FORENSIC EXPLORER

FEX Triage

User Guide

Published: 10-Mar-23 at 20:00:00

GetData

1.1 CONTENTS

1. INTRODUCTION

FEX Triage is a program to enable investigators to access, analyze and collect digital evidence. FEX Triage is designed for:

- Non-Technical investigators with limited computer forensics experience (basic mode).
- Forensic examiners (intermediate and advanced mode).

1.1 WHAT IS COMPUTER FORENSIC TRIAGE?

Computer Forensic Triage is the process of examining, prioritizing, and filtering digital evidence to enable an investigator to make time-critical decisions. **FEX Triage** empowers an investigator to identify digital evidence **on-scene**. It can quickly pin-point relevant computers, USB devices, and other storage media.

1.2 IMPORTANT TERMINOLOGY

FEX Triage users should be familiar with the following important terminology used in this user guide:

Table 1: Important Terminology

Boot-Scan	Boot-scan refers to booting a target computer using boot media (e.g., a boot USB).
Live-Scan	Live scan refers to launching FEX Triage to scan a live computer running Microsoft Windows. In many cases this will be the most appropriate action due to concerns about powering down a running system, for example: • Encryption or disk wiping software will be activated. • The system is critical to an individual or business. The investigator must be aware that insertion of the FEX Triage USB device on a live system will leave a trace on the computer relating to the insertion of the FEX Triage USB device.
Desktop-Scan (Forensic PC)	Desktop-scan is used to describe the launch of FEX Triage from the investigator's forensic computer. The forensic computer can be used to triage stand-alone devices, e.g., hard drives, USB drives, camera cards, etc. (typically connected using a write-blocking device).
Forensic Image	A forensic image is a file (or set of files), is used to preserve an exact bit-for-bit copy of data residing on digital media. The most used format is .E01 by Guidance Software (www.guidancesoftware.com). 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.
.L01 File	A .L01 file (also commonly referred to as a logical evidence file or LEF) is a forensic file format created by Guidance Software (www.guidancesoftware.com). FEX Triage can export files from a target computer system into a L01 file whilst preserving the integrity of the original file information (dates, times, size, etc.). A .L01 is usually used to store a selection of files, rather than a copy of an entire drive, for which the Guidance Software .E01 format is most frequently used.
Wibu Codemeter Dongle	Wibu (https://www.wibu.com/) is a company that specialize in software licensing. FEX Triage uses the Wibu licensing system to activate FEX Triage for the end user. FEX Triage uses a physical Wibu Codemeter USB3 dongle that contains the license, and the dongle must be plugged in for the software to run. The Wibu dongle also has standard USB storage space (16, 32 or 64 gigabyte versions) and FEX Triage can be launched directly from this device.
Forensically Sound	Digital evidence by its very nature is volatile. The term **forensically sound** refers to the accepted industry principle that maintaining the integrity of digital evidence is paramount, and that no action by the investigator should change data that is to be relied upon. FEX Triage examines and collects evidence in a manner that preserves the integrity of evidence and provides an audit trail so that an independent third party can examine the actions undertaken. An investigator should also apply standard principles of crime-scene preservation (photographs, documentation, etc.) to any matter involving digital evidence.
Forensic Explorer	Forensic Explorer is GetData's forensics analysis software, www.getdataforensics.com/product/forensic-explorer-fex/ used by computer forensic examiners). Cases created by FEX Triage are in the Forensic Explorer format and may be opened directly by Forensic Explorer.

1.3 MINIMUM SYSTEM REQUIREMENTS

FEX Triage is designed to be run on computers with the following minimum system requirements:

Minimum System Requirements
Live scan of target computer running Windows Windows 7 64-bit and above 8GB RAM USB3 connectivity
Boot-scan BIOS/UEFI accessible Intel 64bit or compatible 8GB RAM

Recommended System Requirements (Desktop Scan from Forensic PC)
Windows 10 64-bit Intel i7 CPU 16GB of RAM 500GB SSD hard drive

IMPORTANT: FEX Triage requires **Administrator rights** to access physical disks.

1.3.1 SUPPORTED OPERATING SYSTEMS

FEX Triage supports analysis of the following file systems:

- Windows FAT12/16/32, exFAT, NTFS
- MAC HFS, HFS+, APFS
- EXT 2/3/4

1.3.2 SUPPORTED FORENSIC IMAGE FORMATS

FEX Triage supports common image and forensic image formats including:

- AD1, AFF, DD, DMG, BIN, RAW, E01, Ex01, L01, Lx01, VMD, VHD, VHDX.

1.3.3 ENCRYPTION SUPPORT

FEX Triage supports the following drive encryption formats (encryption password must be known):

- Bitlocker (Microsoft Windows).
- File Vault 2 (MAC).

2. DOWNLOAD

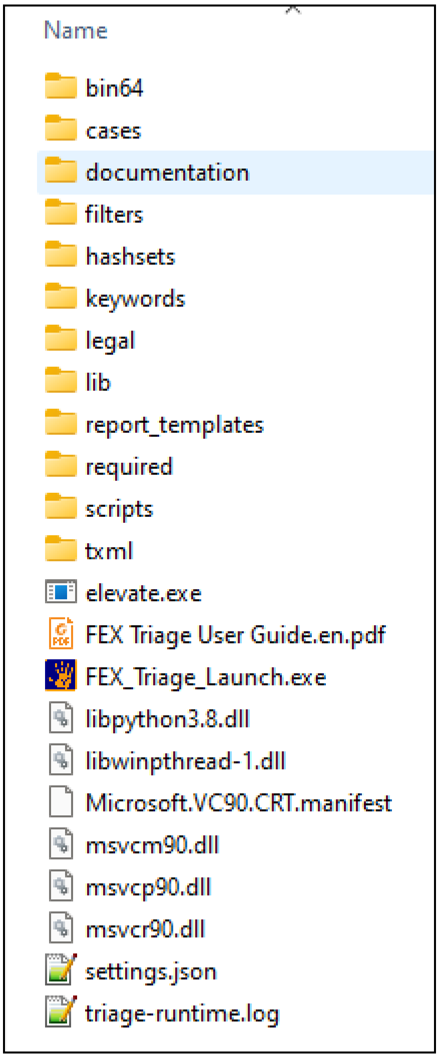
FEX Triage is available for download from https://getdataforensics.com/product/fex-triage/. It is A 64bit application downloaded as a ZIP file with name in the format: ***FEX_Triage_64bit_(v2.4.14.9424A).zip***

The software build number in the example above is defined as follows:

- **v2.4.14** The version number of the GUI (shown in the title bar).
- **9424** The version number of the processing engine.
- **A** The build version (it is reset when the previous numbers change).

2.1.1 ZIP CONTENT:

The zip file contains:



Name
bin64
cases
documentation
filters
hashsets
keywords
legal
lib
report_templates
required
scripts
txml
elevate.exe
FEX Triage User Guide.en.pdf
FEX_Triage_Launch.exe
libpython3.8.dll
libwinpthread-1.dll
Microsoft.VC90.CRT.manifest
msvcm90.dll
msvcp90.dll
msvcr90.dll
settings.json
triage-runtime.log

bin64:	Program files.
cases:	Output from scan.
filters:	Filters used by search profiles.
hashsets:	Hash-sets that are used to match specific profiles.
keywords:	Keywords used by specific search profiles.
legal:	License agreements.
lib:	GUI code.
report_templates:	Search profile report templates.
scripts:	Scripts used by search profiles.
txml:	Search profiles.
FEX_Triage_Launch.exe:	Launch FEX Triage using this file.
settings.json	Stores settings between each run.
triage-runtime.log	Log information for the FEX Triage GUI.

3. FEX TRIAGE DONGLE AND LICENSE

Your FEX Triage purchase includes a Wibu 16gb or 32gb activation and USB3 storage dongle.

	Datasheet: https://www.wibu.com/fileadmin/wibu_downloads/CodeMeter_Datasheets/Seriennummer_03/B_BMC_BMI/CmStick_BMC-1011-03-56x.pdf

The FEX Triage dongle contains your license. The license is managed with the GetData License Manager, available from: http://download.getdata.com/support/LicenseManager.exe. The dongle must be present for FEX Triage to activate.

A FEX Triage license will expire each 12 months. It can be renewed at https://getdataforensics.com/product/fex-triage/ .

3.1 RECOMMENDED HARDWARE

It is recommended that the following hardware be accessible in the field:

Figure 1: FEX Triage recommended hardware.

	A portable SSD storage drive. FEX Triage can be executed directly from this drive (with the Wibu dongle used for activation).
	A high-quality USB hub. This device enables the Wibu dongle and other USB devices to be simultaneously connected.
	USB adaptors for connection of dongles/storage devices.

4. CREATING A FEX TRIAGE LIVE-SCAN USB

Live scan refers to launching FEX Triage to scan a live computer running Microsoft Windows. In many cases this will be the most appropriate action due to concerns about powering down a running system, for example:

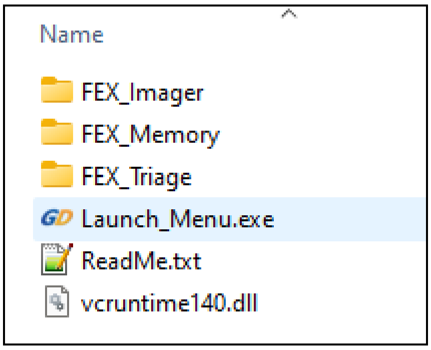
- Encryption or disk wiping software will be activated.
- The system is critical to an individual or business.

The investigator must be aware that insertion of the FEX Triage USB device on a live system will leave a trace on the computer relating to the insertion of the FEX Triage USB device.

4.1.1 ADDING FEX TRIAGE TO A LIVE-SCAN USB

Download the FEX Triage ZIP file and unzip the contents to the USB. The following folder structure will be created:

Figure 2: FEX-Triage folder structure.



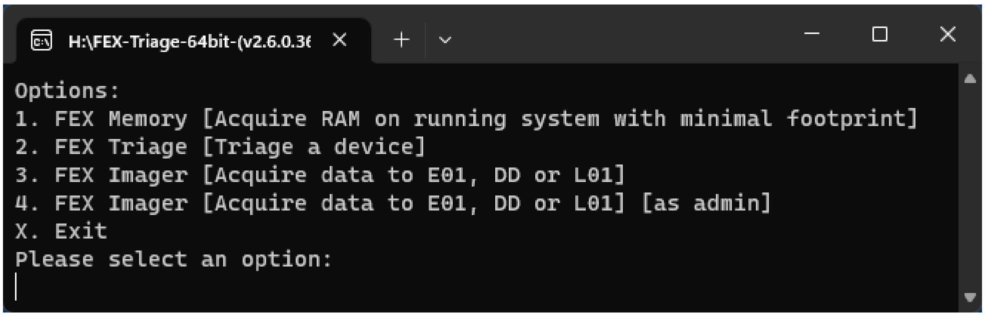
```
Name
FEX_Imager
FEX_Memory
FEX_Triage
Launch_Menu.exe
ReadMe.txt
vcruntime140.dll
```

The folder structure contains three stand-alone applications:

1. **FEX Imager**: Used to acquire a forensic image of a hard disk or partition.
2. **FEX Memory**: Used to acquire a forensic image of RAM.
3. **FEX Triage**: The subject of this user guide.

The **Launch_Menu.exe** is an application that provide a CMD menu to launch those programs.

Figure 3: Launch_Menu.exe



```
Options:
1. FEX Memory [Acquire RAM on running system with minimal footprint]
2. FEX Triage [Triage a device]
3. FEX Imager [Acquire data to E01, DD or L01]
4. FEX Imager [Acquire data to E01, DD or L01] [as admin]
X. Exit
Please select an option:
```

5. CREATE A BOOT USB

In some instances, it will be necessary boot a target computer. This can be accomplished using a Windows boot USB in order to run FEX-Triage and other forensic tools. A Windows boot USB requires a high speed USB3. A 16/32/64 GB FEX-Triage USB3 dongle is suitable for this.

There are multiple options to create a boot environment, including:

Microsoft

- Standard Windows 10/11
  https://www.microsoft.com/en-us/software-download
- Windows PE
  https://learn.microsoft.com/en-us/windows-hardware/manufacture/desktop/winpe-intro
- Windows To Go
  https://learn.microsoft.com/en-us/windows/deployment/planning/windows-to-go-overview

3rd Party adaptations of Microsoft OS Installs

- Atlas OS
- Windows PE FE (Forensic Edition)
- Windows Tiny 10.
- Windows 10 Lite.

Selecting a USB boot platform may ultimately come down to an organization’s accepted forensic process, or simply personal choice by the investigator.

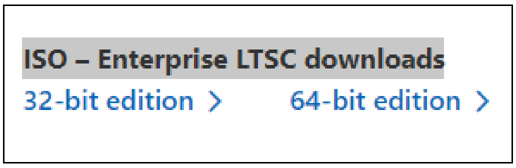
5.1 USB BOOT - WINDOWS TO GO - WIN10 LTSC-E

In this user guide we describe the use of **Windows-To-Go** to create a USB boot drive running **Windows 10 LTSC (Long Term Servicing Channel) Evaluation Edition** (Win10-LTSC-E).

Win10-LTSC-E is a stripped-down enterprise OS based on a specific version of Windows 10. It does not include many of the Microsoft pre-installed applications (such as Edge, Cortana assistant, News, etc.), giving it a smaller installation footprint, reduced RAM usage, and increased speed. **Important**: Note that the Win10-LTSC is a Microsoft corporate licensed product.

Win10-LTSC-E is available for download an ISO file on this page: https://www.microsoft.com/en-us/evalcenter/download-windows-10-enterprise:

Figure 4: Windows LTSC ISO Download



ISO – Enterprise LTSC downloads

32-bit edition ›   64-bit edition ›

5.2 ISO TO USB USING RUFUS

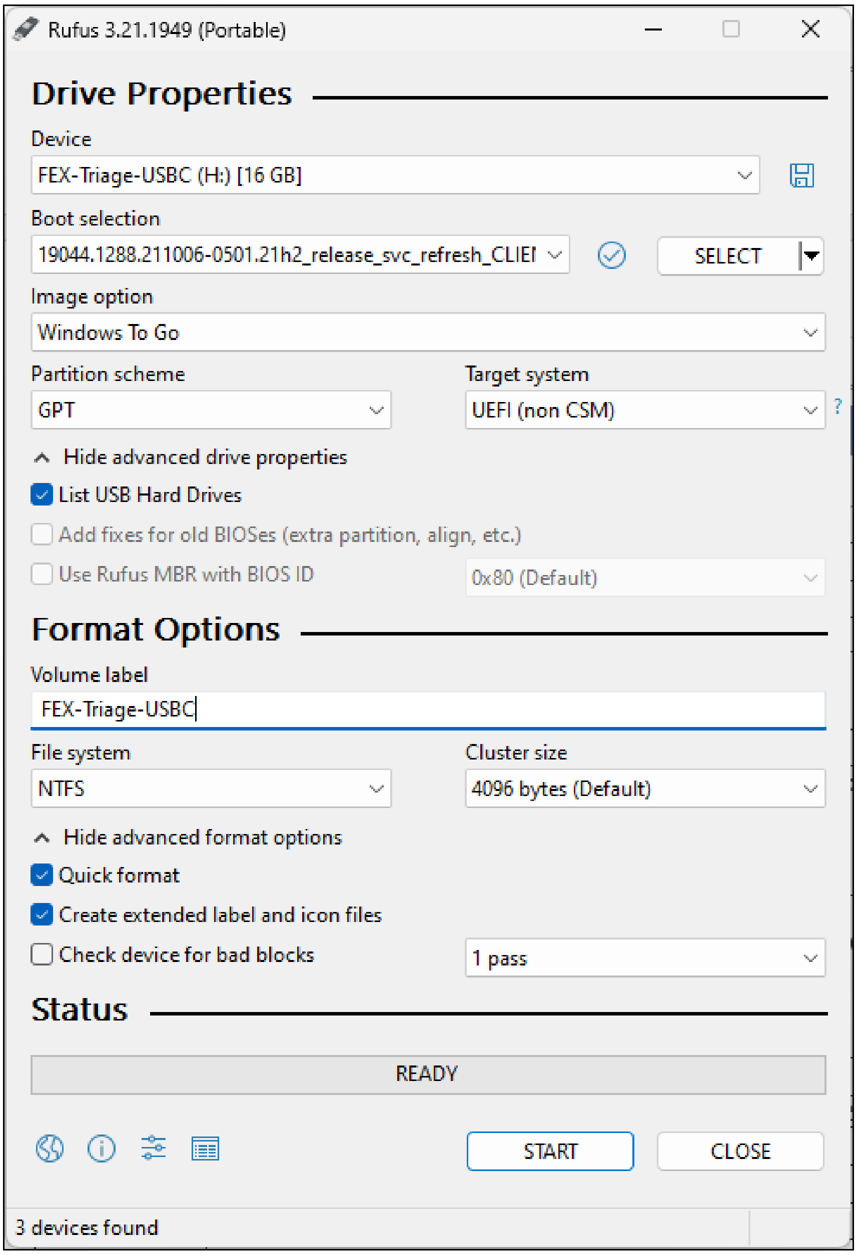
To write the **ISO** file to the **FEX Triage USB dongle** we use Rufus (https://rufus.ie/en/):

1. Insert the FEX Triage Wibu dongle. **WARNING:** The FEX Triage dongle **will be formatted,** and **existing data destroyed.** Ensure any required data is backed up.
2. Run Rufus-[vX.XX].exe.
3. Select the FEX Triage dongle as the device.
4. Click the **SELECT** button and select the **.ISO** file as the **Boot Selection**.
5. In the Image Option select Windows To Go.
6. In the **Volume Label** enter a unique name that is easily identifiable as your boot device.
7. Select the **Target System** (UEFI recommended):

   BIOS (Basic Input-Output system): Due to its inherent limitations (e.g., It can only boot from drives of 2.1 TB or less) it is now considered to be phased out.

   UEFI (Unified Extensible Firmware Interface): Can **generally expected to be used in computer produced after 2018**. UEFI has many advantages over BIOS, including networking and multi-language capabilities.
8. Click **START**.

Figure 5: Rufus: Create boot USB.



Rufus 3.21.1949 (Portable)

Drive Properties

Device: FEX-Triage-USBC (H:) [16 GB]

Boot selection: 19044.1288.211006-0501.21h2_release_svc_refresh_CLIEI

Image option: Windows To Go

Partition scheme: GPT

Target system: UEFI (non CSM)

Hide advanced drive properties

☑ List USB Hard Drives

□ Add fixes for old BIOSes (extra partition, align, etc.)

□ Use Rufus MBR with BIOS ID 0x80 (Default)

Format Options

Volume label: FEX-Triage-USBC

File system: NTFS

Cluster size: 4096 bytes (Default)

Hide advanced format options

☑ Quick format

☑ Create extended label and icon files

□ Check device for bad blocks 1 pass

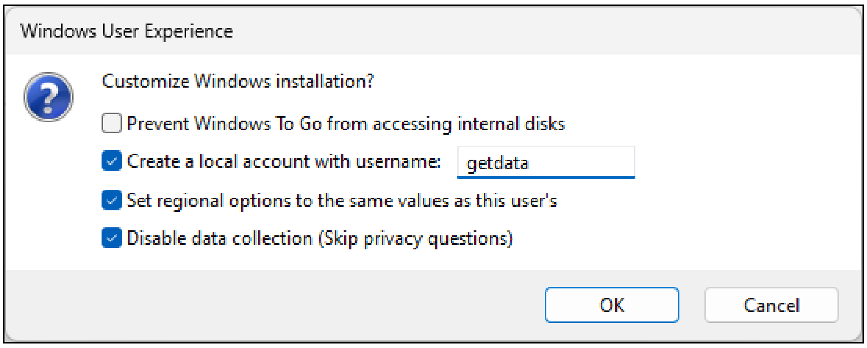
Status

READY

3 devices found

You will be prompted for additional configuration options:

Figure 6: Rufus Windows User Experience.



Windows User Experience

Customize Windows installation?

□ Prevent Windows To Go from accessing internal disks

☑ Create a local account with username: getdata

☑ Set regional options to the same values as this user's

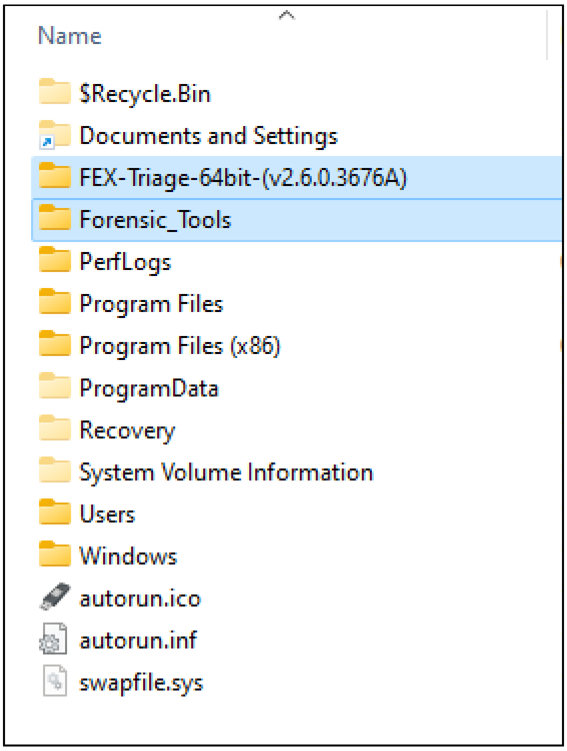
☑ Disable data collection (Skip privacy questions)

5.3 ADD FEX TRIAGE (AND OTHER TOOLS) TO THE BOOT USB

Once the WinPE-FE boot USB has been created:

1. **Unzip the FEX Triage installation file** and **copy it to the USB**.
2. Create a second folder called **Forensic Tools** and add any **additional forensic applications**.

Figure 7: Add FEX Triage to the Boot USB



Name

$Recycle.Bin
Documents and Settings
FEX-Triage-64bit-(v2.6.0.3676A)
Forensic_Tools
PerfLogs
Program Files
Program Files (x86)
ProgramData
Recovery
System Volume Information
Users
Windows
autorun.ico
autorun.inf
swapfile.sys

3. **Boot a test system with the boot USB** and follow the **Microsoft OS setup instructions**.

5.3.1 RECOMMENDED REGISTY EDITS

SANPOLICY

It is possible stop internal drives being brought online automatically by setting the Windows **SanPolicy** in the Windows Registry. Use **RegEdit** to update the following registry value:

- HKLM\System\CurrentControlSet\Services\partmgr\Parameters SanPolicy = REG_DWORD = 3

Lear more about the Windows SanPolicy here: https://learn.microsoft.com/en-us/windows-hardware/manufacture/desktop/winpe-storage-area-network--san--policy

NOAUTOMOUNT

Automount is enabled by default in Windows. When enabled, Windows automatically mounts the file system for a new volume (disk or drive) when it is added (connected) to the system, and then assigns a drive letter to the volume. Disabling automount in the registry prevents Windows from automatically mounting and assigning drive letters to any new basic volumes (disk or drive) added (connected) to the system. See: https://learn.microsoft.com/en-us/windows/win32/api/vds/ne-vds-vds_san_policy.

Use **RegEdit** to update the following registry value:

- HKLM\System\CurrentControlSet\Services\mountmgr NoAutoMount = REG_DWORD = 1

5.3.2 MANUALLY BRINGING A DISK ONLINE AS READ-ONLY

To manually bring an internal drive online in read-only mode:

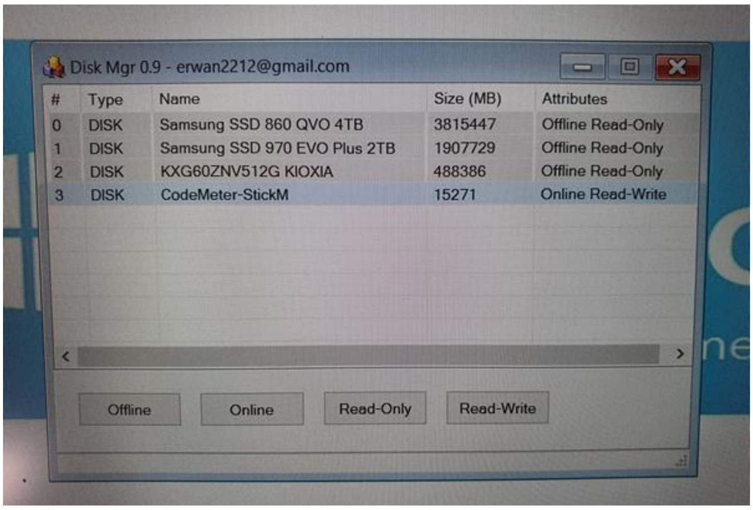
1. Open an **administrator Command Prompt** and run the **diskpart** command.
2. Type **list volume** and press **Enter**. Next type **select volume #**, where # is the number of the volume you're going to lock it as read-only.
3. To make your selected volume read-only, type **attributes volume set readonly,** and press **Enter**.

For more information see: https://www.top-password.com/blog/set-a-disk-or-volume-read-only-in-windows/.

5.3.3 DISK MANAGER BY ERWAN LBALEC

A stand-alone tool, Erwan Lbalec's Disk Manager (also referred to as DSKMGR and Disk Mgr) can assist in bringing in read-only disks online:

Figure 8: Disk Mgr 0.9



Disk Mgr 0.9 - erwan2212@gmail.com

#	Type	Name	Size (MB)	Attributes
0	DISK	Samsung SSD 860 QVO 4TB	3815447	Offline Read-Only
1	DISK	Samsung SSD 970 EVO Plus 2TB	1907729	Offline Read-Only
2	DISK	KXG60ZNV512G KIOXIA	488386	Offline Read-Only
3	DISK	CodeMeter-StickM	15271	Online Read-Write

In the example above there are 4 disks present in the computer. The FEX Triage boot USB, identified by **Codemeter-StickM**, is the only drive which is **Online** and set to **Read-Write**.

If another investigator drive is connected for the purposed of collecting evidence, then it can be configured to be **Online** and **Read-Write** in this screen.

For more information on Disk Manager visit:
http://mistyprojects.co.uk/documents/DiskMgr/index.html

6. RUNNING A BOOT-SCAN – WINDOWS PC

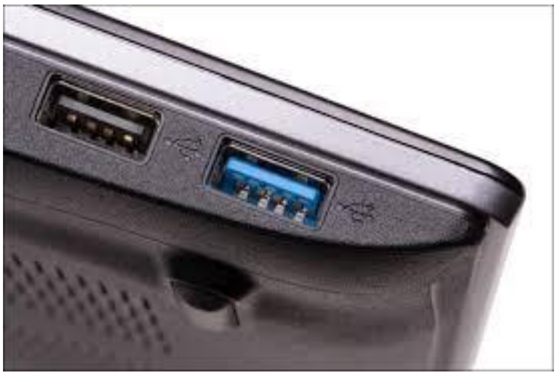
Once a FEX Triage boot USB has been created:

6.1 BEFORE YOU BEGIN

Preparation:

1. Ensure the target computer **is plugged in for power** and not running on battery.
2. Determine how many USB ports are available on the target computer. For speed purposes, FEX Triage scan should be run from a device plugged into a USB3 port. In almost all cases USB3 ports can be easily identified by their blue color, as shown in Figure 9 below:

Figure 9: USB2 port (left), USB3 port (blue, right)



If a **limited number of USB3 ports are available**, devices that are not being used for data transfer (e.g., the computer mouse, keyboard etc.) are best transferred onto a USB hub.

For best data transfer speed, the **FEX Triage dongle** (or the data collection device disk) is plugged **directly into a USB3 port**.

6.2 BIOS/UEFI

Most target computers will **need to be manually configured** by the investigator to boot from the FEX Triage USB3 dongle. This is done by changing the boot options available in the computer **BIOS or UEFI**.

BIOS or UEFI is computer code embedded on a chip on the motherboard that recognizes and controls various devices that make up the computer. The purpose is to make sure all the things plugged into the computer can work properly. (See https://simple.wikipedia.org/wiki/BIOS).

BIOS (Basic Input/Output System) is usually found on older computers made before 2018.

UEFI (Unified Extensible Firmware Interface) is usually found in more modern computers (2105 onward). UEFI supports larger hard drives, faster boot times, and more security features.

Unfortunately, many PC manufactures continue to refer to UEFI as BIOS so it can be difficult tell which is present.

IMPORTANT: If a BIOS computer is encountered it can only be booted using a **boot usb created with BIOS compatibility** (see **Error! Reference source not found. Error! Reference source not found.**).

6.2.1 ADDING A SECONDARY TRIAGE STORAGE DEVICE (E.G. SANDISK SSD)

If using an external drive such as a SanDisk 4tb SSD, consideration should also be given to the format of the drive. A large NTFS formatted drive may not be visible on a BIOS computer. In this case **exFAT** may be the best solution (see: https://www.makeuseof.com/tag/exfat-better-different-fat32/)

6.3 TAKE CONTROL OF THE TARGET COMPUTER

The investigator will configure the BIOS boot sequence to tell the computer to boot from the FEX Triage USB3 rather than its normal device.

1. Insert the FEX Triage Wibu dongle in a USB port.

2. **Power-on** the target computer and **repeatedly press** the **BIOS hot-key.** Common BIOS hot keys include:

    - ESC
    - DEL
    - F12

IMPORTANT: It is important that the investigator take the opportunity to research the specific hot-key sequence using the exact make and model information.

3. The computer will enter into a **BIOS Startup Menu.** This menu will differ greatly in appearance between makes and modules of computers. Some menus will also consist of a single screen, whilst others may have multiple screens.

Figure 10: BIOS Startup Menu, HP Omen I9

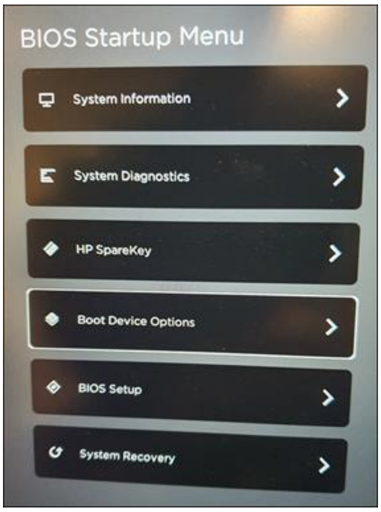
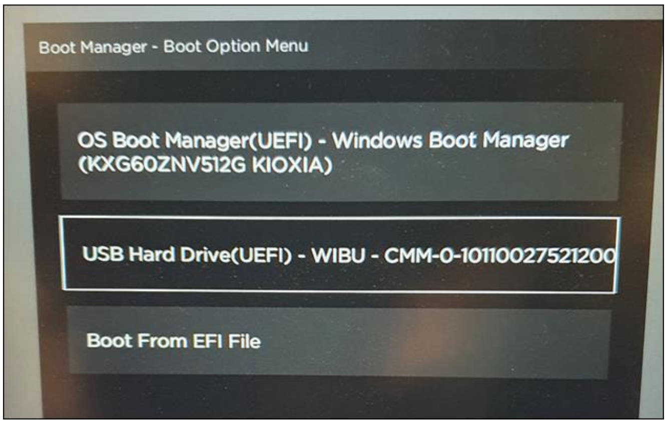


Figure 11: BIOS Startup Menu, HP Omen I9 Sub Menu



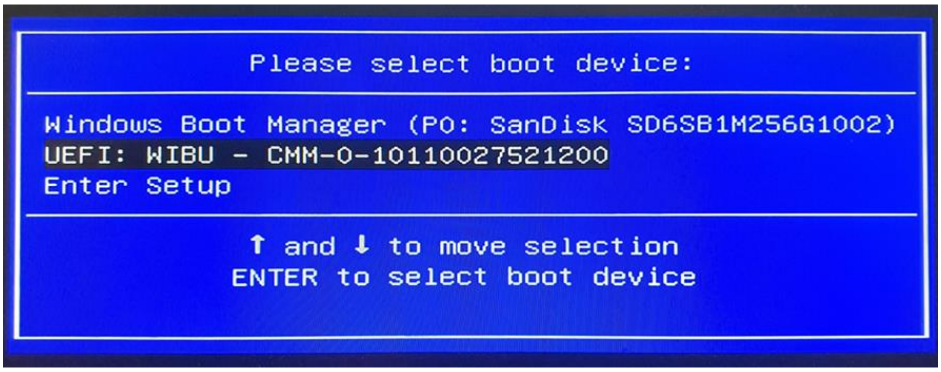
Boot Manager - Boot Option Menu

OS Boot Manager(UEFI) - Windows Boot Manager (KXG60ZNV512G KIOXIA)

USB Hard Drive(UEFI) - WIBU - CMM-0-10110027521200

Boot From EFI File

Figure 12: BIOS Startup Menu, ASUS i7



Please select boot device:

Windows Boot Manager (P0: SanDisk SD6SB1M256G1002)
UEFI: WIBU - CMM-0-10110027521200
Enter Setup

↑ and ↓ to move selection
ENTER to select boot device

4. Select the FEX Triage Wibu dongle and press Enter to boot the target computer.

6.4 USB BOOT: TROUBLE-SHOOTING MODERN UEFI COMPUTERS

An investigator may encounter difficulties booting from USB on UEFI computers. Common problems are:

- A **UEFI** setting has disabled the ‘boot from USB’ option.
- **UEFI Fast-Boot** is turned on (a setting that is intended to make the Windows boot sequence faster and may ignore ‘boot from usb’).

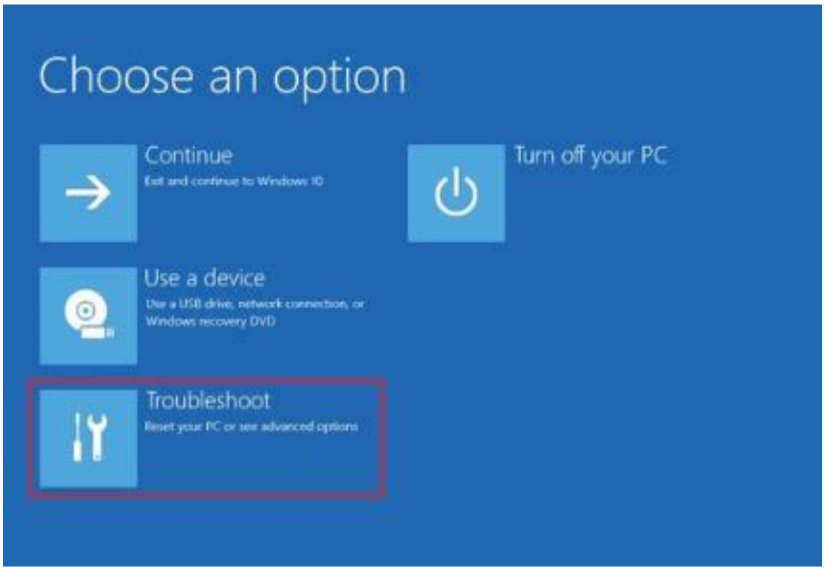
These options can be reset in UEFI settings.

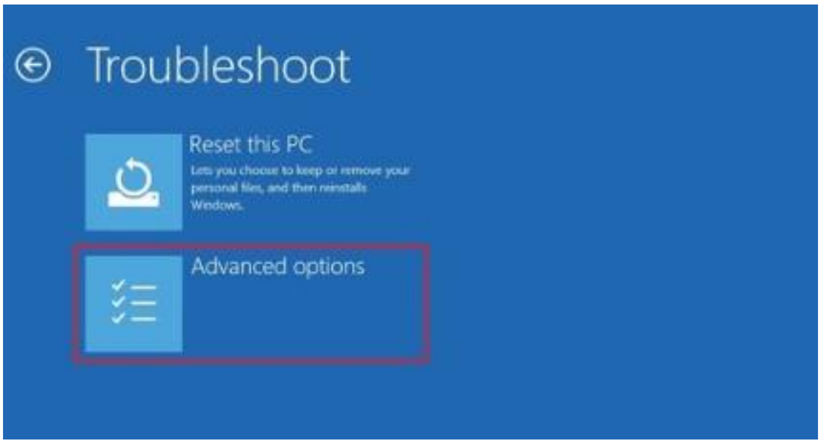
6.4.1 UNINTENDED BOOT INTO WINDOWS 10

Even experience forensic investigators can accidentally boot into Windows 10 when trying to boot from USB. In this situation.

1. Make notes of the boot.
2. Use Windows 10 to set the computer to restart in UEFI mode:
   - Click the **Restart** option from the **Windows 10 Start menu** whilst holding down the **SHIFT** key, or.
   - Open Windows 10 Settings:
     - Click on Update & Security
     - Click on Recovery.
     - Under the "Advanced startup" section, click the Restart now button.

During the Windows 10 restart process select the following options:

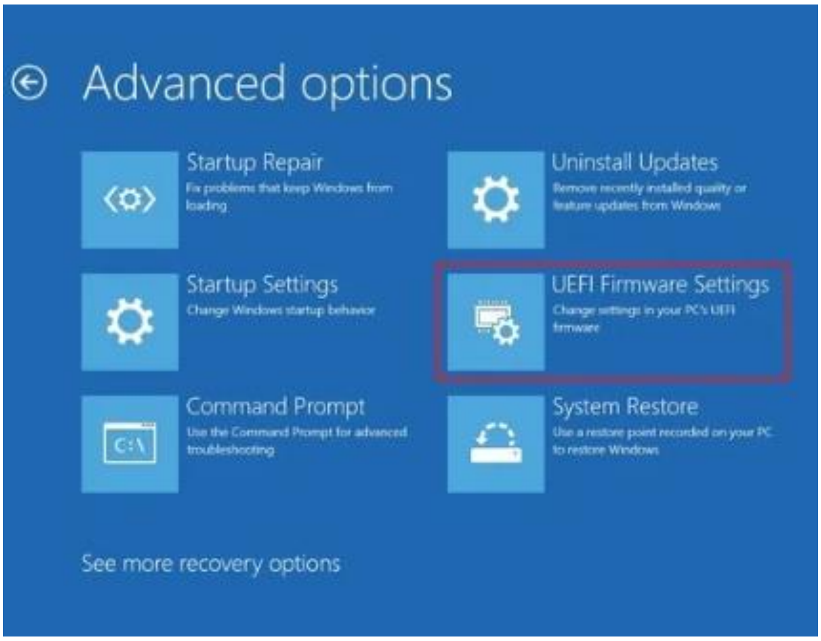

Choose an option
Continue
Exit and continue to Windows 10
Turn off your PC
Use a device
Use a USB drive, network connection, or Windows recovery DVD
Troubleshoot
Reset your PC or see advanced options



Troubleshoot

Reset this PC
Lets you choose to keep or remove your personal files, and then reinstalls Windows.

Advanced options



Advanced options

Startup Repair
Fix problems that keep Windows from loading

Uninstall Updates
Remove recently installed quality or feature updates from Windows

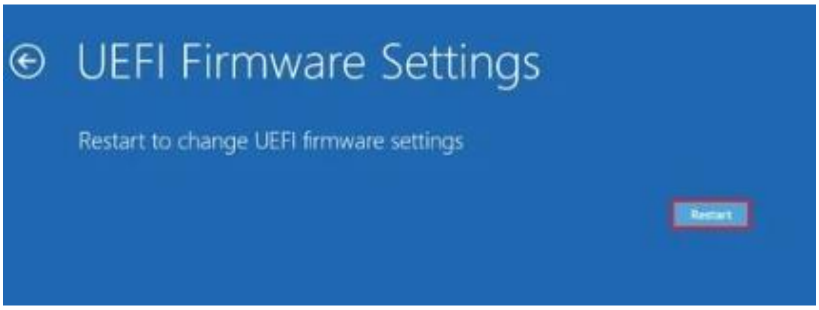
Startup Settings
Change Windows startup behavior

UEFI Firmware Settings
Change settings in your PC's UEFI firmware

Command Prompt
Use the Command Prompt for advanced troubleshooting

System Restore
Use a restore point recorded on your PC to restore Windows

See more recovery options



UEFI Firmware Settings

Restart to change UEFI firmware settings

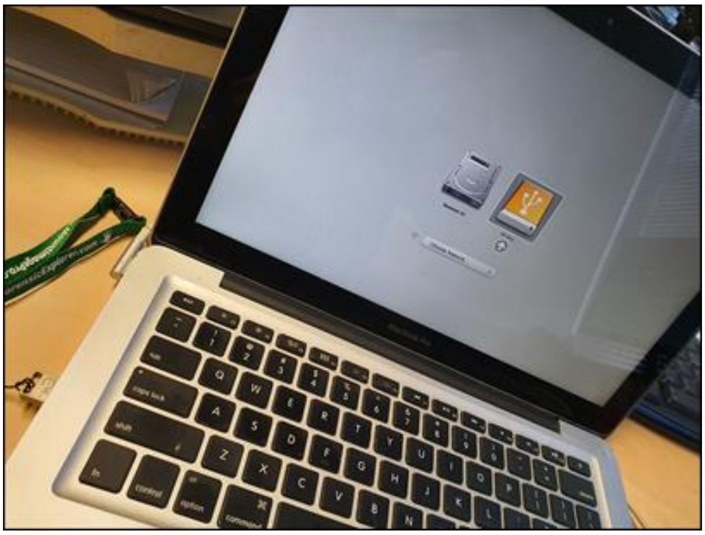
The computer will restart into UEFI settings.

7. RUNNING A BOOT SCAN - MAC

To boot-scan a MAC:

1. Insert the FEX Triage dongle.
2. Turn on the MAC and immediately hold the Option (Alt) key.
3. Release the Option key when you see the Startup Manager window.
4. If the Mac is protected by a firmware password, release the key when you're asked to enter the password.
5. Select your **EFI** startup disk, then click the arrow under its icon, or press Return.

Figure 13: Boot-scan of a MacBook Pro



More information is available at: https://support.apple.com/en-au/HT202796

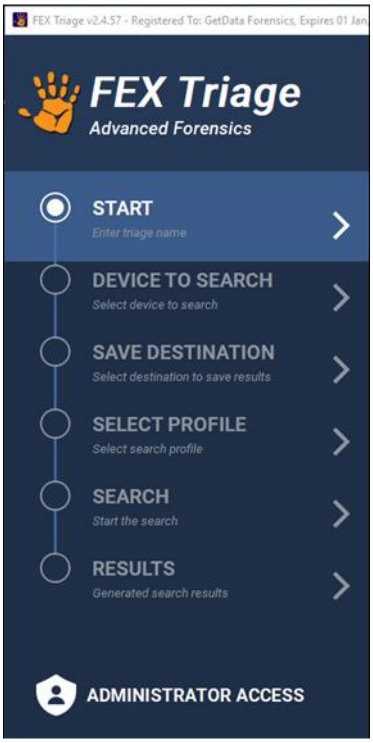
8. RUNNING FEX TRIAGE

The FEX Triage program should only ever be run from the **investigator's media**, that is:

- The Wibu Codemeter USB dongle; or
- A larger/faster storage device, e.g., the SanDisk Extreme SSD (the Wibu Codemeter dongle must also be present to provide access to the FEX Triage license); or
- Run from the investigator's forensic computer.

IMPORTANT: If large volumes of data are to be exported from the target computer the type and speed of the investigators external drive will significantly influence performance. A quality SSD drive, such as the SanDisk Extreme provided with the FEX Triage hardware kit is recommended.

Figure 14: FEX-Triage Navigation Menu



FEX Triage v2.4.57 - Registered To: GetData Forensics, Expires 01 Jan

FEX Triage is launched by double clicking on the **FEX_Triage_Launch.exe**.

8.1 LICENSE INFORMATION

The running FEX Triage will display license information in the topmost display bar of the program. If the license is invalid it will not launch the search.

8.2 ADMINISTRATOR STATUS

FEX Triage will attempt to launch with administrator user rights. It is recommended to run FEX Triage as an administrator to provide the highest-level access privileges.

Administrator access status is displayed in the bottom left corner of the FEX Triage GUI. If administrator access is not achieved, then No Administrator Access will display in red.

In a **Boot-Scan** triage the investigators boot-media will boot with administrator access privileges.

In a **Live-Scan** triage it may be possible to launch FEX Triage only with the access privileges of the currently logged in user.

A triage that is **NOT** run as administrator: May not have access to scan all physical drives in the computer; and may not have Windows security permissions to access all files in the computer.

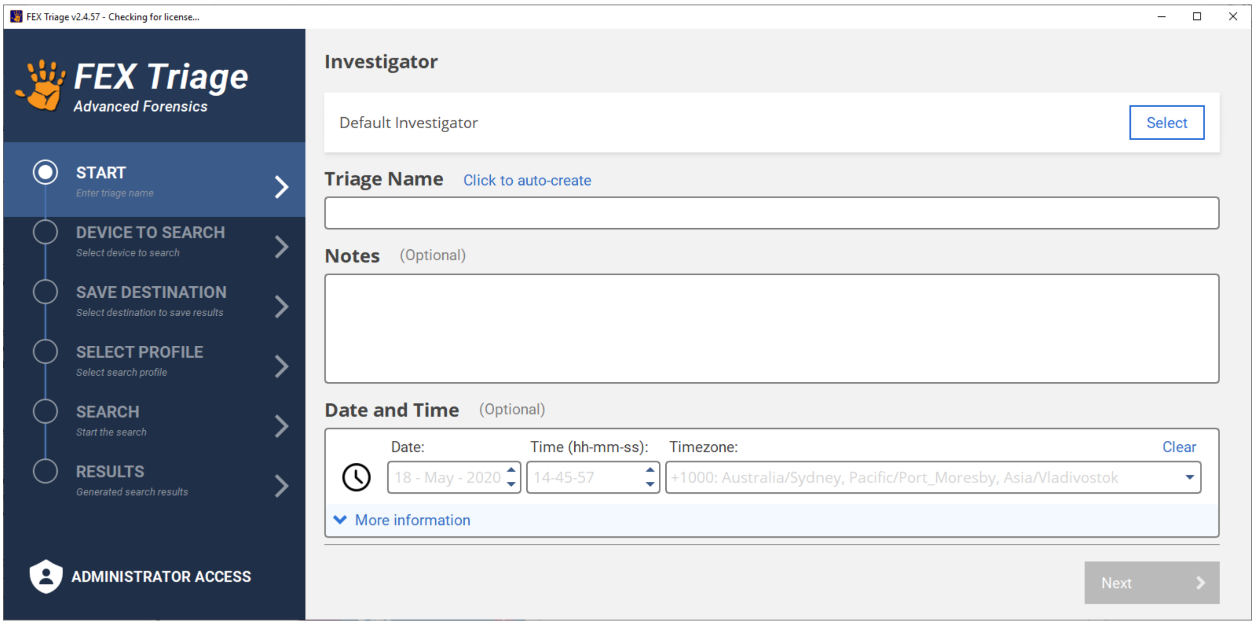
9. FEX TRIAGE STEPS

FEX Triage is navigated using the wizard menu shown in Figure 14. Each link is clickable and can be used to navigate between FEX Triage screens.

9.1 STEP1 - START

When FEX Triage is launched the first window displayed in the **Start** window, shown in Figure 15 below:

Figure 15: FEX Triage Start



FEX Triage v2.4.57 - Checking for license...

Default Investigator

Date: 18 - May - 2020

Time (hh-mm-ss): 14-45-57

Timezone: +1000: Australia/Sydney, Pacific/Port_Moresby, Asia/Vladivostok

The Start window contains the following user input fields:

9.1.1 INVESTIGATOR

Field:	Investigator
Required:	No
Purpose:	Identifies the investigator. Auto populates this information in generated reports.
Description:	This is not a required field and if not edited **Default Investigator** will be used as the name. Click the **Select** button to select an investigator from the available list. If the required name is not present, use the **+ Add New Investigator** button to add a new investigator.

Technical:	Investigator details are held in the file: **…\bin64\Databases\LocalInvestigator.xml**. The Forensics Administrator can re-use this file when preparing the FEX Triage dongle.

9.1.2 TRIAGE NAME

Triage name is a unique name for a scan. It is a required field, but the investigator can elect to **Click to auto-create** a case name. This auto-generates a case name based on the computer's internal clock in the format YYYY-MM-DD-HH-MM-SS.

Field:	Triage Name
Required:	Yes
Purpose:	Creates a triage-name folder where the results of each scan are stored.
Description:	For each FEX Triage scan a new folder is created in **…\cases\[Triage Name]** containing the contents of the scan.
Technical:	Each triage-name folder that is created is a case folder that can be opened directly with the Forensic Explorer GUI (https://getdataforensics.com/product/forensic-explorer-fex/).

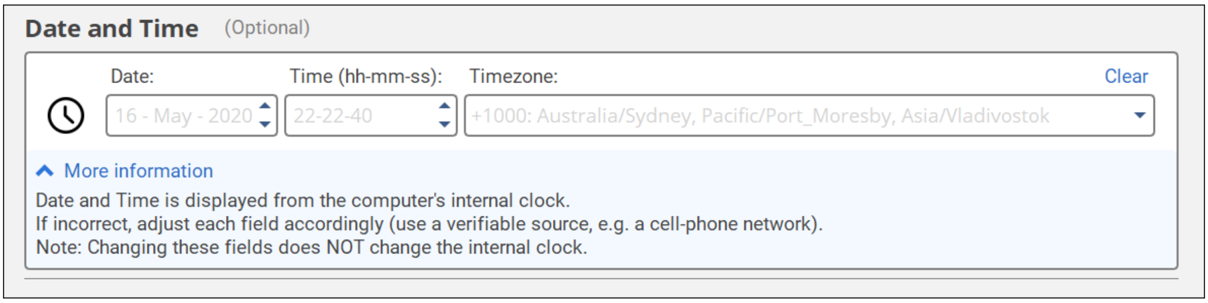
9.1.3 DATE AND TIME

In most cases in involving digital evidence date and time of file creation is important. There are a number of variables which can affect the reliability of date and time information, including:

- The accuracy of the computer's internal clock.
- The format used to configure the computer (e.g., Microsoft NTFS, FAT, exFAT, etc.).
- Whether files have been moved or copied from different devices.

Where issues of date and time are critical, it is important that date and time information be reviewed by a qualified forensic examiner.

Figure 16: Start Screen, Date and Time



Date and Time (Optional)

Date: 16 - May - 2020

Time (hh-mm-ss): 22-22-40

Timezone: +1000: Australia/Sydney, Pacific/Port_Moresby, Asia/Vladivostok

Clear

More information

Date and Time is displayed from the computer's internal clock.
If incorrect, adjust each field accordingly (use a verifiable source, e.g. a cell-phone network).
Note: Changing these fields does NOT change the internal clock.

Field: Date and Time

Required: No

Purpose: Records the difference between the computer clock and an independent time observed by the investigator.

Description: File date and time are recorded according to the setting of the computer internal clock. If the internal clock is inaccurate, then created, modified and accessed file time stamps may also be inaccurate.

Recording an independent date and time is a means of identifying any difference at the time of the triage.

Technical: Information provided in this field is written to: …\cases\[triage-name]\Triage Date Time Information.txt. An Example is shown below:

Triage Name: 2020-05-16-20-33-12 Operation Sundance

Investigator: Default Investigator

The following system time was recorded at FEX Triage Launch:

date: 16-May-2020

time: 20-33-32

timezone: +1000: Australia/Sydney, Pacific/Port_Moresby, Asia/Vladivostok

The following independent comparison time was noted by the investigator:

date: 18-May-2020

time: 20-33-32

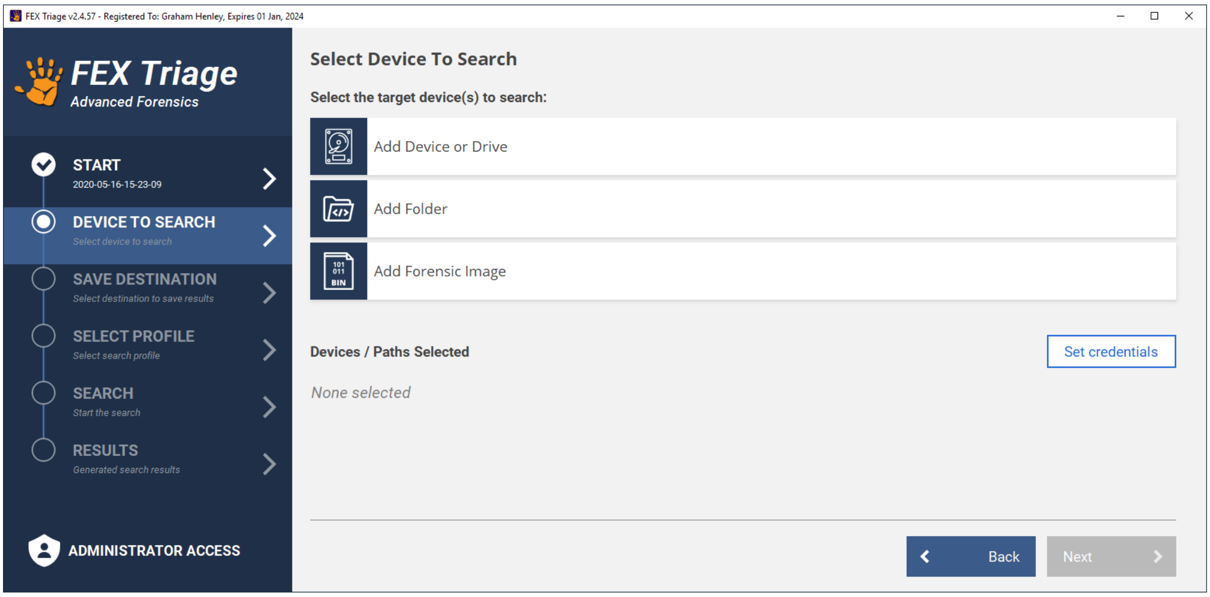
timezone: +1000: Australia/Sydney, Pacific/Port_Moresby, Asia/Vladivostok

9.2 STEP 2 - SELECT DEVICE TO SEARCH

The **Device to Search** screen is where the investigator selects the media to scan. Three options are provided (as shown in Figure 17 below):

- Add Device or Drive.
- Add Folder.
- Add Forensic Image.

Figure 17: FEX Triage, Select Device to Search



9.3 ADD DEVICE OR DRIVE

In most instances an on-scene search will involve search a **Device** or **Drive**:

Device: Is a physical device such as a hard drive or a camera card. Physical devices are usually reference by a computer using a number (0, 1, 2 etc.). These numbers do not necessarily reference a priority but reflect the connection of the device to the computer motherboard.

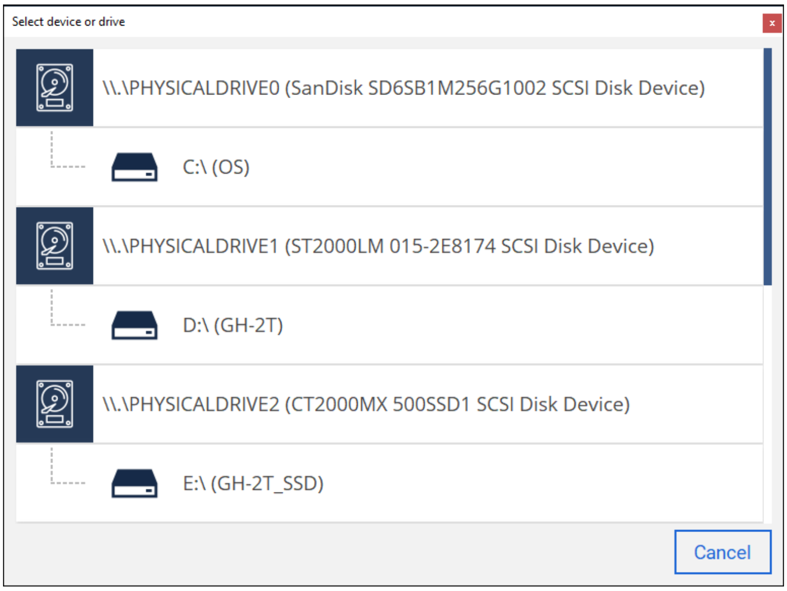
Drive: Is a partition that has been created on a physical device. For example, a hard drive can be partitioned into drives C:\, D:\, E:\ etc.

Selecting a **device** in FEX Triage will mean that the search will encompass all drives (e.g., C:\, D:\, E:\) located on that device. By selecting the Device, it is also possible (using specific search profiles) to search space on the Device that has not been allocated to a Drive (e.g., if the drive is RAW or unpartitioned).

To select a device or drive:

1. Click on the device or drive in the **Select device or drive** window (shown in Figure 18 below):

Figure 18: Select Device or Drive window.



Select device or drive

\\.\PHYSICALDRIVE0 (SanDisk SD6SB1M256G1002 SCSI Disk Device)

C:\ (OS)

\\.\PHYSICALDRIVE1 (ST2000LM 015-2E8174 SCSI Disk Device)

D:\ (GH-2T)

\\.\PHYSICALDRIVE2 (CT2000MX 500SSD1 SCSI Disk Device)

E:\ (GH-2T_SSD)

2. The device or drive will then be added to the **Select Device to Search** window.

3. To add an additional device, repeat this process.

Troubleshooting 1: Not Displaying Devices

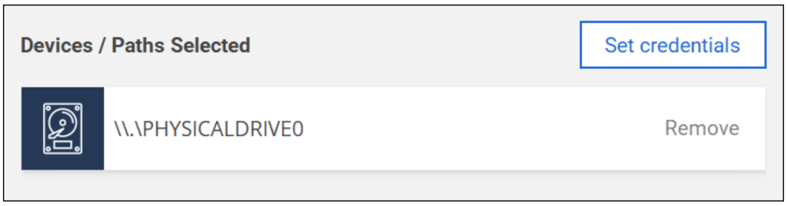
> Troubleshooting: Not displaying devices:
>
> When running a **Live-Scan** the ability to see both a **Device** and a **Drive** can be affected by the Windows security permissions for the currently logged in Windows user. Determine if it is possible to log in with Administrator access or run a **Boot-Scan.**

9.3.1 TO REMOVE AN ITEM FROM THE SEARCH

To Remove an item from the search:

1. Highlight the item to remove and click the **Remove** link to its right:

Figure 19: Removing a Device from the Search



Devices / Paths Selected

\\.\PHYSICALDRIVE0

ENCRYPTION

It is possible that an investigator may encounter a device or drive that has been encrypted.

Important: There are many free and commercial encryption programs that work on a Device, Drive or file level. It is possible to encrypt data in a manner that will be hidden from a forensic examination.

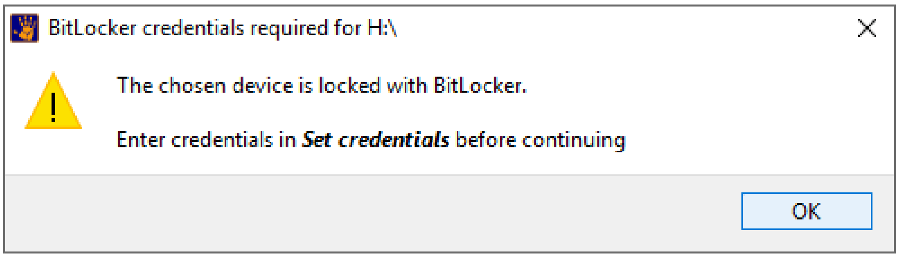
If the investigator suspects encryption is being used, consider seizing the drive for examination by a forensic expert. The investigator should make every attempt to collect as much information as to the type of encryption used and possible encryption passwords etc. whilst on-scene.

BITLOCKER ENCRYPTION

The most common encryption type that an investigator will encounter is likely to be **BitLocker.** This is a full drive encryption feature included with Microsoft Windows.

When a Device or Drive that has Bitlocker encryption enabled is added in the **Select Device to Search** window the following window will display:

Figure 20: Bitlocker drive detected.



BitLocker credentials required for H:\

The chosen device is locked with BitLocker.

Enter credentials in ***Set credentials*** before continuing

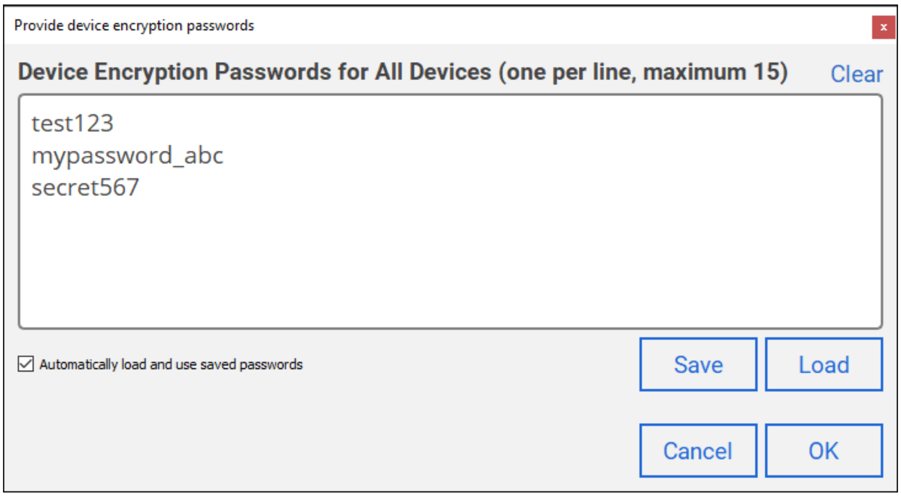
FEX Triage cannot access the data on an encrypted Bitlocker drive without a valid password. If the password is known, it can be added using the **Set Credentials** button.

SET CREDENTIALS

Clicking the **Set Credentials** button opens the **Provide device encryption passwords** window (shown in Figure 21 below). The **Set Credentials** window is used to pass encryption passwords to the FEX Triage processing engine to decrypt the target **Device** or **Drive**.

It is possible to add one or more passwords (maximum 15) to a password list. FEX Triage will try each password in the list until if finds one that will decrypt the drive.

Figure 21: Provide device encryption passwords.



Provide device encryption passwords

Device Encryption Passwords for All Devices (one per line, maximum 15)

```
test123
mypassword_abc
secret567
```

☑ Automatically load and use saved passwords

Save: The **Save** button saves the list of passwords to the file **…\bin64\device_passwords.txt**

Load: The **Load** button loads the passwords stored in **…\bin64\device_passwords.txt** to the window.

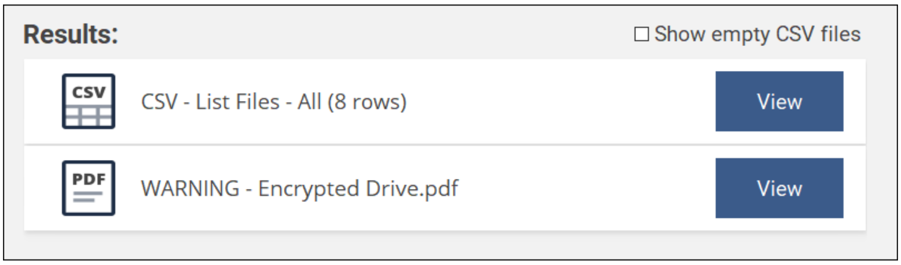
Auto…: The **Automatically load and use saved passwords** will automatically load any passwords stored in **…\bin64\device_passwords.txt** and use them in the search.

To clear passwords, click the **Clear** button and **Save** the blank. Or delete the **…\bin64\device_passwords.txt** passwords file.

RUNNING A SEARCH ON AN ENCRYPTED DRIVE

A search must be run to determine if a drive has successfully been decrypted. Search profiles raise an alert if decryption is not successful, as shown in Figure 22 below, **Warning – Encrypted Drive.pdf**.

Figure 22: Search result alerting that a drive remains encrypted (Profile: List Files to CSV – All)



Results:

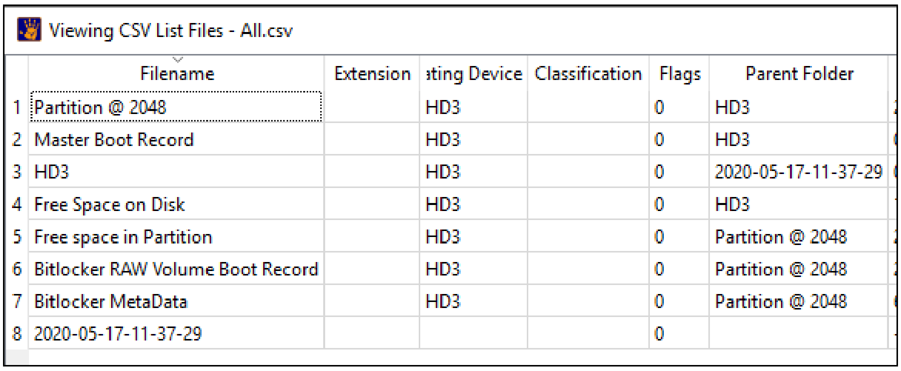
□ Show empty CSV files

CSV - List Files - All (8 rows)

WARNING - Encrypted Drive.pdf

The **CSV** output of this search is typical of an encrypted drive. The CSV lists 8 files in total (there are more than 10,000 on the decrypted drive) and the file names indicate that Bitlocker is in use:

Figure 23: CSV output of a Bitlocker encrypted drive.



Viewing CSV List Files - All.csv

	Filename	Extension	ıting Device	Classification	Flags	Parent Folder
1	Partition @ 2048		HD3		0	HD3
2	Master Boot Record		HD3		0	HD3
3	HD3		HD3		0	2020-05-17-11-37-29
4	Free Space on Disk		HD3		0	HD3
5	Free space in Partition		HD3		0	Partition @ 2048
6	Bitlocker RAW Volume Boot Record		HD3		0	Partition @ 2048
7	Bitlocker MetaData		HD3		0	Partition @ 2048
8	2020-05-17-11-37-29				0	

9.3.2 ADDING A FOLDER

To add a **Folder** to search:

1. In the **Select Device to Search** window, click on the **Add Folder** button.
2. Navigate to the required folder and click on the **Select Folder** button.
3. The folder will then appear in the list of **Devices / Paths Selected**.

9.3.3 ADD A FORENSIC IMAGE

To add a **Forensic Image** to the search:

1. In the Select Device to Search window, click on the Add Forensic Image button.
2. Navigate to the required folder and select the forensic image file.
3. The forensic image will then appear in the list of **Devices / Paths Selected**.

The following forensic image types are accepted:

Forensics Explorer supports the **analysis** of the following file formats:

Type	Extension
Apple DMG	.DMG
DD or RAW	.DD, .BIN, .RAW
EnCase®	.E01, .Ex01, .L01, .Lx01
Forensic File Format	.AFF
FTK®	.E01, .AD1
ISO	.ISO

Macquisition	.00001
Microsoft VHD	.VHD
NUIX	.MFS
ProDiscover®	.EVE
Safeback® v2	.001
SMART	.S01
VMWare®	.VMD, .VMDK
Xways Container	.CTR

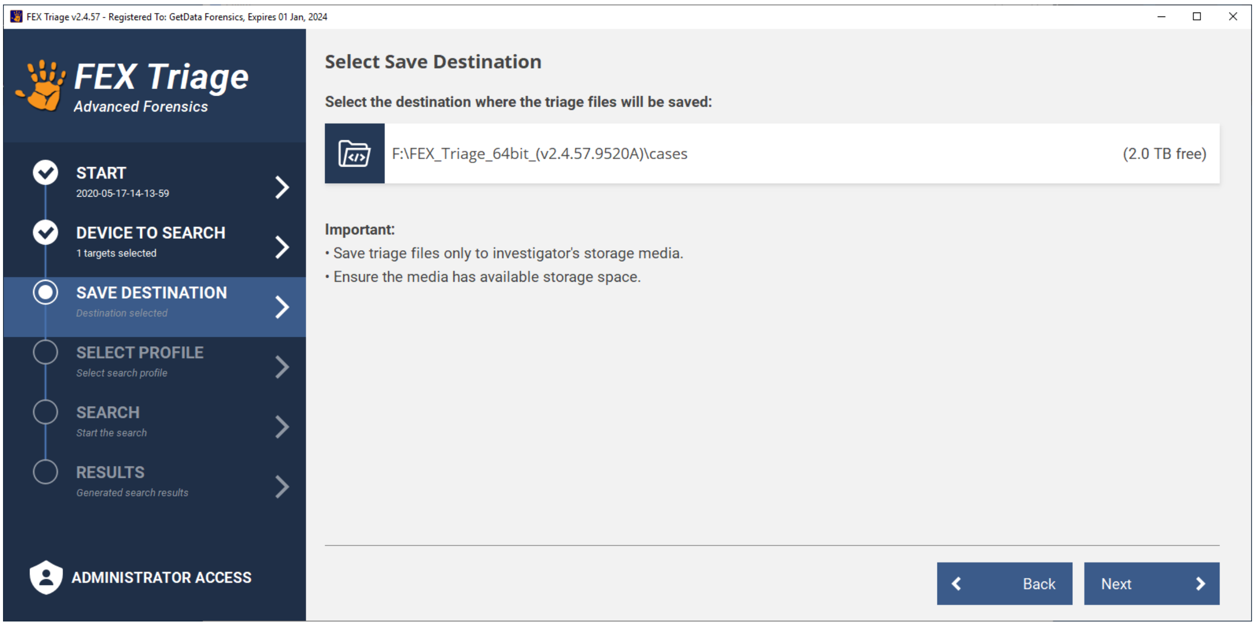
9.4 STEP 3 - SAVE DESTINATION

The **Save Destination** window is where the investigator sets the location to save the search results. By default, the save location is the **cases** folder on the same drive where FEX Triage was launched.

IMPORTANT: To maintain a forensically sound procedure, the **launch location** and the **save location** should **ONLY** be to the investigator's media. In the Figure 24 below, this is **F:\FEX_Triage_64bit_(v2.4.579520A)\cases**.

If the search profiles used involve the export of a large volume of data from the target computer, the investigator should consider the volume of available space on the save destination. In Figure 24 below, the available space is listed as **2.0 TB** (terabyte).

Figure 24: Select Save Destination



FEX Triage v2.4.57 - Registered To: GetData Forensics, Expires 01 Jan, 2024

Select Save Destination

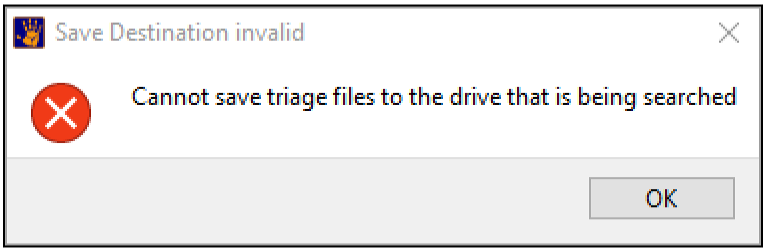
Select the destination where the triage files will be saved:

F:\FEX_Triage_64bit_(v2.4.57.9520A)\cases (2.0 TB free)

Important:
- Save triage files only to investigator's storage media.
- Ensure the media has available storage space.

FEX Triage has inbuilt protection to prohibit data being saved to a drive that is being search. If this is attempted, the following message will display:

Figure 25: Cannot save to a device being searched.



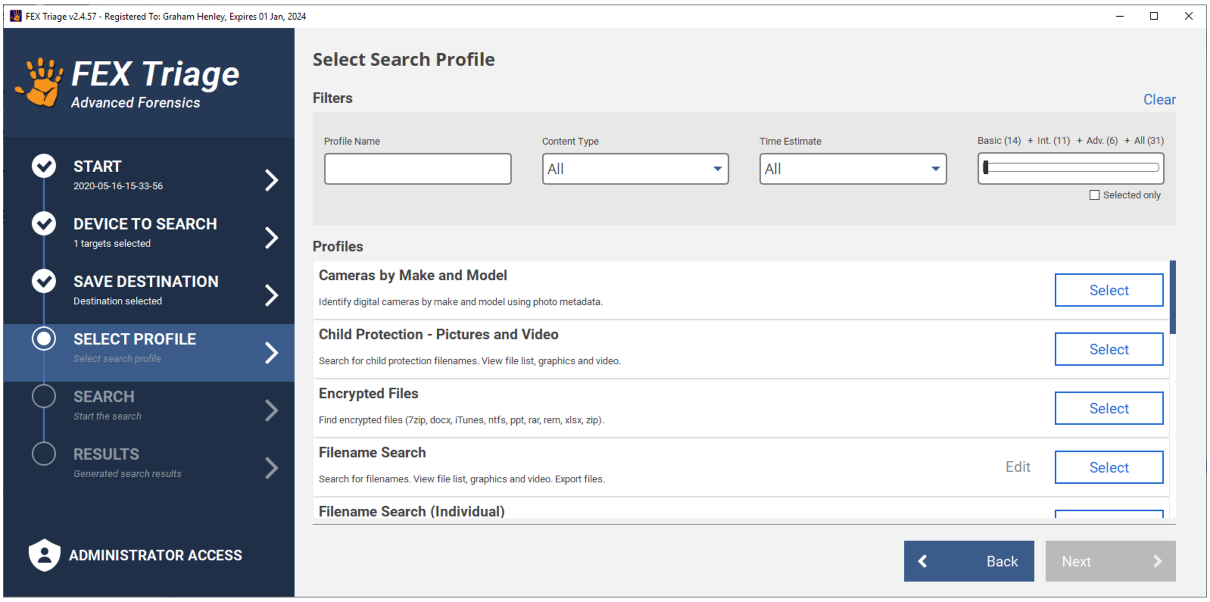
Save Destination invalid

Cannot save triage files to the drive that is being searched

9.5 STEP 4 – SELECT SEARCH PROFILE

The **Select Search Profile** window is where the investigator selects the type of search to run:

Figure 26: Select Search Profile



FEX Triage v2.4.57 - Registered To: Graham Henley, Expires 01 Jan, 2024

- START – 2020-05-16-15-33-56
- DEVICE TO SEARCH – 1 targets selected
- SAVE DESTINATION – Destination selected
- SELECT PROFILE – Select search profile
- SEARCH – Start the search
- RESULTS – Generated search results

Select Search Profile

Filters: Profile Name: (empty); Content Type: All; Time Estimate: All; Basic (14) + Int. (11) + Adv. (6) + All (31); □ Selected only

Profiles

- **Cameras by Make and Model** – Identify digital cameras by make and model using photo metadata.
- **Child Protection - Pictures and Video** – Search for child protection filenames. View file list, graphics and video.
- **Encrypted Files** – Find encrypted files (7zip, docx, iTunes, ntfs, ppt, rar, rem, xlsx, zip).
- **Filename Search** – Search for filenames. View file list, graphics and video. Export files.
- **Filename Search (Individual)**

9.5.1 AVAILABLE SEARCH PROFILES

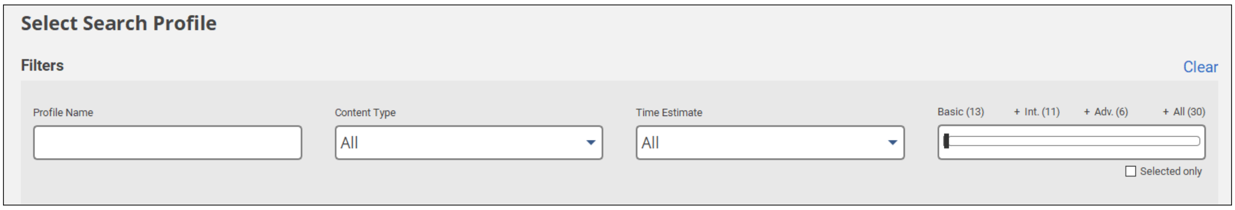
The **forensics administrator** may make specific user profiles available and viewable in the **Select Search Profile** window.

Search profiles are as **.TXML** files located in the FEX Triage **...\txml** (see **Error! Reference source not found.**). This folder has a sub-folder called **txml_not_in_use**. Any .txml file in this folder (or any other sub-folder) will not display in the profiles list (Note: When moving txml files it is necessary to restart FEX Triage for the changes to take effect).

9.5.2 FILTERING FOR A SEARCH PROFILE

The filters bar can be used to find a search profile:

Figure 27: Select Search Profile window, Filters bar.



Select Search Profile

Filters: Profile Name: (empty); Content Type: All; Time Estimate: All; Basic (13) + Int. (11) + Adv. (6) + All (30); □ Selected only

Profiles can be filters by one or more of the following criteria:

Profile Name: Dynamically filters profiles from this list based on profile name.

Content Type: Each profile is given one or more **<context_types>** in the txml. Selecting from the drop-down menu will display only those profiles containing that type.

Time Estimate: This is an estimation of how long the profile takes to run. It is an estimate only can vary according to factors such as:

- The target computer hardware.
- The size of the device or drive being searched.

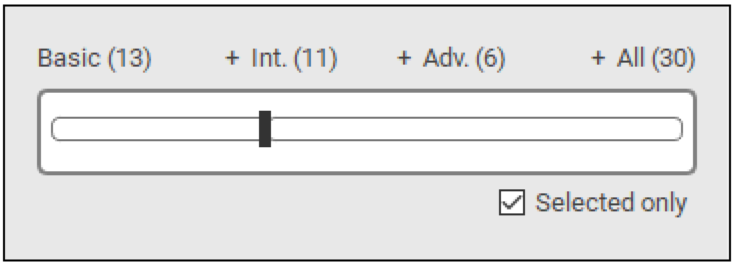
The time estimate does **not** factor in the time take to export data.

Search Level: Search profiles are given a <complexity> rating in the txml:

Basic:		Requires no (or minimal) input by the operator.
Intermediate:	Int.	Can require input by the operator and more in-depth knowledge as to the scope of the profile.
Advanced:	Adv.	Require input by the operator and knowledge of functions such as RegEx.

The slide bar enables the filter of basic, intermediate or advanced. If **selected only** is check the slide-bar is **exclusive**. If unchecked, the slide-bar is cumulative.

Figure 28: Profile filter slide bar

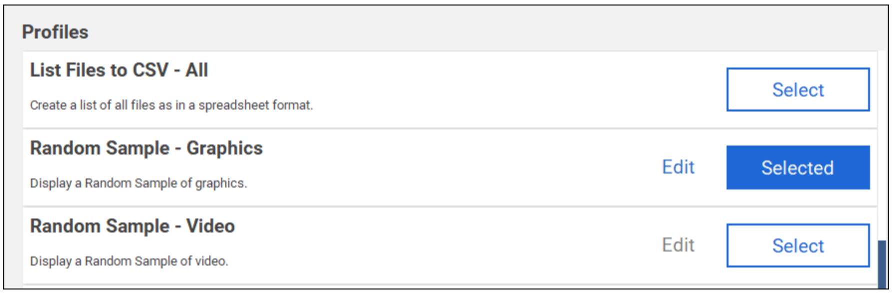


9.5.3 SELECTING A SEARCH PROFILE

To select a search profile:

1. Highlight the search profile in the list.
2. Press the **Select** button so that it turns solid blue (as shown in Figure 29 below).

Figure 29: Selecting a Search Profile



Profiles

List Files to CSV - All
Create a list of all files as in a spreadsheet format.

Random Sample - Graphics
Display a Random Sample of graphics.

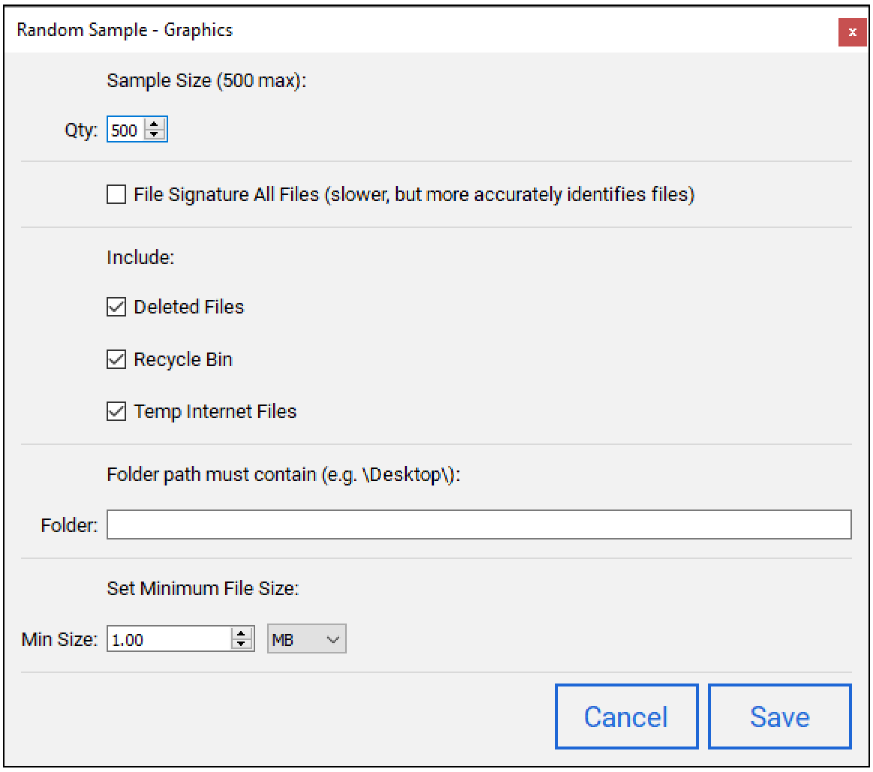
Random Sample - Video
Display a Random Sample of video.

9.5.4 SEARCH PROFILES REQUIRIING USER INPUT (EDIT)

A search profile that requires user input as and **Edit** link to the left of the select button:

1. Ensure that the desired profile is selected.
2. Click the **Edit** link to the left of the **Selected** button.
3. The **input form** will display:

Figure 30: Profile Input Form (Random Sample - Graphics)



Random Sample - Graphics

Sample Size (500 max):

Qty: 500

□ File Signature All Files (slower, but more accurately identifies files)

Include:

☑ Deleted Files

☑ Recycle Bin

☑ Temp Internet Files

Folder path must contain (e.g. \Desktop\):

Folder:

Set Minimum File Size:

Min Size: 1.00 MB

The values entered into the input form are passed to the processing engine.

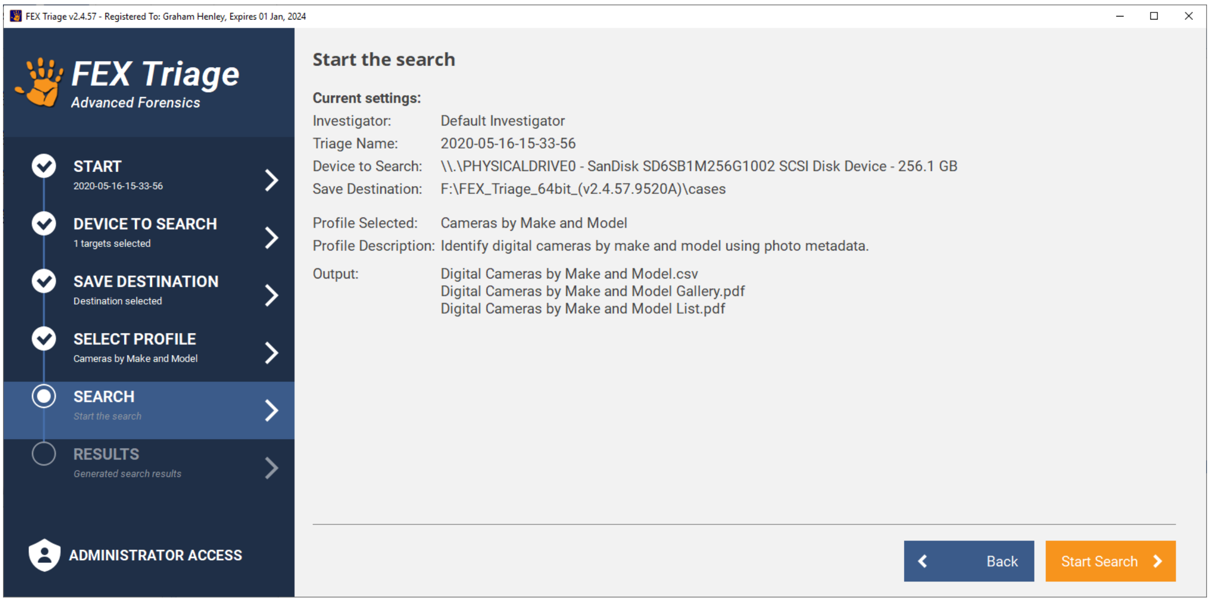
9.6 STEP 5 - START THE SEARCH

The Start the **Start the search** window summarizes the configuration of the search. This includes:

- Investigator name
- Triage name
- Device to search.
- Save destination.
- Selected search profile
- Types of search output

When the investigator is satisfied with the search configuration, press the **Start Search** button to commence the search.

Figure 31: Start the search.



Start the search

Current settings:

Investigator: Default Investigator
Triage Name: 2020-05-16-15-33-56
Device to Search: \\.\PHYSICALDRIVE0 - SanDisk SD6SB1M256G1002 SCSI Disk Device - 256.1 GB
Save Destination: F:\FEX_Triage_64bit_(v2.4.57.9520A)\cases

Profile Selected: Cameras by Make and Model
Profile Description: Identify digital cameras by make and model using photo metadata.

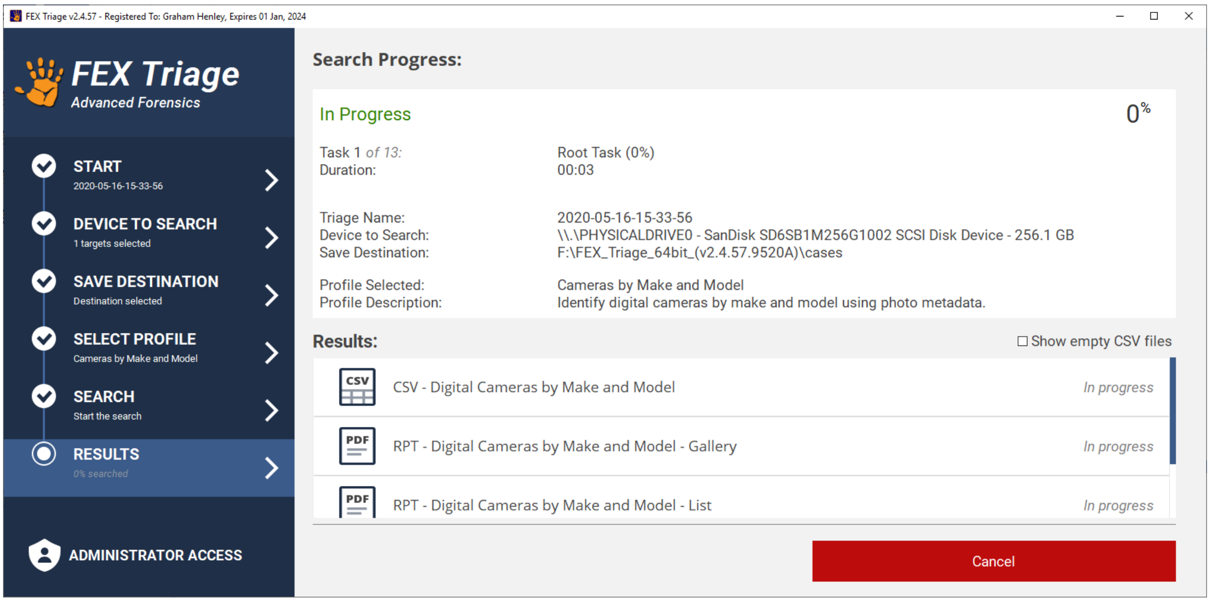
Output: Digital Cameras by Make and Model.csv
Digital Cameras by Make and Model Gallery.pdf
Digital Cameras by Make and Model List.pdf

9.7 STEP 6 – SEARCH PROGRESS AND RESULTS

9.7.1 SEARCH PROGRESS

The progress of the search can be tracked in the **Search Progress** window. A running search will have **In Progress** status, as shown in Figure 32 below:

Figure 32: Search Progress and Results



FEX Triage v2.4.57 - Registered To: Graham Henley, Expires 01 Jan, 2024

Search Progress:

In Progress 0%

Task 1 *of 13:* Root Task (0%)
Duration: 00:03

Triage Name: 2020-05-16-15-33-56
Device to Search: \\.\PHYSICALDRIVE0 - SanDisk SD6SB1M256G1002 SCSI Disk Device - 256.1 GB
Save Destination: F:\FEX_Triage_64bit_(v2.4.57.9520A)\cases

Profile Selected: Cameras by Make and Model
Profile Description: Identify digital cameras by make and model using photo metadata.

Results: □ Show empty CSV files

CSV - Digital Cameras by Make and Model *In progress*
RPT - Digital Cameras by Make and Model - Gallery *In progress*
RPT - Digital Cameras by Make and Model - List *In progress*

9.7.2 CANCELLING A SEARCH IN PROGRESS

To cancel a search in progress:

1. Click the red **Cancel** button.
2. The **Search Progress** status will change to **Cancelled** (red).

The point at which the search is cancelled will determine what data has been written to the FEX Triage case folder.

9.7.3 A COMPLETED SEARCH

When a search is complete:

- Search progress (green) will display **Finished 100%**
- The button will change to **New Search** (orange).

At this point the FEX Triage case has been saved in the destination path.

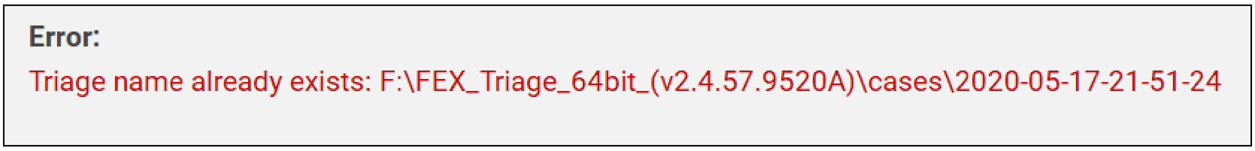
9.7.4 LAUNCHING A NEW SEARCH FROM THE RESULTS WINDOW

To launch a new search from the **Search Progress/Results** window:

1. Click on the **New Search** button (orange). This will return the user to the **Start** window where the user can begin configuration of the new search.

Or,

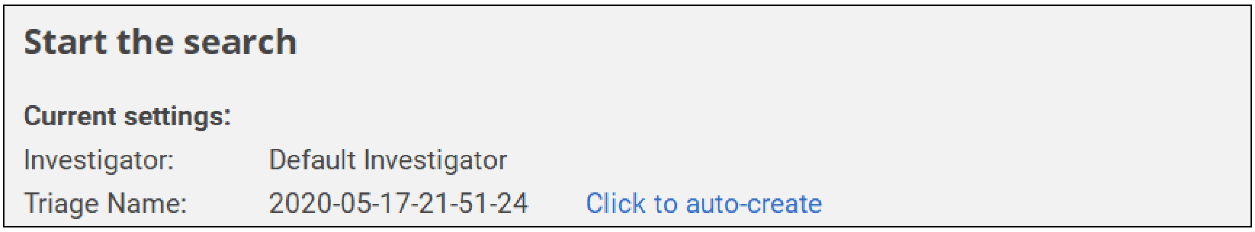
1. Select a screen from the left-hand menu, e.g., **Select Profile**, and begin the configuration again from that point in the process.
2. If this option is used, when the investigator reaches the **Start the Search** window, if the triage name already exists from the previous search the following error will be displayed:



Error:

Triage name already exists: F:\FEX_Triage_64bit_(v2.4.57.9520A)\cases\2020-05-17-21-51-24

3. A new case name can be auto created in the **Start the Search** window by clicking the **click to auto-create** link:



Start the search

Current settings:

Investigator: Default Investigator

Triage Name: 2020-05-17-21-51-24 Click to auto-create

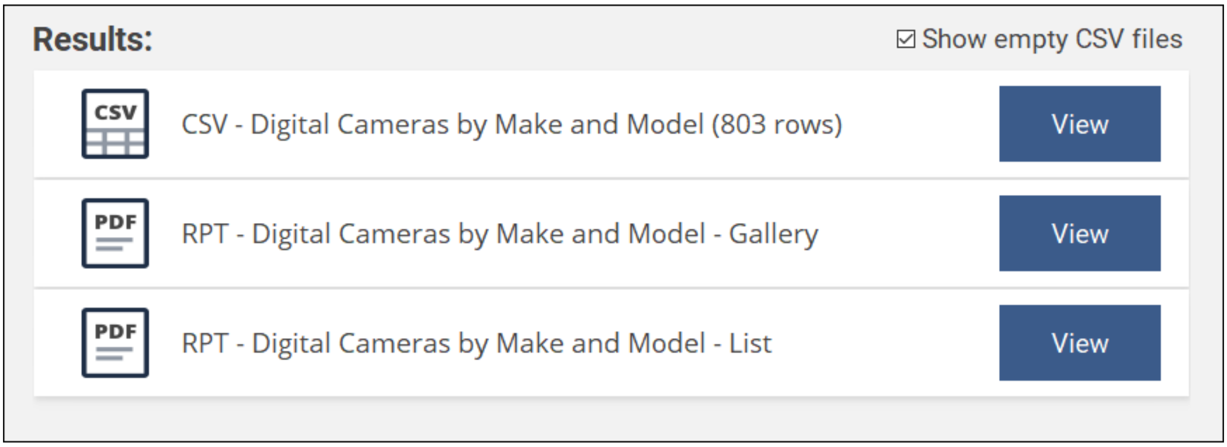
Or the user can click **Start** to return to this window and enter a new triage name.

9.7.5 VIEWING SEARCH RESULTS

A FEX Triage profile is divided into tasks. If a task has visible output (e.g., a CSV, or PDF) the output is visible even as remaining tasks in the profile are still running. This gives the investigator real time feedback without the need for the entire search to have completed.

Output is visible when a row in the **results** table changes from a ***in progress*** status to a solid blue **View** button, as shown in Figure 33 below:

Figure 33: Results Table (Search Profile Cameras by Make and Model shown)



Results: ☑ Show empty CSV files

CSV	CSV - Digital Cameras by Make and Model (803 rows)	View
PDF	RPT - Digital Cameras by Make and Model - Gallery	View
PDF	RPT - Digital Cameras by Make and Model - List	View

IMPORTANT: The result view capability of FEX Triage is intended to give the FEX Triage user real time feedback as to the outcome of the search. To maintain a forensically sound procedure it is important that any detailed examination of results or files exported from the target computer, be conducted on the investigators forensic computer and **NOT** the target system being searched.

Results are created in the following formats:

CSV (COMMA SEPARATED VALUES)

CSV is a file format that stores records in rows and columns, such as a spreadsheet. FEX Triage uses its own internal viewing software to display the CSV when the view button is clicked (CSV files can be opened on the investigators computer with programs like Microsoft Excel).

CSV files are used in FEX Triage to provide the investigator with lists of files (usually a list of files from the target computer that is the result of a specific search). An example is shown in Figure 34 below.

A CSV file in the results table means that the file of the same name has been created on the FEX Triage disk. The CSV output path is coded into the Search Profile (.txml). The standard output path is:

...\FEX_Triage_64bit_(vX.X.X.XXXXX)\cases\[triage name]\Reports\

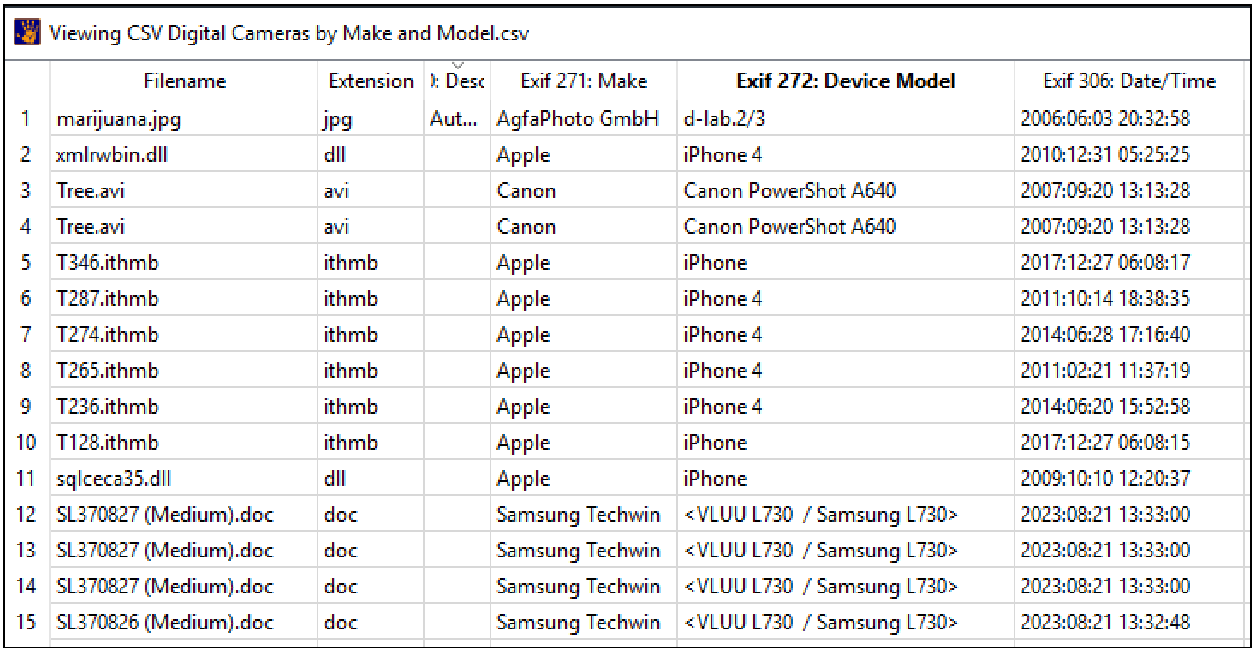
Or,

...\FEX_Triage_64bit_(vX.X.X.XXXXX)\cases\[triage name]\Exported\

The Results table will specify the number of rows contained in the CSV file (e.g., 803 rows are found in Figure 33 above). CSV output where 0 rows are found are not displayed unless the **Show empty CSV files** checkbox is ticked.

Note: CSV columns are specified in the Search Profile (.txml) and can be customized on request.

Figure 34: CSV Output (Search Profile Cameras by Make and Model shown)



Viewing CSV Digital Cameras by Make and Model.csv

	Filename	Extension	): Desc	Exif 271: Make	Exif 272: Device Model	Exif 306: Date/Time
1	marijuana.jpg	jpg	Aut...	AgfaPhoto GmbH	d-lab.2/3	2006:06:03 20:32:58
2	xmlrwbin.dll	dll		Apple	iPhone 4	2010:12:31 05:25:25
3	Tree.avi	avi		Canon	Canon PowerShot A640	2007:09:20 13:13:28
4	Tree.avi	avi		Canon	Canon PowerShot A640	2007:09:20 13:13:28
5	T346.ithmb	ithmb		Apple	iPhone	2017:12:27 06:08:17
6	T287.ithmb	ithmb		Apple	iPhone 4	2011:10:14 18:38:35
7	T274.ithmb	ithmb		Apple	iPhone 4	2014:06:28 17:16:40
8	T265.ithmb	ithmb		Apple	iPhone 4	2011:02:21 11:37:19
9	T236.ithmb	ithmb		Apple	iPhone 4	2014:06:20 15:52:58
10	T128.ithmb	ithmb		Apple	iPhone	2017:12:27 06:08:15
11	sqlceca35.dll	dll		Apple	iPhone	2009:10:10 12:20:37
12	SL370827 (Medium).doc	doc		Samsung Techwin	<VLUU L730 / Samsung L730>	2023:08:21 13:33:00
13	SL370827 (Medium).doc	doc		Samsung Techwin	<VLUU L730 / Samsung L730>	2023:08:21 13:33:00
14	SL370827 (Medium).doc	doc		Samsung Techwin	<VLUU L730 / Samsung L730>	2023:08:21 13:33:00
15	SL370826 (Medium).doc	doc		Samsung Techwin	<VLUU L730 / Samsung L730>	2023:08:21 13:32:48

PDF (PORTABLE DOCUMENT FORMAT)

PDF is a read only document format that is used to view both text and pictures. FEX Triage uses its own internal viewing software to display CSV and PDF results. It does not use software installed on the target computer.

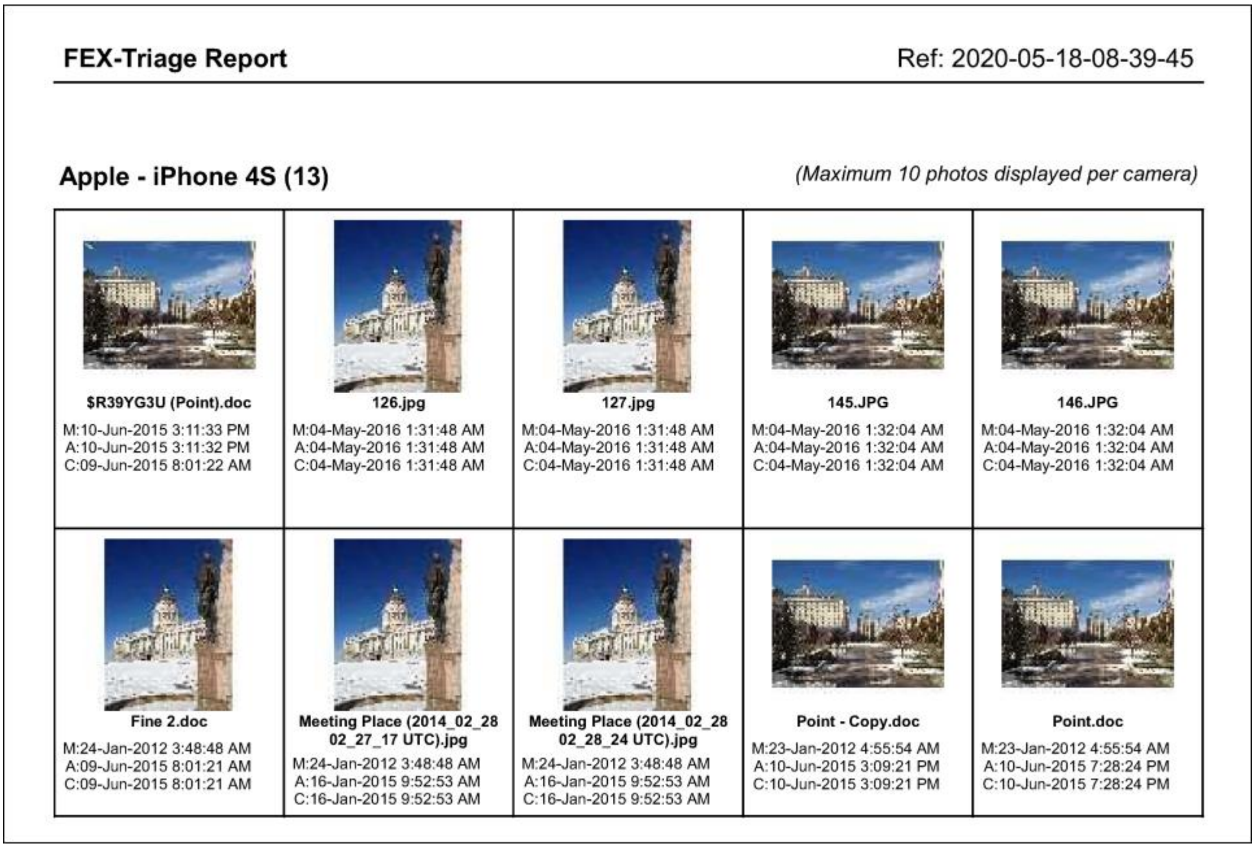
A PDF file in the results table means that the file of the same name has been created on the FEX Triage disk. The PDF output path is coded into the Search Profile (.txml). The standard output path is:

...\FEX_Triage_64bit_(vX.X.X.XXXXX)\cases\[triage name]\Reports\

PDF reports are customizable and can be tailored to an organizations specific need.

Generating a gallery view PDF is resource intensive. In order to maintain processing speed gallery reports are usually limited to 500 pictures. If the number of files found is greater than 500 a random sample is used.

Figure 35: FEX Triage PDF Report (Search Profile Cameras by Make and Model shown)



FEX-Triage Report

Ref: 2020-05-18-08-39-45

Apple - iPhone 4S (13)

(Maximum 10 photos displayed per camera)

$R39YG3U (Point).doc M:10-Jun-2015 3:11:33 PM A:10-Jun-2015 3:11:32 PM C:09-Jun-2015 8:01:22 AM	**126.jpg** M:04-May-2016 1:31:48 AM A:04-May-2016 1:31:48 AM C:04-May-2016 1:31:48 AM	**127.jpg** M:04-May-2016 1:31:48 AM A:04-May-2016 1:31:48 AM C:04-May-2016 1:31:48 AM	**145.JPG** M:04-May-2016 1:32:04 AM A:04-May-2016 1:32:04 AM C:04-May-2016 1:32:04 AM	**146.JPG** M:04-May-2016 1:32:04 AM A:04-May-2016 1:32:04 AM C:04-May-2016 1:32:04 AM
Fine 2.doc M:24-Jan-2012 3:48:48 AM A:09-Jun-2015 8:01:21 AM C:09-Jun-2015 8:01:21 AM	**Meeting Place (2014_02_28 02_27_17 UTC).jpg** M:24-Jan-2012 3:48:48 AM A:16-Jan-2015 9:52:53 AM C:16-Jan-2015 9:52:53 AM	**Meeting Place (2014_02_28 02_28_24 UTC).jpg** M:24-Jan-2012 3:48:48 AM A:16-Jan-2015 9:52:53 AM C:16-Jan-2015 9:52:53 AM	**Point - Copy.doc** M:23-Jan-2012 4:55:54 AM A:10-Jun-2015 3:09:21 PM C:10-Jun-2015 3:09:21 PM	**Point.doc** M:23-Jan-2012 4:55:54 AM A:10-Jun-2015 7:28:24 PM C:10-Jun-2015 7:28:24 PM

10. SEARCH PROFILES

FEX Triage search profiles are created using a combination of:

- FEX Triage GUI input.
- Processing tasks specified in the profile .txml file.
- Filters and scripts; and
- Report templates.

Custom profiles can be provided upon request by contacting support@getdata.com.

10.1 REMOVING A SEARCH PROFILE FROM DISPLAY

To remove a profile from the FEX Triage interface:

- Move the .\txml\[profile name].txml file into the subfolder txml_not_in_use.
- Or by deleting the relevant txml file: **...\txml\[profile name].txml**.

Note: When changes are made to the txml files the FEX Triage GUI must be re-launched for the changed to take effect.

10.2 DEFAULT SEARCH PROFILES

The following default search profiles are provided with FEX Triage:

10.2.1 BASIC

Search Profile Name	Rated	Purpose	Input
Cameras by Make Model	Basic	Identified cameras using the metadata contained in photos (e.g., Make/Model).	
Child Protection - Pictures and Video	Basic	Locates pictures and video by commonly used CAM filenames.	
Encrypted Files	Basic	Identifies encrypted files for common file formats (7zip, docx, iTunes, NTFS, ppt, rar, rem, xlsx, zip).	
Filename Search	Basic	Custom search for filenames. Includes Quick Add for file categories. Options to filter by size.	Y
Filename Search - Individual	Basic	Custom search for filenames added one by one.	Y
Internet - Browsers	Basic	Internet browser history.	
Internet - Chat	Basic	Extract chat records from common chat applications.	
Internet - Mobile	Basic	Extract cell phone data from cell phone backups (e.g., iTunes)	
ITunes Backup	Basic	Extracts iTunes backup information. Can identify devices, phone numbers, IMEI etc.	
Memory Acquisition	Basic	Acquires RAM of the target computer to a DD image.	
Random Sample - Graphics	Basic	Provides a random sample of graphics. Options to set filters for size and location.	
Random Sample - Video	Basic	Provides a random sample of video. Options to set filters for size and location.	
Registry - Current	Basic	Extracts information from the current Windows registry files. Identifies usernames, last used documents, last login time, USBs etc.	
Windows - Thumbnails	Basic	Extract pictures from thumbnail cache.	

10.2.2 INTERMEDIATE

Search Profile Name	Rated	Purpose	Input
Email – Attachments (EDB, Mbox, OST, PST)	Int.	List email attachments.	
Email - Find Messages	Int.	Search for email message using Subject, From, To and other filter options.	Y
Email - Keyword Search (EDB, Mbox, OST, PST)	Int.	Email body keyword search.	Y
Export – Extensions (Checkbox)	Int.	Select and export files by extension.	Y
Export – Windows System (Checkbox)	Int.	Select and export system files.	Y
Filename Search (Exact)	Int.	Search for files names using an exact match	Y
Hash Match (Auto) – Graphics and Video	Int.	Will apply all hash sets located in the folder …\hashsets\auto\	
Keyword Search – MS Office	Int.	Keyword search MS Office documents (doc, docx, ppt, pptx, xlsx)	Y
Operating System Artifacts	Int.	Extracts Operating System artifacts for MAC and Windows	
Random Sample - Graphics	Int.	Randomly selects up to five hundred graphics with filter options and gallery display.	
Windows – Shortcuts (.lnk)	Int.	Extracts information for Windows shortcut files. Can indicate other devices that have been connected to the computer.	

10.2.3 ANCED

Search Profile Name	Rated	Purpose	Input
Email – Find Messages (Regex)	Adv.	Search for email messages (EDB, Mbox, OST, PST) using regex.	Y
Export – Custom Global Search	Adv.	Use a global search pattern to locate and export files.	Y
Filename Search (Regex)	Adv.	Filename search using regex.	Y
Hash Match (Checkbox) – Graphics and Video	Adv.	Will add to the checkbox list any hash-set in …\hashsets\ (except for \excluded\)	Y
Hash Match (Hard-Coded) – Graphics and Video	Adv.	Hash match using hash sets hard coded into the profile txml.	Y
List Files to CSV – Custom Global Search	Adv.	List files to CSV.	Y

10.3 PROFILES TO EXPORT DATA

There are generally four available options available in profiles that can export data:

1. None
2. Do Not Export – Calculate Space Required
3. Export to L01
4. Export to Disk – Without Folder Structure
5. Export to Disk – With Folder Structure

It is generally prudent to first run a search that calculates the space required for export before running the search that actually exports the data.

The L01 format is considered the most forensically sound option as it preserves the attributes of the files inside the forensic L01 container.

The advantage of exporting directly to the investigators disk is that it sequentially exports files. If time is limited and it may be necessary to end the triage on short notice, this can be the most reliable way of collecting data up to the point where the search is terminated.

10.4 HASH MATCH PROFILES

A **hash** is a calculation that creates a digital fingerprint for a file. A **hash-set** is a collection of hashes.

A hash-set can be used to positively identify specific files and are commonly used in the fight against child-pornography. Your forensic administrator will provide relevant hash-sets.

The default search profiles:

Hash Match (Auto) – Graphics and Video	Will apply all hash sets located in the folder …\hashsets\auto\
Hash Match (Checkbox) – Graphics and Video	Will add to the checkbox list any hash-set in …\hashsets\ (except for \excluded\)

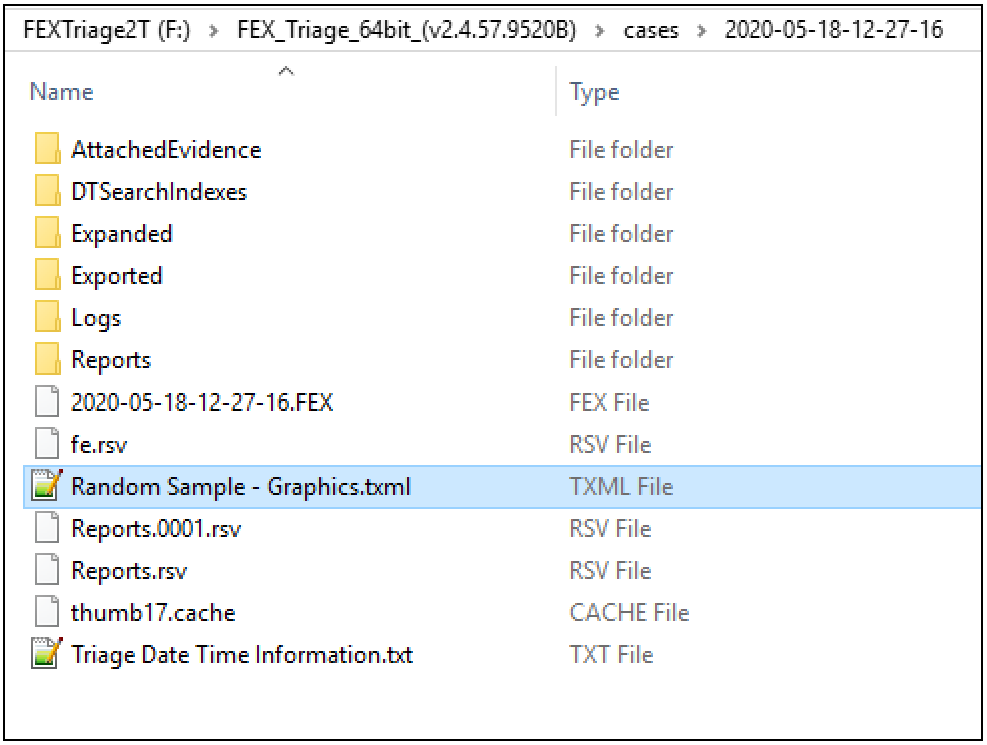
Hash-sets are an effective way to positively identify files. However, as the hash calculation is resource processing intensive, hash-set match may not suit all triage situations due to the time needed.

11. FEX TRIAGE CASE FOLDER

Each FEX Triage scan creates a forensic explorer case folder for that scan. The case folder includes:

1. [Search Profile].txml — This is the search profile .txml used to process the case;
2. Triage Date Time Information.txt — This file contains information about the target computer clock setting.
3. Reports Folder — This is usually the location for saved PDF and CSV files.
4. Exported — This is the default location for exported files (L01 and save to disk).
5. [Triage Name].FEX — This is the Forensic Explorer case file. Use the file to open the case with the Forensic Explorer GUI.

Figure 36: Forensic Explorer case folder for profile Random Sample - Graphics.txml



FEXTriage2T (F:) › FEX_Triage_64bit_(v2.4.57.9520B) › cases › 2020-05-18-12-27-16

Name	Type
AttachedEvidence	File folder
DTSearchIndexes	File folder
Expanded	File folder
Exported	File folder
Logs	File folder
Reports	File folder
2020-05-18-12-27-16.FEX	FEX File
fe.rsv	RSV File
Random Sample - Graphics.txml	TXML File
Reports.0001.rsv	RSV File
Reports.rsv	RSV File
thumb17.cache	CACHE File
Triage Date Time Information.txt	TXT File

At the completion of the FEX Triage ensure that the required case folders are backed up and secured.

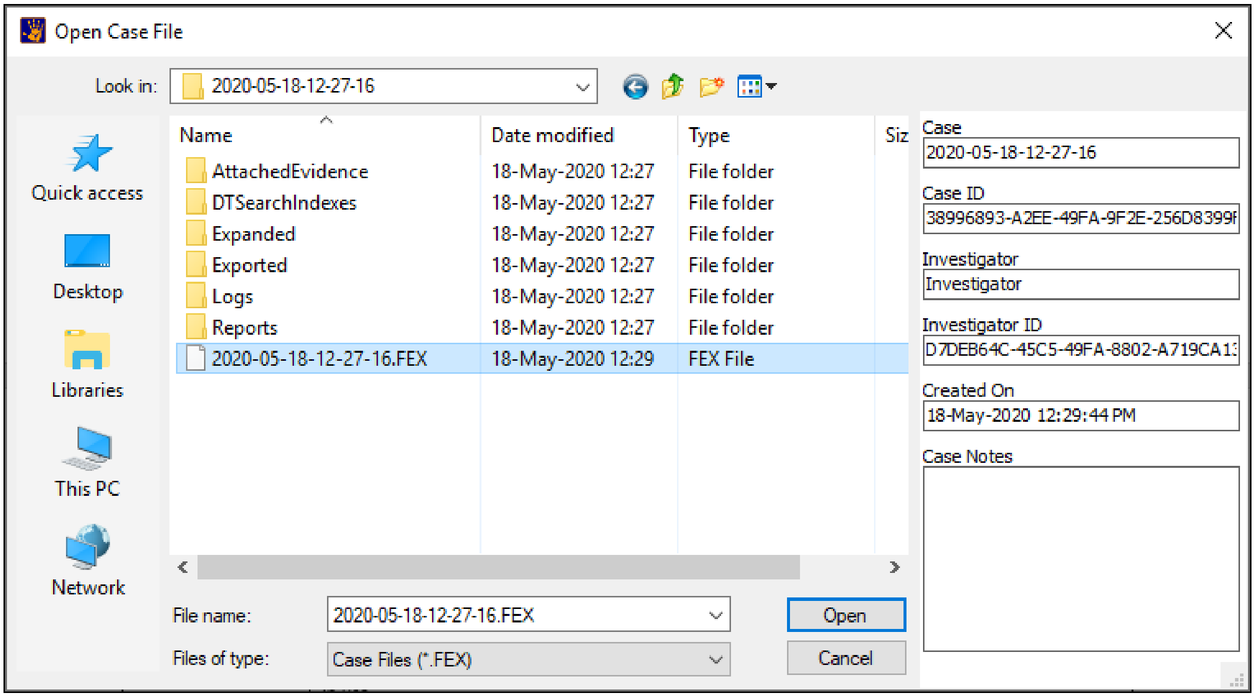
11.1 TO OPEN A FEX TRIAGE CASE IN FORENSIC EXPLORER

Licensed users of Forensic Explorer can open a FEX Triage case.

1. In the Forensic Explorer Evidence module, click the open button.

2. Navigate to the FEX Triage case folder and select the [Case Name].FEX file:

Figure 37: Opening a FEX Triage case in Forensic Explorer



Open Case File

Look in: 2020-05-18-12-27-16

Name	Date modified	Type	Siz
AttachedEvidence	18-May-2020 12:27	File folder	
DTSearchIndexes	18-May-2020 12:27	File folder	
Expanded	18-May-2020 12:27	File folder	
Exported	18-May-2020 12:27	File folder	
Logs	18-May-2020 12:27	File folder	
Reports	18-May-2020 12:27	File folder	
2020-05-18-12-27-16.FEX	18-May-2020 12:29	FEX File	

File name: 2020-05-18-12-27-16.FEX

Files of type: Case Files (*.FEX)

Case: 2020-05-18-12-27-16

Case ID: 38996893-A2EE-49FA-9F2E-256D8399F

Investigator: Investigator

Investigator ID: D7DEB64C-45C5-49FA-8802-A719CA1

Created On: 18-May-2020 12:29:44 PM

Case Notes:

The Forensic Explorer case will show FEX Triage, bookmarks, reports etc.

12. DEFINITIONS

ARM Device	An ARM device has a processor based on the RISC (reduced instruction set computer) architecture developed by Advanced RISC Machines (ARM). “ARM processors are extensively used in consumer electronic devices such as smartphones, tablets, multimedia players and other mobile devices, such as wearables. Because of their reduced instruction set, they require fewer transistors, which enables a smaller die size for the integrated circuitry (IC). The ARM processor’s smaller size, reduced complexity and lower power consumption makes them suitable for increasingly miniaturized devices.” Source: https://whatis.techtarget.com/
Boot-scan	Boot-scan refers to starting a target computer using investigators boot media (e.g., a boot USB). A boot-scan is considered a **forensically sound** process as files on the target computer system are not in use
BIOS UEFI	BIOS, computing, stands for Basic Input/Output System. The BIOS is a computer program embedded on a chip on a computer's motherboard that recognizes and controls various devices that make up the computer. The purpose of the BIOS is to make sure all the things plugged into the computer can work properly. (https://simple.wikipedia.org/wiki/BIOS). BIOS is being phased out by computer manufactures and replaced with a new method called UEFI (Unified Extensible Firmware Interface). UEFI supports larger hard drives, faster boot times, and more security features. Unfortunately, many PC manufactures continue to refer to UEFI as BIOS so it can be difficult tell which is present. Most computers built from 2015 on-ward are more likely to be UEFI.
Bitlocker	A full drive encryption feature included with Microsoft Windows.
CSV	CSV is a file format that stores records in rows and columns, such as a spreadsheet. CSV files are opened by programs like Microsoft Excel. FEX Triage uses the CSV format to display lists of files in the search results screen. FEX Triage CSV files are usually saved to the folder ...\cases\[triage name]\Reports\.
Desktop-scan	Desktop-scan is used to describe the launch of FEX Triage from the investigator’s forensic computer. The forensic computer can be used to triage stand-alone

	devices, e.g., hard drives, USB drives, camera cards, etc. (typically connected using a write-blocking device).
Device	Device refers to a physical device like a hard drive or a camera card. A device can have one or more drives on it, for example a hard drive device can be partitioned to have drives C:\, D:\, E:\ etc. In FEX Triage the most comprehensive search will be when the device is selected, because this will include all drives located on the device.
Drive	A drive refers to a partition located on a physical device. For example, a hard drive device can be partitioned to have drive C:\, D:\, E:\ etc. When a drive is selected in FEX Triage it is only that drive that is searched.
Forensic Image	A "forensic image is a file (or set of files), is used to preserve an exact "bit-forbit" copy of data residing on digital media. The most used format is .E01 by Guidance Software (www.guidancesoftware.com). The image contains all data, including deleted and system files, ad 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. FEX Triage can examine forensic image files.
Forensically Sound	Digital evidence by its very nature is volatile. The term forensically sound refers to the accepted industry principle that maintaining the integrity of digital evidence is paramount, and that no action by the investigator should change data that is to be relied upon. FEX Triage examines and collects evidence in a manner that preserves the integrity of evidence and provides an audit trail so that an independent third party can examine the actions undertaken. An investigator should also apply standard principles of crime-scene preservation (photographs, documentation, etc.) to any matter involving digital evidence.
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.; and **Bad Hash Sets**: virus files, malware, Trojans, child pornography, Steganography, hacking tools etc.
Live scan	Live scan refers to launching FEX Triage to scan a live computer running Microsoft Windows. In many cases will be the most appropriate action due to concerns about powering down a running system, for example: • Encryption or disk wiping software will be activated. • The system is critical to an individual or business. The investigator must be aware that insertion of the FEX Triage USB device on a live system will leave a trace on the computer relating to the insertion of the FEX Triage USB device.
.L01 File	A .L01 file (also commonly referred to as a logical evidence file or LEF) is a forensic file format created by Guidance Software (www.guidancesoftware.com). FEX Triage can export files from a target computer system into a L01 file whilst preserving the integrity of the original file information (dates, times, size, etc.). A .L01 is usually used to store a selection of files, rather than a copy of an entire drive, for which the Guidance Software .E01 format is most frequently used.
RPT (Report)	RPT is the abbreviation for Report. FEX Triage creates reports as PDF files, and they are usually saved into the folder ...\cases\[triage name]\Reports\.
Search Profile	FEX Triage uses pre-configured search profiles to perform specific tasks.
Set Credentials	The Set Credentials button the **Device to Search** window is used to add passwords to decrypt a Bitlocker device or drive. Up to fifteen passwords may be added to this list.
Signature Analysis	Signature analysis compares a files header (the starting bytes of the file) with its extension. 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. Some files, such as iTunes backups, do not have an extension so can only be accurately identified by a signature analysis. FEX Triage automatically run signature analysis in a profile when it is deemed necessary. At other times it may present signature analysis as a checkbox option to the end user.

	Signature analysis requires processing. As a result, it slows down process. It is recommended that a search first be run without signature analysis (for speed purposes). If it returns a negative result the investigator can then select to run a second more intensive search.
UEFI	See BIOS / UEFI.
Wibu Codemeter Dongle	Wibu (https://www.wibu.com/) is a company that specialize in software licensing. FEX Triage uses the Wibu licensing system to activate FEX Triage for the end user. FEX Triage uses a physical Wibu Codemeter USB3 dongle that contains the license, and the dongle must be plugged in for the software to run. The Wibu dongle also has standard USB storage space (16, 32 or 64 gigabyte versions) and FEX Triage can be launched directly from this device.
WinFE	Windows Forensic Environment (WinFE) is a lightweight forensic USB boot system based on the Windows Preinstallation Environment. For more information about WinFE visit: • https://www.winfe.net/home • https://winfe.wordpress.com/2020/04/06/mini-winfe-10-and-winfe-10-updated/

13. LICENSE AGREEMENT

GetData® Forensics Pty Ltd (“GetData”) – ACN: 143458039

IMPORTANT – END USER LICENSE AGREEMENT

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT (“AGREEMENT”) CAREFULLY BEFORE USING FORENSIC EXPLORER (“the SOFTWARE”). BY USING THE SOFTWARE, YOU ARE AGREEING TO BE BOUND TO THE TERMS AND CONDITIONS OF THIS LICENSE SET OUT BELOW. IF YOU DO NOT AGREE TO BE BOUND BY THE TERMS AND CONDITIONS SET OUT BELOW, DO NOT INSTALL AND/OR USE THE SOFTWARE. PLEASE TERMINATE INSTALLATION IMMEDIATELY AND DO NOT USE THE SOFTWARE.

1. Software Covered by This License

1.1. This license agreement applies only to the version of the Forensic Explorer software package with which this agreement is included. Different license terms may apply to other software packages from GetData and license terms for later versions of Forensic Explorer may also be changed.

2. General

2.1. GetData is and remains the exclusive owner of the Software. You acknowledge that copyright in the Software remains at all times with GetData.

2.2. The Software and any other materials included under this license, are licensed, not sold to you by GetData for use only under the terms of this Agreement.

2.3. GetData or its licensors own the Software, including all materials included with this package. GetData owns the names and marks of ‘GetData,’ and ‘Forensic Explorer’ under copyright, trademark and intellectual property laws and all other applicable laws.

3. Permitted License Uses and Restrictions

3.1. Subject to the terms and conditions of this License, a single License of the Software permits you to run a single Licensed instance of the Software. Where multiple Licenses have been purchased, the License permits you to run concurrent instances of the Software equal to the number of Licenses purchased.

3.2. You are solely responsible for the protection of your data, your systems and your hardware used in connection with the Software. GetData will not be liable for any loss or damage suffered from the use of the Software.

3.3. You and others are not permitted to copy (except as expressly permitted by this Agreement), decompile, reverse engineer, disassemble, attempt to derive the source code of, decrypt, modify (except to the extent allowed in the documentation accompanying this Agreement) or remove or alter any proprietary legends contained in the Software.

3.4. You are not permitted to share the product activation information provided to you for this Software with other users.

3.5. You may not publicly display the Software or provide instruction or training for compensation in any form without the express written permission of GetData.

3.6. GetData reserves the right to check any and all license details at any time in any reasonable manner.

3.7. GetData may from time-to-time revise or update the Software and may make such revisions or updates available to you subject to payment of the applicable license fee.

3.8. The Software is protected under United States law and international law and international conventions and treaties. You may not rent, lease, lend, sell, redistribute or sublicense the Software without the express written permission of GetData.

3.9. If you purchase a site license, there will be terms and conditions listed in the appendix of the site license.

4. Disclaimer of Warranty

4.1. To the extent not prohibited by applicable law, by using the Software, you expressly agree that all risks associated with performance and quality of the Software is solely held by you. GetData shall not be liable for any direct, indirect, special or consequential damages arising out of the use or inability to use the software, even if GetData has been advised of the possibility of such damages.

4.2. To the extent not prohibited by applicable law, the Software is made available by GetData 'As Is' and 'With all Faults,' GetData or any GetData authorised representative does not make any representations or warranties of any kind, either expressly or implied concerning the quality, safety, accuracy or suitability of the Software, including without limitation any implied warranties of merchantability, fitness for a particular purpose, non-infringement or that the Software is error free.

4.3. GetData or any GetData authorised representative makes no representations or warranties as to the truth, accuracy or completeness of any information, statements or materials concerning the Software.

4.4. No oral or written information or advice given by GetData or a GetData authorised representative shall create a warranty. Should the Software prove defective, you assume the entire cost of all necessary servicing, repair or correction. Some jurisdictions do not allow the exclusion of implied warranties or limitations on applicable statutory rights of a consumer, the above exclusions and limitations may not apply to you.

5. Limitation of Liability

5.1. To the extent not prohibited by applicable law, in no event will GetData, its officers, employees, affiliates, subsidiaries or parent organisation be liable for any direct, indirect, special, incidental, exemplary, consequential or punitive damages whatsoever relating to the use of the Software.

5.2. Any and all data obtained from the use of the Software becomes the user's sole responsibility and liability.

5.3. Any and all data obtained from the use of the Software in any civil or criminal jurisdiction that results in wrongful conviction, erroneous charges, misrepresentation of data or death or any other civil or tortious wrong against a person, company, corporation or any other entity, GetData shall bear no liability for any death, wrongful conviction or any other civil or tortious wrong against a person, company, corporation or any other entity.

5.4. Any and all data obtained from the use of the Software is the sole responsibility of the user. In the event the user misconstrues, misinterprets or misunderstands the data and causes it to be used in any and all civil or criminal jurisdictions, GetData shall bear no liability.

5.5. In no event will GetData's liability to you, whether in contract, tort (including negligence) or otherwise, exceed the amount paid by you for the License under this Agreement.

5.6. In the event that a company bearing the name of GetData operating as a separate legal entity, leases the Software to you, and you misconstrue, misinterpret or misunderstand the data that results in any wrongful conviction, erroneous charges, misrepresentation of data, death or any other civil or tortious wrong against a person, corporation or any other entity, GetData ACN: 143458039 shall bear no liability to you, the liability shall be borne by whatever company bearing the name of GetData operating as a separate legal entity.

6. Applicable Law

6.1. This Agreement and any dispute relating to the Software or to this Agreement shall be governed by the laws of the State of New South Wales and the Commonwealth of Australia, without regard to any other Country or State choice of law rules.

6.2. You agree and consent that jurisdiction and proper venue for all claims, actions and proceedings of any kind relating to GetData or the matters in this Agreement shall be exclusively in Courts located in NSW, Australia. If any part or provision of this Agreement is held to be unenforceable for any purpose, including but not limited to public policy grounds, then you agree that the remainder of the Agreement shall be fully enforceable as if the unenforced part or provision never existed. There are no third-party beneficiaries, or any promises, obligations or representations made by GetData therein.

7. Export

7.1. You acknowledge that the Software is subject to Australian export jurisdiction. You agree to comply with all applicable international and national laws that apply to the Software including destination restrictions issued by GetData.

8. Termination

8.1. This Agreement is effective on the date you receive the Software and remains effective until terminated. If you fail to comply with any and all terms set out above, your rights under this Agreement will terminate immediately without notice from GetData. GetData may terminate this Agreement immediately should any part of the Software become or in GetData's reasonable opinion likely to become the subject of a claim of intellectual property infringement or trade secret misappropriation. Upon termination, you will cease use of and destroy all copies of the Software under your control and confirm compliance in writing to GetData.

9. Entire Agreement

9.1. This Agreement constitutes the entire Agreement between you and GetData relating to the Forensic Explorer Software herein. This Agreement supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgement or other communication between the parties relating to its subject matter during the term of this Agreement. No modification, amendment or addendum to this Agreement will be binding, unless it is set out in writing and signed by an authorised representative of each party.

10. Translations

10.1. This agreement is translated into other languages. It is the English version which is the language that will be controlling in all respects. No version of this agreement other than English shall be binding or have any effect.

14. TECHNICAL SUPPORT

GetData Forensics Pty Ltd has its headquarters in Sydney, New South Wales, Australia:

Support

Documentation	https://getdataforensics.com/product/fex-triage/
Email	support@getdata.com
Support Ticket	https://login.getdata.com/
Phone Support	USA: +1.844.300.0552 x801 – Sales x802 – Support X804 – Training Australia: + +61 (0)2 8208 6053
Secure Post	GetData Forensics Pty Ltd P.O. Box 71 Engadine, New South Wales, 2233 Australia
Head Office	GetData Forensics Pty Ltd Suite 204, 13A Montgomery Street Kogarah, New South Wales, 2217 Australia

The following log files can assist with troubleshooting:

triage-runtime.log	Located in the FEX Triage root folder. This logs interaction with the FEX Triage GUI. It may contain case reference information, such as Triage Name etc.

15. APPENDIX 3 - HOT KEYS FOR BOOTMENU / BIOS SETTINGS

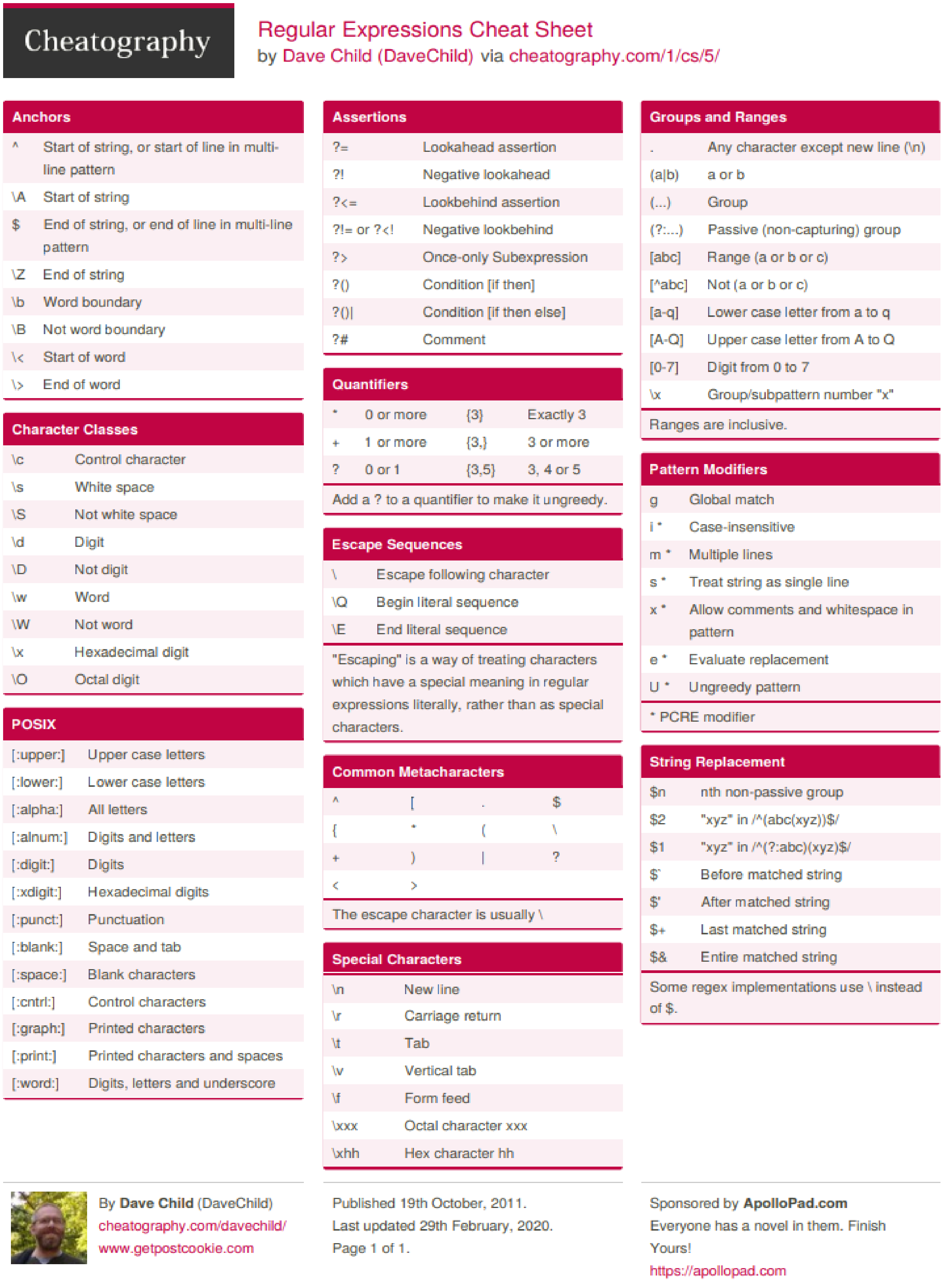
Source: WinFE, Colin Ramsden, https://www.winfe.net/use (accessed 4 June 2020)

Manufacturer	Model(s)	Boot Menu Key(s)
Acer	Generic	Esc, F12, F9
Acer	Aspire One zg5, zg8, Aspire Timeline, Aspire v3, v5, v7	F12
Asus	VivoBook f200ca, f202e, q200e, s200e, s400ca, s500ca, u38n, v500ca, v550ca, v551, x200ca, x202e, x550ca, z202e	Esc
Asus	Generic	F8
Asus	N550JV, N750JV, N550LF, Rog g750jh, Rog g750jw, Rog g750jx, Zenbook Infinity ux301, Infinity ux301la, Prime ux31a, Prime ux32vd, R509C, Taichi 21, Touch u500vz, Transformer Book TX300, Eee PC 1015, 1025c	Esc
Asus	k25f, k35e, k34u, k35u, k43u, k46cb, k52f, k53e, k55a, k60ij, k70ab, k72f, k73e, k73s, k84l, k93sm, k93sv, k95vb, k501, k601, R503C, x32a, x35u, x54c, x61g, x64c, x64v, x75a, x83v, x83vb, x90, x93sv, x95gl, x101ch, x102ba, x200ca, x202e, x301a, x401a, x401u, x501a, x502c, x750ja	F8
Compaq	Presario	Esc
Dell	Dimension, Inspiron, Latitude, Optiplex, Precision, Vostro, XPS	F12
Dell	PowerEdge Servers	F11
eMachines	Generic	F12
Fujitsu	Generic	F12
HP	Generic	Esc, F9
Intel	Generic	F10
Lenovo	Generic	F18, F10, F12
NEC	Generic	F5
Packard Bell	Generic	F8
Samsung	Generic	Esc, F12
Samsung	NC10, np300e5c, np300e5e, np350v5c, np355v5c, np365e5c, np550p5c, Series 5 Ultra, Series 7 Chronos, Series 9 Ultrabook	Escape

Sony	VAIO Duo, Pro, Flip, Tap, Fit	Assist Button
Sony	VAIO, PCG, VGN	Esc, F10, F11
Toshiba	Kira, Kirabook 13, Ultrabook, Qosmio g30, g35, g40, g50, Qosmio x70, x75, x500, x505, x870, x875, x880	F12
Toshiba	Protege, Satellite, Tecra	F12
Toshiba	Equium	F12
VMware	Workstation	Esc

See Also: Active Boot Disk: http://boot-disk.com/quest_bootmenu.htm

16. REGEX GUIDE



Cheatography

Regular Expressions Cheat Sheet
by Dave Child (DaveChild) via cheatography.com/1/cs/5/

Anchors

^	Start of string, or start of line in multi-line pattern
\A	Start of string
$	End of string, or end of line in multi-line pattern
\Z	End of string
\b	Word boundary
\B	Not word boundary
\<	Start of word
\>	End of word

Character Classes

\c	Control character
\s	White space
\S	Not white space
\d	Digit
\D	Not digit
\w	Word
\W	Not word
\x	Hexadecimal digit
\O	Octal digit

POSIX

[:upper:]	Upper case letters
[:lower:]	Lower case letters
[:alpha:]	All letters
[:alnum:]	Digits and letters
[:digit:]	Digits
[:xdigit:]	Hexadecimal digits
[:punct:]	Punctuation
[:blank:]	Space and tab
[:space:]	Blank characters
[:cntrl:]	Control characters
[:graph:]	Printed characters
[:print:]	Printed characters and spaces
[:word:]	Digits, letters and underscore

Assertions

?=	Lookahead assertion
?!	Negative lookahead
?<=	Lookbehind assertion
?!= or ?<!	Negative lookbehind
?>	Once-only Subexpression
?()	Condition [if then]
?()|	Condition [if then else]
?#	Comment

Quantifiers

*	0 or more	{3}	Exactly 3
+	1 or more	{3,}	3 or more
?	0 or 1	{3,5}	3, 4 or 5

Add a ? to a quantifier to make it ungreedy.

Escape Sequences

\	Escape following character
\Q	Begin literal sequence
\E	End literal sequence

"Escaping" is a way of treating characters which have a special meaning in regular expressions literally, rather than as special characters.

Common Metacharacters

^	[	.	$
{	*	(	\
+	)	|	?
<	>		

The escape character is usually \

Special Characters

\n	New line
\r	Carriage return
\t	Tab
\v	Vertical tab
\f	Form feed
\xxx	Octal character xxx
\xhh	Hex character hh

Groups and Ranges

.	Any character except new line (\n)
(a|b)	a or b
(...)	Group
(?:...)	Passive (non-capturing) group
[abc]	Range (a or b or c)
[^abc]	Not (a or b or c)
[a-q]	Lower case letter from a to q
[A-Q]	Upper case letter from A to Q
[0-7]	Digit from 0 to 7
\x	Group/subpattern number "x"

Ranges are inclusive.

Pattern Modifiers

g	Global match
i *	Case-insensitive
m *	Multiple lines
s *	Treat string as single line
x *	Allow comments and whitespace in pattern
e *	Evaluate replacement
U *	Ungreedy pattern

* PCRE modifier

String Replacement

$n	nth non-passive group
$2	"xyz" in /^(abc(xyz))$/
$1	"xyz" in /^(?:abc)(xyz)$/
$`	Before matched string
$'	After matched string
$+	Last matched string
$&	Entire matched string

Some regex implementations use \ instead of $.

By **Dave Child** (DaveChild)
cheatography.com/davechild/
www.getpostcookie.com

Published 19th October, 2011.
Last updated 29th February, 2020.
Page 1 of 1.

Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com