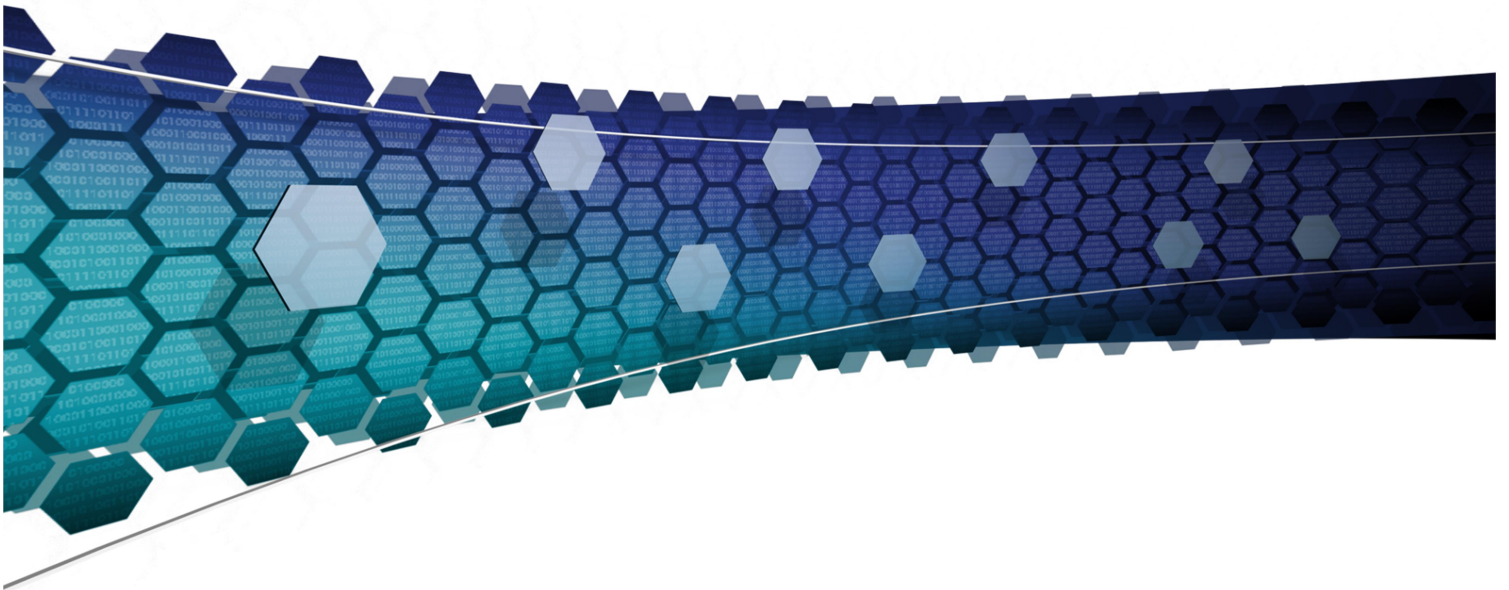




Triage Investigator

User Guide

Version 4.2



Contents

1.	INTRODUCTION	2
2.	INSTALLATION	3
3.	DATA MIGRATION TO NEW VERSIONS.....	12
4.	SUPPORTED TARGET DEVICES/OPERATING SYSTEMS.....	13
5.	USER INTERFACE	14
6.	SETTINGS	16
7.	DEFAULT SEARCH PROFILES AND CAPTURES	18
8.	PREPARING A COLLECTION KEY.....	20
9.	BIOS/UEFI	23
10.	BOOT SCAN	31
11.	LIVE SCAN	34
12.	DESKTOP SCAN	35
13.	REVIEW SCAN RESULTS	41
14.	REPORTING.....	57
15.	CUSTOM SEARCH PROFILES AND FILE CAPTURES	65
16.	FAQ.....	67
17.	GLOSSARY	68

APPENDIX A - BIOS ACCESS KEYS

APPENDIX B - REGEX CHEAT SHEET

1. Introduction

Thank you for purchasing Triage-Investigator, a new digital investigation tool built from the ground up that leverages ADF's proven track record of reducing forensic backlogs. Triage-Investigator enables you to conduct digital investigations easier, faster and smarter.

ADF Solutions is the leading provider of digital forensic and media exploitation tools. These tools are used for processing and analyzing computers, external drives, drive images, and other media storage (e.g. USB flash drives and memory cards).

ADF forensic tools are all about speed, scalability, ease-of-use, and relevant results. The tools have a proven track record in reducing forensic backlogs, streamlining digital investigations and rapid access to digital evidence and intelligence.

Triage-Investigator full kit contents are as follows:

Triage-Investigator Full Kit Contents
USB Authentication Key
USB Collection Key - Samsung T3 256GB SSD
4 Port USB Hub
Boot CD
CD Opener
Installation Reference Booklet

2. Installation

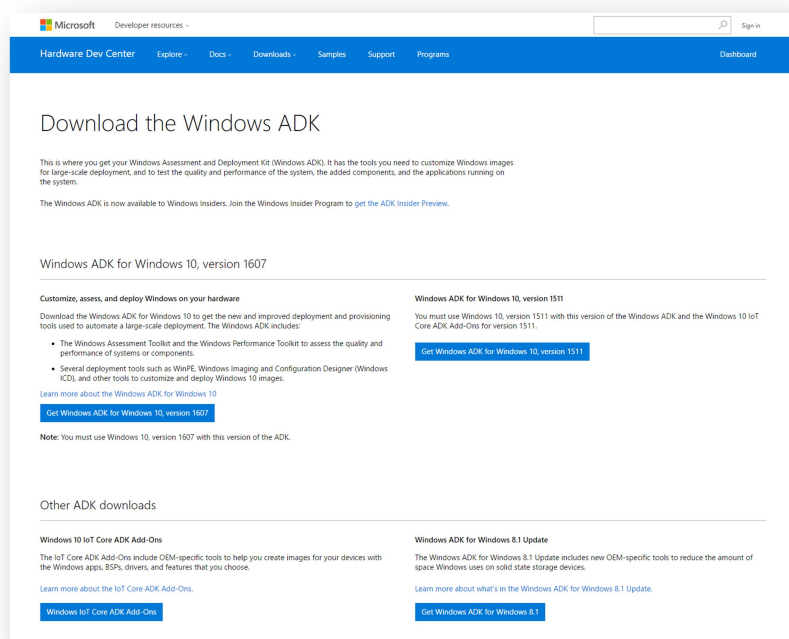
Triage-Investigator is designed to run on the following computers:

Operating System	Minimum System Requirements
Windows 7 32/64-bit	2GB of RAM, 20 GB of free hard drive space
Windows 8.1 32/64-bit	4GB of RAM, 20 GB of free hard drive space
Windows 10 32/64-bit	4GB of RAM, 20 GB of free hard drive space

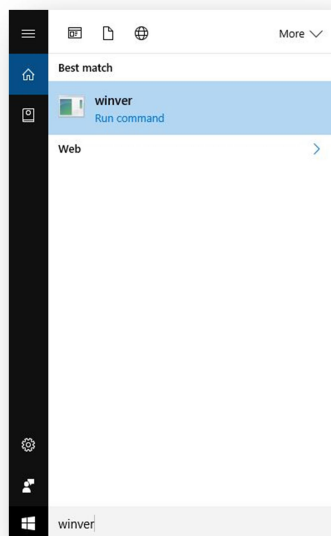
During the installation, you will be prompted to install the Microsoft Windows Assessment and Deployment Kit (WADK) 10 which is required for boot scans. In order to do this, your computer must be connected to the internet. Instructions for online installation can be found following the offline instructions. If you are installing on a computer that has no internet connection, follow the Windows ADK Offline Installation instructions first.

Offline ADK Installation

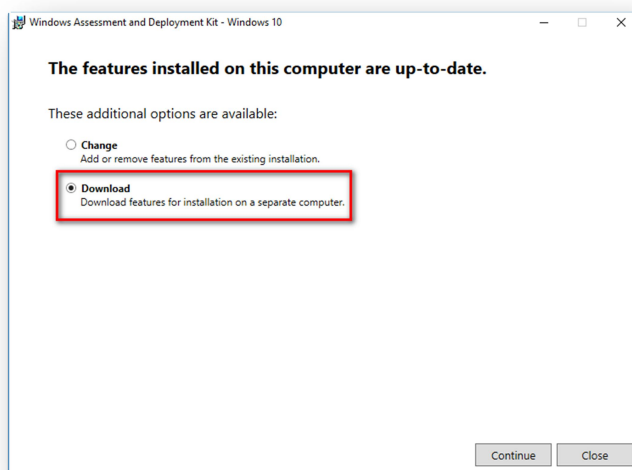
1. On a computer connected to the Internet search for “Windows ADK Downloads”
As of this printing the WADK can be found at the following location:
<https://developer.microsoft.com/en-us/windows/hardware/windows-assessment-deployment-kit>



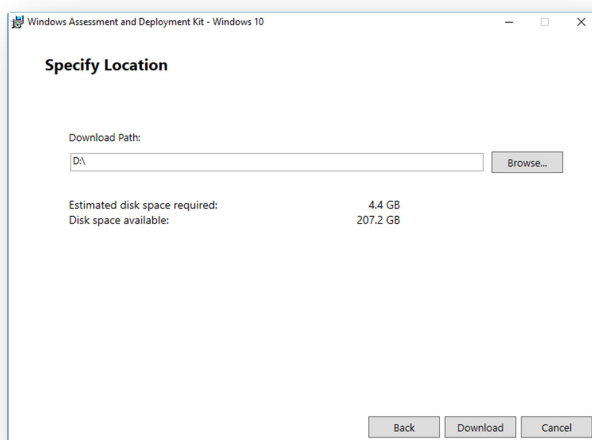
2. Download the latest ADK Installer (adksetup.exe) relevant to your version of Windows. Version 1607 of Windows 10 requires the WADK version 1607. All other versions of Windows require WADK version 1511. If you are using Windows 10 establish the installed version on your computer by pressing the Windows Key and typing winver then pressing enter.



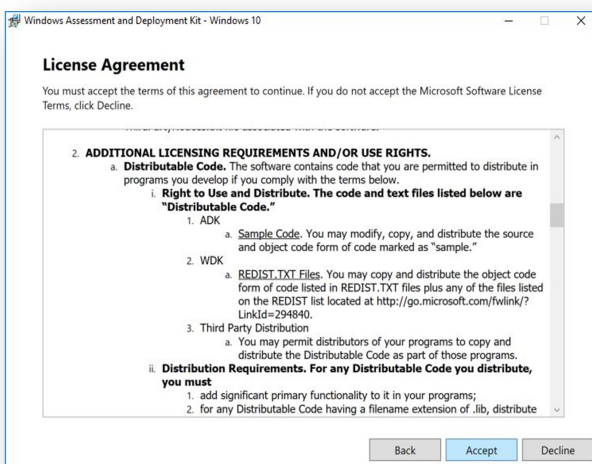
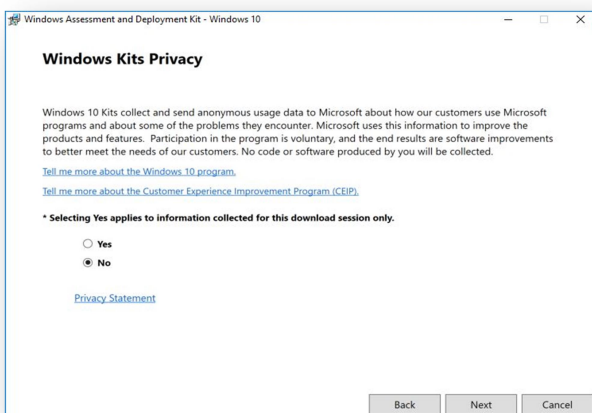
3. Execute adksetup.exe which will guide you through the installation process. When prompted to specify a location - Choose Download for installation on a separate computer. You will need approximately 4.4 GB of space.



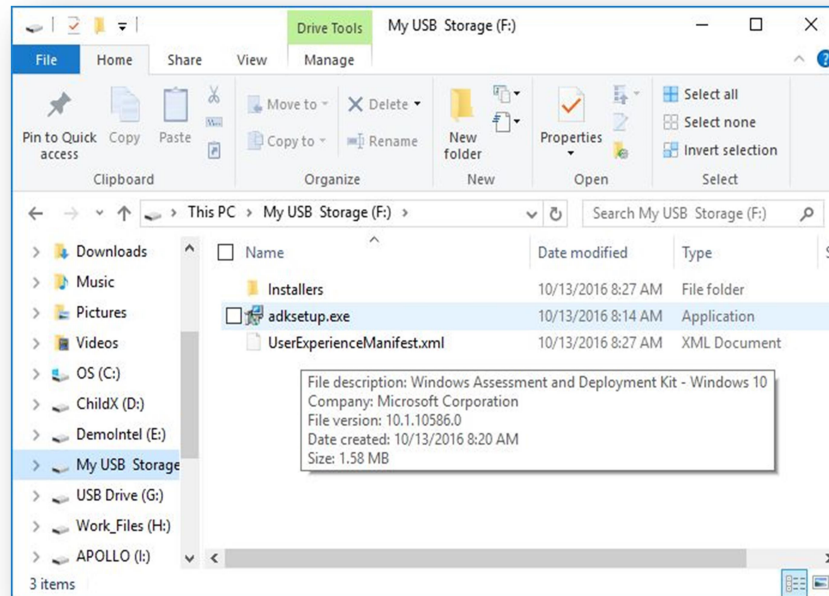
4. Save the downloaded files on an external removable device.



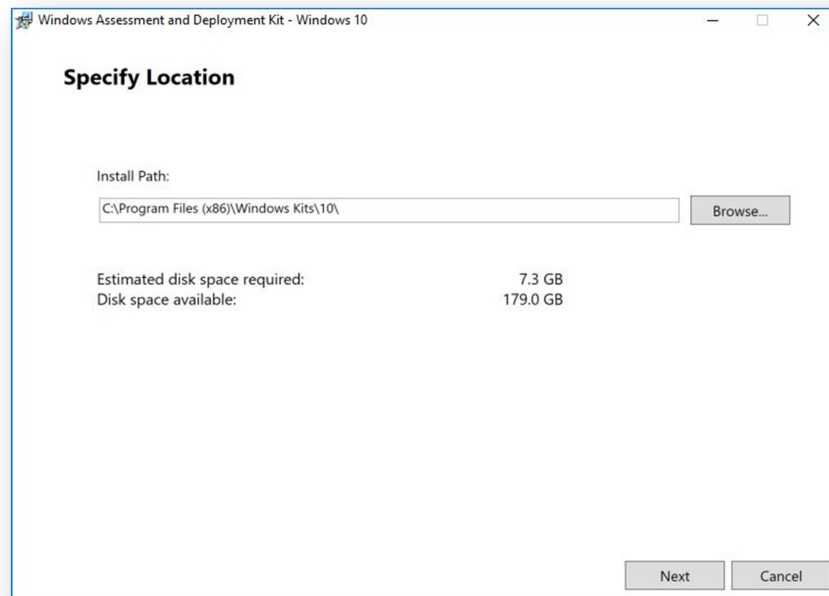
5. Choose the Privacy Options you prefer and accept the License Agreement.



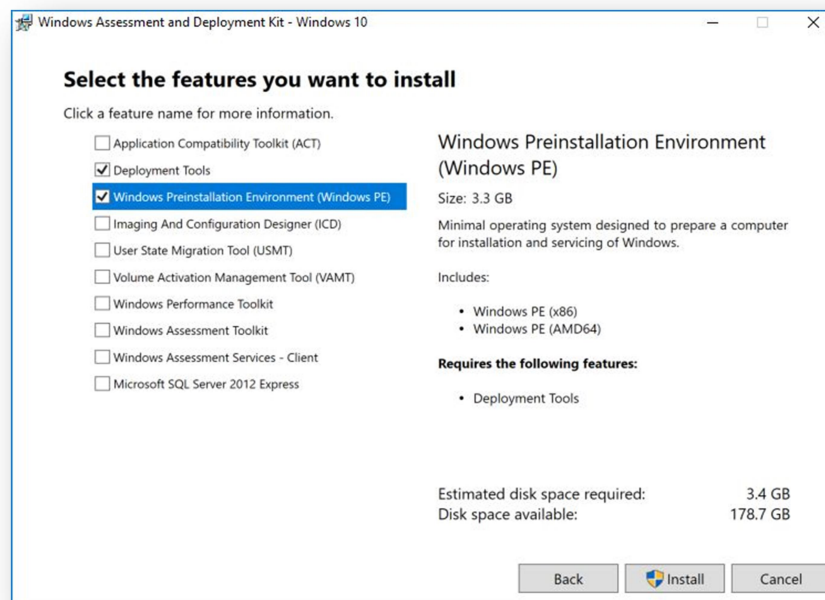
6. On your offline computer, navigate to the download on your removable storage device and execute the installer `adksetup.exe`.



7. Specify Location - Default is already selected.



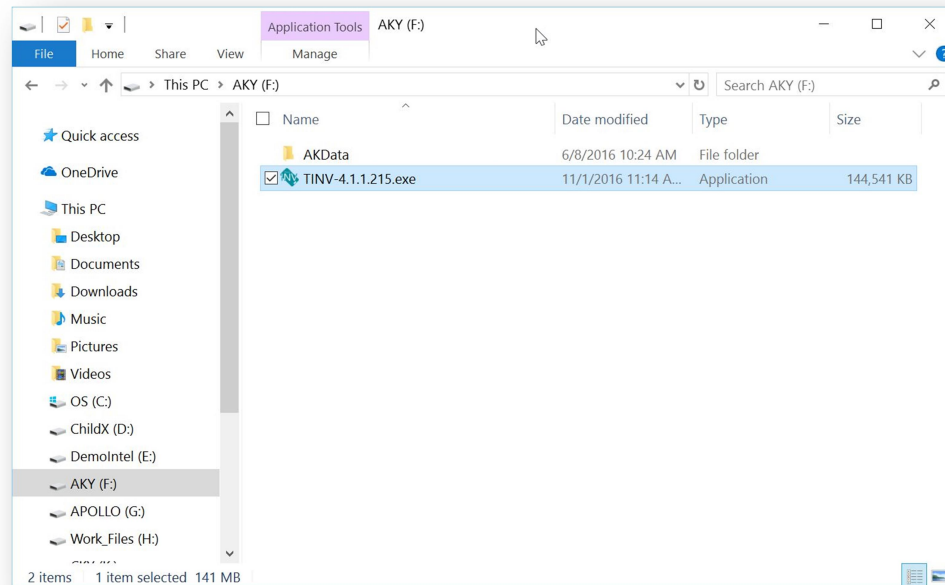
8. Choose the Privacy Options you prefer and accept the License Agreement (as shown above) and then select the following features to install - Windows Preinstallation Environment (Windows PE) and Deployment Tools - Click Install.



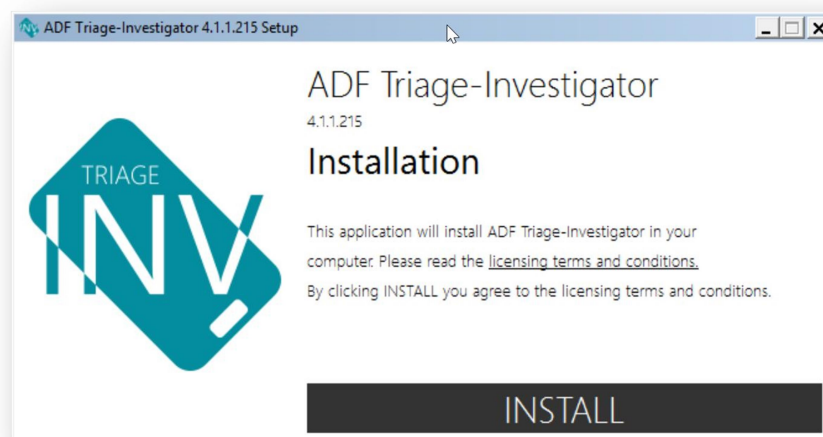
9. Once complete proceed to Online Triage-Investigator Installation instructions.

Online Triage-Investigator Installation

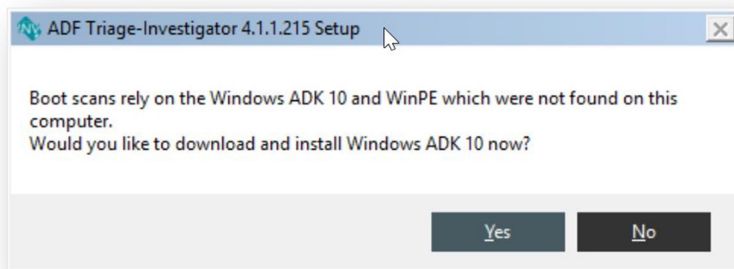
1. Locate and execute the program installer called TINV-xxxxxx.exe (where xxxxxx represents the version number). The latest installer program may be located on your supplied Triage-Investigator Authentication Key or is available at http://www.adfsolutions.com/Product_Version_Updates.html.



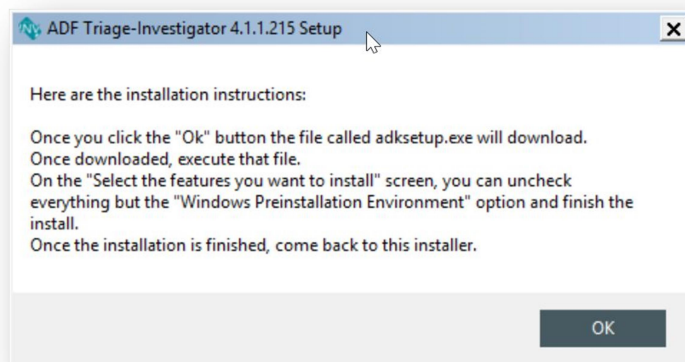
2. Follow the installation wizard instructions - Click Install to start.



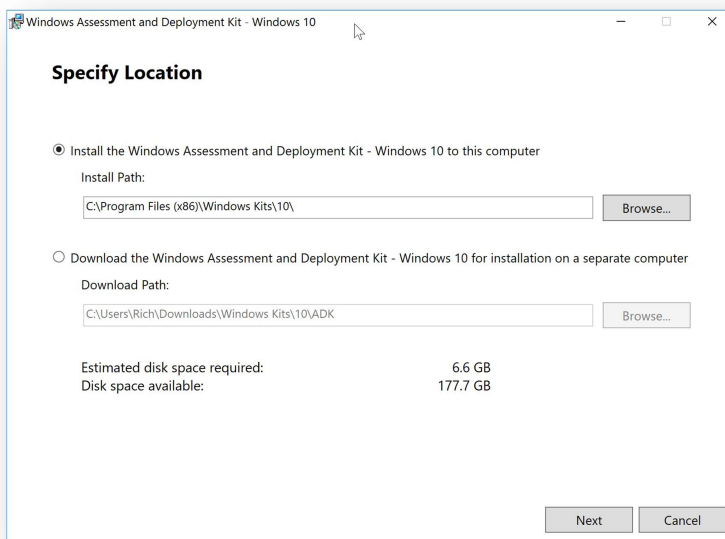
3. You will be prompted to install Windows 10 ADK if it is not installed – if this is the case select Yes.



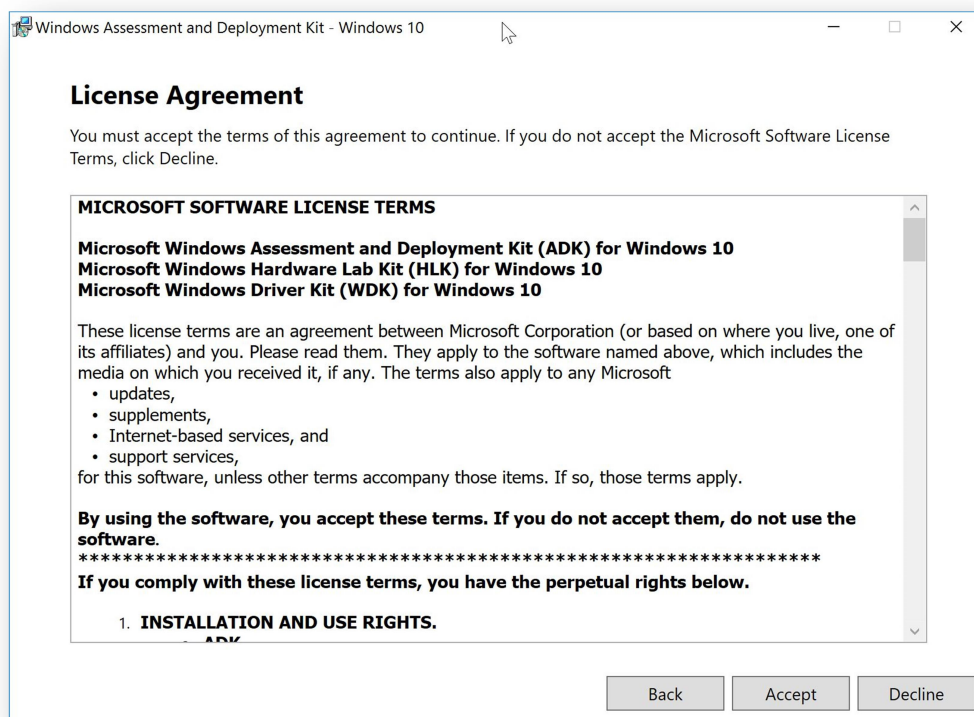
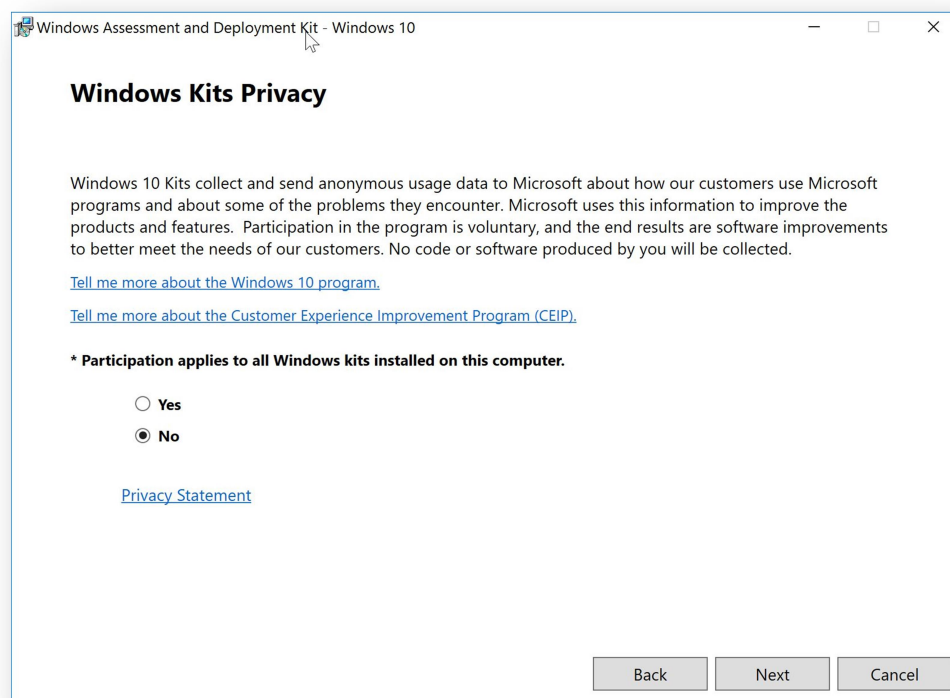
4. Click OK in the next window – a file entitled adksetup.exe will be downloaded. Locate this downloaded file and execute it.



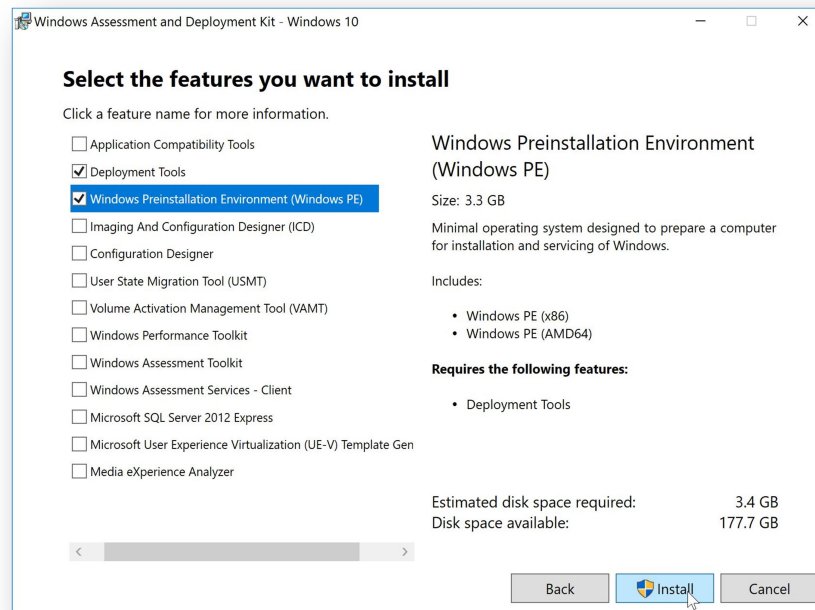
5. Specify Location - Default is already selected.



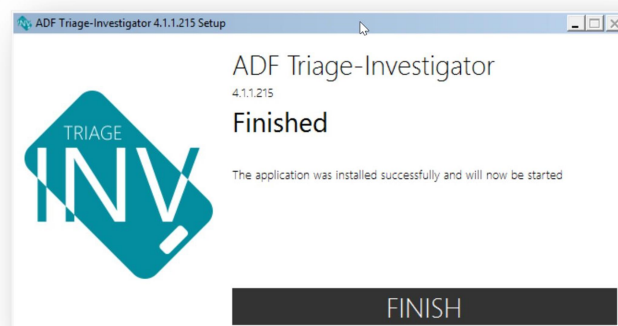
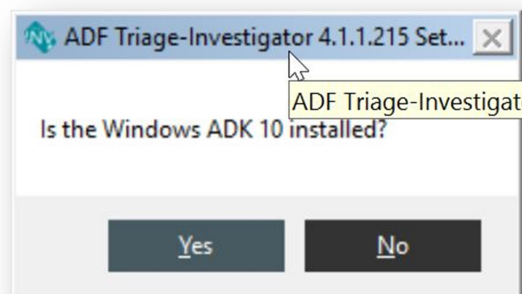
6. Choose the Privacy Options you prefer and accept the License Agreement.



7. Select the following features to install - Windows Preinstallation Environment (Windows PE) and Deployment Tools - Click Install.



8. Once the WADK is installed return to the Triage Investigator installer and click on Yes to complete the installation.



3. Data Migration to New Versions

Triage-Investigator contains functionality that migrates user configured Search Profiles, File Captures, and Scan Results from a previous version to a new version. One of the known limitations of this feature is that the File Captures in previous versions may be using an outdated data structure. User configured File Captures will automatically be migrated to the new version. Any Capture that has been restructured will not be migrated and a warning message will be shown advising you this Capture will not be referenced by your Search Profiles.

4. Supported Target Devices/Operating Systems

Triage-Investigator is designed to scan the following systems:

- Powered-off target computer (boot scan)
 - Firmware: BIOS, UEFI, Secure UEFI, Mac EFI 2.0 (released after 2010)
 - CPU: Intel 64-bit or compatible
 - RAM: 2GB or more
 - File systems: FAT, NTFS, HFS+, EXT2/3/4
 - RAID volumes for supported RAID storage controllers
- Powered-on target computer (live scan)
 - Windows Vista/7/8/10 32/64-bit, Server 2008/2012 32/64-bit
 - Windows Dynamic Disks: simple volumes only
- Drive image scan from the Desktop application
 - Format: dd and e01
 - File systems: FAT, NTFS, HFS+, EXT2/3/4
 - OS: Windows, Mac, Linux, iOS, Android
 - Images of RAIDs are supported if imaged as a logical disk
- Folder scan from the Desktop application
 - OS: Windows, Mac, Linux, iOS, Android

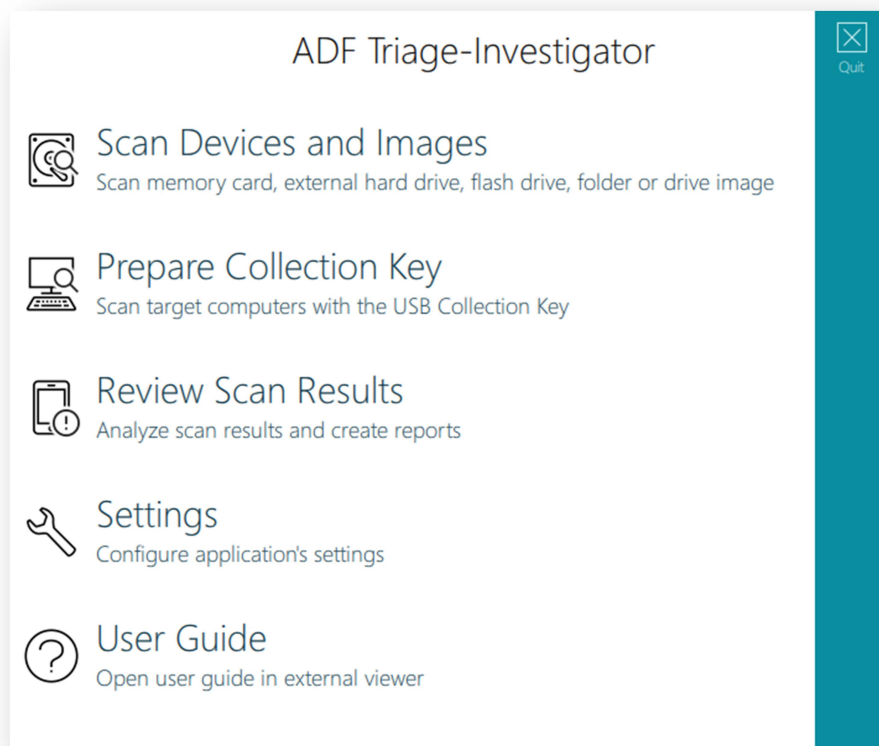
Triage-Investigator does not support the scanning of:

- Any Windows Dynamic disks during a boot scan
- Windows Dynamic striped, spanned or mirrored volumes during a live scan

5. User Interface

When executing the program the Home Screen is displayed, from here you can access all the functions of Triage-Investigator.

Triage-Investigator Home Screen



Scan Devices and Images

This option enables you to scan hard drives, USB devices, memory cards, forensic images (E01 and dd) and folders.

Prepare Collection Key

This option enables you to create a bootable USB Collection Key containing Search Profile(s) in order to conduct live or boot scans on target computers.

Review Scan Results

This option enables you to review and analyze scan results.

Settings

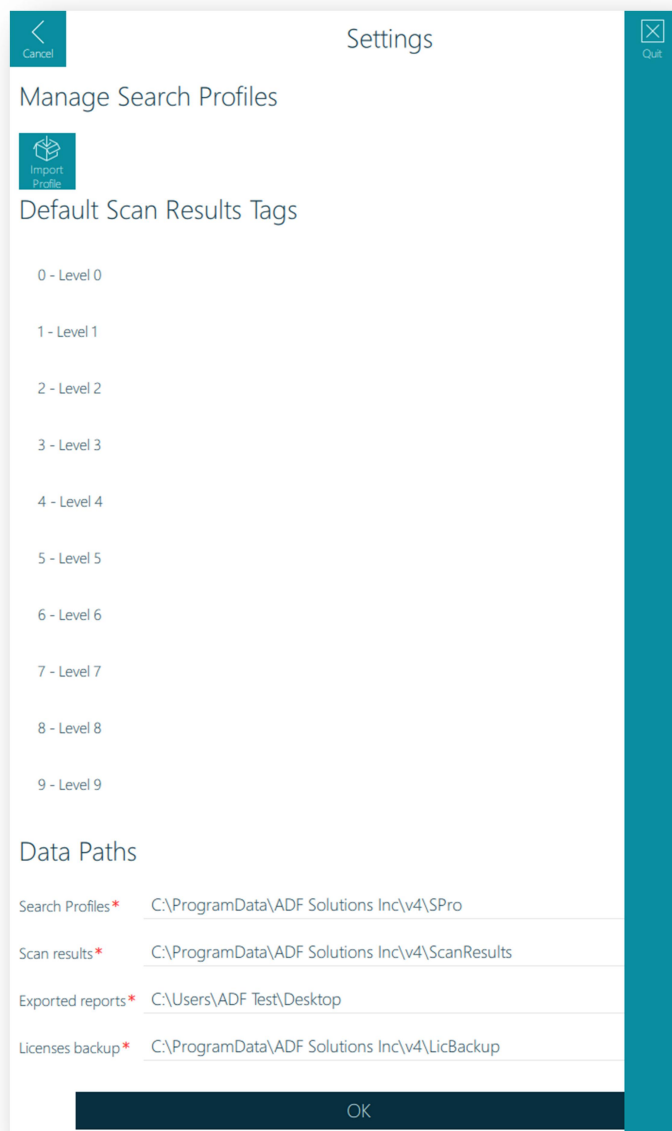
This option enables you to change the default locations of Search Profiles, scan results, exported reports and the license backup. Tag names can also be modified here. The Settings screen also allows you to import Search Profiles created in Digital Evidence Investigator.

User Guide

Selecting this option will open a PDF copy of this user guide.

6. Settings

Settings Screen



Manage Search Profiles

Clicking on the Import Profile button will allow you to import a Search Profile that has been created and exported within Digital Evidence Investigator. When the button is clicked a file browser dialog window is opened allowing you to search for and select the search profile, these files are identified as containing a .profile file extension.

Default Tag Names

This option enables you to set a default Tag Name for each of nine available tags. Tags are described further in section 13 of this guide. Changes to the default tag names will not be applied retroactively to previous scan results. To rename a tag double click on the highlighted name and type in the new name or click on the Rename button. In subsequent scan results the new tag names will be available.

Data Paths

The default locations (as shown below) of Search Profiles, Scan Results, Exported Reports and the License Backup can be changed via the folder browser dialog button:

Setting	Default Location
Search Profiles	C:\ProgramData\ADF Solutions Inc\v4\SPro
Scan Results	C:\ProgramData\ADF Solutions Inc\v4\ScanResults
Exported Reports	C:\Users\<user>\Desktop
License Backup	C:\ProgramData\ADF Solutions Inc\v4\LicBackup

Search Profiles

Search Profiles contains default and user created Search Profiles for Digital Evidence Investigator.

Scan Results

Scan Results contains scan results of scans carried out by the desktop application and any scan results imported from Collection Keys.

NOTE: it is not recommended at this time to save scan results on a shared folder as concurrent access of scan results is not supported.

Exported Reports

Exported Reports default to the user's Desktop for ease of access.

License Backup

License Backup contains a backup of any licenses you have used with Digital Evidence Investigator.

7. Default Search Profiles and Captures

Triage-Investigator comes with eight (8) ready to use default Search Profiles. A Search Profile is a combination of Captures. Artifact Captures recover specific records or information e.g. browsing history records or user account information. Users cannot create or edit Artifact Captures. File Captures recover files matching certain criteria such as file properties, inclusion of keywords or matching hash values.

Default Search Profiles

Quick – IPOC
This Indecent Pictures of Children (IPOC) Search Profile runs all Artifact Captures except email. It collects pictures and video frames in web browser caches, and searches for common IPOC keywords in filenames and artifacts.
Quick - General Profiling
This General Profiling Search Profile runs all the Artifact Captures except email and P2P Captures. Collects pictures in browser cache and identifies Social Media and Anti- Forensic Traces.
Quick – Collection - iOS Backup
This file collection profile specifically targets the iOS backup folder and collects all files within.
Intermediate – IPOC
This Indecent Pictures of Children Search Profile runs all Artifact Captures, collects pictures and video frames in user folders, searches for common IPOC keywords and known hash values in user folders, collects pictures with EXIF and GPS data and collects protected files and files not processed by the parser.
Intermediate - General Profiling
This general profiling Search Profile runs all Artifact Captures, excluding P2P captures, collects pictures, video frames, and Office documents in user folders. Collects protected files and files not processed by parser.
Comprehensive – IPOC
This Indecent Pictures of Children Search Profile runs all Artifact Captures, collects allocated, embedded, deleted pictures and videos, and carves images from unallocated space. Searches for common IPOC keywords, and searches for known hash values. Collects files from the Skype received files and media cache folders, and collects protected files and files not processed by parser.

Comprehensive - General Profiling
Runs all artifact captures, excluding P2P captures, collects allocated, embedded, and deleted pictures, videos and video frames from videos over 100MB, and all office documents. Collects Registry files, searches for anti-forensics applications, and collects user Desktop shortcuts. Collects protected files and files not processed by parser.
Comprehensive – Collect Pictures from Free Space
Runs one file capture: Collect Deleted Pictures from Unallocated Clusters.

Further information concerning the precise configuration of each default Search Profile can be seen in **Error! Reference source not found..**

8. Preparing a Collection Key

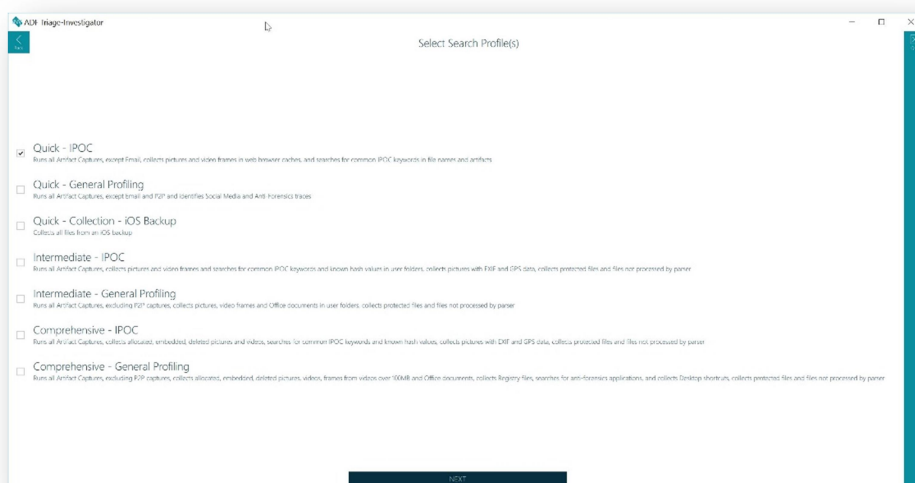
Preparing a Collection Key will make any USB storage device, a bootable USB device. A prepared Collection Key will enable you to boot the majority of powered off personal computers or conduct a live scan of a powered-on computer running the Microsoft Windows operating system. Search Profile(s) and an operating system are copied to the Collection Key during Collection Key preparation. Prepared Collection Keys have a volume name of CKY.

How to Prepare a Collection Key

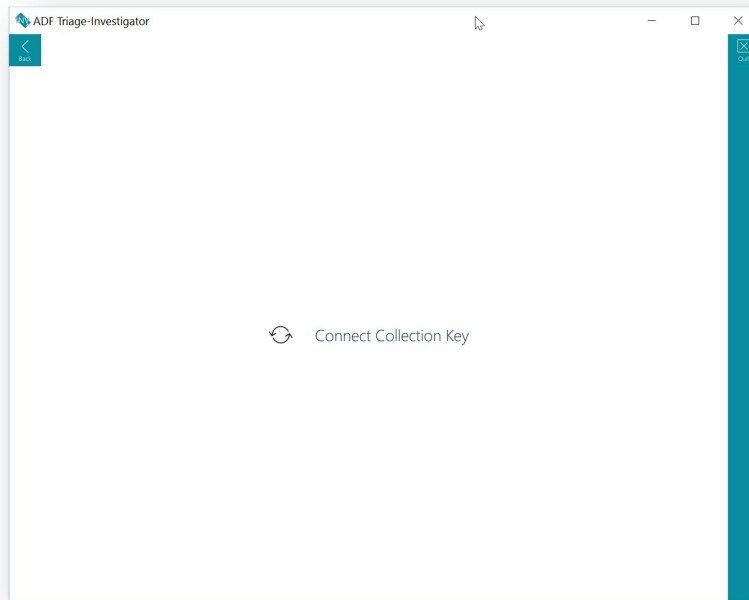
1. Insert a USB storage device that will be prepared as a Collection Key
Select Prepare Collection Key.



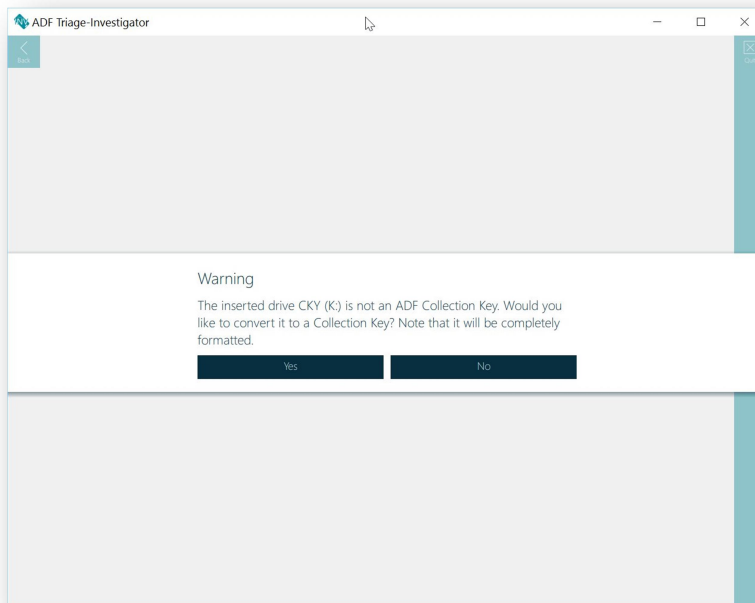
2. Select the Search Profile(s) you want to be available on the Collection Key.
Select next



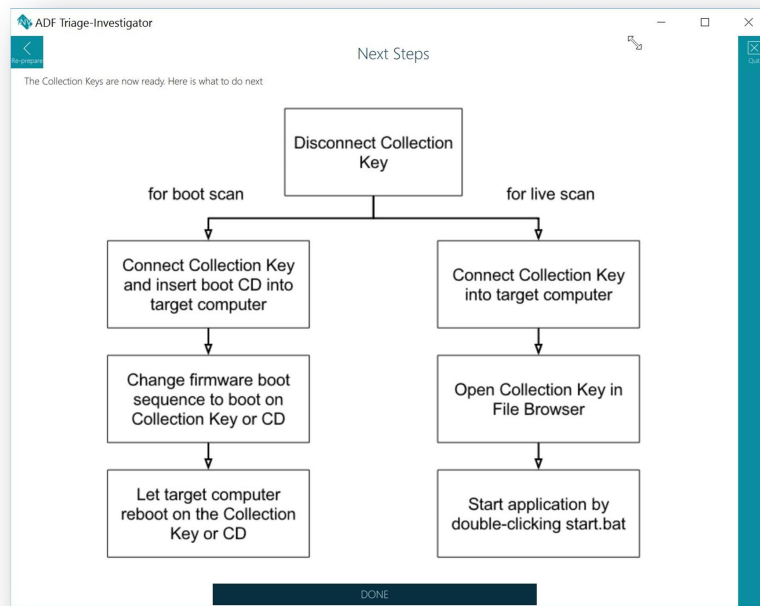
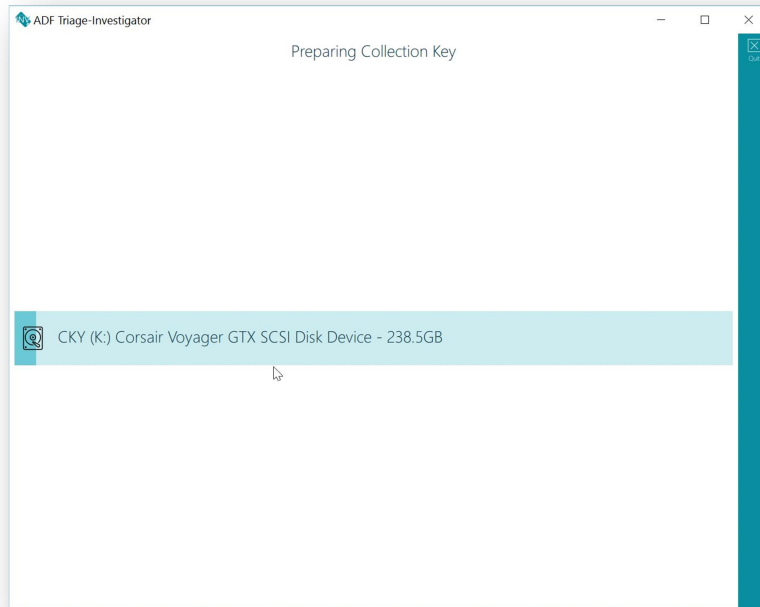
3. Insert the USB device you would like to prepare as your bootable Collection Key.



4. Once inserted you will be prompted that the Collection Key will be formatted and prepared.



5. When yes is selected, the preparation will commence and you will be prompted with the next steps for proper usage upon completion.



9. BIOS/UEFI

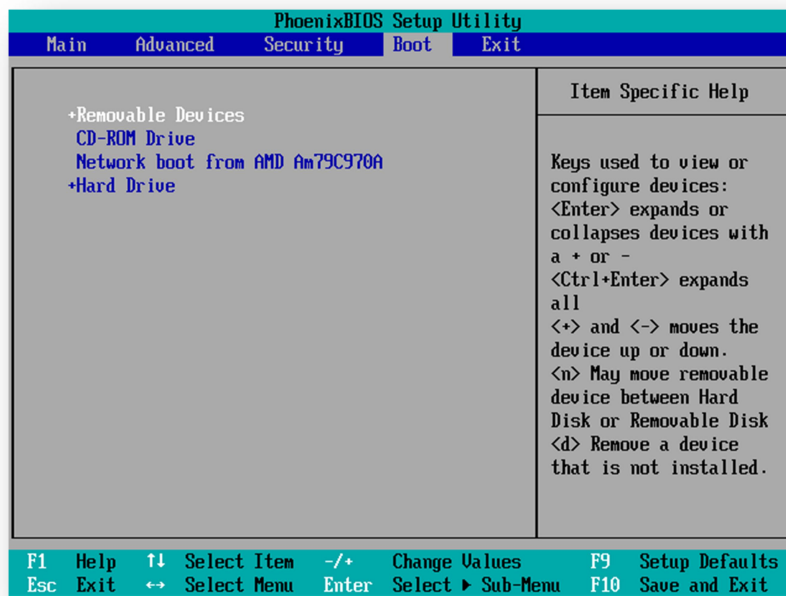
Most target computers will have to be configured to boot from the Collection Key. You will need to take control of the target computer. Computer manufacturers facilitate two ways to do this. Within the BIOS or UEFI firmware setup there is generally a boot sequence area where the computer may be configured to boot from a removable device first or alternatively many manufacturers provide a single use boot menu. Access to either the BIOS/UEFI setup or the single use boot menu is achieved by a user repeatedly pressing a hotkey on startup. The precise hotkey needed varies from manufacturer to manufacturer and model to model. Prior to booting, operators will have to research the appropriate manufacturers website to establish how to boot from a removable device.

Triage-Investigator will boot computers with UEFI Secure Boot enabled.

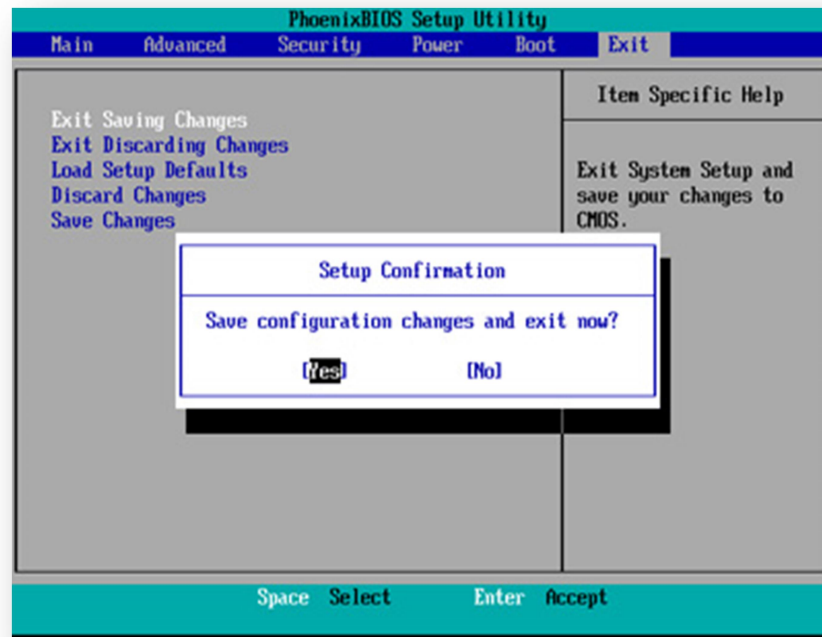
Steps to take control of the target computer BIOS/UEFI

1. Research Bios/UEFI Hotkey and use it (see Appendix A - BIOS Access Keys).

2. Locate the boot menu and reorder to boot from:
 - Removable Device
 - CD-ROM Drive
 - Hard Drive



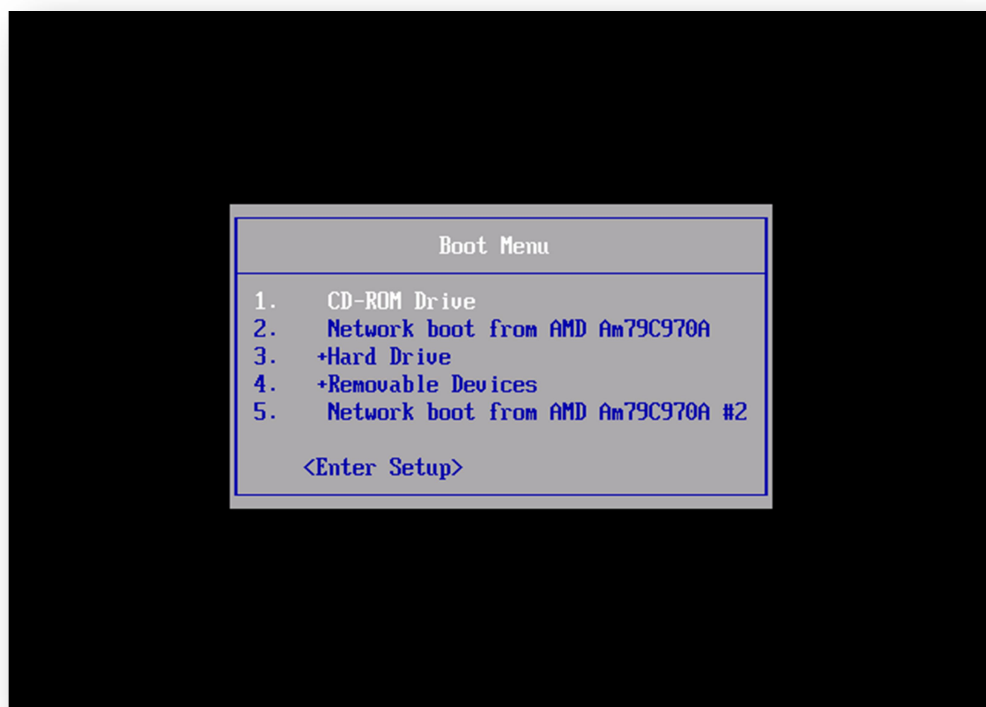
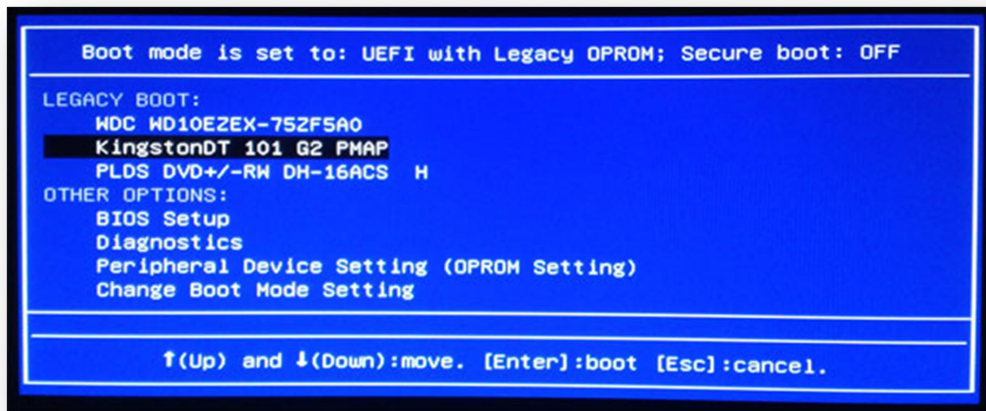
3. Save your changes and exit.
Boot to USB.



NOTE: you might have to connect the USB Collection Key for the removable devices option to appear.

Steps to take control of the target computer - Single Use Boot Menu

1. Establish the hotkey to access the Single Use Boot Menu, turn on the computer and repeatedly press the hot key until the menu appears then choose your Collection Key from the list.



NOTE: you have to connect the USB Collection Key for the removable devices option to appear.

Fast Boot / Ultra-Fast Boot enabled computers

Fast Boot is a feature of UEFI enabled computers that allows a computer to boot faster. The following booting issues are created when Fast Boot or Ultra-Fast Boot are enabled on the target computer:

1. Fast Boot - Booting from USB Device disabled
2. Ultra-Fast - Booting from USB device disabled as well as access to the UEFI Firmware settings.

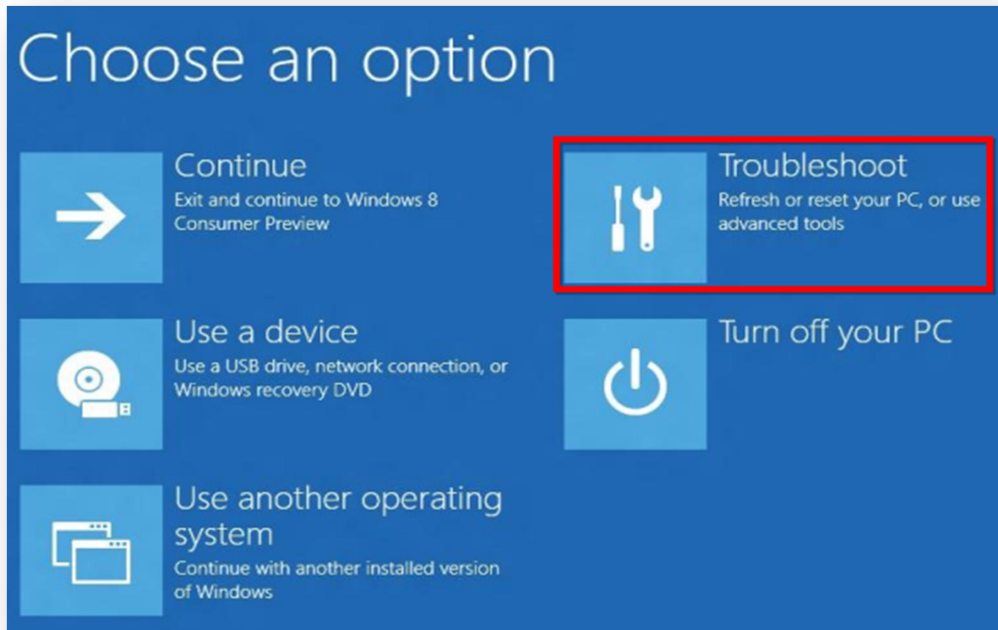
Fast Boot can be turned off by accessing the UEFI firmware via the appropriate hotkey and modifying the Fast Boot configuration. Please consult the relevant computer manufacturers web site for details on how to modify this setting.

Inadvertent boot to Windows 8/10

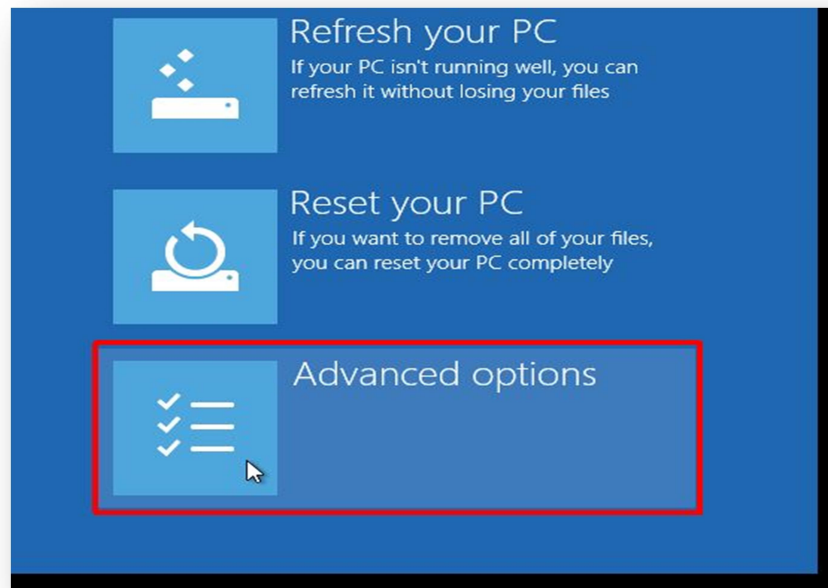
If you find that you cannot access the UEFI firmware settings or you have inadvertently booted to Windows here are the steps to restart automatically and access UEFI Firmware settings.

1. Hold down the shift key and select restart computer. This method also works if you have not signed into Windows 8/10, as long as you are on the login screen and can access the restart menu option. If the computer signed in automatically click the Restart option from the Start menu while holding the shift key down.

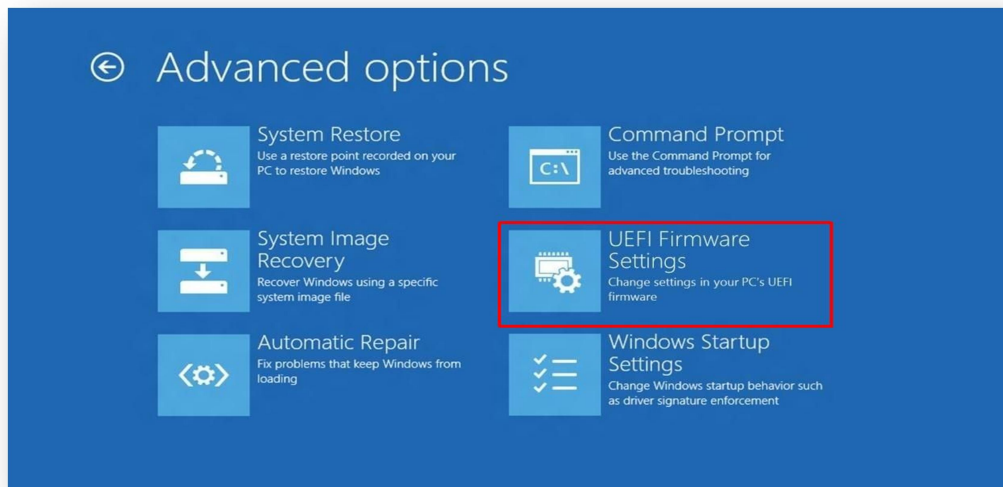
2. While shutting down you will be presented with menu options, Choose Troubleshoot.



3. Choose Advanced Options.



4. Choose UEFI Firmware Settings.



5. Choose restart to UEFI Settings. The computer will restart and allow access to the UEFI Firmware settings.

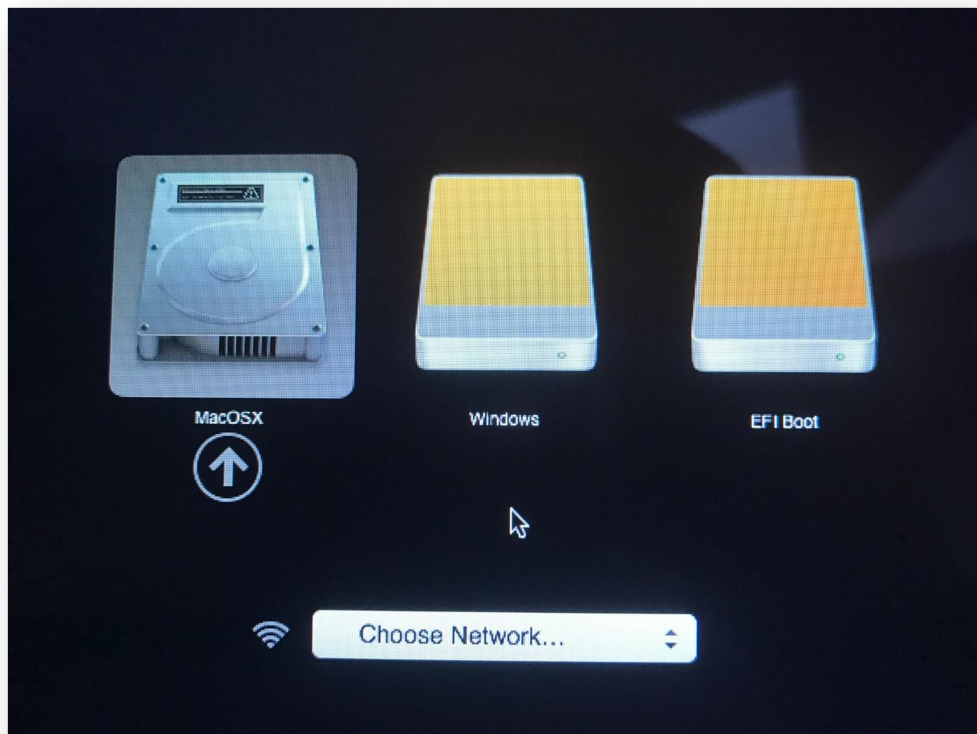


Apple Mac Computers

1. On an Apple Mac computer insert the Collection Key and as soon as the start up chime is heard, press the Option Key and hold it down until the Apple Startup Manager is displayed – as shown below.



2. The Apple Startup Manager is displayed – selecting either Windows or EFI Boot will boot to the Collection Key.



Plop Boot Manager

You can also boot from the USB device without BIOS support using the included Plop Boot Manager CD. This disk should only be used for legacy devices that cannot boot directly from USB. The Plop Boot Manager is a small program to boot different operating systems. The boot manager has a built-in IDE CD-ROM and USB driver to access that hardware without the help/need of a BIOS. When booted to the CD select the USB option to boot from the Collection Key.

Plop Boot Manager



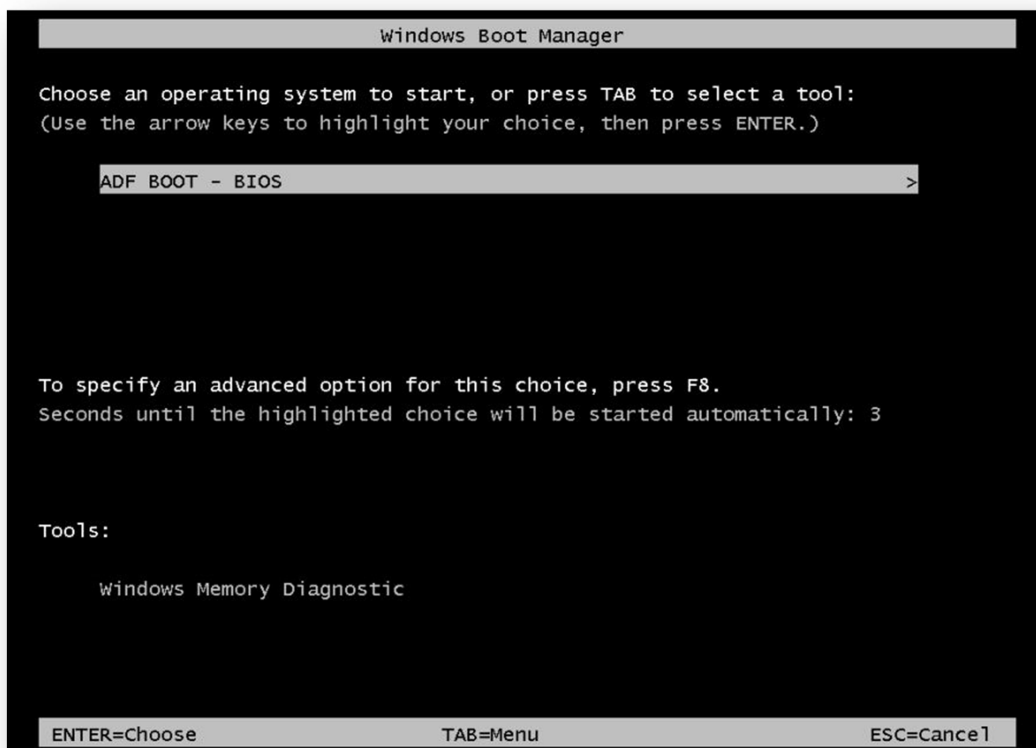
10. Boot Scan

When conducting a boot scan Triage-Investigator is forensically sound. This means that no changes are made to the target media.

Prior to conducting a Boot Scan establish how many USB ports are available and determine if a 4-port USB hub is required. Two ports are required in order to complete a scan, one for the Collection Key and one for the Authentication Key. Once the scan has started the Authentication Key can be removed.

When booting to the Collection Key Triage-Investigator will automatically launch the application to scan the computer. No user input is required within the Windows Boot Manager.

Windows Boot Manager



You will be presented with three options to complete prior to starting the scan:

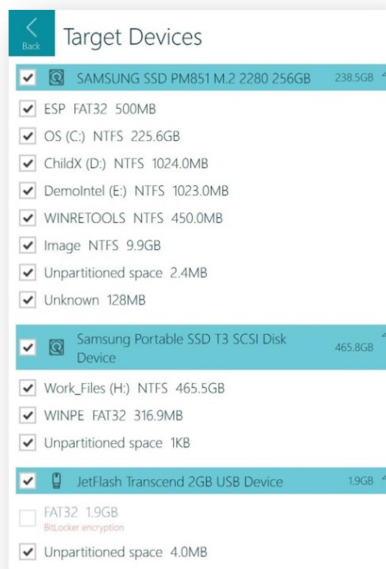
1. **Select your target device(s)**

Physical Drives are denoted by a hard disk icon

Logical volumes are listed beneath the physical drive entry

Attached devices are denoted by a flash drive icon

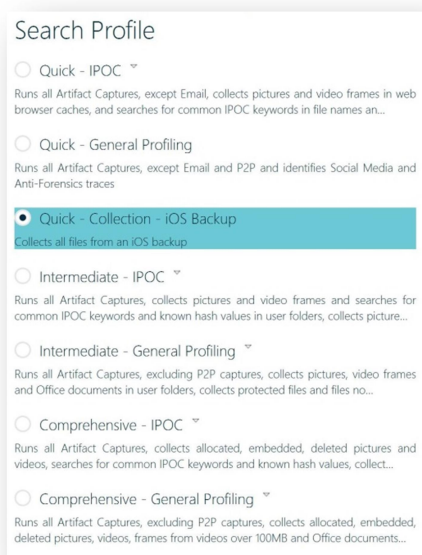
Bitlocker/FileVault 2 volumes are flagged (volume will be disabled if not decrypted).



2. **Select your Search Profile** - See Section 7 - Default Search Profiles and Captures for descriptions

All Search Profiles selected during Collection Key preparation will be available for scans.

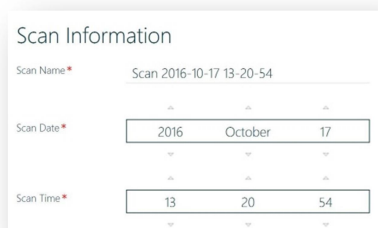
Only one Search Profile can be used per scan.



3. **Enter your scan information**

The Scan Name field defaults to the word Scan followed by a real-time date and timestamp but is user modifiable – TIP: Customize the name so the results are easily identifiable in Review Scan Results.

The Scan Date and Time fields are populated by querying the system clock of the device about to be scanned and can be modified to reflect the actual time if the system clock is incorrect.



Scan Information

Scan Name* Scan 2016-10-17 13-20-54

Scan Date* 2016 October 17

Scan Time* 13 20 54

4. To start the scan, insert your Authentication Key and then click on the scan button. If your Authentication Key is not inserted, you will be prompted with the message No license file found to run the scan. Please insert your Authentication Key.

5. Once started the scan activity will be shown with the following:

Progress bar - Current area and files being scanned (along with estimated percentage complete)

Matches window - Real time preview (thumbnail) of File Capture matches collected. Images and Video files are represented by thumbnail images, keyword matches will show the keyword found, all other matches will be represented by an associated icon.

Capture results - Cumulative count of capture results

Pause / Resume button - If the scan is paused for review of the captured results up to this point, the user can then either resume or stop the scan. If the user stops the scan, all files collected and capture results to this point are saved on the Collection Key.

6. Once the scan has completed you will be prompted to view the results.

7. Scan results are stored on the Collection Key and may be reviewed and analyzed using the target computer. Alternatively scan results stored on a Collection Key may be reviewed and reports created, using the Digital Evidence Investigator software used to prepare your Collection Key or on any other computer where Digital Evidence Investigator software is installed.

Further help on Reviewing Scan Results and Reporting can be found in sections 13 and 14 of this guide.

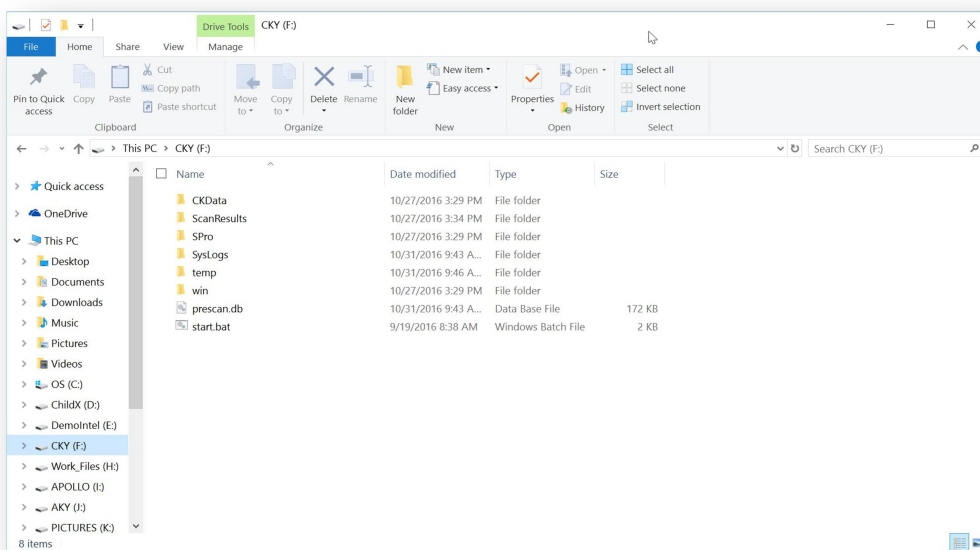
11. Live Scan

Triage-Investigator accesses files on the target computer without modifying their timestamps. However, it should be expected that running Triage-Investigator on a live system will leave traces related to the insertion of both the Collection Key and Authentication Key and the execution of the Triage-Investigator application.

Two USB ports are required in order to complete a scan, one for the Collection Key and one for the Authentication Key, once the scan has started the Authentication Key can be removed. A USB hub may be used in cases where the target computer only has one USB port.

To run a Live Scan:

1. Insert the Collection Key and Authentication Key into USB ports upon the target computer and execute the Start.bat file stored on the Collection Key by double clicking on it. You will be presented with three options to complete prior to starting the scan.



The rest of the process is identical to that described in the section 10 - Boot Scan above.

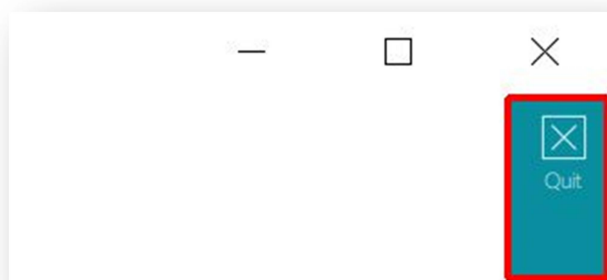
12. Desktop Scan

The Triage-Investigator application when installed upon your laboratory examination computer has the ability to scan attached drives (other than the system drive), devices (typically connected via a write blocking device), forensic image files (E01 and dd) and the contents of folders.

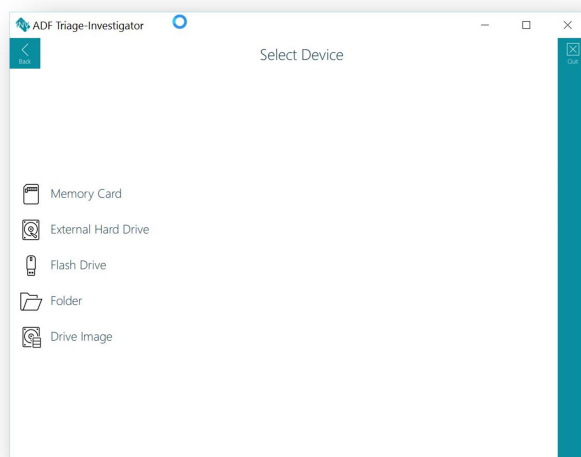
Function Toolbar

Located vertically on the right side of the application is the Function Toolbar. This toolbar changes depending on the task at hand and contains the functionality for the displayed screen.

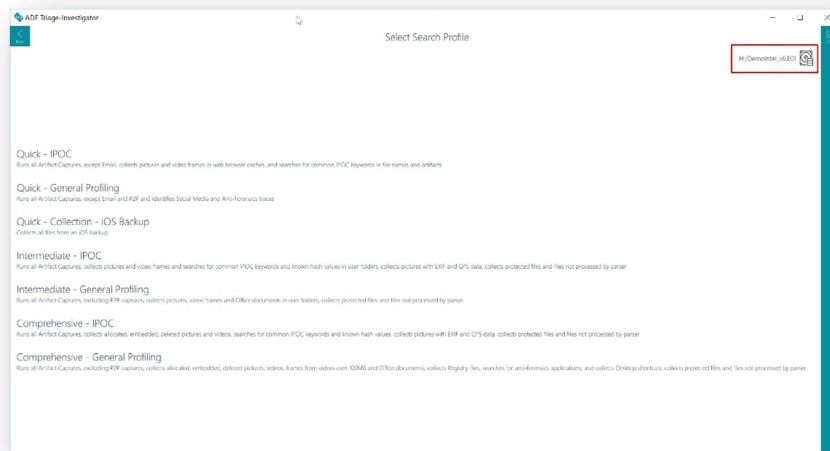
Option	Function
Quit	Closes the application immediately



1. Select your target device(s)
Select Memory Card – then connect device to computer
Select External Hard Drive – then connect device to computer
Select Flash Drive - then connect device to computer
Select Folder – then point at folder or logical volume
Select Drive Image – then navigate to E01 or .dd image file



2. Select your Search Profile - See Section 7 - **Default Search Profiles and Captures** for descriptions. All Search Profiles will be available.
In the upper right corner your device selection will be denoted.
 - Physical Drives are denoted by a hard disk icon
 - Logical volumes are listed beneath the physical drive entry
 - Attached devices are denoted by a flash drive icon
 - Bitlocker / FileVault 2 volumes are flagged (volume will be disabled if not decrypted)
 - Specific targeted folders are denoted by a folder icon
 - Image Files - E01 or .dd are denoted by an image icon.



3. Enter your scan information

The Scan Name field defaults to the word Scan followed by a real-time date and timestamp but is user modifiable – TIP: Customize the name so the results are easily identifiable in Review Scan Results.

The Scan Date and Time fields are populated by querying the system clock of the device about to be scanned and can be modified to reflect the actual time if the system clock is incorrect.

Device and Search Profile selections are denoted in the upper right

ADF Triage-Investigator

Verify Scan Information

H:/DemoIntel_v6.E01
Quick - General Profiling

Scan Name * Drive Image 2017-01-10 13-56-36

Date * 2017 January 10

Time * 13 56 36

SCAN

4. To start the scan, insert your Authentication Key and then click on the scan button. If your Authentication Key is not inserted, you will be prompted No license file found to run the scan. Please insert your Authentication Key.

5. Once started the scan activity will be shown with the following:

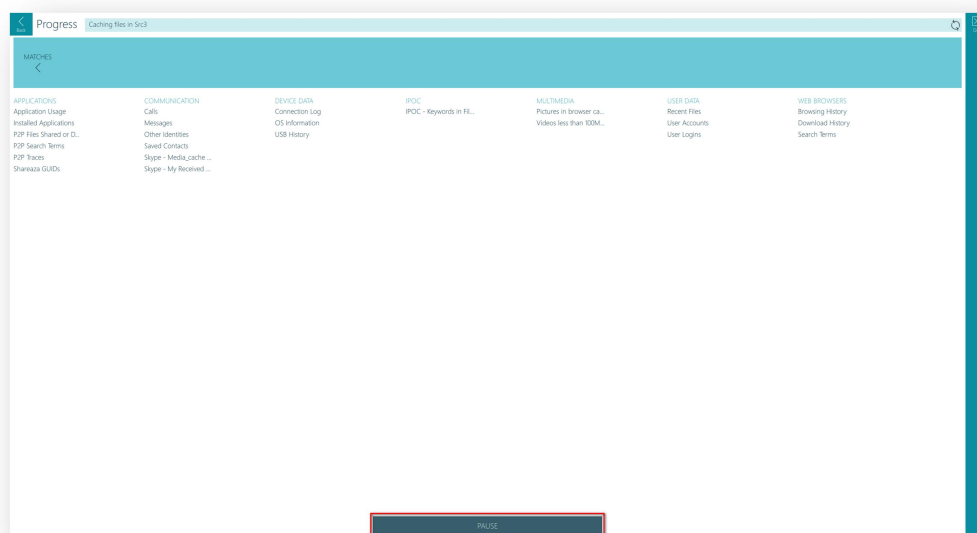
Progress bar - Current area and files being scanned (along with estimated percentage complete)

Matches window - Real time preview (thumbnail) of File Capture matches collected. Images and Video files are represented by thumbnail images, keyword matches will show the keyword found, all other matches will be represented by an associated icon.

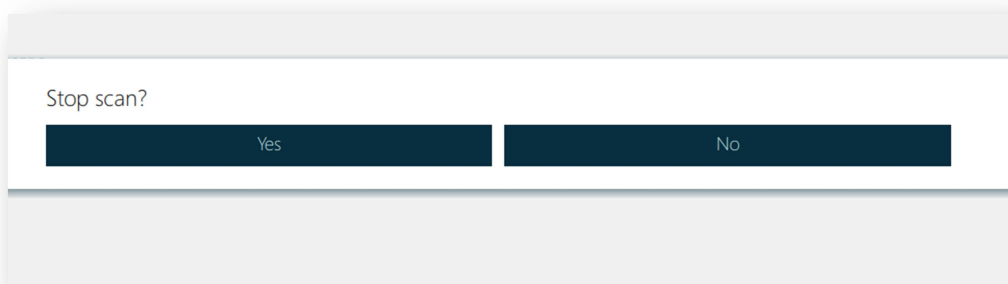
Capture results - Cumulative count of capture results

Pause / Resume button - If the scan is paused for review of the captured results up to this point, the user can then either resume or cancel the scan. If the user cancels the scan, all files collected and capture results to this point are saved on the Collection Key.

6. Whilst a scan is running it can be paused to review the results gathered thus far. Click on the Pause button at the bottom of the screen. This will enable to you view any current results. To resume the scan press the Back button at the top of the Navigation toolbar (if it is not available you need to browse away from the Summary screen) and press the Resume button.



7. There is no limit on the number of times a scan can be paused and resumed. To stop a scan after it has been paused click on the back button again and answer Yes at the Stop Scan dialog box.



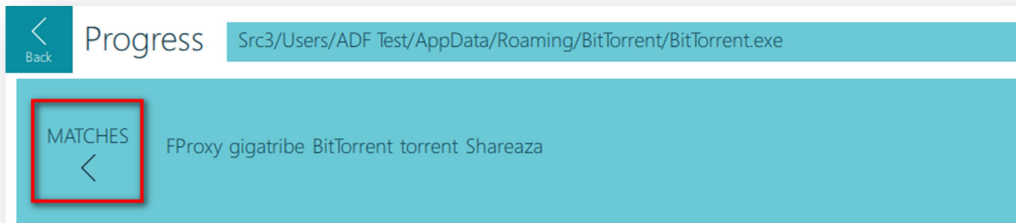
8. Once the scan has completed you will be prompted to view the results. Scan results are stored in the Scan Results folder (\ProgramData\ADF Solutions Inc\v4\ScanResults by default).

Further help on Reviewing Scan Results and Reporting can be found in sections 13 and 14 of this guide.

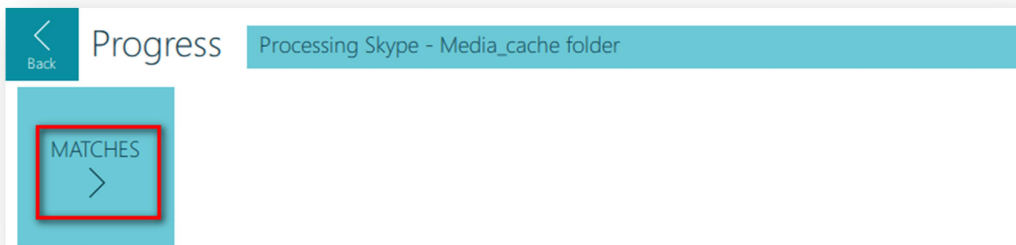
File Preview

During a scan the file preview pane will be populate with keyword hits and previews of files identified during the scan.

1. While file previews are active pressing the Matches button will disable file previews.



2. When the file preview has been switched off, clicking on the Matches button will re-enable file previews.












13. Review Scan Results

Here you will be able to review the results of your scan, filter, sort, analyze, tag, and prepare a comprehensive report.

Capture and Navigation Toolbar





Located vertically on the left side of the application is the capture and navigation toolbar. This toolbar will allow navigation through the results and will be visible when in Review Scan Results. The following buttons are located on this toolbar.




Option	Function
	Returns to the index of all stored scan results
	A gallery view of all pictures identified by captures
	A listing of all video files identified by Captures together with access to frame view and video player functionality
	Direct access to all keyword hits from any keyword Captures
	A listing of all artifact and file Capture records in a single timeline
	A summary containing the scan parameters, results and tagging statistics

Option	Function
 Scan log	A log of encountered protected files and parsing or scanning issues
 Report	Access the report creation screen
 More	Access to individual Capture results

Function Toolbars

A Function Toolbar is located vertically on the right side of the results viewer. This toolbar is context specific and will adapt depending on what is being viewed:

Function	Option
Closes the application immediately	 Quit
Add or remove or reorder columns from view. Changes made to column display also modify columns displayed within reports.	 Columns
Deselects (unchecks) any selected records within the current view	 Deselect All
Allows the application of context specific filters to the displayed records	 Filter




Function	Option
Apply tags for selected record(s) in the current view. Renaming of Tags is available here.	
Apply a comment to selected record(s) in the current view	
Toggles the display of the Details Pane which provides further information and functionality for the selected record	

Details Pane


The details pane provides further information for individual file or artifact records. The options are displayed in a series of horizontal tabs. Further functionality is accessible via a toolbar displayed on the right side of the details pane. The following table details some of the options available in the details pane:

Option	Function
Properties	Individual properties of the selected record
Metadata	Metadata extracted from the selected file.
Excerpts	Displays keywords hits identified in a file as bold text with surrounding text visible. There is also an Excerpt column in the main table for keywords that will show individual excerpts. The Excerpt column will only show the first keyword hit if multiple hits exist in a file.
Frames	50 frames of a video, first frame, last frame, and 48 frames taken from the video at regular intervals.
Preview	Pictures will be viewable in this pane at their actual size, other records such as documents will need to be viewed by accessing the undock button on the vertical Function Toolbar. Videos are viewable in an internal player and are dependent on installed codecs.

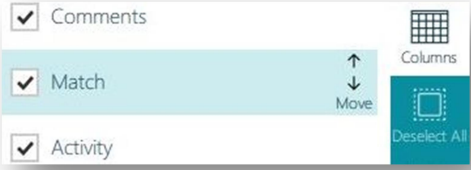
Function Toolbar of Details Pane

Function	Option
Open the file in a separate internal viewer window. This option will become active if the preview tab is accessed.	
Open the file with the default program on the computer or associate a program where no association exists	
Save the file to a location of your choice	


Columns





Left click and hold in between columns will allow resizing column width



Drag column name up and down in the Columns function pane to reposition column L or R
Show or hide a column by using the checkbox





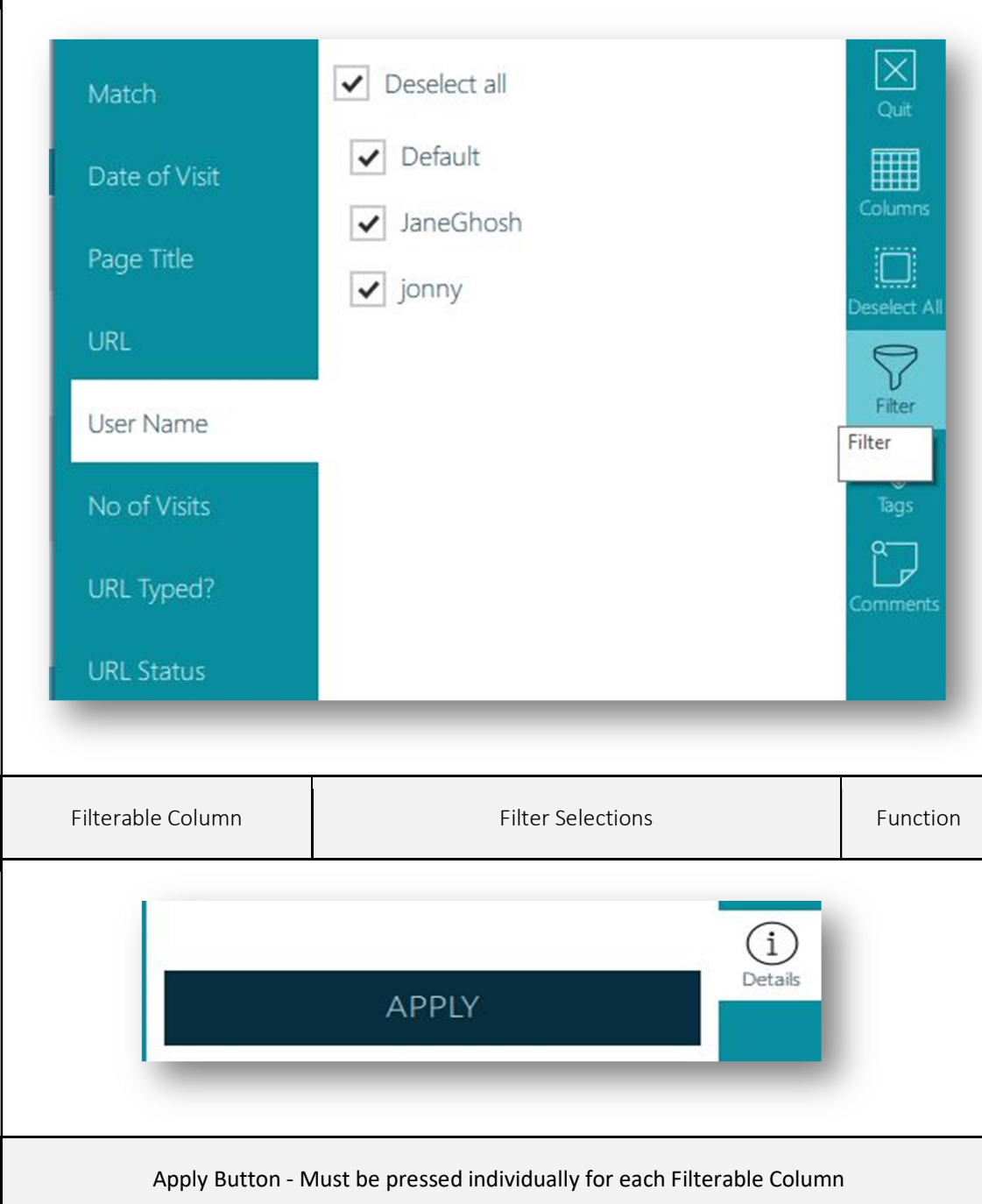
Left click, hold, drag to reposition column L or R





Click on the column to sort Ascending or Descending (not all columns are sortable)

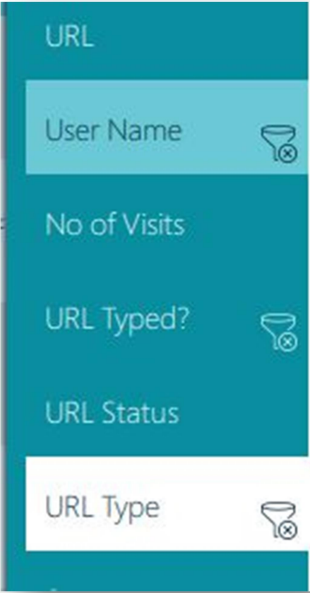



Filtering

Filtering is achieved by selecting the Filter button on the function toolbar. This will open the filter pane and present you with filters for the current view. After selecting your filter click the **APPLY** button on the bottom of the Filter Pane. To remove your filter, you can click the  on the filter above the table view or click the  next to the filter in the filter pane. Each table view will have its own set of filters depending on the type of records being previewed.



Filterable Column	Filter Selections	Function
		<div> <div>APPLY</div> <div>  Details </div> </div>

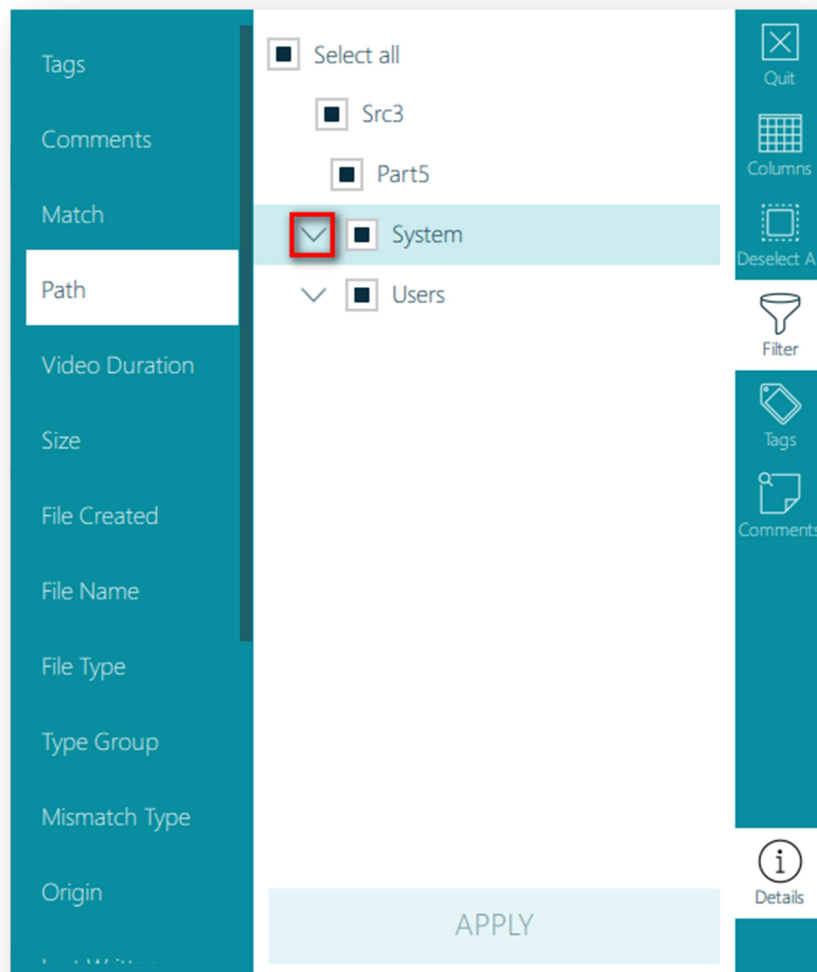
Apply Button - Must be pressed individually for each Filterable Column

Option	Function
	<p>Active Filters are shown next to the column name that has been filtered (represented by the  icon). The filter can be removed by clicking on that icon.</p>
	<p>Active Filters are also shown on the top of the columns with the  icon. These filters can be removed by clicking on that icon.</p>

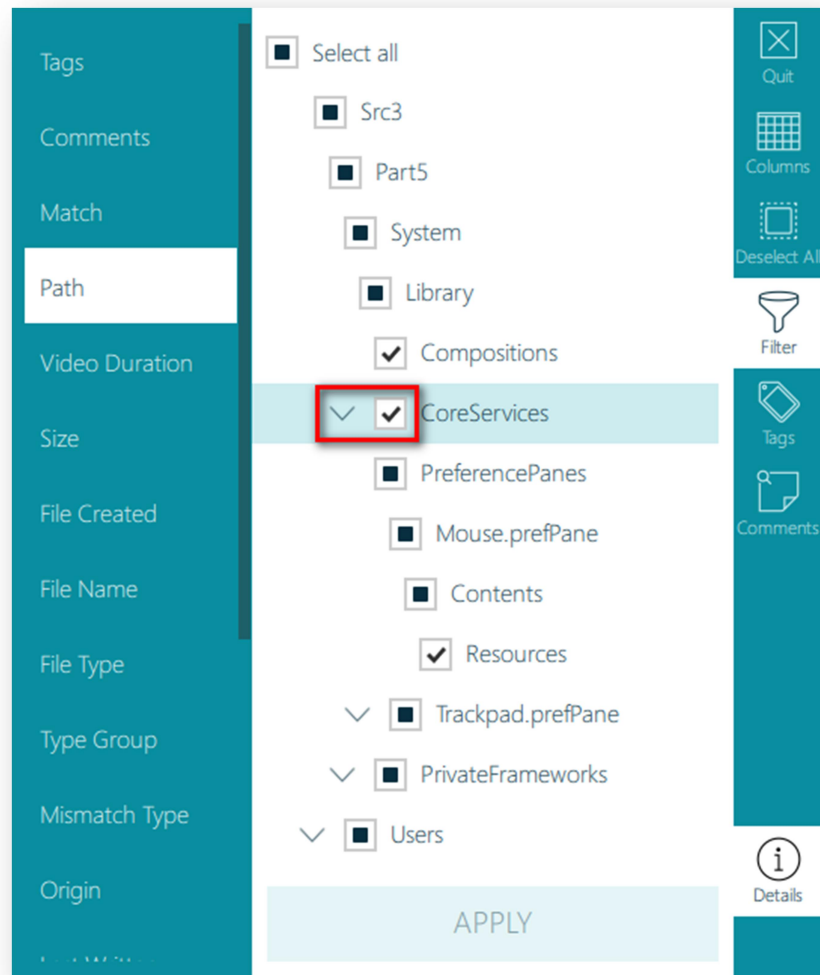
Filtering by Path

Filtering files by their path allows you to quickly identify files that reside in areas of interest to your investigation. There are a number of options available within the Path filter to allow you to identify only the most pertinent of files.

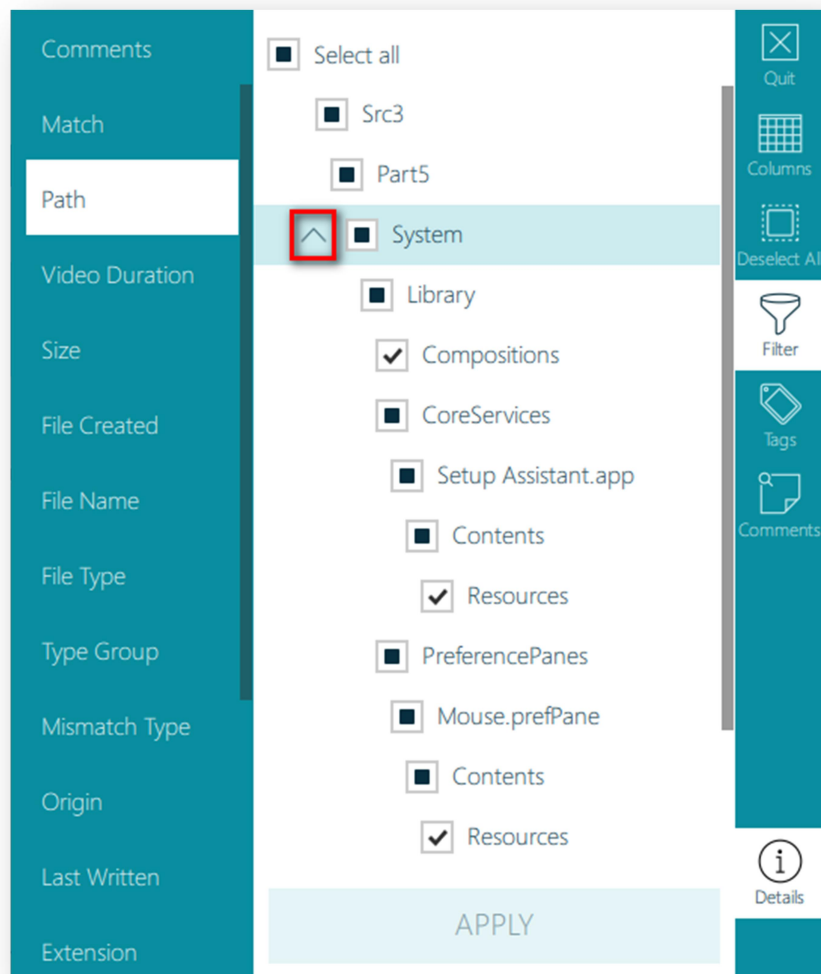
1. Pressing the Path button within the Filter option will display a hierarchical view of the folder structure of the evidential material. A black check box indicates one or more directories have been selected below the corresponding directory, but not all of them. Pressing a down arrow will reveal further sub directories.



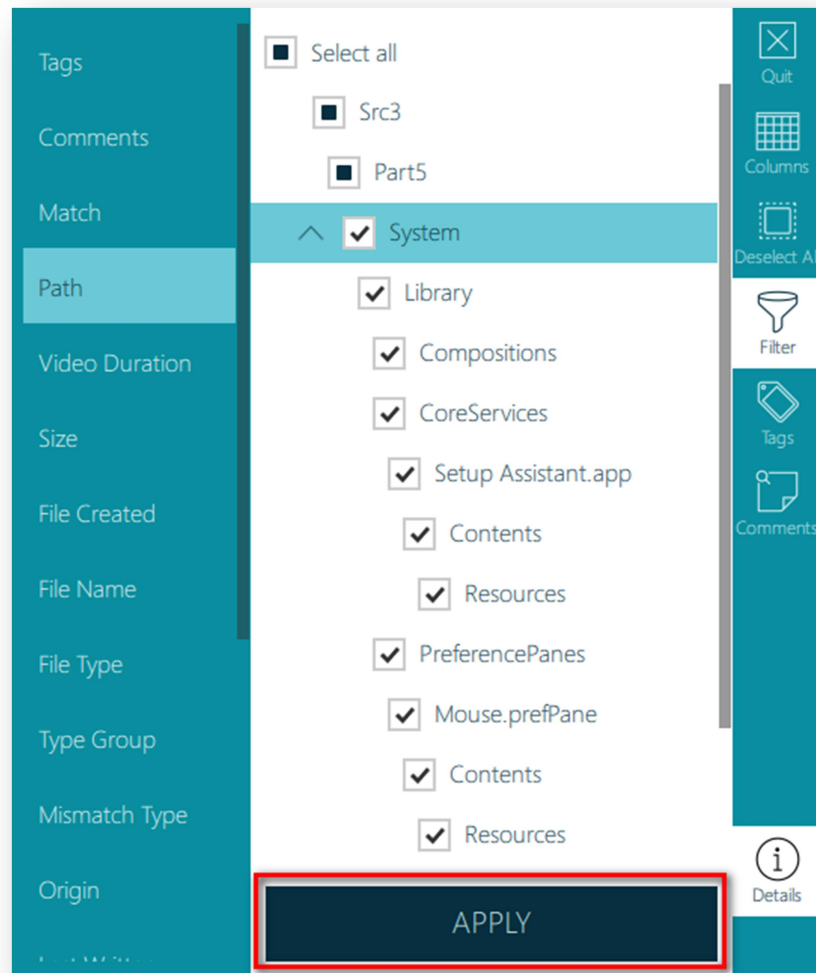
2. Pressing the checkbox next to a directory will place a tick mark in the checkbox. This will select all sub directories of the corresponding directory. Selecting a checkbox that contains a tick already will remove the selection from the corresponding directory and all sub directories.



3. Pressing an up arrow will collapse the hierarchical view to the corresponding directory.



4. When you have selected the directories you desire clicking on Apply will create your desired filter.

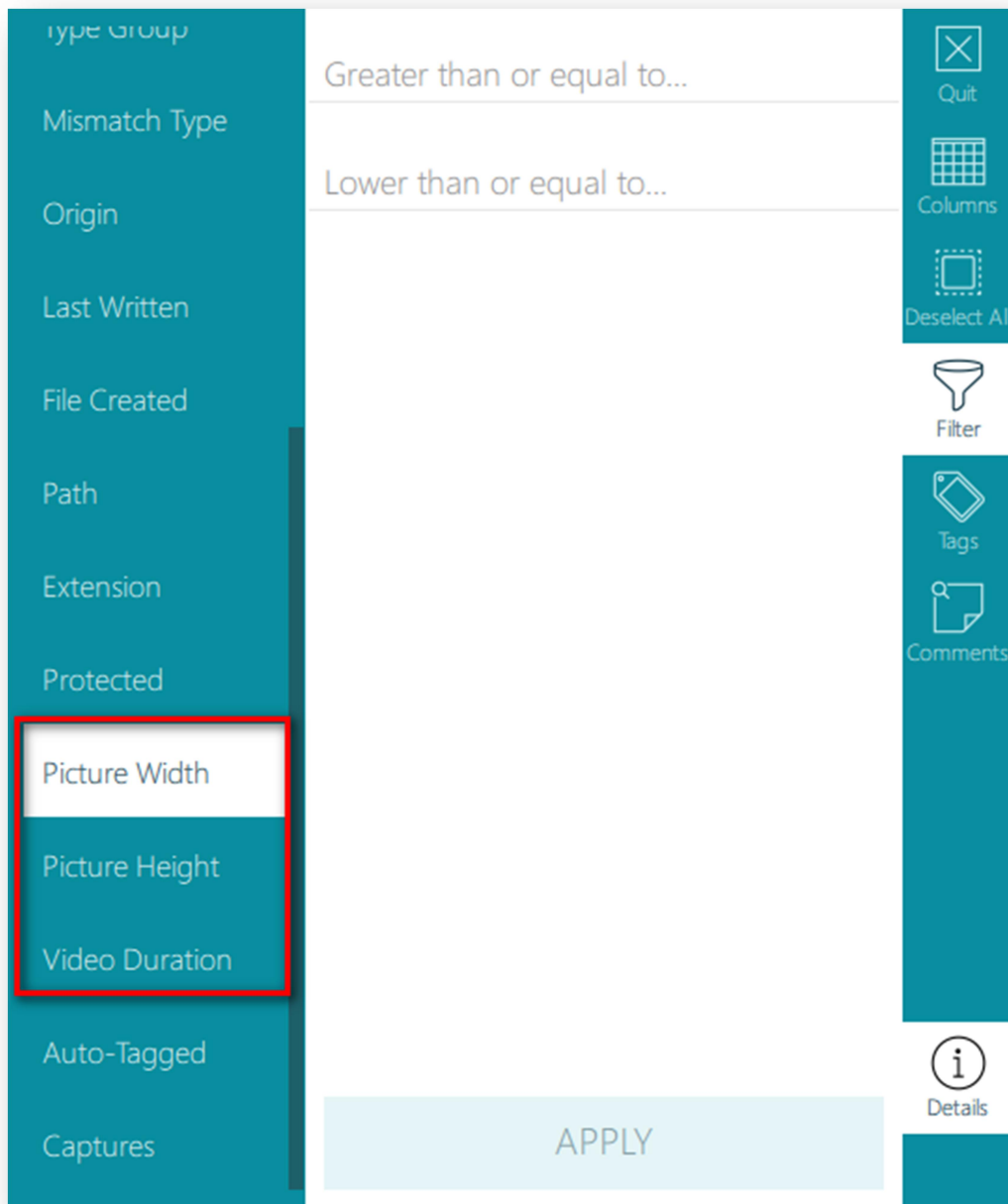


Enhanced Filtering Pictures & Videos

It is possible to apply enhanced filters when searching for Pictures and Videos. These options are available within the Filter when viewing the Picture or Video gallery.


Within the Picture gallery it is possible to filter within a Picture Width and Picture Height range. Within the Video gallery it is possible to filter by Video Duration (where this information has been extracted).

Picture and Video Filter Options



Sorting



Each table view will have different columns depending on the type of capture being viewed. A column, if sortable, will display whether ascending or descending with an arrow and line icon when clicked.

Ascending	Descending
	

Records Selection and Navigation

There are several options for selecting records to be tagged:

A Selected Picture

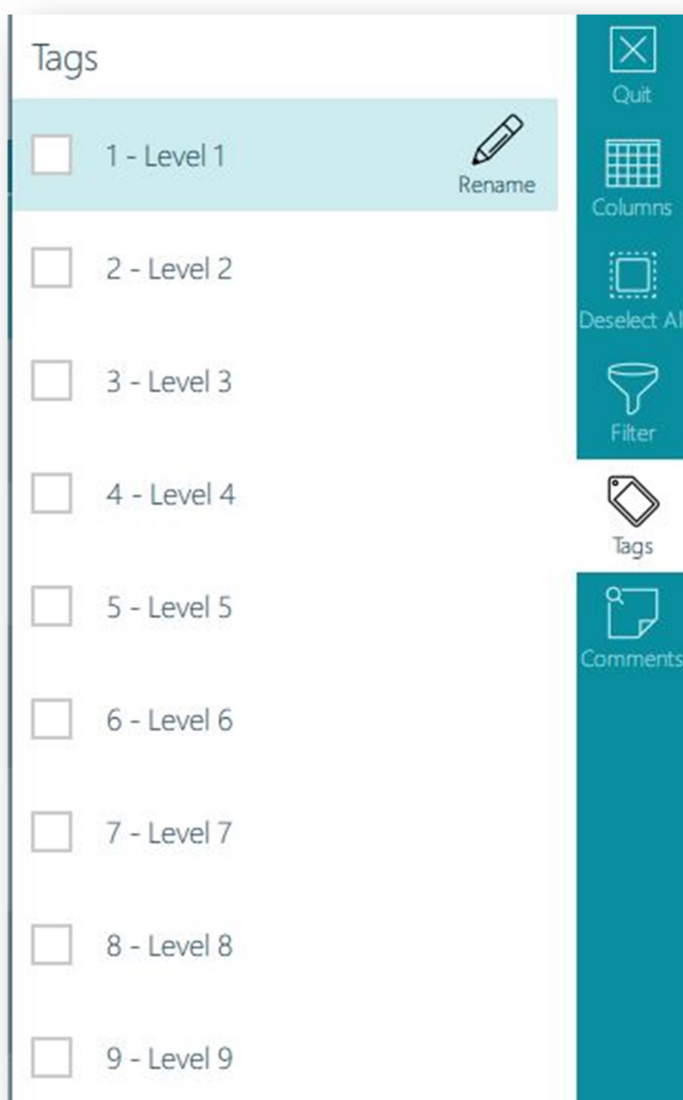
	Preview	File Name	File Type	Type Group
<input type="checkbox"/>				
<input checked="" type="checkbox"/>		iNode1669281	Portable Network Graphic	Picture

1. Select one record - Single click.
2. Select or Deselect multiple records:
 Shift + Click - select first record then shift and click on last record
 + (Plus) - Selects all fully visible records
 - (Minus) - Deselects all fully visible records
3. Page Down - . (Period on numeric keypad) or Page Down key.
4. Page Up - * (Star on numeric keypad) or Page Up key.
5. Navigation:
 Arrow keys (left-right-up-down)
 Scroll bar
 Mouse scroll wheel

Tagging

After you have selected your records there are nine tags available that you can customize for your reporting needs. The default tags are named Level 1 through Level 9 and can be customized by selecting Rename in the Tag function toolbar. Tag names will be applied to the current scan and do not apply to previous scan results. Tagging is also available in the picture gallery.

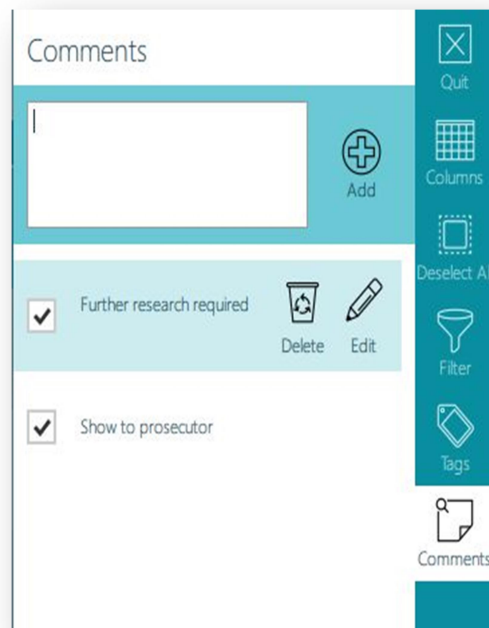
1. To tag records with a specific tag:
Select record(s) then select the appropriate tag in the Tag section of function toolbar
Select record(s) then press numeric key 1-9 as appropriate
Pressing numeric key 0 will un-tag selected records
Records can have multiple tags



Comments

Comments can be added to individual or multiple records by pressing the comments button on the function toolbar or pressing the comment button within the preview icon shown in the picture gallery. Clicking on the comment button opens the comment pane with a text box. Comments will be saved in a list under the Comments text box. Highlighting the individual comments will reveal an edit and delete button for that comment.

1. To add comment to record(s):
Type your comment in the text box and press add
The comment will be added to the selected records
2. To remove/edit/delete a comment from record(s):
Select records with comment(s)
Open Comment pane
Deselect comment - Affects selected records only
Edit Comment - Affects all records with that comment
Delete Comment - Affects all records with that comment



Timeline

The Timeline feature shows specific information regarding files that have been identified during a scan. The information displayed can include file creation and last written times, a user logging in, a P2P search being carried out or a USB stick being inserted into the computer. The information is sorted by the timestamp allowing a greater understanding of what was happening on the computer around times of interest or when a file of interest was interacted with.

Timeline Screen

TIMELINE

Records: 7
Selected Activities: 1
Tags:

	Timestamp	Activity	Info	Preview	Principal
<input type="checkbox"/>	2017/03/10 09:37:41	File created	IPOC - Keywords.csv		
<input type="checkbox"/>	2017/03/10 09:35:08	Last written	IPOC - Keywords.csv		
<input type="checkbox"/>	2016/05/18 14:53:05	Last written	software		
<input type="checkbox"/>	2016/05/17 11:28:18	Last written	Shareaza Install		

Properties **Excerpts**

Preview *File Name* IPOC - Keywords.csv

<i>File Type</i>	Comma-Separated Variables	<i>Type Group</i>	Database File
<i>File System Type</i>	File	<i>Origin</i>	Allocated
<i>Size</i>	815	<i>Last Written</i>	2017/03/10 09:35:08
<i>File Created</i>	2017/03/10 09:37:41	<i>Last Accessed</i>	2017/03/10 09:37:41
<i>Path</i>	Src4	<i>Extension</i>	csv
<i>Protected</i>	Not protected		
<i>Integrity SHA1</i>	VL3Q44HXVVHUY2BXDKQEYIZCJHD6HLKX		
<i>Collected File Path</i>	original_files/allocated_0.zip	<i>Auto-Tagged</i>	No
<i>Match</i>			
<i>Captures</i>	IPOC - Keywords Comprehensive		

Details

Scan Summary

The Scan Summary screen, available by clicking the Summary button when reviewing a scan, provides information about the result of a scan.

Scan Summary Screen

SUMMARY

Scan Name: Scan 2017-03-10 16-33-17
 Scan Date: 2017-03-10
 Scan Time: 16:33:17
 System Date: 2017-03-10
 System Time: 16:33:17
 Viewer Time: Europe/London
 Zone: Europe/London

Name: Comprehensive - IPOC
 Notes: Comprehensive scan - Runs all artifact Captures, collects allocated, embedded, and deleted pictures and videos. Searches for common IPOC keywords, and searches for known hash values. Collects protected files. Files not properly read by parser

Scan Duration: 1h 50m 32s
 Status: Finished
 Files Collected: 64436

CAPTURES

APPLICATIONS

Anti-Forensics Traces	0
Application Usage	0
Installed Applications	170
P2P Files Shared or D...	0
P2P Search Terms	0
P2P Traces	1
Shareaza GUIDs	0

COMMUNICATION

Calls	72
Emails	31
Messages	2418
Other Identities	0
Saved Contacts	98
Skype - Media_cache ...	37
Skype - My Received ...	0

DEVICE DATA

Connection Log	16
OS Information	2
USB History	4

IPOC

IPOC - Hash Set Com...	0
IPOC - Keywords Co...	3
IPOC - Keywords in Fil...	0

MULTIMEDIA

Pictures - with EXIF D...	1
Pictures comprehensive	64124
Videos less than 100M...	326
Videos over 100MB co...	0

USER DATA

Recent Files	4
User Accounts	4
User Logins	39

WEB BROWSERS

Browsing History	1477
Download History	17
Search Terms	226

TARGET DEVICES

Source 3 - //nas-store/homes/stuart.beck1/Images/Macs/ElCapitan_060416/MacBkAir_ElCapitan_060416.E01

Partition 4

Size	200MB
File system	FAT32
Time Zone	Europe/London

Partition 5

Size	111.9GB
File system	HFS
Time Zone	Europe/London

Partition 6

Size	619.9MB
File system	HFS
Time Zone	Europe/London

Unpartitioned space

Size	40KB
------	------

General information such as the scan name, scan duration and Search Profile used can be found at the top of the summary page. The Captures section of the summary page identifies the results of individual file captures. It should be noted that captures running a keyword search within files will display the number of files identified and not the number of keyword matches identified overall.

Clicking on the name of an individual File Capture will take you to the results screen for that File Capture.

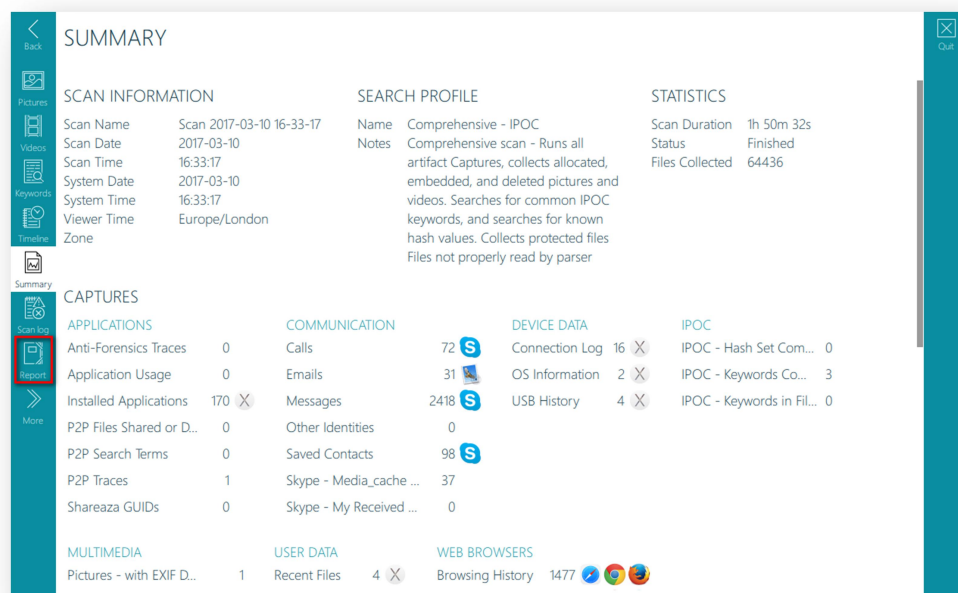
14. Reporting

Reporting is available when reviewing scan results on your laboratory computer, reporting is not available while running Triage-Investigator from the Collection Key. Reviewing, sorting, filtering, and tagging are available whilst reviewing scan results on the target computer. The report creation wizard can be accessed from the Capture and Navigation toolbar as well as the Navigation Pane. Reports can be created in HTML or CSV formats. Additionally, scan results can be exported together with a stand-alone viewer.

HTML Report

The HTML report is customizable allowing the choice of specific Captures and tags to show in your report. Alternatively, all records can also be included in a report. The underlying original files may also be exported (if collected) with the report and the source location of these files is replicated within the exported Zip archive file. If the original files have been collected they can be opened directly from the HTML report providing there are associated applications on the computer opening the report.

1. Select Report button.



2. Select Format – HTML.

CREATE REPORT

Format

- ☒ HTML
- ☐ CSV
- ☐ Standalone viewer

Content Selection

All records	1 - Level 1	2 - Level 2	3 - Level 3	4 - Level 4	5 - Level 5	6 - Level 6	7 - Level 7	8 - Level 8	9 - Level 9	No tag	Include on...	List layout
<input type="checkbox"/> APPLICATIONS>Installed Applica...										170		
<input type="checkbox"/> APPLICATIONS>P2P Traces										1		
<input type="checkbox"/> COMMUNICATION>Calls										72		
<input type="checkbox"/> COMMUNICATION>Emails										31		
<input type="checkbox"/> COMMUNICATION>Messages										2418		
<input type="checkbox"/> COMMUNICATION>Saved Cont...										98		
<input type="checkbox"/> COMMUNICATION>Skype - Me...										37		
<input type="checkbox"/> DEVICE DATA>Connection Log										16		
<input type="checkbox"/> DEVICE DATA>OS Information										2		
<input type="checkbox"/> DEVICE DATA>USB History										4		
<input type="checkbox"/> IPOC>IPOC - Keywords Compre...										9		
<input type="checkbox"/> IPOC>IPOC - Keywords in Filena...										1		
<input type="checkbox"/> MULTIMEDIA>Pictures - with EXL...										28		
<input type="checkbox"/> MULTIMEDIA>Pictures compreh...										2537...		
<input type="checkbox"/> MULTIMEDIA>Videos less than 1...										638		
<input type="checkbox"/> USER DATA>Recent Files										4		
<input type="checkbox"/> USER DATA>User Accounts										4		
<input type="checkbox"/> USER DATA>User Logins										39		
<input type="checkbox"/> WEB BROWSERS>Browsing Hist...										1477		
<input type="checkbox"/> WEB BROWSERS>Download Hist...										17		
<input type="checkbox"/> WEB BROWSERS>Search Terms										226		
<input type="checkbox"/> TIMELINE										2587...		
<input type="checkbox"/> SUMMARY												
<input type="checkbox"/> SCAN LOG										1895...		

EXPORT

3. By default, all tagged records are selected and original files will be exported

CREATE REPORT

Format

- ☒ HTML
- ☐ CSV
- ☐ Standalone viewer

Content Selection

All records	1 - Level 1	2 - Level 2	3 - Level 3	4 - Level 4	5 - Level 5	6 - Level 6	7 - Level 7	8 - Level 8	9 - Level 9	No tag	Include on...	List layout
<input type="checkbox"/> APPLICATIONS>Installed Applica...										170		
<input type="checkbox"/> APPLICATIONS>P2P Traces										1		
<input type="checkbox"/> COMMUNICATION>Calls										72		
<input type="checkbox"/> COMMUNICATION>Emails										31		
<input type="checkbox"/> COMMUNICATION>Messages										2418		
<input type="checkbox"/> COMMUNICATION>Saved Cont...										98		
<input type="checkbox"/> COMMUNICATION>Skype - Me...										37		
<input type="checkbox"/> DEVICE DATA>Connection Log										16		
<input type="checkbox"/> DEVICE DATA>OS Information										2		
<input type="checkbox"/> DEVICE DATA>USB History										4		
<input type="checkbox"/> IPOC>IPOC - Keywords Compre...										9		
<input type="checkbox"/> IPOC>IPOC - Keywords in Filena...										1		
<input checked="" type="checkbox"/> MULTIMEDIA>Pictures - with EXL...										27		
<input checked="" type="checkbox"/> MULTIMEDIA>Pictures compreh...										2537...		
<input type="checkbox"/> MULTIMEDIA>Videos less than 1...										638		
<input type="checkbox"/> USER DATA>Recent Files										4		
<input type="checkbox"/> USER DATA>User Accounts										4		
<input type="checkbox"/> USER DATA>User Logins										39		
<input type="checkbox"/> WEB BROWSERS>Browsing Hist...										1477		
<input type="checkbox"/> WEB BROWSERS>Download Hist...										17		
<input type="checkbox"/> WEB BROWSERS>Search Terms										226		
<input checked="" type="checkbox"/> TIMELINE										2587...		
<input type="checkbox"/> SUMMARY												
<input type="checkbox"/> SCAN LOG										1895...		

EXPORT

- Optional - Select the all records checkbox to include all records.

CREATE REPORT

Format
☒ HTML ☐ CSV ☐ Standalone viewer

Content Selection

	1 - Level 1	2 - Level 2	3 - Level 3	4 - Level 4	5 - Level 5	6 - Level 6	7 - Level 7	8 - Level 8	9 - Level 9	No logs	Include all	Use report
<input checked="" type="checkbox"/> APPLICATIONS>Installed Applica...	<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/> APPLICATIONS>P2P Traces	<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/> COMMUNICATION>Calls	<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/> COMMUNICATION>Emails	<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/> COMMUNICATION>Messages	<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/> COMMUNICATION>Saved Cont...	<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/> COMMUNICATION>Skype - Me...	<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/> DEVICE DATA>Connection Log	<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/> DEVICE DATA>OS Information	<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/> DEVICE DATA>USB History	<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/> IPOC>IPOC - Keywords Compre...	<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/> IPOC>IPOC - Keywords in Filena...	<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/> MULTIMEDIA>Pictures - with EXI...	<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/> MULTIMEDIA>Pictures compreh...	<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/> MULTIMEDIA>Videos less than 1...	<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/> USER DATA>Recent Files	<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/> USER DATA>User Accounts	<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/> USER DATA>User Logins	<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/> WEB BROWSERS>Browsing Hist...	<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/> WEB BROWSERS>Download Hist...	<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/> WEB BROWSERS>Search Terms	<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/> TIMELINE	<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/> SUMMARY	<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/> SCAN LOG	<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>		

EXPORT

- Optional - Select the checkbox next to each capture to include all records in that capture within the report.

CREATE REPORT

Format
☒ HTML ☐ CSV ☐ Standalone viewer

Content Selection

	1 - Level 1	2 - Level 2	3 - Level 3	4 - Level 4	5 - Level 5	6 - Level 6	7 - Level 7	8 - Level 8	9 - Level 9	No logs	Include all	Use report
<input type="checkbox"/> APPLICATIONS>Installed Applica...	<input type="checkbox"/>									<input checked="" type="checkbox"/>		
<input type="checkbox"/> APPLICATIONS>P2P Traces	<input type="checkbox"/>									<input checked="" type="checkbox"/>		
<input type="checkbox"/> COMMUNICATION>Calls	<input type="checkbox"/>									<input checked="" type="checkbox"/>		
<input type="checkbox"/> COMMUNICATION>Emails	<input type="checkbox"/>									<input checked="" type="checkbox"/>		
<input type="checkbox"/> COMMUNICATION>Messages	<input type="checkbox"/>									<input checked="" type="checkbox"/>		
<input type="checkbox"/> COMMUNICATION>Saved Cont...	<input type="checkbox"/>									<input checked="" type="checkbox"/>		
<input type="checkbox"/> COMMUNICATION>Skype - Me...	<input type="checkbox"/>									<input checked="" type="checkbox"/>		
<input type="checkbox"/> DEVICE DATA>Connection Log	<input type="checkbox"/>									<input checked="" type="checkbox"/>		
<input type="checkbox"/> DEVICE DATA>OS Information	<input type="checkbox"/>									<input checked="" type="checkbox"/>		
<input type="checkbox"/> DEVICE DATA>USB History	<input type="checkbox"/>									<input checked="" type="checkbox"/>		
<input type="checkbox"/> IPOC>IPOC - Keywords Compre...	<input type="checkbox"/>									<input checked="" type="checkbox"/>		
<input type="checkbox"/> IPOC>IPOC - Keywords in Filena...	<input type="checkbox"/>									<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/> MULTIMEDIA>Pictures - with EXI...	<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>		
<input type="checkbox"/> MULTIMEDIA>Pictures compreh...	<input type="checkbox"/>									<input checked="" type="checkbox"/>		
<input type="checkbox"/> MULTIMEDIA>Videos less than 1...	<input type="checkbox"/>									<input checked="" type="checkbox"/>		
<input type="checkbox"/> USER DATA>Recent Files	<input type="checkbox"/>									<input checked="" type="checkbox"/>		
<input type="checkbox"/> USER DATA>User Accounts	<input type="checkbox"/>									<input checked="" type="checkbox"/>		
<input type="checkbox"/> USER DATA>User Logins	<input type="checkbox"/>									<input checked="" type="checkbox"/>		
<input type="checkbox"/> WEB BROWSERS>Browsing Hist...	<input type="checkbox"/>									<input checked="" type="checkbox"/>		
<input type="checkbox"/> WEB BROWSERS>Download Hist...	<input type="checkbox"/>									<input checked="" type="checkbox"/>		
<input type="checkbox"/> WEB BROWSERS>Search Terms	<input type="checkbox"/>									<input checked="" type="checkbox"/>		
<input type="checkbox"/> TIMELINE	<input type="checkbox"/>									<input checked="" type="checkbox"/>		
<input type="checkbox"/> SUMMARY	<input type="checkbox"/>									<input checked="" type="checkbox"/>		
<input type="checkbox"/> SCAN LOG	<input type="checkbox"/>									<input checked="" type="checkbox"/>		

EXPORT

6. Optional - Select the checkbox above each tag to include all of these tagged records in within the report.

CREATE REPORT

Format

- HTML
- CSV
- Standalone viewer

Content Selection

	All records	Level 1	Level 2	Level 3	Level 4	Level 5	Level 6	Level 7	Level 8	Level 9	No tag	Include all	List legend
APPLICATIONS>Installed Applica...	<input checked="" type="checkbox"/>												
APPLICATIONS>P2P Traces	<input type="checkbox"/>												
COMMUNICATION>Calls	<input type="checkbox"/>												
COMMUNICATION>Emails	<input type="checkbox"/>												
COMMUNICATION>Messages	<input type="checkbox"/>												
COMMUNICATION>Saved Cont...	<input type="checkbox"/>												
COMMUNICATION>Skype - Me...	<input type="checkbox"/>												
DEVICE DATA>Connection Log	<input type="checkbox"/>												
DEVICE DATA>OS Information	<input type="checkbox"/>												
DEVICE DATA>USB History	<input type="checkbox"/>												
IPOC>IPOC - Keywords Compre...	<input type="checkbox"/>												
IPOC>IPOC - Keywords in Fila...	<input type="checkbox"/>												
MULTIMEDIA>Pictures - with EXIF...	<input checked="" type="checkbox"/>											<input checked="" type="checkbox"/>	
MULTIMEDIA>Pictures compreh...	<input checked="" type="checkbox"/>											<input checked="" type="checkbox"/>	
MULTIMEDIA>Videos less than 1...	<input type="checkbox"/>												
USER DATA>Recent Files	<input type="checkbox"/>												
USER DATA>User Accounts	<input type="checkbox"/>												
USER DATA>User Logins	<input type="checkbox"/>												
WEB BROWSERS>Browsing Hist...	<input type="checkbox"/>												
WEB BROWSERS>Download Hist...	<input type="checkbox"/>												
WEB BROWSERS>Search Terms	<input type="checkbox"/>												
TIMELINE	<input checked="" type="checkbox"/>												
SUMMARY	<input type="checkbox"/>												
SCAN LOG	<input type="checkbox"/>												

EXPORT

7. Optional - Select the checkbox to export original files where collected.

CREATE REPORT

Format

- HTML
- CSV
- Standalone viewer

Content Selection

	All records	Level 1	Level 2	Level 3	Level 4	Level 5	Level 6	Level 7	Level 8	Level 9	No tag	Include all	List legend
APPLICATIONS>Installed Applica...	<input checked="" type="checkbox"/>												
APPLICATIONS>P2P Traces	<input type="checkbox"/>												
COMMUNICATION>Calls	<input type="checkbox"/>												
COMMUNICATION>Emails	<input type="checkbox"/>												
COMMUNICATION>Messages	<input type="checkbox"/>												
COMMUNICATION>Saved Cont...	<input type="checkbox"/>												
COMMUNICATION>Skype - Me...	<input type="checkbox"/>												
DEVICE DATA>Connection Log	<input type="checkbox"/>												
DEVICE DATA>OS Information	<input type="checkbox"/>												
DEVICE DATA>USB History	<input type="checkbox"/>												
IPOC>IPOC - Keywords Compre...	<input type="checkbox"/>												
IPOC>IPOC - Keywords in Fila...	<input type="checkbox"/>												
MULTIMEDIA>Pictures - with EXIF...	<input checked="" type="checkbox"/>											<input checked="" type="checkbox"/>	
MULTIMEDIA>Pictures compreh...	<input checked="" type="checkbox"/>											<input checked="" type="checkbox"/>	
MULTIMEDIA>Videos less than 1...	<input type="checkbox"/>												
USER DATA>Recent Files	<input type="checkbox"/>												
USER DATA>User Accounts	<input type="checkbox"/>												
USER DATA>User Logins	<input type="checkbox"/>												
WEB BROWSERS>Browsing Hist...	<input type="checkbox"/>												
WEB BROWSERS>Download Hist...	<input type="checkbox"/>												
WEB BROWSERS>Search Terms	<input type="checkbox"/>												
TIMELINE	<input checked="" type="checkbox"/>												
SUMMARY	<input type="checkbox"/>												
SCAN LOG	<input type="checkbox"/>												

EXPORT

8. Optional - Select the checkbox to have a list instead of table layout within the report.

CREATE REPORT

Format

- HTML
- CSV
- Standalone viewer

Content Selection

	All records	1 - Level 1	2 - Level 2	3 - Level 3	4 - Level 4	5 - Level 5	6 - Level 6	7 - Level 7	8 - Level 8	9 - Level 9	No tag	Include on	List layout
APPLICATIONS>Installed Applica...	<input type="checkbox"/>										170	<input type="checkbox"/>	<input type="checkbox"/>
APPLICATIONS>P2P Traces	<input type="checkbox"/>										1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
COMMUNICATION>Calls	<input type="checkbox"/>										72	<input type="checkbox"/>	<input type="checkbox"/>
COMMUNICATION>Emails	<input type="checkbox"/>										31	<input checked="" type="checkbox"/>	<input type="checkbox"/>
COMMUNICATION>Messages	<input type="checkbox"/>										2418	<input type="checkbox"/>	<input type="checkbox"/>
COMMUNICATION>Saved Cont...	<input type="checkbox"/>										98	<input type="checkbox"/>	<input type="checkbox"/>
COMMUNICATION>Skype - Me...	<input type="checkbox"/>										37	<input checked="" type="checkbox"/>	<input type="checkbox"/>
DEVICE DATA>Connection Log	<input type="checkbox"/>										16	<input type="checkbox"/>	<input type="checkbox"/>
DEVICE DATA>OS Information	<input type="checkbox"/>										2	<input type="checkbox"/>	<input type="checkbox"/>
DEVICE DATA>USB History	<input type="checkbox"/>										4	<input type="checkbox"/>	<input type="checkbox"/>
IPOC>IPOC - Keywords Compre...	<input type="checkbox"/>										9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
IPOC>IPOC - Keywords in Fila...	<input type="checkbox"/>										1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
MULTIMEDIA>Pictures - with EX...	<input checked="" type="checkbox"/>										27	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
MULTIMEDIA>Pictures compreh...	<input checked="" type="checkbox"/>										2537...	<input checked="" type="checkbox"/>	<input type="checkbox"/>
MULTIMEDIA>Videos less than 1...	<input type="checkbox"/>										638	<input checked="" type="checkbox"/>	<input type="checkbox"/>
USER DATA>Recent Files	<input type="checkbox"/>										4	<input type="checkbox"/>	<input type="checkbox"/>
USER DATA>User Accounts	<input type="checkbox"/>										4	<input type="checkbox"/>	<input type="checkbox"/>
USER DATA>User Logins	<input type="checkbox"/>										39	<input type="checkbox"/>	<input type="checkbox"/>
WEB BROWSERS>Browsing Hist...	<input type="checkbox"/>										1477	<input type="checkbox"/>	<input type="checkbox"/>
WEB BROWSERS>Download Hist...	<input type="checkbox"/>										17	<input type="checkbox"/>	<input type="checkbox"/>
WEB BROWSERS>Search Terms	<input type="checkbox"/>										226	<input type="checkbox"/>	<input type="checkbox"/>
TIMELINE	<input checked="" type="checkbox"/>										2587...	<input type="checkbox"/>	<input type="checkbox"/>
SUMMARY	<input type="checkbox"/>												<input type="checkbox"/>
SCAN LOG	<input type="checkbox"/>										1895...	<input type="checkbox"/>	<input type="checkbox"/>

EXPORT

9. Optional - Select the checkbox to have a Summary page included within the report.

CREATE REPORT

Format

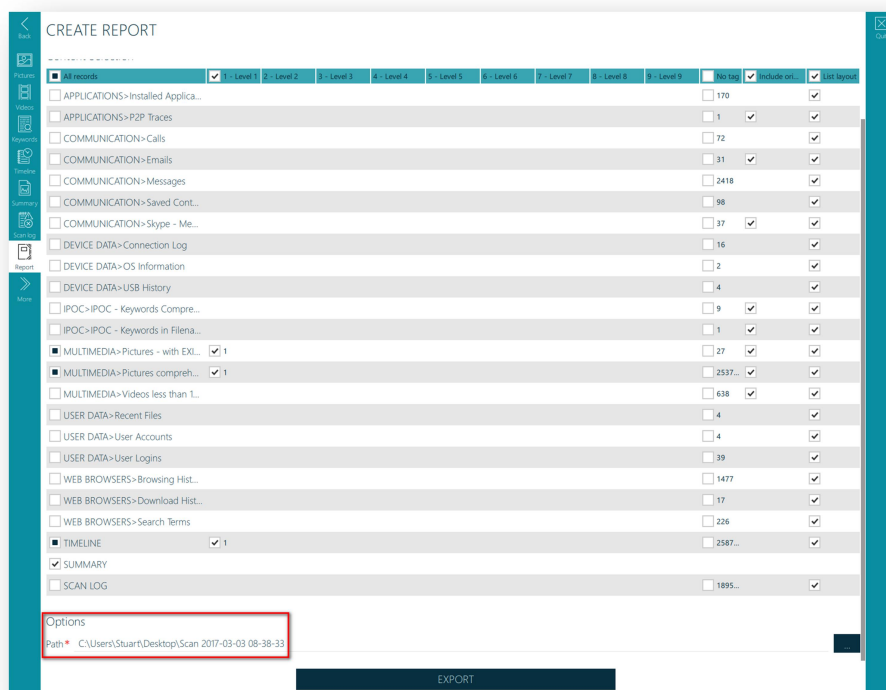
- HTML
- CSV
- Standalone viewer

Content Selection

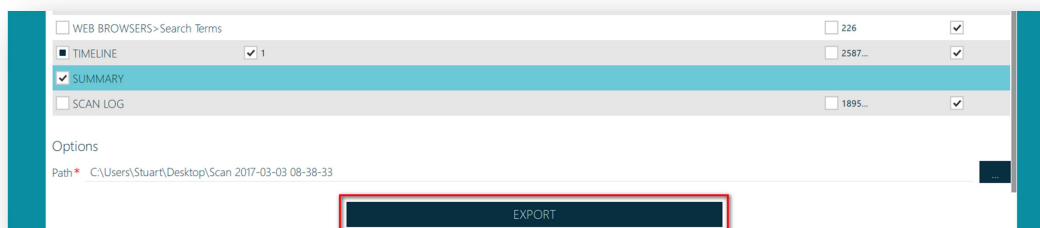
	All records	1 - Level 1	2 - Level 2	3 - Level 3	4 - Level 4	5 - Level 5	6 - Level 6	7 - Level 7	8 - Level 8	9 - Level 9	No tag	Include on	List layout
APPLICATIONS>Installed Applica...	<input type="checkbox"/>										170	<input type="checkbox"/>	<input type="checkbox"/>
APPLICATIONS>P2P Traces	<input type="checkbox"/>										1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
COMMUNICATION>Calls	<input type="checkbox"/>										72	<input type="checkbox"/>	<input type="checkbox"/>
COMMUNICATION>Emails	<input type="checkbox"/>										31	<input checked="" type="checkbox"/>	<input type="checkbox"/>
COMMUNICATION>Messages	<input type="checkbox"/>										2418	<input type="checkbox"/>	<input type="checkbox"/>
COMMUNICATION>Saved Cont...	<input type="checkbox"/>										98	<input type="checkbox"/>	<input type="checkbox"/>
COMMUNICATION>Skype - Me...	<input type="checkbox"/>										37	<input checked="" type="checkbox"/>	<input type="checkbox"/>
DEVICE DATA>Connection Log	<input type="checkbox"/>										16	<input type="checkbox"/>	<input type="checkbox"/>
DEVICE DATA>OS Information	<input type="checkbox"/>										2	<input type="checkbox"/>	<input type="checkbox"/>
DEVICE DATA>USB History	<input type="checkbox"/>										4	<input type="checkbox"/>	<input type="checkbox"/>
IPOC>IPOC - Keywords Compre...	<input type="checkbox"/>										9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
IPOC>IPOC - Keywords in Fila...	<input type="checkbox"/>										1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
MULTIMEDIA>Pictures - with EX...	<input checked="" type="checkbox"/>										27	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
MULTIMEDIA>Pictures compreh...	<input checked="" type="checkbox"/>										2537...	<input checked="" type="checkbox"/>	<input type="checkbox"/>
MULTIMEDIA>Videos less than 1...	<input type="checkbox"/>										638	<input checked="" type="checkbox"/>	<input type="checkbox"/>
USER DATA>Recent Files	<input type="checkbox"/>										4	<input type="checkbox"/>	<input type="checkbox"/>
USER DATA>User Accounts	<input type="checkbox"/>										4	<input type="checkbox"/>	<input type="checkbox"/>
USER DATA>User Logins	<input type="checkbox"/>										39	<input type="checkbox"/>	<input type="checkbox"/>
WEB BROWSERS>Browsing Hist...	<input type="checkbox"/>										1477	<input type="checkbox"/>	<input type="checkbox"/>
WEB BROWSERS>Download Hist...	<input type="checkbox"/>										17	<input type="checkbox"/>	<input type="checkbox"/>
WEB BROWSERS>Search Terms	<input type="checkbox"/>										226	<input type="checkbox"/>	<input type="checkbox"/>
TIMELINE	<input checked="" type="checkbox"/>										2587...	<input type="checkbox"/>	<input type="checkbox"/>
SUMMARY	<input checked="" type="checkbox"/>												<input type="checkbox"/>
SCAN LOG	<input type="checkbox"/>										1895...	<input type="checkbox"/>	<input type="checkbox"/>

EXPORT

10. Optional - Choose path to save report to (Default Desktop).



11. Click on the Export button to create the HTML report.



NOTE: the HTML report displays the same columns that were visible in the viewer in the order they were displayed. To remove columns from the HTML report, simply hide them in the viewer.

CSV Report

The CSV report is customizable allowing the choice of specific Captures and tags to show in your report, all records can also be shown in the report. Results where files were captured can be set to export the files which will be maintained in a ZIP archive in its' original path. The CSV report has the same options as the HTML report with the exception that all the records' properties are always exported, and exporting the results in a list view is not an option.

CSV Report

The screenshot shows the 'CREATE REPORT' dialog box. The 'Format' section has 'HTML' and 'Standalone viewer' options, with 'CSV' selected and highlighted by a red box. The 'Content Selection' section contains a table with various content categories and their counts. The table has columns for 'All records', '1 - Level 1', '2 - Level 2', '3 - Level 3', '4 - Level 4', '5 - Level 5', '6 - Level 6', '7 - Level 7', '8 - Level 8', '9 - Level 9', 'No tag', and 'Include only'. The 'All records' column is checked. The 'Include only' checkbox is also checked. The table lists various content categories with their respective counts and checkboxes for selection.

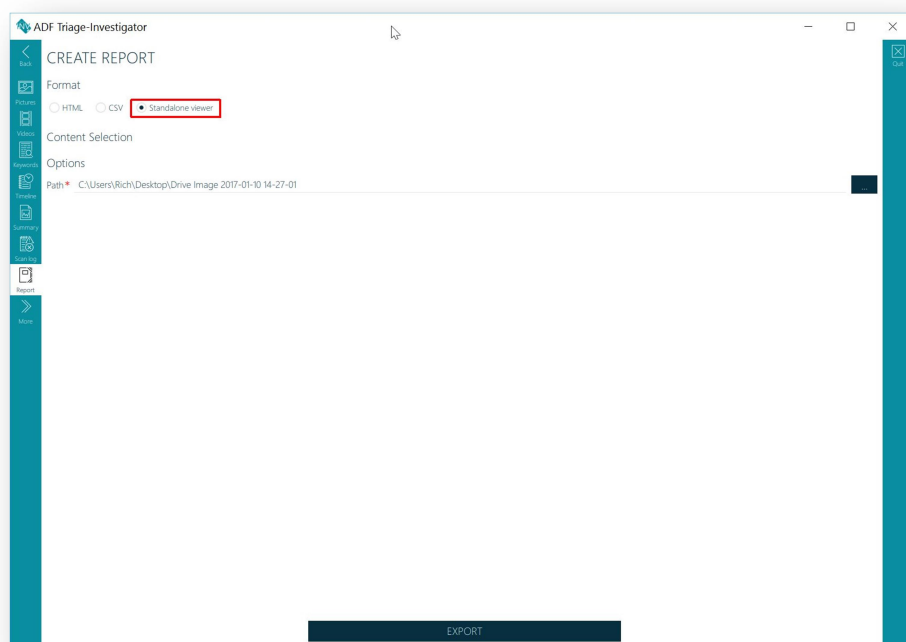
	All records	1 - Level 1	2 - Level 2	3 - Level 3	4 - Level 4	5 - Level 5	6 - Level 6	7 - Level 7	8 - Level 8	9 - Level 9	No tag	Include only
APPLICATIONS>Installed Applica...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	170	<input type="checkbox"/>
APPLICATIONS>P2P Traces	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	<input checked="" type="checkbox"/>
COMMUNICATION>Calls	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	72	<input type="checkbox"/>
COMMUNICATION>Emails	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	31	<input checked="" type="checkbox"/>
COMMUNICATION>Messages	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2418	<input type="checkbox"/>
COMMUNICATION>Saved Cont...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	98	<input type="checkbox"/>
COMMUNICATION>Skype - Me...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	37	<input checked="" type="checkbox"/>
DEVICE DATA>Connection Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	16	<input type="checkbox"/>
DEVICE DATA>OS Information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2	<input type="checkbox"/>
DEVICE DATA>USB History	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	4	<input type="checkbox"/>
IPOC>IPOC - Keywords Compre...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	9	<input checked="" type="checkbox"/>
IPOC>IPOC - Keywords in Fila...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	<input checked="" type="checkbox"/>
MULTIMEDIA>Pictures - with EX...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>
MULTIMEDIA>Pictures compreh...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2537...	<input checked="" type="checkbox"/>
MULTIMEDIA>Videos less than 1...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	638	<input checked="" type="checkbox"/>
USER DATA>Recent Files	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	4	<input type="checkbox"/>
USER DATA>User Accounts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	4	<input type="checkbox"/>
USER DATA>User Logins	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	39	<input type="checkbox"/>
WEB BROWSERS>Browsing Hist...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1477	<input type="checkbox"/>
WEB BROWSERS>Download Hist...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	17	<input type="checkbox"/>
WEB BROWSERS>Search Terms	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	226	<input type="checkbox"/>
TIMELINE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2587...	<input type="checkbox"/>
SCAN LOG	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1895...	<input type="checkbox"/>

EXPORT

Standalone Viewer

The Standalone Viewer displays all results in the Review Scan Results Mode of the software, all analysis and work completed on the results to that point are exported and maintained. This allows for collaboration and sharing with others to review and identify records of value to the case. The viewer does not require a license and allows for the creation of an HTML or CSV report. The viewer will require that the computer user has permissions to execute a Batch File (.bat). The Standalone Viewer cannot be executed from a read-only storage device such as CD or DVD.

Standalone Viewer



15. Custom Search Profiles and File Captures

Triage-Investigator comes with seven (7) ready to use default Search Profiles. A Search Profile is a combination of Captures. Artifact Captures recover specific records or information e.g. browsing history records or user account information. Users cannot create or edit Artifact Captures. File Captures recover files matching certain criteria such as file properties, inclusion of keywords or matching hash values. File Captures are supplied with the program and can also be user created.

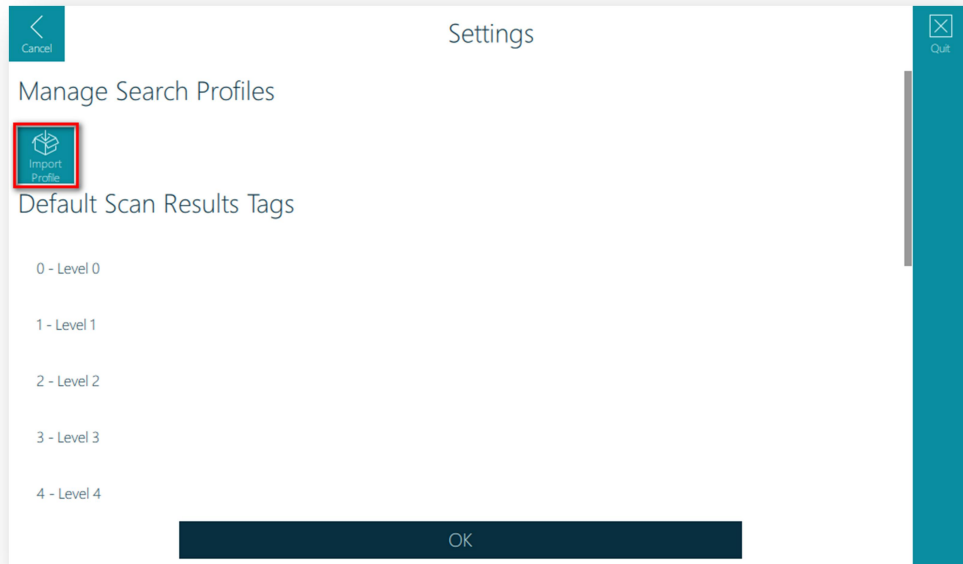
Triage-Investigator does not have the capability to edit or create custom profiles or captures but it is possible to import Search Profiles created within Digital Evidence Investigator.

Upgrading to Digital Evidence Investigator allows the creation of custom Search Profiles by selecting default Artifact and File Captures and adding user created File Captures to the profile.

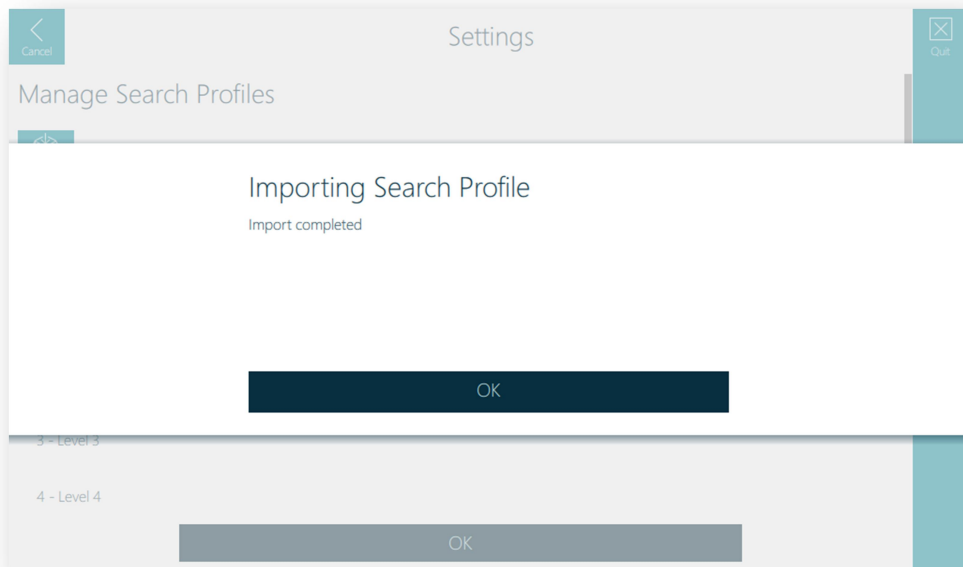
For further information visit <http://adfsolutions.com/dei.html>

Importing a Search Profile

1. Within the Settings screen, click on the Import Profile button. This will open a file browser dialog window, from here you can select the profile you wish to import.



2. After the profile has been imported a message will be displayed to show the process has completed.



16. FAQ

Question: Do the scan logs contain evidence and are they safe to send to ADF?

The application creates multiple log files that are useful to identify the source of potential issues. These files do not contain scan results and are safe to share with ADF's support team. Log files can be found in:

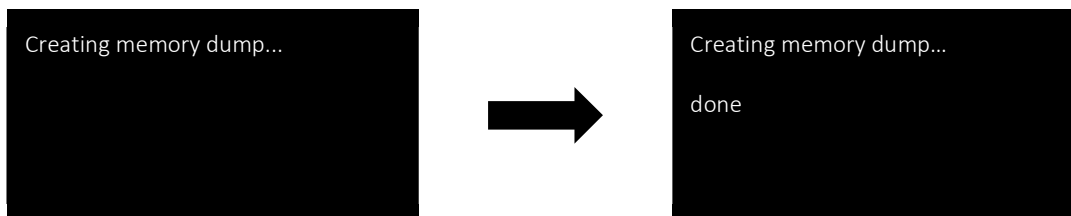
- Log files created by the desktop application:
 - C:\ProgramData\ADF Solutions Inc\v4\ScanResults\<SCAN NAME>\SysLogs
 - C:\ProgramData\ADF Solutions Inc\v4\SysLogs
- Log files created by the scanner application on the Collection Key:
 - \ScanResults\<SCAN NAME>\SysLogs
 - \SysLogs

Question: If the system has a crash where can I gather the information?

On the rare occasion the application crashes, a process memory dump is created in the following locations:

- Desktop application:
 - C:\ProgramData\ADF Solutions Inc\v4\CrashDump
 - C:\ProgramData\ADF Solutions Inc\v4\ScanResults\<SCAN NAME>\CrashDump
- Scanner application on the Collection Key:
 - \CrashDump
 - \ScanResults\<SCAN NAME>\CrashDump

NOTE: Wait until the application has finished creating the crash dump before closing it!



17. Glossary

Term	Meaning
Artifact	A digital record created by a computer process.
Artifact Capture	An automated process that collects and analyzes artifacts on the target device.
Authentication Key	A USB device that contains the license file for Triage Investigator
BIOS	BIOS (basic input/output system) is the program a personal computer's microprocessor uses to get the computer system started after you turn it on.
Carving	Recovering data that has been deleted and no longer referenced by the file system. This is done by searching for file signatures within unallocated space.
Collection Key	A bootable USB device used to conduct a Boot Scan or Live Scan and collect and store the scan results.
Encryption	Data encryption translates data into another form, or code, so that only people with access to a secret key or password can read it.
Evidence Image File	A forensic image is a container that is used to store a digitally identical copy of the target media.
File Capture	An automated process that collects files based on file properties and or keywords and or hash values.
File Extension	A file extension is typically 3 characters after the full stop in a file name. The extension identifies the file type.
File Header	Generally, a short sequence of bytes placed at the beginning of the file used to identify the format of the file.
File System	A File System is used to control how data is stored on and retrieved from digital storage devices.
Firmware	Firmware is a software program or set of instructions programmed onto a hardware device. It provides the necessary instructions for how the device communicates with the other computer hardware.
Gigabyte (GB)	A gigabyte (also referred to as GB) is a unit of data equal to 1,000,000,000 bytes of data.
Hash Hash Value Hashing	A hash value is a numeric value of a fixed length that uniquely identifies data. Hash values are useful to prove that computer data has not changed or to quickly identify certain known files.
HTML	Hyper Text Markup Language (HTML) is the standard markup language for creating web pages and web applications.
Kilobyte (KB)	A Kilobyte (KB) is a unit of data equal to 1,024 bytes.

Term	Meaning
Logical Drive	A logical drive is a drive space that is created on top of a physical hard disk drive. A logical drive is a separate partition with its own parameters and functions, and it operates independently. A logical drive can also be called a logical drive partition or logical disk partition.
Megabyte (MB)	A Megabyte (MB) is a unit of data equal to 1,048,576 bytes.
Partition	A partition is a section of a hard disk that is treated as a separate unit by operating systems and file systems.
Physical Disk	A physical disk (also known a hard disk drive) is a data storage device used for storing and retrieving digital information using one or more rigid rapidly rotating disks (platters) coated with magnetic material.
Pixel	The <i>pixel</i> (a word invented from "picture element") is the basic unit of programmable color on a computer display or in a computer image file.
Regular Expression (Regex)	Regular expressions enable users to create complex search terms following the Regular Expression search pattern language and specify what to do when each pattern match is found.
Search Profile	A compilation of Artifact Captures and File Captures used to scan a target device.
Solid State Drive (SSD)	A data storage device containing non-volatile flash memory, used in place of a hard disk drive for its much greater speed.
Standalone Viewer	Triage Investigator's tool that enables the export of Scan Results for review and analysis on another computer without requiring a license.
Substring	A string of characters or symbols that is part of a longer string or characters or symbols.
UEFI (Unified Extensible Firmware Interface)	Unified Extensible Firmware Interface (UEFI) is a specification that defines a more modernized model for the interface between computer operating systems and platform firmware during the boot, or start-up, process.
Unallocated	Unallocated clusters (also referred to as unallocated space or free space) are the available drive storage space that is not allocated to file storage by a volume. Unallocated clusters can be a valuable source of evidence in a computer forensics examination because they can contain deleted files or remnants of deleted files created by the Operating System and / or computer users.
USB (Universal Serial Bus)	A hardware interface for attaching peripherals to a computer.
Volume	A volume or logical drive) is a single accessible storage area with a single file system, typically (though not necessarily) resident on a single partition of a hard disk.

Appendices

Appendix A - BIOS Access Keys

Manufacturer	Type	Models	Boot Menu	Boot Once	BIOS/UEFI Key	Change Priority
Acer			<u>F12</u>		Del, F2	
Acer	netbook	Aspire One zg5, zg8	<u>F12</u>		F2	
Acer	netbook	Aspire Timeline	<u>F12</u>		F2	
Acer	netbook	Aspire v3, v5, v7	<u>F12</u>	The "F12 Boot Menu" must be enabled in BIOS. It is disabled by default.	<u>F2</u>	
Apple		After 2006	<u>Option</u>			
Asus	desktop		<u>F8</u>		F9	
Asus	laptop	VivoBook f200ca, f202e, q200e, s200e, s400ca, s500ca, u38n, v500ca, v550ca, v551, x200ca, x202e, x550ca, z202e	<u>Esc</u>		Delete	
Asus	laptop	N550JV, N750JV, N550LF, Rog g750jh, Rog g750jw, Rog g750jx	<u>Esc</u>	Disable "Fast Boot" and "Secure Boot Control" in order to boot from MBR formatted media.	F2	
Asus	laptop	Zenbook Infinity ux301, Infinity ux301la, Prime ux31a, Prime ux32vd, R509C, Taichi 21, Touch u500vz, Transformer Book TX300	<u>Esc</u>	Disable "Fast Boot" and "Secure Boot Control" in order to boot from MBR formatted media.	F2	

Manufacturer	Type	Models	Boot Menu	Boot Once	BIOS/UEFI Key	Change Priority
Asus	notebook	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	<u>F8</u>		DEL	
Asus	netbook	Eee PC 1015, 1025c	<u>Esc</u>		F2	Boot Tab, Boot Device Priority, 1st Boot Device, Removable Device, F10
Compaq		Presario	<u>Esc, F9</u>		F10	BIOS "Advanced Tab", Boot Order
Dell	desktop	Dimension, Inspiron, Latitude, Optiplex	<u>F12</u>	Select "USB Flash Drive".	F2	
Dell	desktop	Alienware Aurora, Inspiron One 20, Inspiron 23 Touch, Inspiron 620, 630, 650, 660s, Inspiron 3000, X51, XPS 8300, XPS 8500, XPS 8700, XPS 18 Touch, XPS 27 Touch	<u>F12</u>	Select "USB Flash Drive".	F2	
Dell	desktop	Inspiron One 2020, 2305, 2320, 2330 All-In-One	<u>F12</u>	Select "USB Flash Drive".	F2	

Manufacturer	Type	Models	Boot Menu	Boot Once	BIOS/UEFI Key	Change Priority
Dell	laptop	Inspiron 11 3000 series touch, 14z Ultrabook, 14 7000 series touch, 15z Ultrabook touch, 15 7000 series touch, 17 7000 series touch	<u>F12</u>	Select "USB Storage Device"	F2	Settings->General->Boot Sequence->"USB Storage Device", then up arrow, [Apply]--[Exit]
Dell	laptop	Inspiron 14R non-touch, 15 non-touch, 15R non-touch, 17 non-touch, 17R non-touch	<u>F12</u>	Select "USB Storage Device"	F2	Settings->General->Boot Sequence->"USB Storage Device", then up arrow, [Apply]--[Exit]
Dell	laptop	Latitude c400, c600, c640, d610, d620, d630, d830, e5520, e6320, e6400, e6410, e6420, e6430, e6500, e6520, 6430u Ultrabook, x300	<u>F12</u>	Select "USB Storage Device" from boot menu.	F2	
Dell	laptop	Precision m3800, m4400, m4700, m4800, m6500, m6600, m6700, m6800	<u>F12</u>	Select "USB Storage Device" from boot menu.	F2	
Dell	laptop	Alienware 14, Alienware 17, Alienware 18, XPS 11 2-in-1, XPS 12 2-in-1, XPS 13, XPS 14 Ultrabook, XPS 15 Touch,	<u>F12</u>	Select "USB Storage Device" from boot menu.	F2	
eMachines			<u>F12</u>		Tab, Del	
Fujitsu			<u>F12</u>		F2	
HP	generic		<u>Esc, F9</u>		Esc, F10, F1	
HP	desktop	Pavilion Media Center a1477c	<u>Esc</u>		F10	BIOS "Advanced" tab, Boot Order, Move "USB Device" before "Hard Drive"

Manufacturer	Type	Models	Boot Menu	Boot Once	BIOS/UEFI Key	Change Priority
HP	desktop	Pavilion 23 All In One	<u>Esc</u>	Select boot media from the menu.	F10	UEFI/BIOS "Advanced" tab, Boot Order, Move "USB Device" before "Hard Drive". For non-UEFI media, disable secure boot and enable legacy support.
HP	desktop	Pavilion Elite e9000, e9120y, e9150t, e9220y, e9280t	<u>Esc, F9</u>		F10	
HP	desktop	Pavilion g6 and g7	<u>Esc</u>		F10	UEFI/BIOS "Advanced" tab, Boot Order, Move "USB Device" before "Hard Drive"
HP	desktop	Pavilion HPE PC, h8-1287c	<u>Esc</u>	Then F9 for "Boot Menu"	Esc	F10, Storage tab, Boot Order, Legacy Boot Sources
HP	desktop	Pavilion PC, p6 2317c	<u>Esc</u>	Then F9 for "Boot Menu"	Esc	F10, Storage tab, Boot Order, Legacy Boot Sources
HP	desktop	Pavilion PC, p7 1297cb	<u>Esc</u>	Then F9 for "Boot Menu"	Esc	F10, Storage tab, Boot Order, Legacy Boot Sources
HP	desktop	TouchSmart 520 PC	<u>Esc</u>	Then F9 for "Boot Menu"	Esc	F10, Storage tab, Boot Order, Legacy Boot Sources
HP	laptop	2000	<u>Esc</u>	Then F9 for "Boot Menu". Select "Patriot Memory" on the Boot Option Menu.	Esc	Then F10, Storage tab, Boot Order, Legacy Boot Sources
HP	notebook	Pavilion g4	<u>Esc</u>		F10	BIOS "Advanced" tab, Boot Order, Move "USB Device" before "Hard Drive"
HP	notebook	ENVY x2, m4, m4-1015dx, m4-1115dx, sleekbook m6, m6-1105dx, m6-1205dx, m6-k015dx, m6-k025dx, touchsmart m7	<u>Esc</u>	Then F9 for "Boot Menu"	Esc	Then F10, Storage tab, Boot Order, Legacy Boot Sources
HP	notebook	Envy, dv6 and dv7 PC, dv9700, Spectre 14, Spectre 13	<u>Esc</u>	Then F9 for "Boot Menu"	Esc	Then F10, Storage tab, Boot Order, Legacy Boot Sources

Manufacturer	Type	Models	Boot Menu	Boot Once	BIOS/UEFI Key	Change Priority
HP	notebook	2000 - 2a20nr, 2a53ca, 2b16nr, 2b89wm, 2c29wm, 2d29wm	<u>Esc</u>	Then F9 for "Boot Menu"	Esc	Then F10, Storage tab, Boot Order, Legacy Boot Sources
HP	notebook	Probook 4520s, 4525s, 4540s, 4545s, 5220m, 5310m, 5330m, 5660b, 5670b	<u>Esc</u>		F10	BIOS "Advanced" tab, Boot Order, Move "USB Device" before "Hard Drive"
HP	tower	Pavilion a410n	<u>Esc</u>		F1	BIOS "Boot" tab, Boot Device Priority, Hard Drive Boot Priority, Move "USB-HDD0" up to #1 position.
IBM	ThinkPad		<u>F11</u>			
Intel			<u>F10</u>			
Lenovo	desktop		<u>F12, F8, F10</u>		F1, F2	
Lenovo	laptop		<u>F12</u>		F1, F2	
Lenovo	laptop	ThinkPad edge, e431, e531, e545, helix, l440, l540, s431, t440s, t540p, twist, w510, w520, w530, w540, x140, x220, x230, x240, X1 carbon	<u>F12</u>		F1	
Lenovo	laptop	IdeaPad s300, u110, u310 Touch, u410, u510, y500, y510, yoga 11, yoga 13, z500	<u>Novobutton</u>	Small button on the side next to the power button.	Novo button	Small button on the side next to the power button.
Lenovo	laptop	IdeaPad P500	<u>F12 or Fn + F11</u>		F2	
Lenovo	netbook	IdeaPad S10-3	<u>F12</u>		F2	
Lenovo	notebook	g460, g470, g475, g480, g485	<u>F12</u>		F2	
NEC			<u>F5</u>		F2	
Packard Bell			<u>F8 or F11</u>		F1, Del	
Samsung			<u>F12, Esc</u>			

Manufacturer	Type	Models	Boot Menu	Boot Once	BIOS/UEFI Key	Change Priority
Samsung	netbook	NC10	<u>Esc</u>		F2	Boot Tab, Select "Boot Device Priority", Press Return, Up/Down to Highlight, F6/F5 to change priority.
Samsung	notebook	np300e5c, np300e5e, np350v5c, np355v5c, np365e5c, np550p5c	<u>Esc</u>		F2	Boot Tab, Select "Boot Device Priority", Press Return, Up/Down to Highlight, F6/F5 to change priority.
Samsung	ultrabook	Series 5 Ultra, Series 7 Chronos, Series 9 Ultrabook	<u>Esc</u>	Note that you must first disable fast boot in BIOS/UEFI to boot from a USB drive.	F2	Boot Tab, Select "Boot Device Priority", Press Return, Up/Down to Highlight, F6/F5 to change priority.
Samsung	ultrabook	Ativ Book 2, 8, 9	<u>F2</u>	Note that you must first disable fast boot in BIOS/UEFI to boot from a USB drive or use the F2 boot menu.	F10	Boot Tab, Select "Boot Device Priority", Press Return, Up/Down to Highlight, F6/F5 to change priority.
Sharp					F2	
Sony		VAIO Duo, Pro, Flip, Tap, Fit	<u>assist</u> button		assist button	
Sony		VAIO, PCG, VGN	<u>F11</u>		F1, F2, F3	
Sony		VGN	<u>Esc, F10</u>		F2	BIOS "BOOT" section, "External Device Boot" enabled
Toshiba	laptop	Kira, Kirabook 13, Ultrabook	<u>F12</u>		F2	
Toshiba	laptop	Qosmio g30, g35, g40, g50	<u>F12</u>		F2	
Toshiba	laptop	Qosmio x70, x75, x500, x505, x870, x875, x880	<u>F12</u>		F2	
Toshiba		Protege, Satellite, Tecra	<u>F12</u>		F1, Esc	
Toshiba		Equium	<u>F12</u>		F12	

Appendix B - RegEx Cheat Sheet



Anchors		Sample Patterns	
^	Start of line +	([A-Za-z0-9-]+)	Letters, numbers and hyphens
\A	Start of string +	(\d{1,2}\d{1,2}\d{4})	Date (e.g. 21/3/2006)
\$	End of line +	([^\s]+(?:\.(jpg gif png))\.\s{2})	jpg, gif or png image
\Z	End of string +	(^[1-9]{1}\$ ^[1-4]{1}[0-9]{1}\$ ^50\$)	Any number from 1 to 50 inclusive
\b	Word boundary +	(#[A-Fa-f0-9]{3}([A-Fa-f0-9]{3})?)	Valid hexadecimal colour code
\B	Not word boundary +	((?=[\d])(?=[a-z])(?=[A-Z]).{8,15})	8 to 15 character string with at least one upper case letter, one lower case letter, and one digit (useful for passwords).
\<	Start of word	(\w+@[a-zA-Z_]+?\.[a-zA-Z]{2,6})	Email addresses
\>	End of word	(\s+/?[^\s]+>)	HTML Tags
Character Classes			
\c	Control character		
\s	White space		
\S	Not white space		
\d	Digit		
\D	Not digit		
\w	Word		
\W	Not word		
\xhh	Hexadecimal character hh		
\Oxxx	Octal character xxx		
POSIX Character Classes			
[[: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		
Note		Items marked + should work in most regular expression implementations.	

Note		These patterns are intended for reference purposes and have not been extensively tested. Please use with caution and test thoroughly before use.		
Quantifiers		Ranges		
*	0 or more +	.	Any character except new line (\n) +	
*?	0 or more, ungreedy +	(a b)	a or b +	
+	1 or more +	(...)	Group +	
+?	1 or more, ungreedy +	(?:...)	Passive Group +	
?	0 or 1 +	[abc]	Range (a or b or c) +	
??	0 or 1, ungreedy +	[^abc]	Not a or b or c +	
{3}	Exactly 3 +	[a-q]	Letter between a and q +	
{3,}	3 or more +	[A-Q]	Upper case letter + between A and Q +	
{3,5}	3, 4 or 5 +	[0-7]	Digit between 0 and 7 +	
{3,5}?	3, 4 or 5, ungreedy +	\n	nth group/subpattern +	
Special Characters		Note		
\	Escape Character +	Ranges are inclusive.		
\n	New line +	Pattern Modifiers		
\r	Carriage return +	g	Global match	
\t	Tab +	i	Case-insensitive	
\v	Vertical tab +	m	Multiple lines	
\f	Form feed +	s	Treat string as single line	
\a	Alarm	x	Allow comments and white space in pattern	
[\b]	Backspace	e	Evaluate replacement	
\e	Escape	U	Ungreedy pattern	
\N{name}	Named Character	Metacharacters (must be escaped)		
String Replacement (Backreferences)		^	[.
\$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			
\$_	Entire input string			
\$\$	Literal "\$"			

Available free from