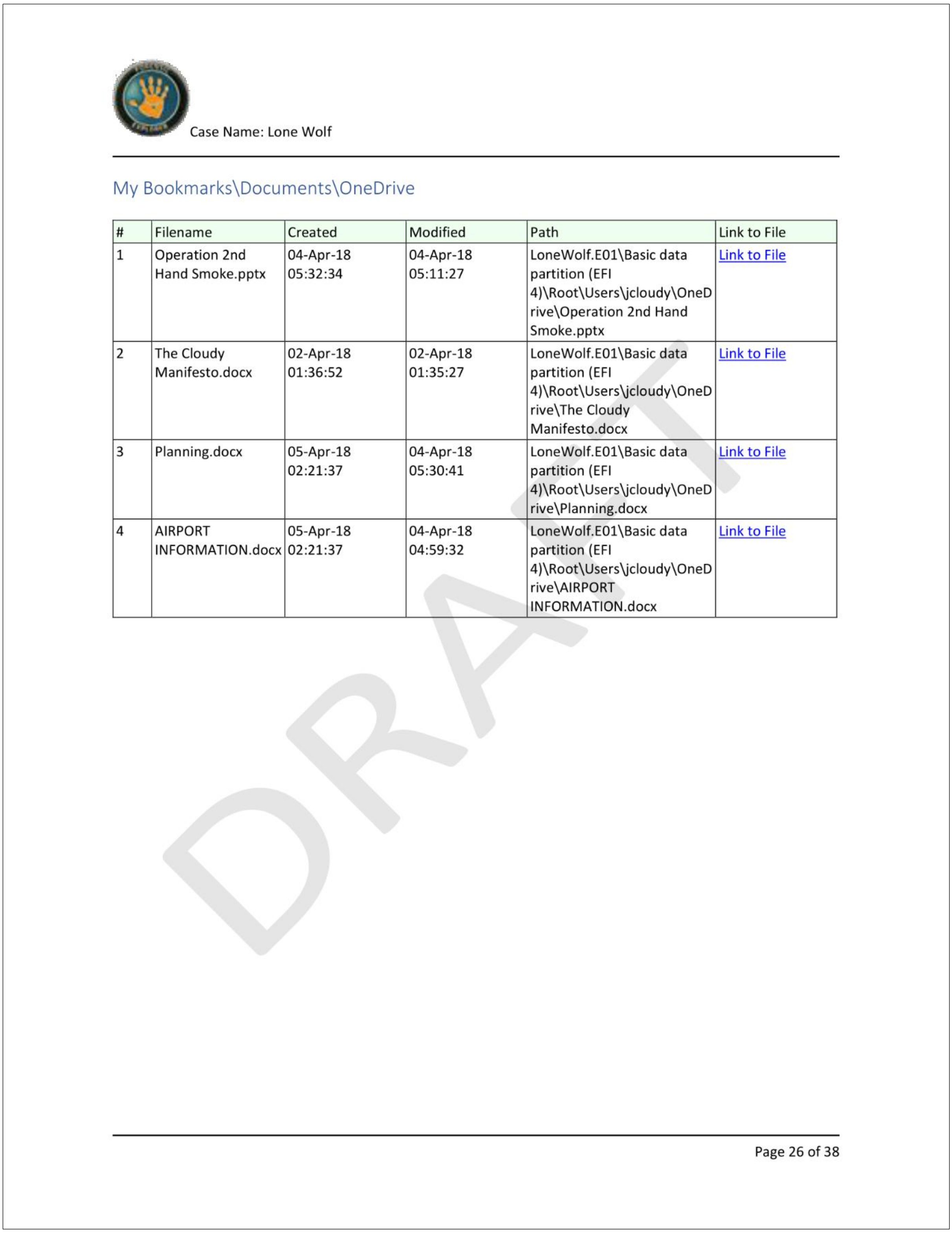


Case Name: Lone Wolf

My Bookmarks\Documents\Google Drive

#	Filename	Created	Modified	Path	Link to File
1	Operation 2nd Hand Smoke.pptx	04-Apr-18 05:31:54	04-Apr-18 05:11:27	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Google Drive\Operation 2nd Hand Smoke.pptx	Link to File
2	The Cloudy Manifesto.docx	02-Apr-18 01:36:28	02-Apr-18 01:35:27	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Google Drive\The Cloudy Manifesto.docx	Link to File
3	Brother Chat.gdoc	31-Mar-18 20:09:54	06-Apr-18 07:20:00	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\Google Drive\Brother Chat.gdoc	

Page 25 of 38



Case Name: Lone Wolf

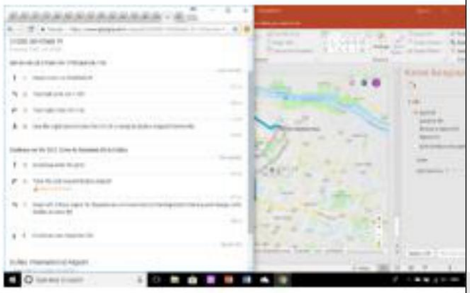
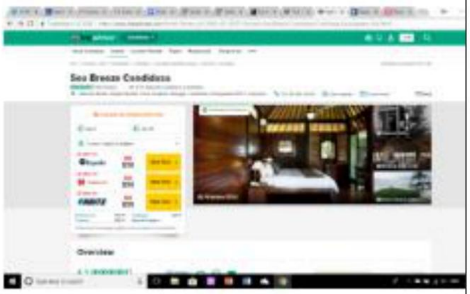
My Bookmarks\Documents\OneDrive

#	Filename	Created	Modified	Path	Link to File
1	Operation 2nd Hand Smoke.pptx	04-Apr-18 05:32:34	04-Apr-18 05:11:27	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\Operation 2nd Hand Smoke.pptx	Link to File
2	The Cloudy Manifesto.docx	02-Apr-18 01:36:52	02-Apr-18 01:35:27	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\The Cloudy Manifesto.docx	Link to File
3	Planning.docx	05-Apr-18 02:21:37	04-Apr-18 05:30:41	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\Planning.docx	Link to File
4	AIRPORT INFORMATION.docx	05-Apr-18 02:21:37	04-Apr-18 04:59:32	LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\AIRPORT INFORMATION.docx	Link to File

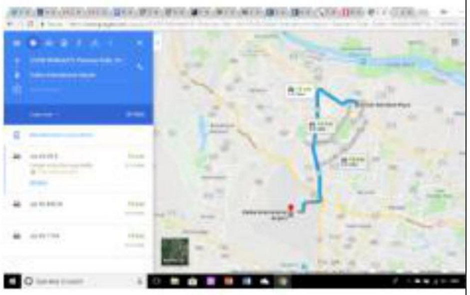
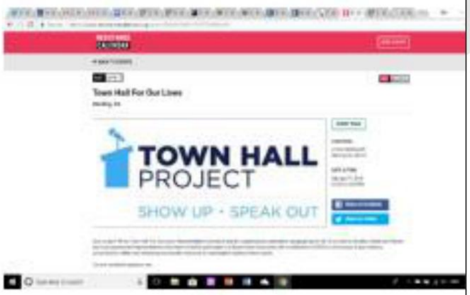
Page 26 of 38

Gallery

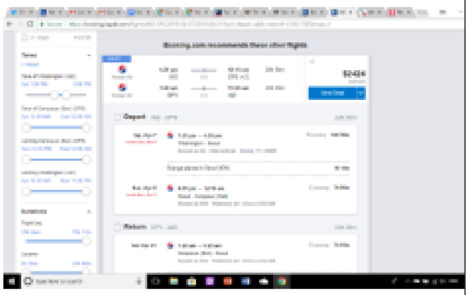
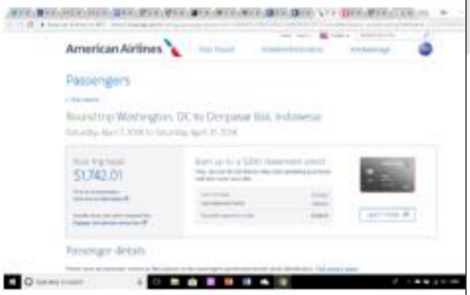
My Bookmarks\Pictures\OneDrive

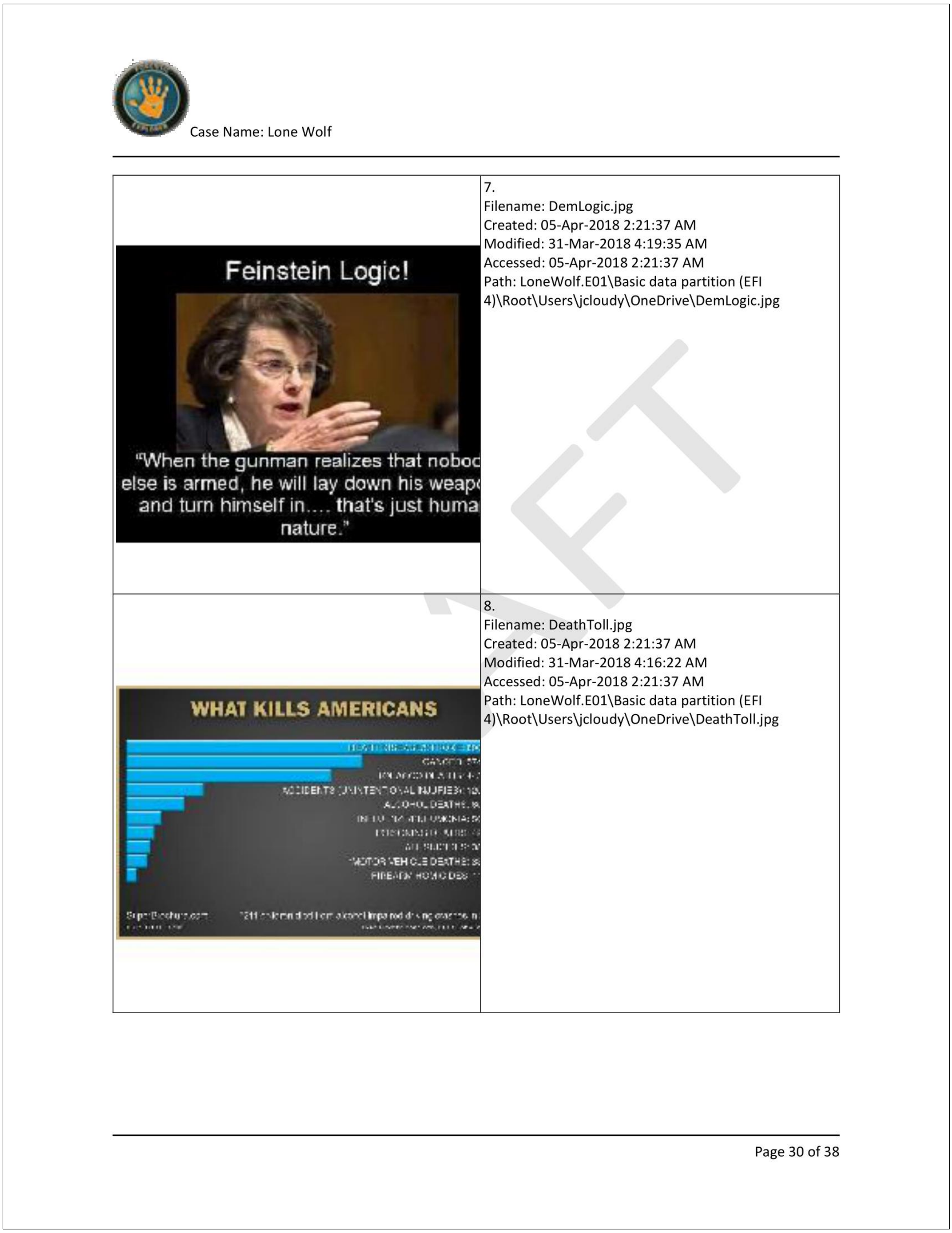
	1. Filename: 2018-04-04 (1).png Created: 04-Apr-2018 4:51:05 AM Modified: 04-Apr-2018 4:51:05 AM Accessed: 04-Apr-2018 4:51:05 AM Path: LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\Pictures\Screenshots\2018-04-04 (1).png
	2. Filename: 2018-04-04 (4).png Created: 04-Apr-2018 5:08:44 AM Modified: 04-Apr-2018 5:08:44 AM Accessed: 04-Apr-2018 5:08:44 AM Path: LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\Pictures\Screenshots\2018-04-04 (4).png

Case Name: Lone Wolf

	3. Filename: 2018-04-03 (1).png Created: 03-Apr-2018 6:39:37 AM Modified: 03-Apr-2018 6:39:37 AM Accessed: 03-Apr-2018 6:39:37 AM Path: LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\Pictures\Screenshots\2018-04-03 (1).png
 Town Hall For Our Lives TOWN HALL PROJECT SHOW UP · SPEAK OUT	4. Filename: 2018-04-03 (2).png Created: 03-Apr-2018 6:40:34 AM Modified: 03-Apr-2018 6:40:34 AM Accessed: 03-Apr-2018 6:40:34 AM Path: LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\Pictures\Screenshots\2018-04-03 (2).png

Case Name: Lone Wolf

 Booking.com recommends these other flights Depart Return	5. Filename: 2018-04-04 (3).png Created: 04-Apr-2018 5:05:33 AM Modified: 04-Apr-2018 5:05:33 AM Accessed: 04-Apr-2018 5:05:33 AM Path: LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\Pictures\Screenshots\2018-04-04 (3).png
 American Airlines Passengers Roundtrip Washington, DC to Denpasar Bali, Indonesia Your trip total $1,742.01 Passenger details	6. Filename: 2018-04-03.png Created: 03-Apr-2018 6:37:42 AM Modified: 03-Apr-2018 6:37:42 AM Accessed: 03-Apr-2018 6:37:42 AM Path: LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\Pictures\Screenshots\2018-04-03.png

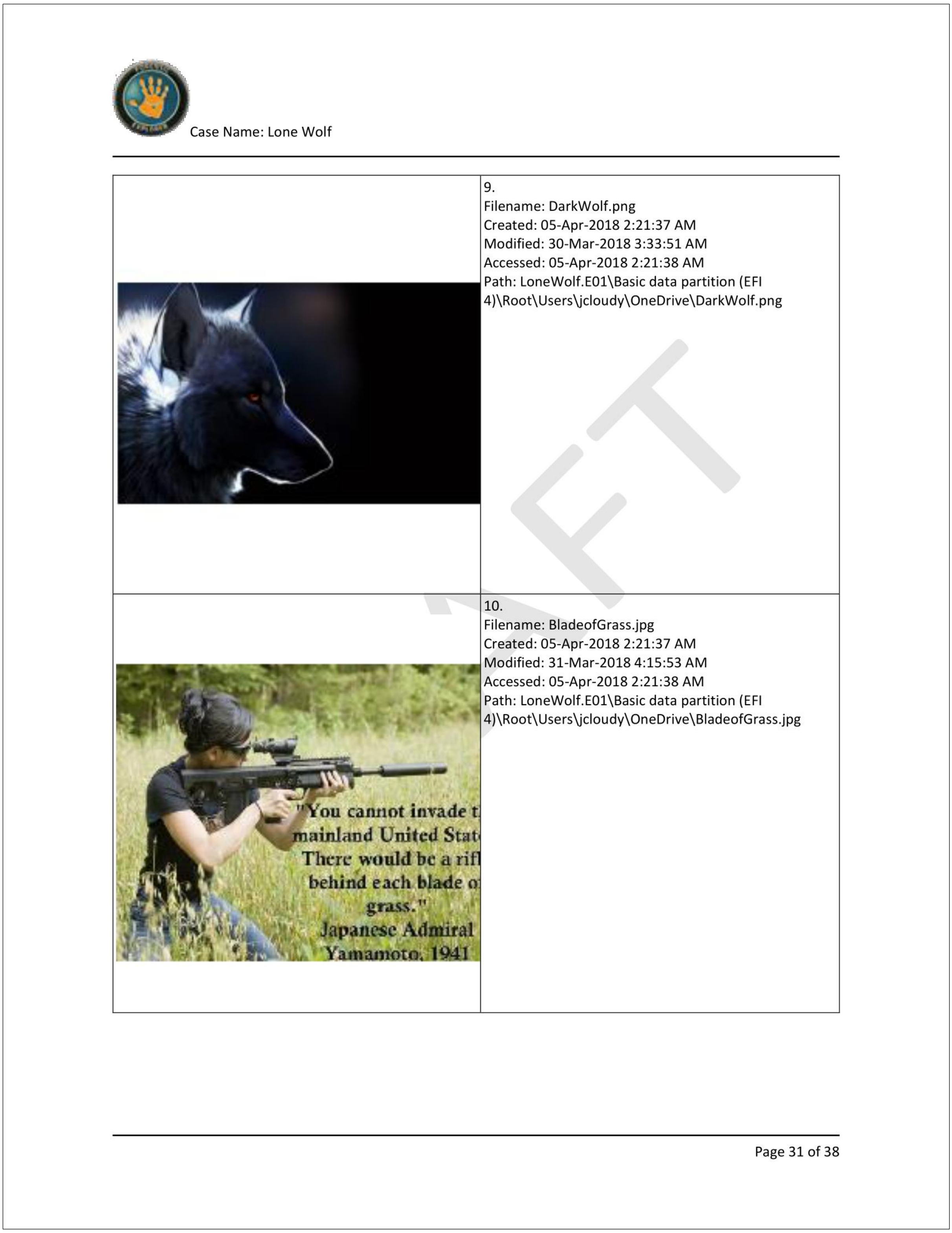


Case Name: Lone Wolf

	7. Filename: DemLogic.jpg Created: 05-Apr-2018 2:21:37 AM Modified: 31-Mar-2018 4:19:35 AM Accessed: 05-Apr-2018 2:21:37 AM Path: LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\DemLogic.jpg
	8. Filename: DeathToll.jpg Created: 05-Apr-2018 2:21:37 AM Modified: 31-Mar-2018 4:16:22 AM Accessed: 05-Apr-2018 2:21:37 AM Path: LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\DeathToll.jpg

Feinstein Logic!
"When the gunman realizes that nobod
else is armed, he will lay down his weap
and turn himself in.... that's just huma
nature."
WHAT KILLS AMERICANS
CANCER
ACCIDENTS (UNINTENTIONAL INJURIES)
ALCOHOL DEATHS
MOTOR VEHICLE DEATHS
FIREARM HOMICIDES

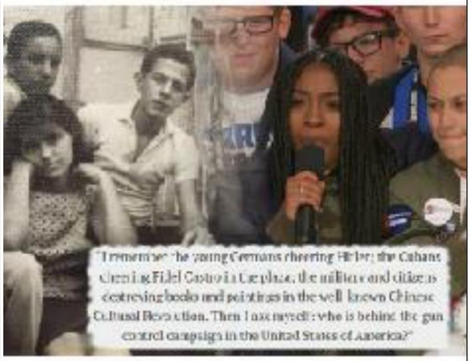
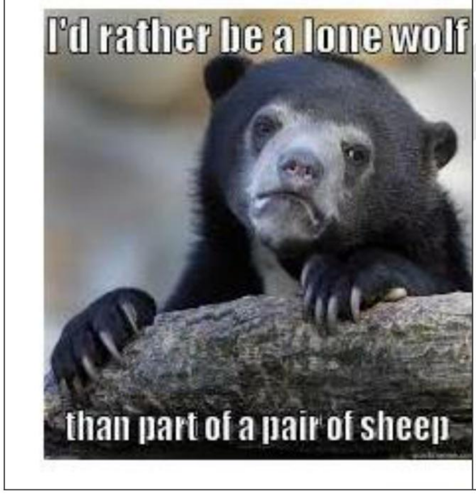
Page 30 of 38



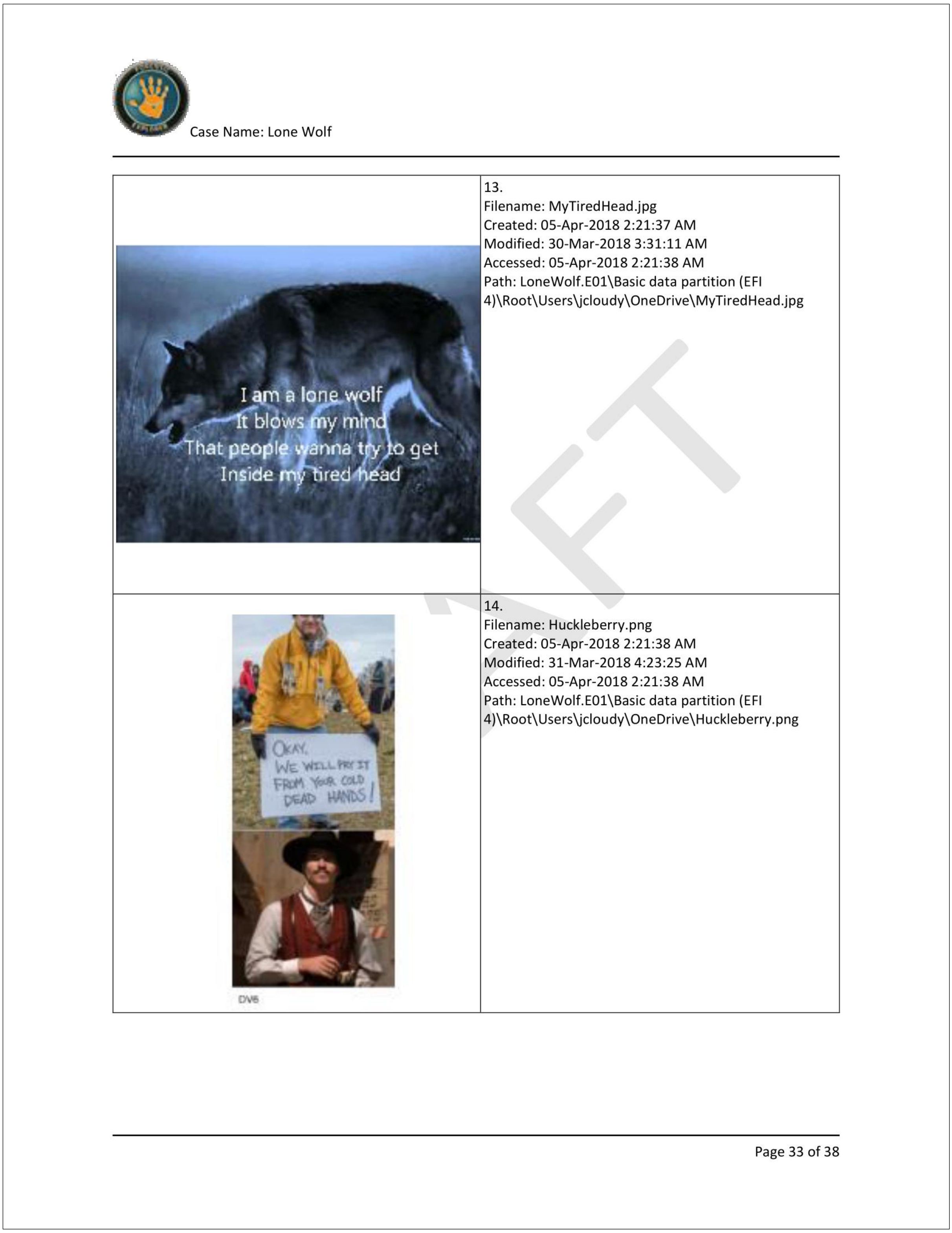
Case Name: Lone Wolf

	9. Filename: DarkWolf.png Created: 05-Apr-2018 2:21:37 AM Modified: 30-Mar-2018 3:33:51 AM Accessed: 05-Apr-2018 2:21:38 AM Path: LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\DarkWolf.png
	10. Filename: BladeofGrass.jpg Created: 05-Apr-2018 2:21:37 AM Modified: 31-Mar-2018 4:15:53 AM Accessed: 05-Apr-2018 2:21:38 AM Path: LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\BladeofGrass.jpg

Case Name: Lone Wolf

 "I remember the young Germans cheering Hitler; the Cubans cheering Fidel Castro in the plaza, the military and citizens destroying books and paintings in the well known Chinese Cultural Revolution. Then I ask myself: who is behind the gun control campaign in the United States of America?"	11. Filename: CubaDearmed.jpg Created: 05-Apr-2018 2:21:37 AM Modified: 30-Mar-2018 9:22:56 PM Accessed: 05-Apr-2018 2:21:38 AM Path: LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\CubaDearmed.jpg
	12. Filename: Sheep.jpg Created: 05-Apr-2018 2:21:37 AM Modified: 30-Mar-2018 3:32:40 AM Accessed: 05-Apr-2018 2:21:38 AM Path: LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\Sheep.jpg

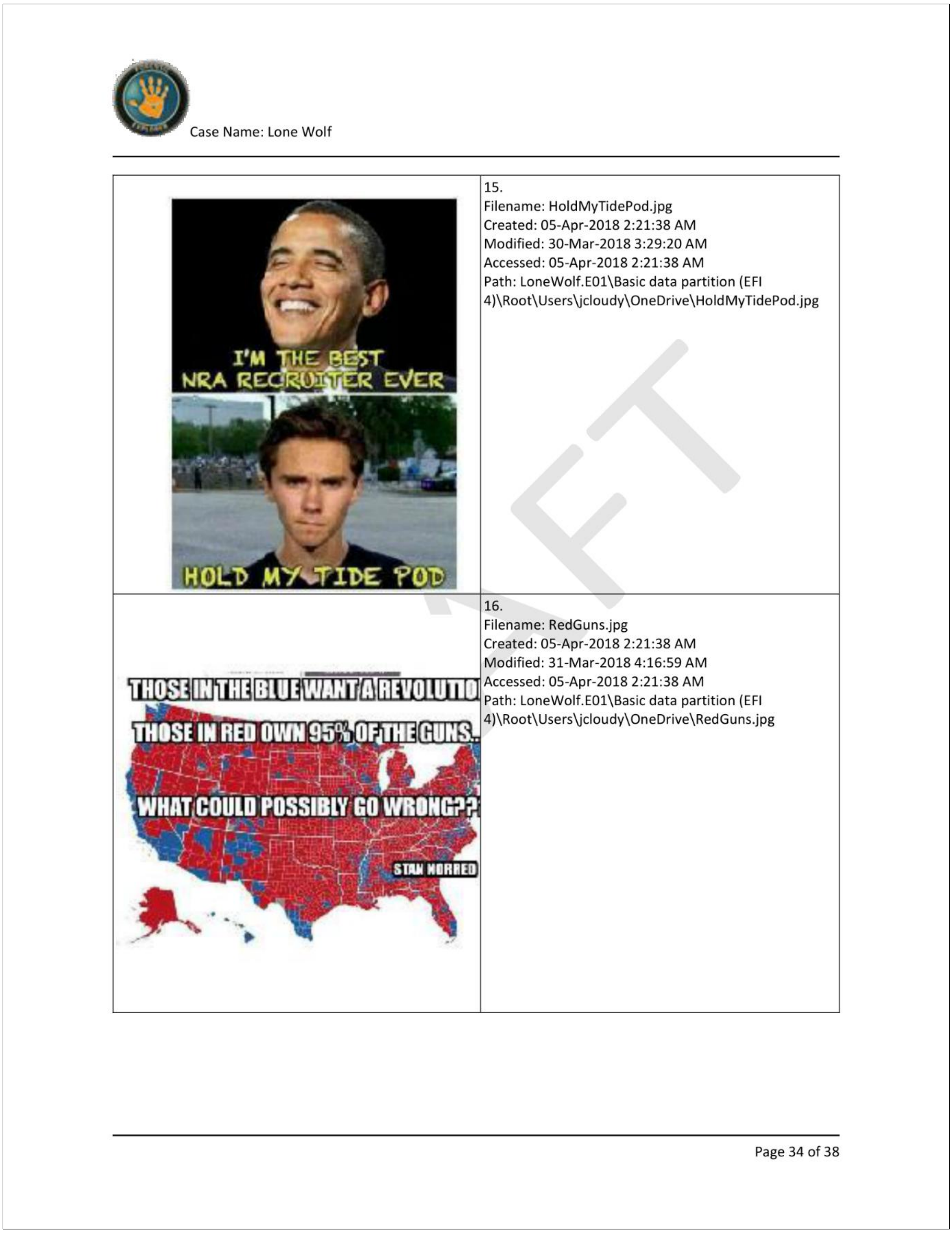
Page 32 of 38



Case Name: Lone Wolf

	13. Filename: MyTiredHead.jpg Created: 05-Apr-2018 2:21:37 AM Modified: 30-Mar-2018 3:31:11 AM Accessed: 05-Apr-2018 2:21:38 AM Path: LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\MyTiredHead.jpg
	14. Filename: Huckleberry.png Created: 05-Apr-2018 2:21:38 AM Modified: 31-Mar-2018 4:23:25 AM Accessed: 05-Apr-2018 2:21:38 AM Path: LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\Huckleberry.png

Page 33 of 38



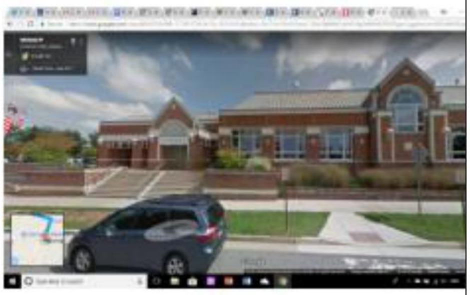
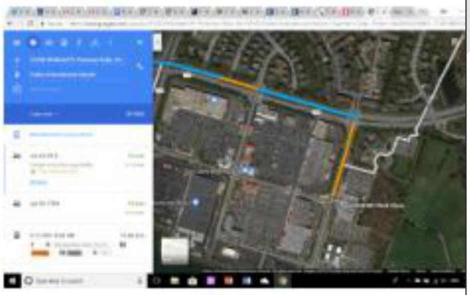
Case Name: Lone Wolf

HoldMyTidePod.jpg	15. Filename: HoldMyTidePod.jpg Created: 05-Apr-2018 2:21:38 AM Modified: 30-Mar-2018 3:29:20 AM Accessed: 05-Apr-2018 2:21:38 AM Path: LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\HoldMyTidePod.jpg
RedGuns.jpg	16. Filename: RedGuns.jpg Created: 05-Apr-2018 2:21:38 AM Modified: 31-Mar-2018 4:16:59 AM Accessed: 05-Apr-2018 2:21:38 AM Path: LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\RedGuns.jpg

I'M THE BEST
NRA RECRUITER EVER
HOLD MY TIDE POD
THOSE IN THE BLUE WANT A REVOLUTIO
THOSE IN RED OWN 95% OF THE GUNS..
WHAT COULD POSSIBLY GO WRONG??
STAN NORRED

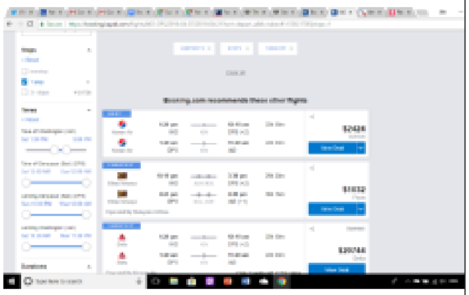
Page 34 of 38

Case Name: Lone Wolf

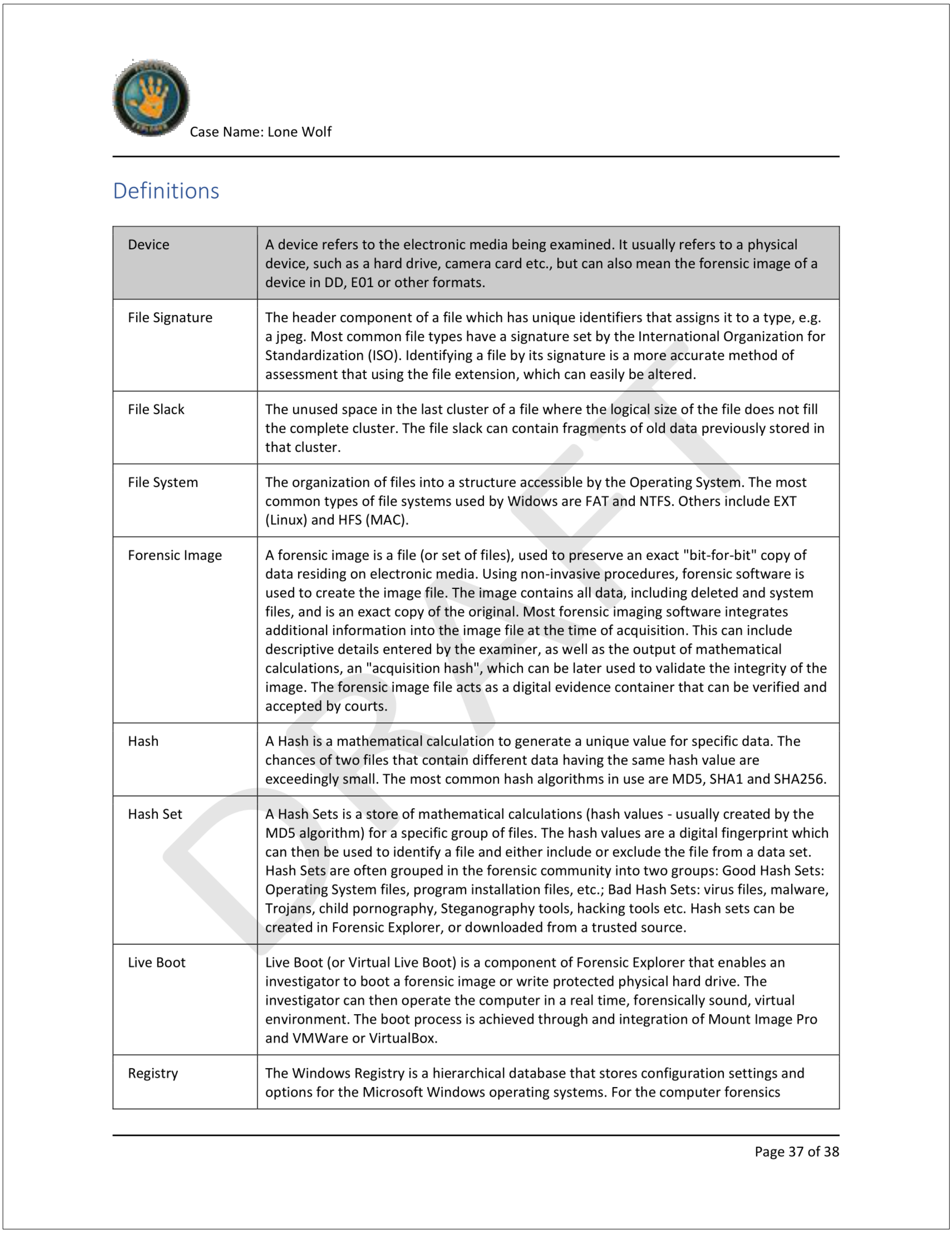
	17. Filename: 2018-04-03 (3).png Created: 03-Apr-2018 6:43:24 AM Modified: 03-Apr-2018 6:43:24 AM Accessed: 03-Apr-2018 6:43:24 AM Path: LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\Pictures\Screenshots\2018-04-03 (3).png
	18. Filename: 2018-04-04.png Created: 04-Apr-2018 4:35:29 AM Modified: 04-Apr-2018 4:35:29 AM Accessed: 04-Apr-2018 4:35:29 AM Path: LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\Pictures\Screenshots\2018-04-04.png

Page 35 of 38

Case Name: Lone Wolf



19.
Filename: 2018-04-04 (2).png
Created: 04-Apr-2018 5:05:08 AM
Modified: 04-Apr-2018 5:05:08 AM
Accessed: 04-Apr-2018 5:05:08 AM
Path: LoneWolf.E01\Basic data partition (EFI 4)\Root\Users\jcloudy\OneDrive\Pictures\Screenshots\2018-04-04 (2).png

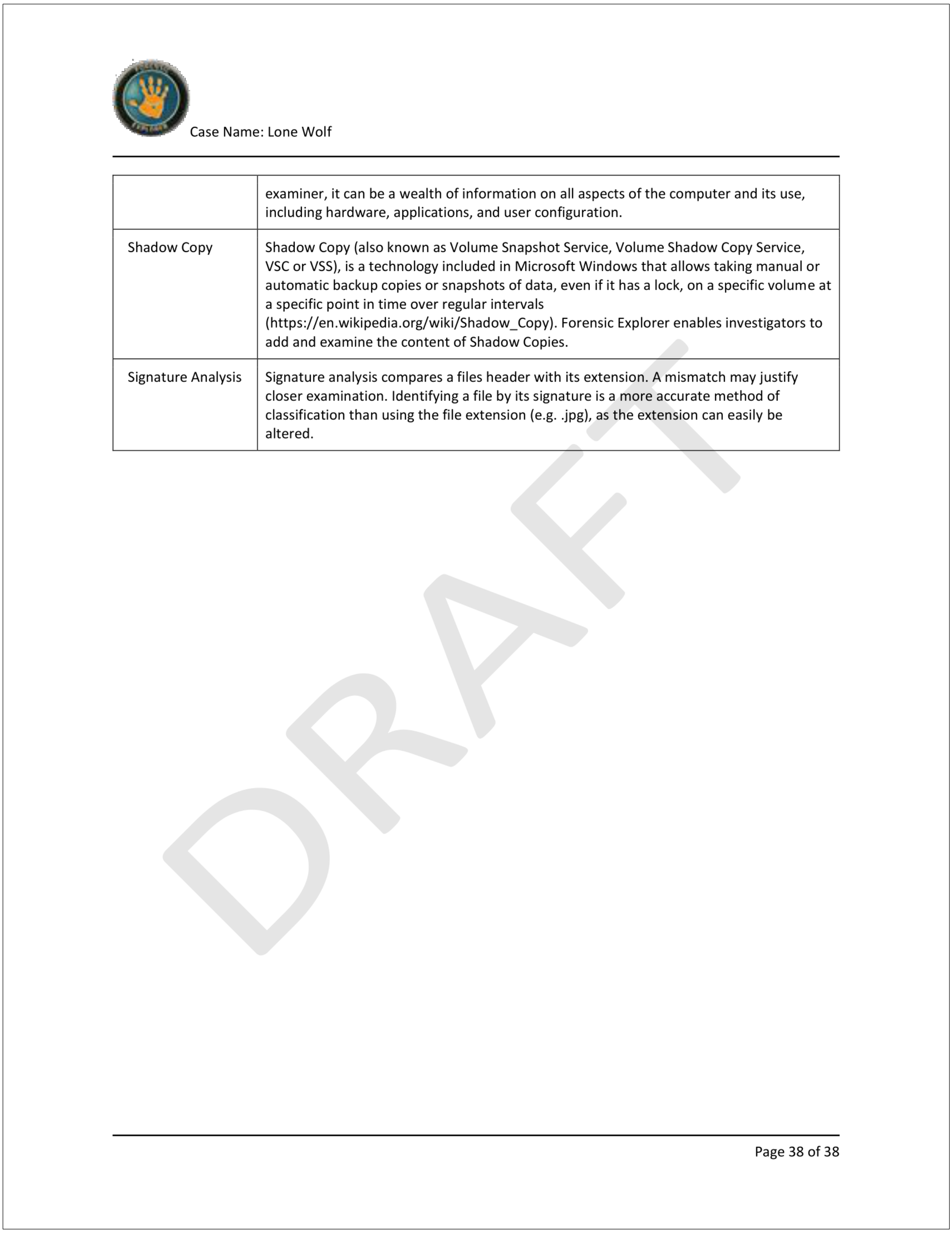


Case Name: Lone Wolf

Definitions

Device	A device refers to the electronic media being examined. It usually refers to a physical device, such as a hard drive, camera card etc., but can also mean the forensic image of a device in DD, E01 or other formats.
File Signature	The header component of a file which has unique identifiers that assigns it to a type, e.g. a jpeg. Most common file types have a signature set by the International Organization for Standardization (ISO). Identifying a file by its signature is a more accurate method of assessment that using the file extension, which can easily be altered.
File Slack	The unused space in the last cluster of a file where the logical size of the file does not fill the complete cluster. The file slack can contain fragments of old data previously stored in that cluster.
File System	The organization of files into a structure accessible by the Operating System. The most common types of file systems used by Widows are FAT and NTFS. Others include EXT (Linux) and HFS (MAC).
Forensic Image	A forensic image is a file (or set of files), used to preserve an exact "bit-for-bit" copy of data residing on electronic media. Using non-invasive procedures, forensic software is used to create the image file. The image contains all data, including deleted and system files, and is an exact copy of the original. Most forensic imaging software integrates additional information into the image file at the time of acquisition. This can include descriptive details entered by the examiner, as well as the output of mathematical calculations, an "acquisition hash", which can be later used to validate the integrity of the image. The forensic image file acts as a digital evidence container that can be verified and accepted by courts.
Hash	A Hash is a mathematical calculation to generate a unique value for specific data. The chances of two files that contain different data having the same hash value are exceedingly small. The most common hash algorithms in use are MD5, SHA1 and SHA256.
Hash Set	A Hash Sets is a store of mathematical calculations (hash values - usually created by the MD5 algorithm) for a specific group of files. The hash values are a digital fingerprint which can then be used to identify a file and either include or exclude the file from a data set. Hash Sets are often grouped in the forensic community into two groups: Good Hash Sets: Operating System files, program installation files, etc.; Bad Hash Sets: virus files, malware, Trojans, child pornography, Steganography tools, hacking tools etc. Hash sets can be created in Forensic Explorer, or downloaded from a trusted source.
Live Boot	Live Boot (or Virtual Live Boot) is a component of Forensic Explorer that enables an investigator to boot a forensic image or write protected physical hard drive. The investigator can then operate the computer in a real time, forensically sound, virtual environment. The boot process is achieved through and integration of Mount Image Pro and VMWare or VirtualBox.
Registry	The Windows Registry is a hierarchical database that stores configuration settings and options for the Microsoft Windows operating systems. For the computer forensics

Page 37 of 38



	examiner, it can be a wealth of information on all aspects of the computer and its use, including hardware, applications, and user configuration.
Shadow Copy	Shadow Copy (also known as Volume Snapshot Service, Volume Shadow Copy Service, VSC or VSS), is a technology included in Microsoft Windows that allows taking manual or automatic backup copies or snapshots of data, even if it has a lock, on a specific volume at a specific point in time over regular intervals (https://en.wikipedia.org/wiki/Shadow_Copy). Forensic Explorer enables investigators to add and examine the content of Shadow Copies.
Signature Analysis	Signature analysis compares a files header with its extension. A mismatch may justify closer examination. Identifying a file by its signature is a more accurate method of classification than using the file extension (e.g. .jpg), as the extension can easily be altered.