

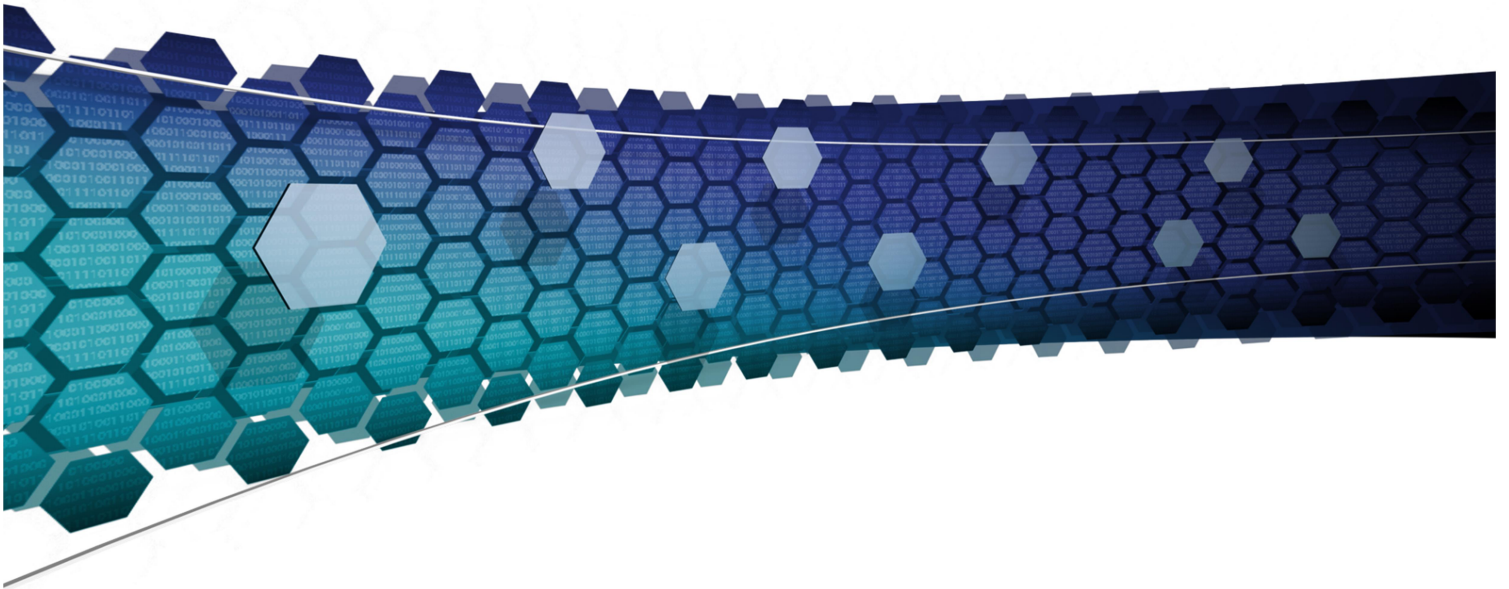


 Rosoka ADD-ON

Triage-G2

User Guide

Version 5.2



Contents

1. INTRODUCTION	2
2. INSTALLATION	4
3. USER INTERFACE	16
4. SETTINGS	18
5. PREPARING A COLLECTION KEY.....	23
6. BIOS/UEFI	25
7. BOOT SCAN	31
8. RAM DUMP	44
9. LIVE SCAN	45
10. DESKTOP SCAN	53
11. REVIEW SCAN RESULTS	64
12. REPORTING.....	98
13. MANAGING AND CREATING SEARCH PROFILES	113
14. MANAGING AND CREATING FILE CAPTURES.....	130
15. IMAGING COMPUTERS AND OTHER STORAGE DEVICES	167
16. MOBILE DEVICE SCREENSHOTS	175
17. GLOSSARY	185

APPENDIX A - BIOS ACCESS KEYS

APPENDIX B - REGEX CHEAT SHEET

1. Introduction

Triage-G2 is the latest evolution of ADF's award winning media exploitation tool which is deployed by Special Forces, military and intelligence agencies worldwide. The tool has a proven track record supporting site exploration operations (including DOMEX, MEDEX, and bio-metric identity).

Designed for non-technical operators, a simple two-step process is all it takes to rapidly scan, extract, and analyze critical intelligence from computers and digital devices. The tool can be deployed on a small, portable USB key and does not require dedicated computer hardware.

Triage-G2 full kit contents are as follows:

Triage-G2 Full Kit Contents
Portable Case
USB Collection Key – Corsair GTX 256GB SSD
4 Port USB Hub
Boot CD
CD Opener
USB Extension Cable
Installation Reference Booklet

Triage-G2 Pro - Mobile Device Module

The mobile device module of Triage-G2 Pro requires the installation of drivers to allow the application to communicate with connected devices over USB:

System	Requirement
Apple iOS	Install the drivers supplied with the ADF Smartphone Driver Pack Installation
Google Android drivers	https://developer.android.com/studio/run/win-usb
Samsung Android drivers	https://developer.samsung.com/galaxy/others/android-usb-driver-for-windows
Other Android brands	If your smartphone is not detected by Windows, please download the appropriate OEM drivers for it.

Technical Specification

A technical specification document is available and can be found at the following location:

<https://www.adfsolutions.com/technical-specifications>

User Guide

The latest version of this user guide can be found at the following location:

<https://www.adfsolutions.com/product-user-guides>

2. Installation

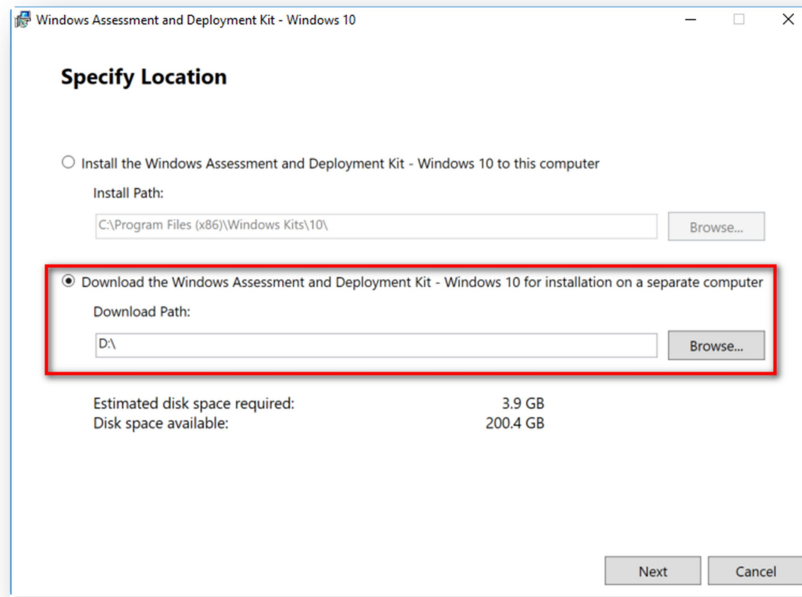
Triage-G2 is designed to run on the following computers:

Operating System	Minimum System Requirements
Windows 7 64-bit	8GB of RAM, 20 GB of free hard drive space (16GB of RAM with Rosoka Add-on)
Windows 8.1 64-bit	8GB of RAM, 20 GB of free hard drive space (16GB of RAM with Rosoka Add-on)
Windows 10 64-bit	8GB of RAM, 20 GB of free hard drive space (16GB of RAM with Rosoka Add-on)

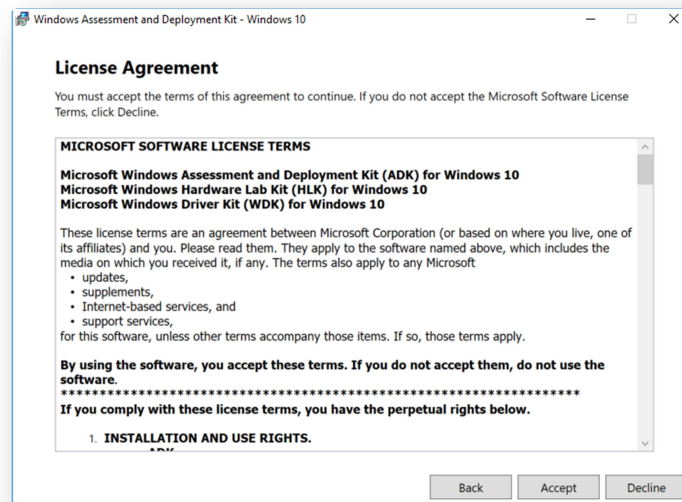
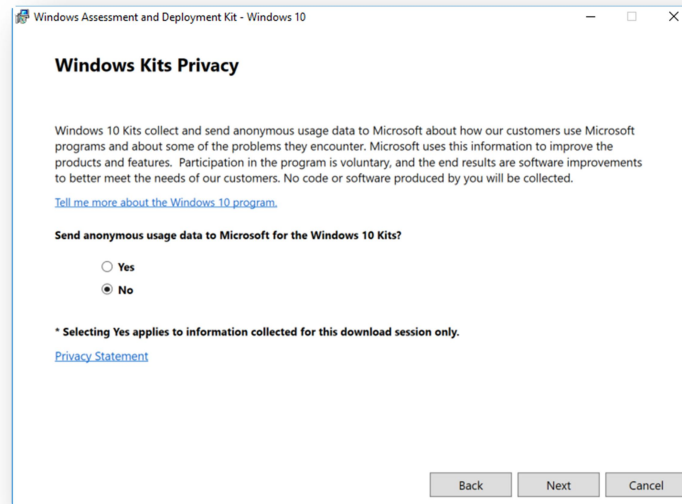
During the installation, a prompt will appear to install the Microsoft Windows Assessment and Deployment Kit (WADK) 10 which is required for boot scans. To do this, the computer must be connected to the internet. Instructions for online installation can be found after the offline instructions. When installing on a computer that has no internet connection, follow the Windows ADK Offline Installation instructions first.

Offline ADK Installation

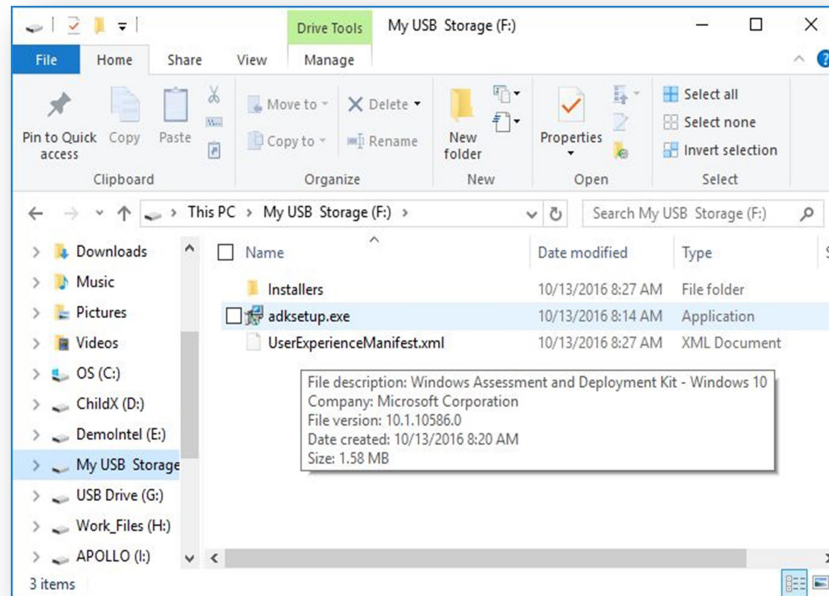
1. On a computer connected to the Internet go to wadk.adfsolutions.com to download the `adksetup.exe`. Execute `adksetup.exe` which will continue the installation process. When prompted to specify a location - Choose Download for installation on a separate computer. Approximately 3.9 GB of space will be required. Save the downloaded files on a removable device



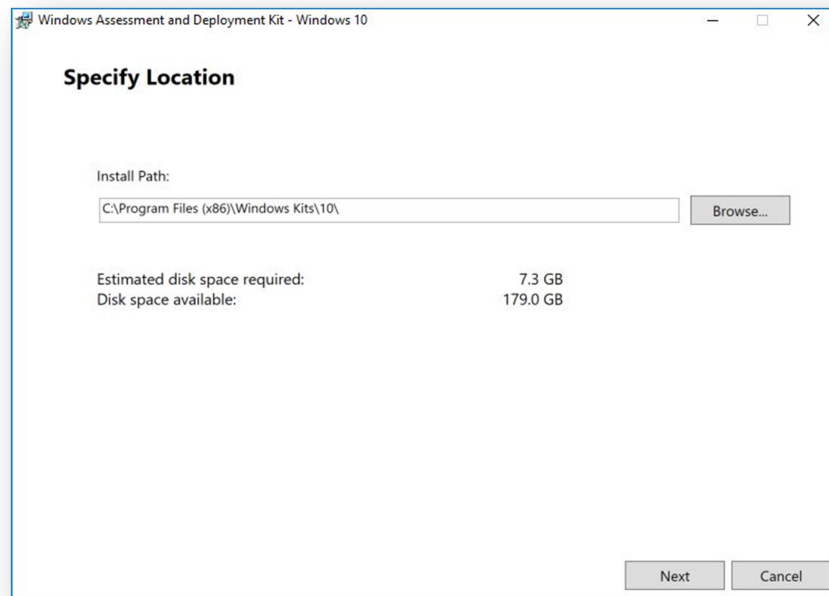
2. Choose the Privacy Options desired and accept the License Agreement by clicking on the Accept button.



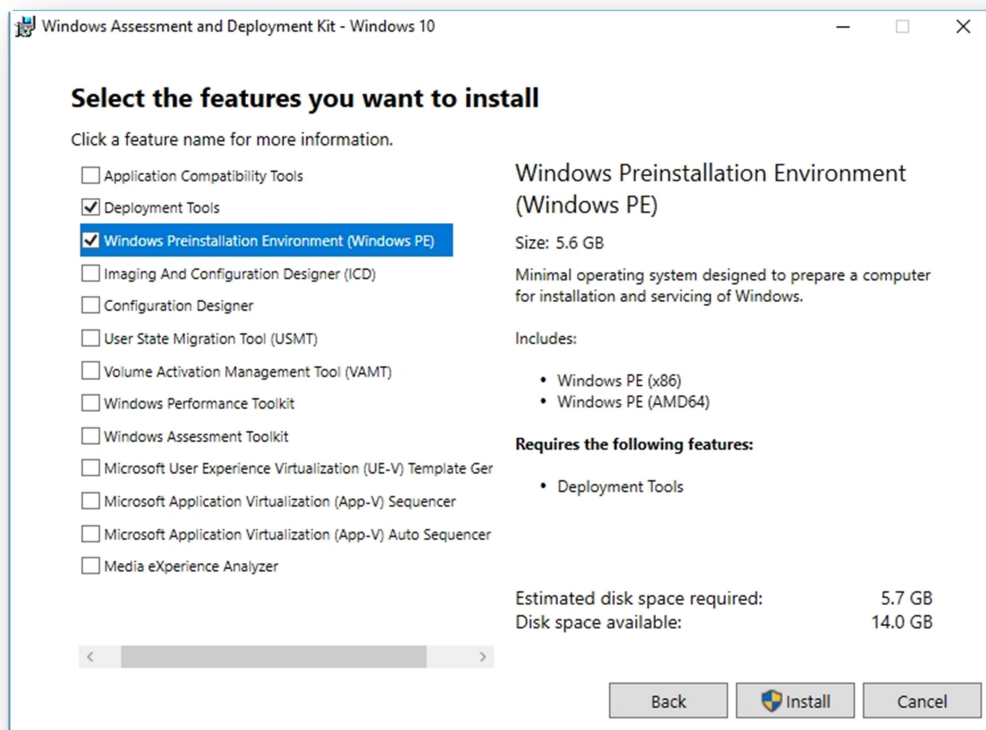
3. On the offline computer, navigate to the download on the removable storage device and execute the installer adksetup.exe.



4. Accept default installation path and click Next



5. Choose the Privacy Options desired 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 the Install button.



6. Once complete proceed to Online Triage-G2 Installation instructions.

Online Triage-G2 Installation

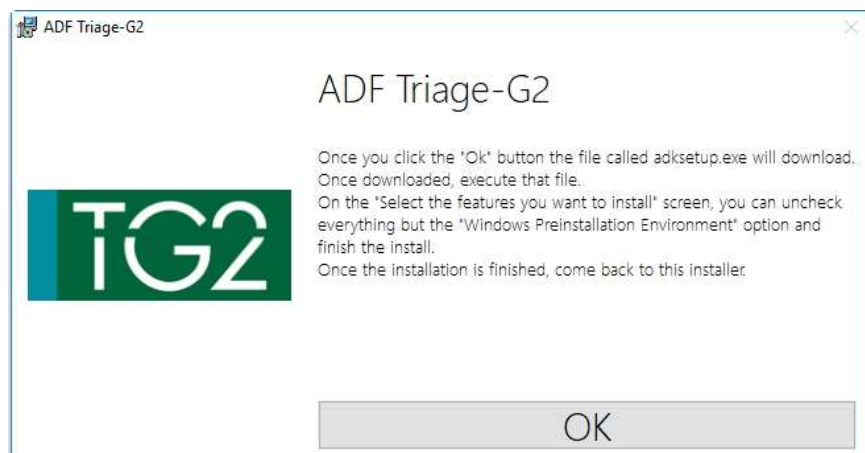
1. Locate and execute the program installer called TG2-xxxxxx.exe (where xxxxxx represents the version number). The latest installer program can be found on the web page <http://www.adfsolutions.com/Downloads>.
2. Follow the installation wizard instructions – Click the licensing and terms and conditions button to view the License Agreement. Click Install to start.



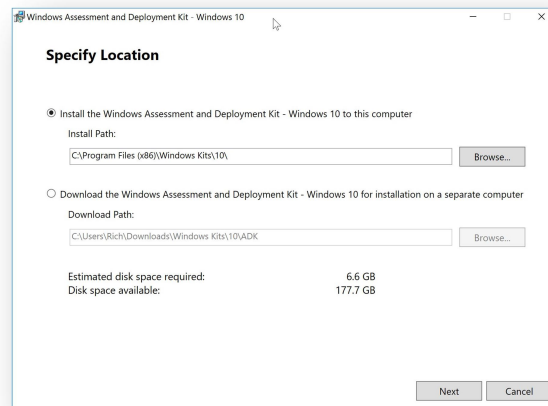
3. If the Windows 10 ADK is not installed the program prompts to do so– click the Yes button to install this.



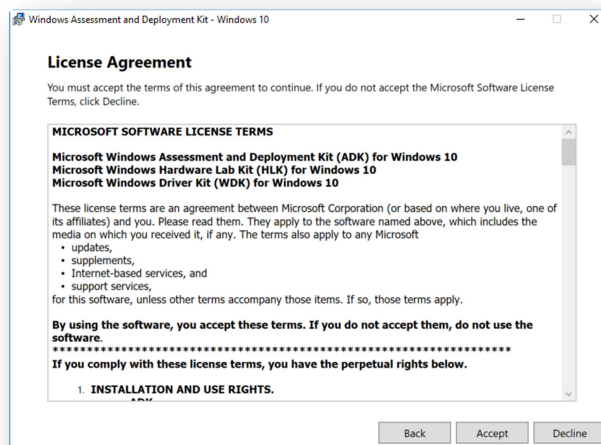
4. Instructions will be displayed detailing how to install the Windows 10 ADK. Click the OK button in this window – a file entitled adksetup.exe will be downloaded. Locate this downloaded file and execute it.



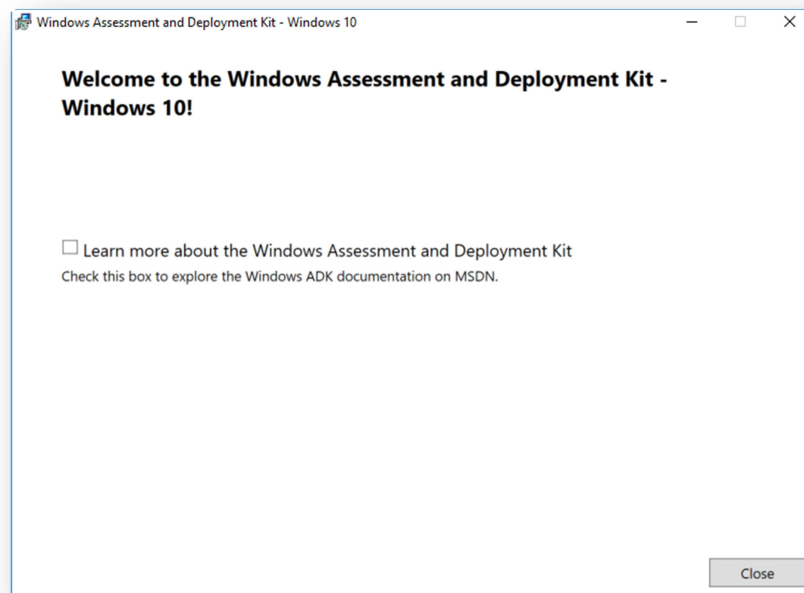
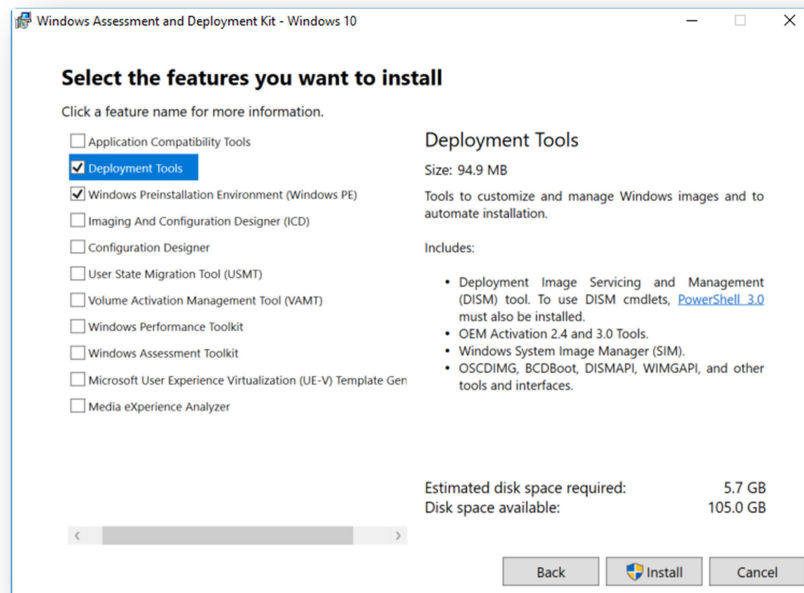
5. Accept default installation path and click Next



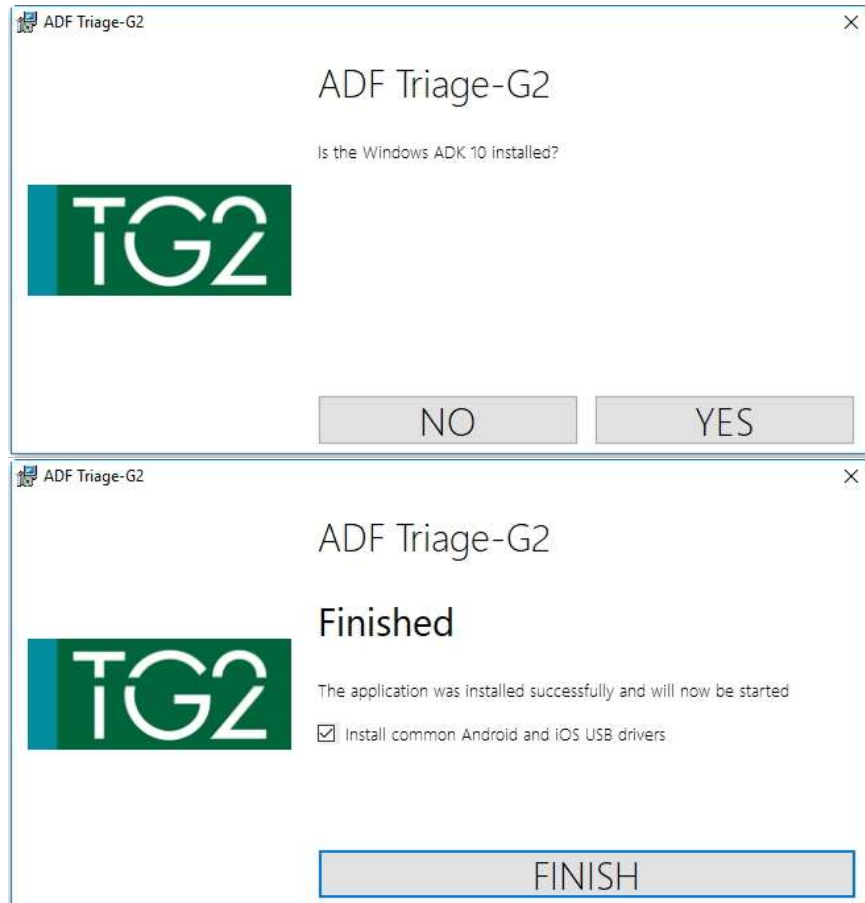
6. Choose the Privacy Options desired and accept the License Agreement.



7. Select the following features to install - Windows Preinstallation Environment (Windows PE) and Deployment Tools - Click Install. It is possible to learn more about the Windows Assessment and Deployment Kit after installation has completed.

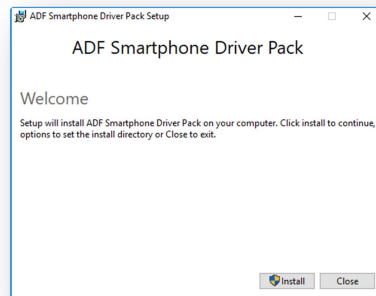


8. Once the WADK is installed return to the Triage-G2 installer and click on Yes. To install common Android and iOS USB drivers select the checkbox, clicking Finish will complete the installation.

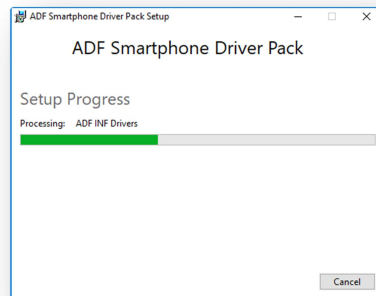


ADF Smartphone Driver Pack Installation

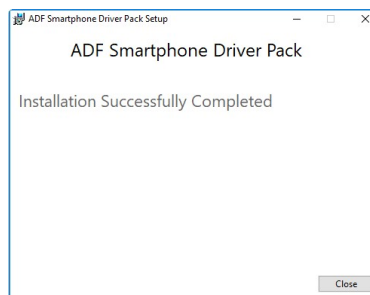
1. Selecting the option to install common Android and iOS USB drivers during the installation of Mobile Device Investigator will start the ADF Smartphone Driver Pack installation process.



2. A progress bar will be displayed showing the progress of the installation. The user may be requested to confirm the installation of some drivers.

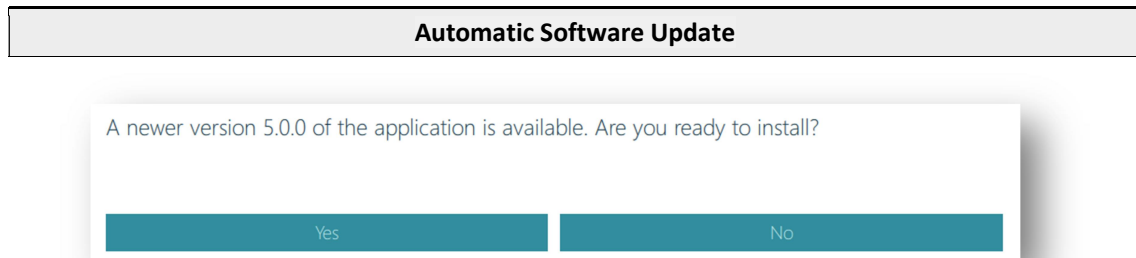


3. A prompt will appear when installation is complete, clicking the Close button will end the installation process.



Automatic Software Update

Internet connected workstations will check for new versions when the application is started. When a new version is detected the latest version will be downloaded. When closing the application a prompt will appear to install the latest version or keep the current version on the workstation.

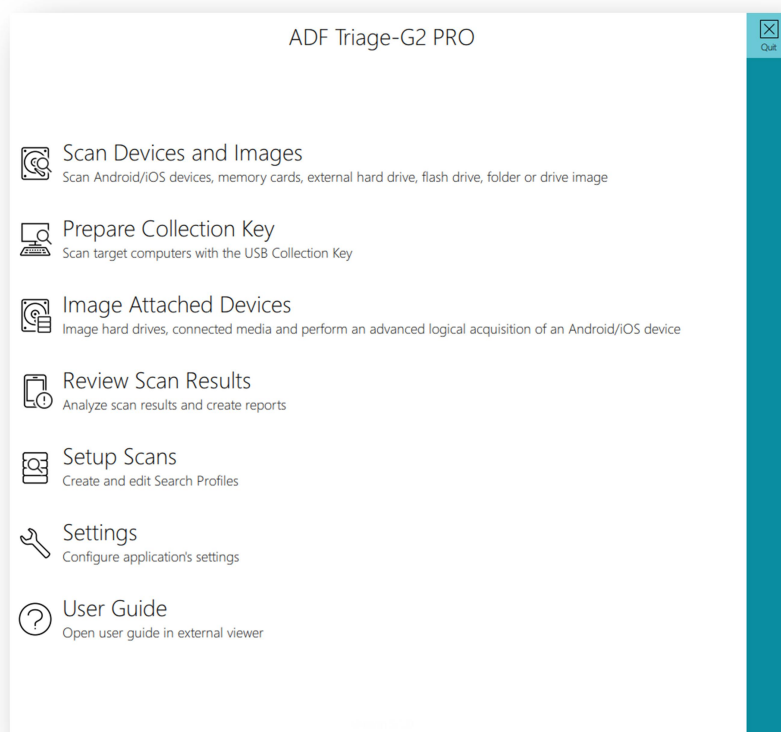


Clicking the Yes button will install the latest version, clicking the No button will leave the current version on the workstation.

3. User Interface

When executing the program the Home Screen is displayed, from here it is possible to access all the functions of Triage-G2.

Triage-G2 Home Screen



Scan Devices and Images

This option enables the scanning of hard drives, USB devices, memory cards, forensic images (E01 and dd), folders, network drives, mobile devices and backups of mobile devices.

Prepare Collection Key

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

Image Attached Devices

This option enables the creation of forensic images of attached devices such as hard drives, USB devices or memory cards. It is possible to create backups of Android and iOS devices.

Review Scan Results

This option enables the user to review and analyze scan results.

Setup Scans

This option enables the creation and editing of Search Profiles and Captures.

Settings

This option allows the user to specify the default locations of Search Profiles, scan results, exported reports and the license backup. Tag names can also be modified here. It is also possible to view and delete backed up licenses.

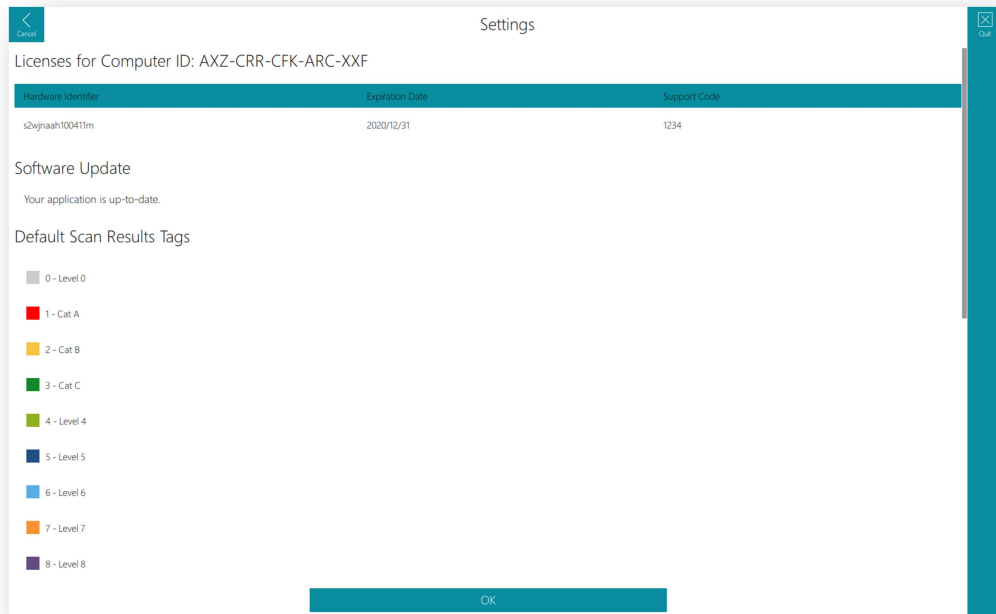
User Guide

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

4. Settings

The settings view stores details relating to licenses, tags, scan information fields and data paths.

Settings View



Backed-up Licenses

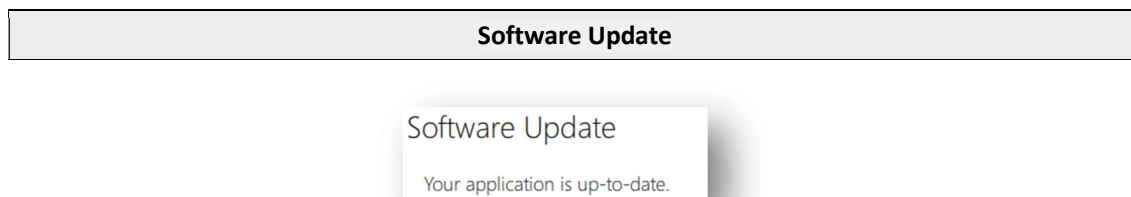
Backed-up Licenses		
Licenses for Computer ID: AXZ-CRR-CFK-ARC-XXF		
Hardware Identifier	Expiration Date	Support Code
07bc0c07442a430e	2020/12/01	1209
PRODUCT	ADF Digital Evidence Investigator	
EXP	2020/12/01	
SUPPORT	1209	
SUPEXP	2020/12/01	
KEYSN	07bc0c07442a430e	
MODULES	smartphone,2020/12/01	
s2wjnaah201361x	2020/12/01	1209
s2wjnaah100411m	2020/04/30	0001
Expiring soon		

The Computer ID can be used with an electronic license file stored on your computer. This can be generated by contacting ADF and should be placed in ProgramData\ADF Solutions Inc\v4\LicGen. The electronic license file negates the requirement for a license to be stored on a USB device connected to the workstation.

A list of licenses that have been backed up are displayed. By highlighting a license it is possible to delete it by clicking the Delete button that appears when highlighted.

Clicking the Expand button will display further details about the license such as the product and modules the license is valid for.

Software Update



Details of available software updates will be displayed here.

Default Tag Names

Default Tag Names

Default Scan Results Tags

- 0 - Level 0
- 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

This option enables the allocation of a default Tag Name for each of ten (10) available tags. Tags are described further in section 11 of this guide. Changes to the default tag names will not be applied retrospectively 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.

Default tag names can also be changed by editing the config.json file (\Users\<User Account>\AppData\Local\ADF Solutions Inc\ ADF Triage-G2\config.json). Within the “Tags” section of the JSON file editing the “name” value of the appropriate “level” will change the Default Tag value within the application when it is next started.

Editing Default Tag Names Within config.json

```
"Tags": [  
  {  
    "level": 0,  
    "name": "Level 0"  
  },  
  {  
    "level": 1,  
    "name": "Cat A"  
  },  
  {  
    "level": 2,  
    "name": "Cat B"  
  },  
  {  
    "level": 3,  
    "name": "Cat C"  
  },  
]
```

Default Scan Results Tags

- 0 - Level 0
- 1 - Cat A
- 2 - Cat B
- 3 - Cat C
- 4 - Level 4

Scan Information Fields

Scan Information Fields

Scan Information Fields

Prompt for the following scan information before a scan







Field Name	Default Value	Mandatory (*)
Scan Name	NA	<input checked="" type="checkbox"/>
Scan Date	NA	<input checked="" type="checkbox"/>
Scan Time	NA	<input checked="" type="checkbox"/>
Enter new field name...		

By default, at the start of a scan, the user is requested to input a scan name, a scan date and a scan time. If additional fields are required for all scans, these fields can be defined here by specifying the name of the field in the row containing the prompt "Enter new field name...". Any field with the mandatory check box selected must be completed prior to the scan commencing.

Data Paths

Data Paths

Data Paths

Search Profiles *	C:\ProgramData\ADF Solutions Inc\4\SPPro	
Scan results *	C:\Users\Stuart\Documents\ADF\Scan Results	
Android/iOS backup *	C:\ProgramData\ADF Solutions Inc\4\phone_backup	
Exported reports *	C:\Users\Stuart\Desktop	
Licenses backup *	C:\ProgramData\ADF Solutions Inc\4\LicBackup	
Whitelists *	C:\ProgramData\ADF Solutions Inc\4\Whitelists	

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

Default Paths can also be changed by editing the config.json file (\Users\<User Account>\AppData\Local\ADF Solutions Inc\ ADF Triage-G2\config.json). Within the "Paths" section of the JSON file editing the "value" value of the appropriate "name" will change the Default Path value within the application when it is next started.

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

Search Profiles

Search Profiles contains default and user created Search Profiles for Triage-G2.

Scan Results

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

Android/iOS backup

Backups created with Triage-G2 Pro will be stored here.

Exported Reports

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

License Backup

License Backup contains a backup of any licenses used with Triage-G2.

Whitelists

Whitelists incorporated into Search Profiles will be stored here and can be used within other user created Search Profiles.

5. Preparing a Collection Key

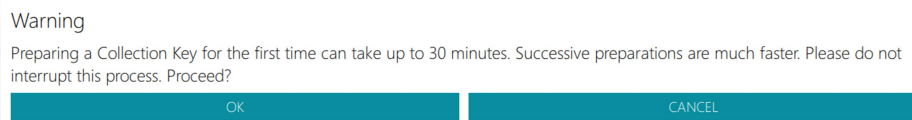
Preparing a Collection Key will make any USB storage device, a bootable USB device. A prepared Collection Key enables the booting of the majority of powered off personal computers or conduct a live scan of a powered-on computer running the Microsoft Windows operating system. Search Profile(s) and an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

How to Prepare a Collection Key

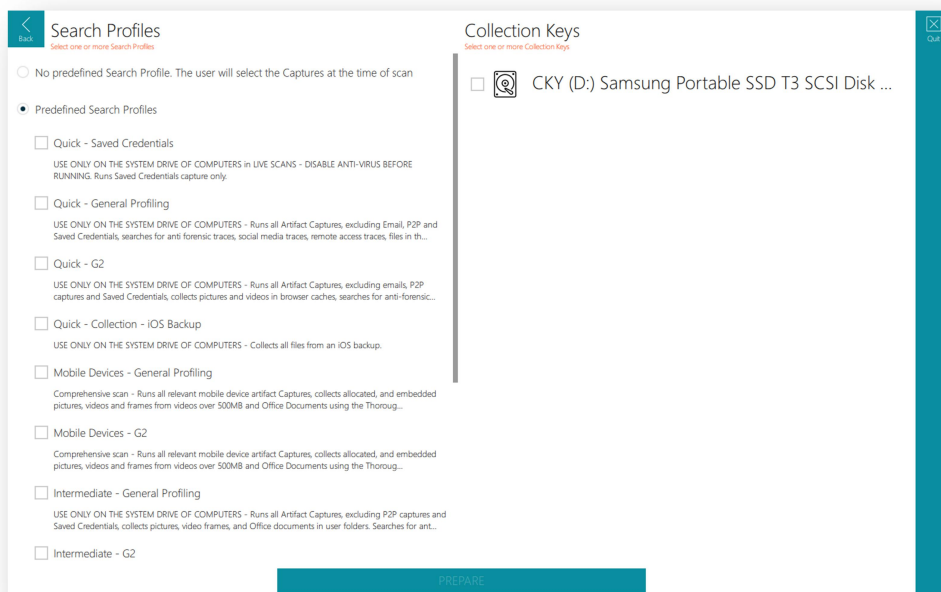
1. Insert a USB storage device that will be prepared as a Collection Key
Select Prepare Collection Key.



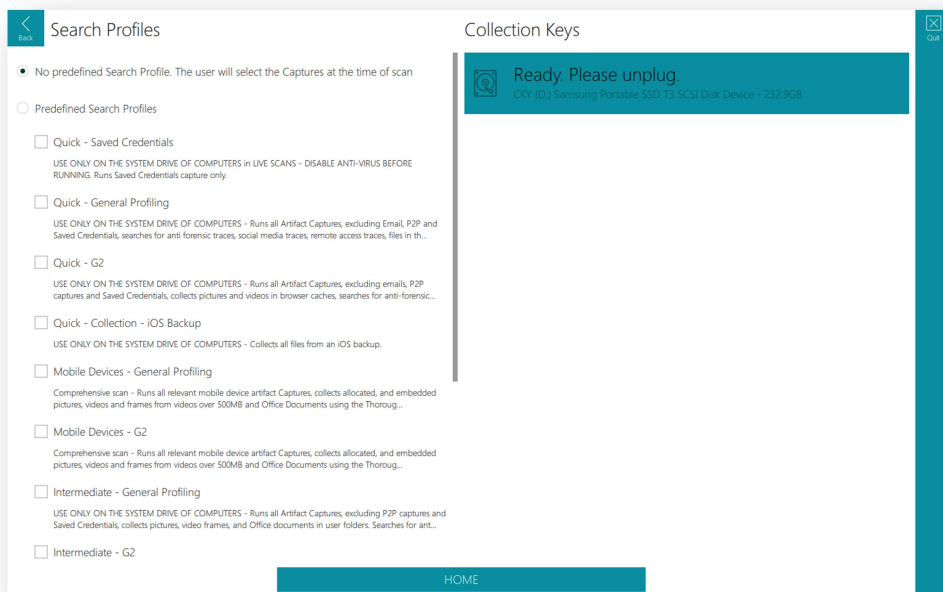
2. When preparing a Collection Key for the first time a warning message will displayed stating that the first time a collection key is prepared it can take a longer time than usual, subsequent Collection Key preparation will be quicker.



3. Choose between having no predefined Search Profile(s) on the Collection Key or having Predefined Search Profile(s) on the Collection Key. No Predefined Search Profile requires Search Profiles to be created at the time of the scan.
Select the Search Profile(s) to be available on the Collection Key.
Select the USB Device(s) to be prepared as Collection Key(s).
Ensure the correct USB Device(s) is selected as all existing data will be deleted.
Click on Prepare.



4. Unplug USB device when prompted. On some occasions it is not possible to eject the disk, a warning message will be displayed in these instances. The Collection Key is now prepared.



6. BIOS/UEFI

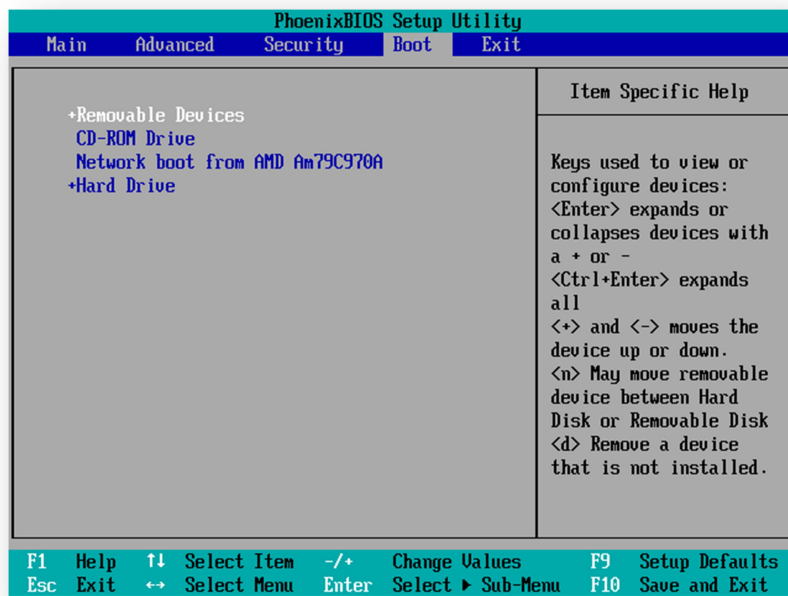
Most target computers will have to be configured to boot from the Collection Key. Computer manufacturers facilitate two ways to do this. Within the BIOS or UEFI firmware setup there is generally a boot sequence area where the computer may be configured to boot from a removable device first or alternatively 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 start up. The precise hotkey needed varies from manufacturer to manufacturer and model to model. Prior to booting, operators should research the appropriate manufacturers website to establish how to boot from a removable device.

Triage-G2 will boot computers with UEFI Secure Boot enabled.

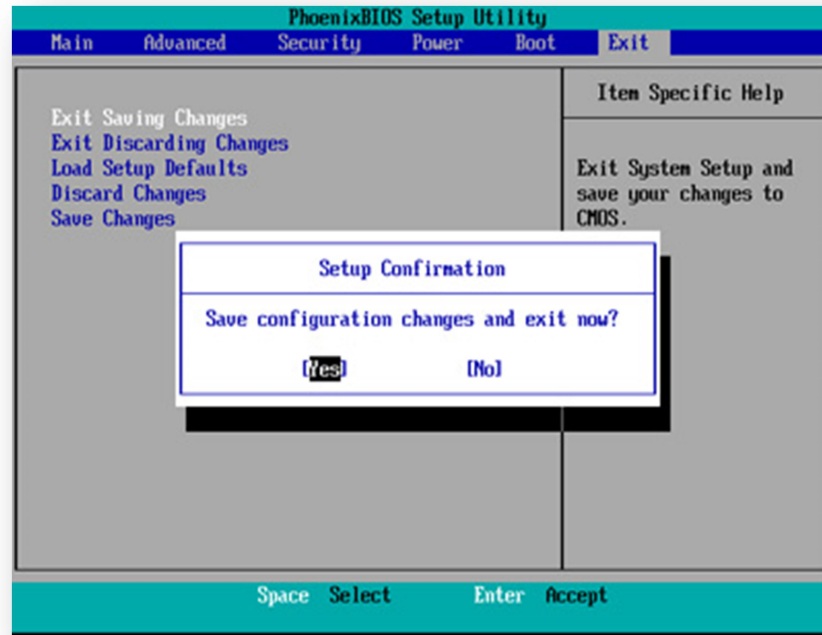
Steps to take control of the target computer BIOS/UEFI

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 (sometimes referred to USB HDD or similar)
CD-ROM Drive
Hard Drive



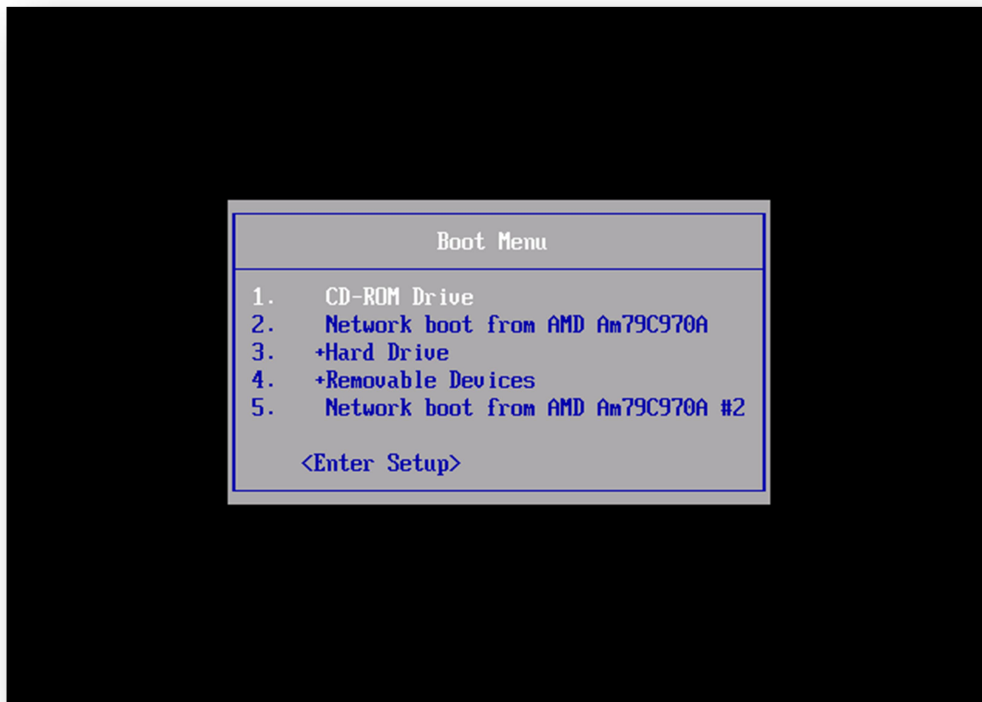
3. Save the changes and exit.
Boot to USB.



NOTE: the USB Collection Key might have to be connected in order 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 the Collection Key from the list.



NOTE: the USB Collection Key may have to be connected in order 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.

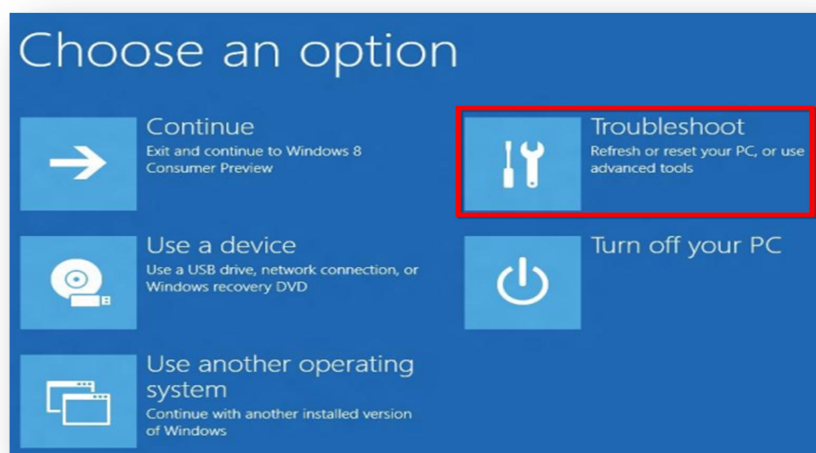
Fast Boot can be turned off by accessing the UEFI firmware via the appropriate hotkey and modifying the Fast Boot configuration. Please consult the relevant computer manufacturers web site for details on how to modify this setting.

Inadvertent boot to Windows 8/10

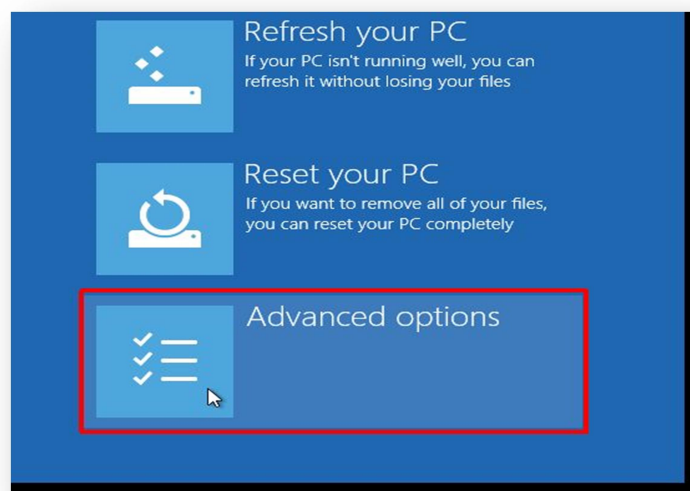
If the UEFI firmware settings cannot be accessed or Windows has been inadvertently booted here are the steps to restart automatically and access UEFI Firmware settings.

1. Hold down the shift key and select restart computer. This method also works if Windows 8/10 is not signed into, and the login screen is displayed allowing access to the restart menu option. If the computer signed in automatically click the Restart option from the Start menu while holding the shift key down.

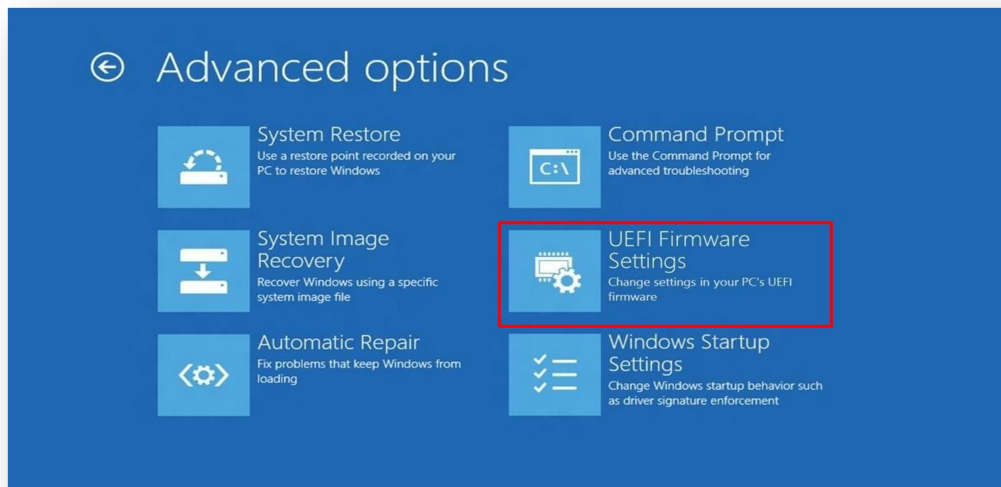
2. While shutting down Choose Troubleshoot from the menu options.



3. Choose Advanced Options.



4. Select UEFI Firmware Settings.



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

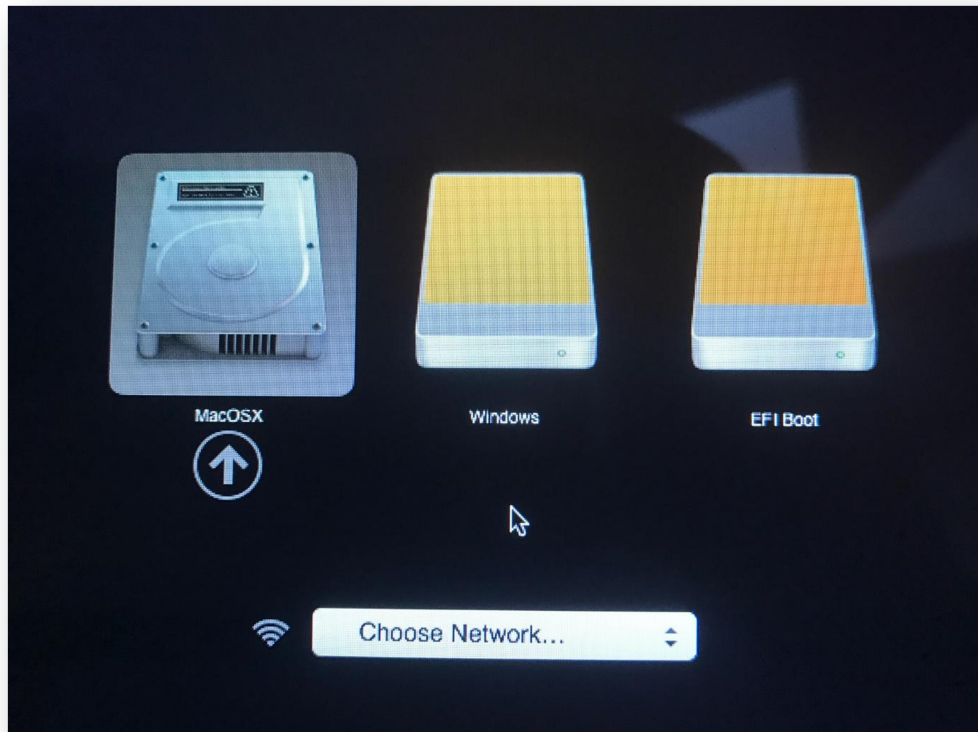


Apple Mac Computers

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.

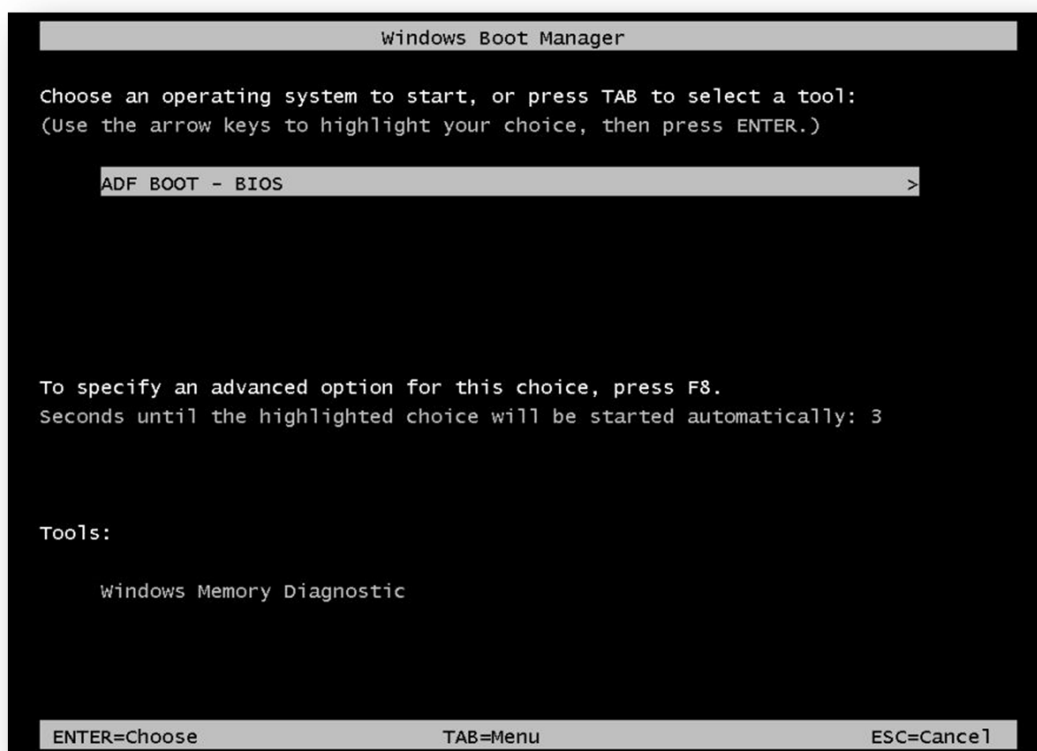


7. Boot Scan

When conducting a boot scan Triage-G2 is forensically sound. This means that no changes are made to the target media.

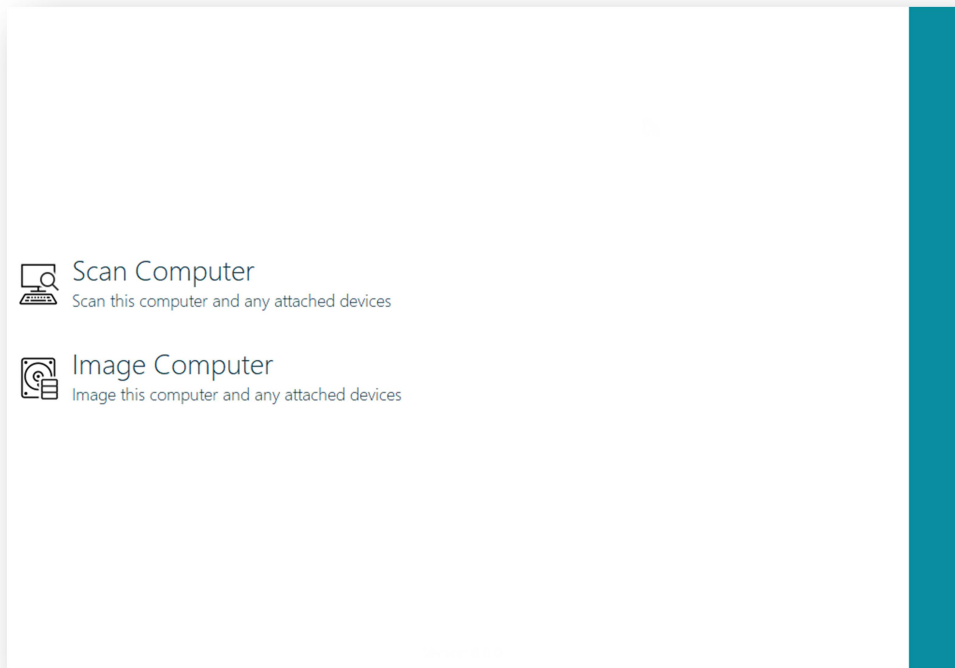
When booting to the Collection Key Triage-G2 will automatically launch the application to scan the computer. No user input is normally required within the Windows Boot Manager. In situations where the computer does not boot successfully, pressing F8 and accessing Windows Safe Mode could be an option.

Windows Boot Manager



Scan Computer

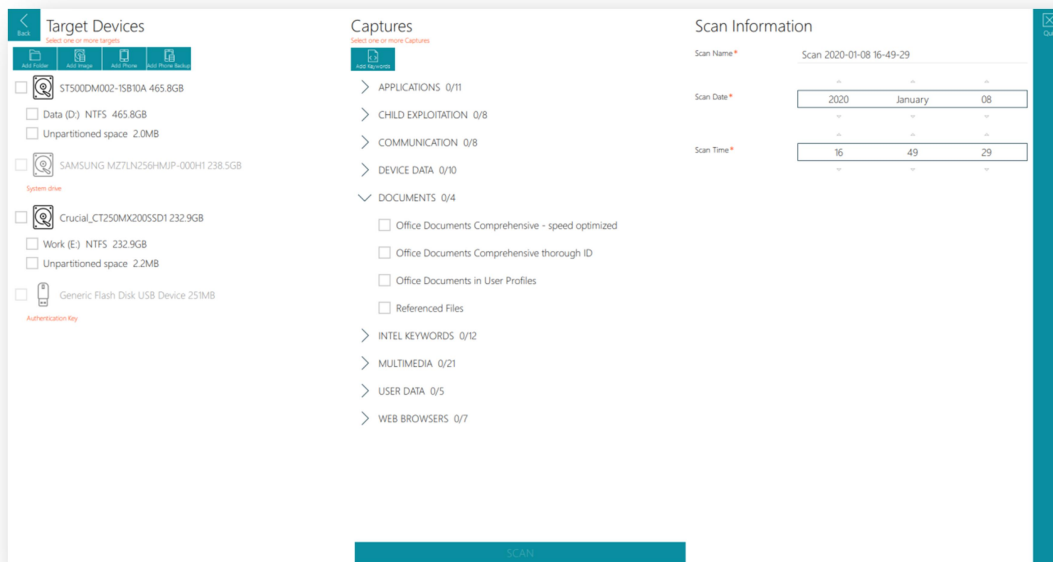
1. There are two options available: Scan Computer and Image Computer. To proceed with the boot scan click on Scan Computer. See section 15 for further details on imaging a computer.



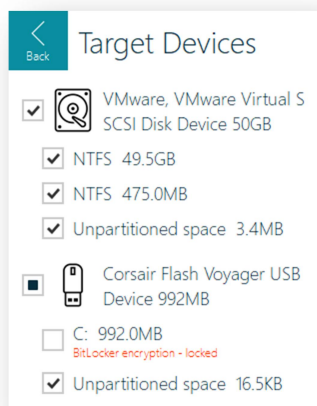
No Predefined Search Profiles

A Collection Key that is created with no Predefined Search Profile will require a Search Profile to be created prior to running a scan.

No Predefined Search Profiles



1. **Select the 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).

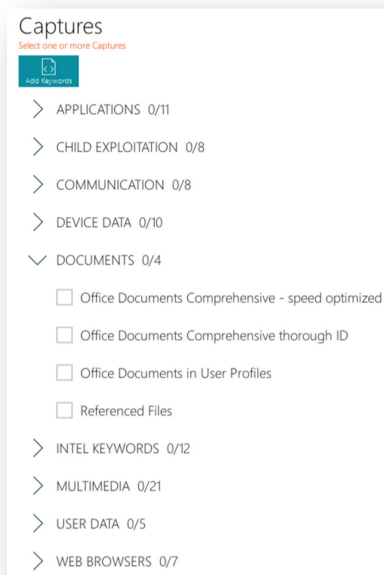


2. Create the Search Profile -

Captures are displayed in the centre pane within Capture groups (Applications, Child Exploitation etc.). Captures that have been hidden prior to the Collection Key being created will not be present here.

Select the desired Captures by clicking on the checkbox next to them.

Clicking on a Capture group will display the option to Collapse the group, clicking on a collapsed group will give the option to expand the group

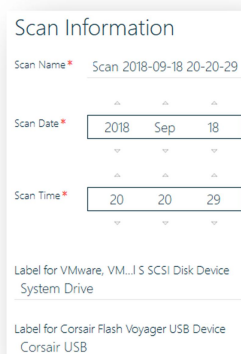


3. Enter scan information

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.

It is possible to supply a label for each device within the label field below the scan time field. This will allow easier identification of devices within the scan results.



Duplicate Captures

When selecting multiple Captures a warning will be displayed if any of these Captures appear to duplicate work carried out by another Capture, this will result in a scan taking longer than necessary to complete.

Duplicate Capture Warning

Warning

The following Captures are targeting the same files and may result in a longer scan. We recommend deselecting the overlapping Captures:

- MULTIMEDIA > Collect Deleted Pictures from Unallocated ...
- MULTIMEDIA > Pictures - with EXIF Data (Picture)
- MULTIMEDIA > Pictures - with GPS Location Data (Picture)
- MULTIMEDIA > Pictures Comprehensive - speed optimize...
- MULTIMEDIA > Pictures Comprehensive Thorough ID no c...

PROCEED

CANCEL

Clicking the Proceed button will continue the scan with the current overlapping Captures, clicking the Cancel button will allow overlapping Captures to be deselected.

Predefined Search Profiles

A Collection Key that is created with Predefined Search Profile will have them available to select prior to running a scan.

Predefined Search Profiles

Target Devices

- ☒ VMware, VMware Virtual S SCSI Disk Device 50GB
 - ☒ NTFS 49.5GB
 - ☒ NTFS 475.0MB
 - ☒ Unpartitioned space 3.4MB

Search Profile

- ☒ Quick - General Profiling
USE ONLY ON THE SYSTEM DRIVE OF COMPUTERS - Runs all Artifact Captures...
- ☐ Mobile Devices - General Profiling
Comprehensive scan - Runs all relevant mobile device artifact Captures, collect...
- ☐ Intermediate - General Profiling
USE ONLY ON THE SYSTEM DRIVE OF COMPUTERS - Runs all Artifact Captures...
- ☐ Comprehensive - General Profiling
Runs all Artifact Captures, excluding P2P captures and Saved Credentials, collect...

Scan Information

Scan Name * Scan 2020-01-08 10-54-43

Scan Date * 2020 Jan 08

Scan Time * 10 54 43

Test

Examiner * Mandatory field. Enter a value.

Label for VMware VM...I S SCSI Disk Device

SCAN

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

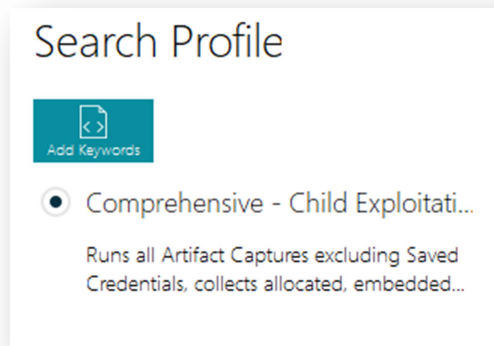
Physical Drives are denoted by a hard disk icon
Logical volumes are listed beneath the physical drive entry
Attached devices are denoted by a flash drive icon
BitLocker/FileVault 2 volumes are flagged (volume will be disabled if not decrypted).

Target Devices

- ☒ VMware, VMware Virtual S SCSI Disk Device 50GB
 - ☒ NTFS 49.5GB
 - ☒ NTFS 475.0MB
 - ☒ Unpartitioned space 3.4MB
- ☐ Corsair Flash Voyager USB Device 992MB
 - ☐ C: 992.0MB
BitLocker encryption - locked
 - ☒ Unpartitioned space 16.5KB

2. Select the Search Profile -

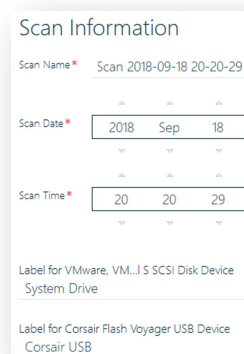
Select the desired Search Profile from the list of Search Profiles added to the Collection Key by clicking the radio button next to the desired Profile.

**3. Enter 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.

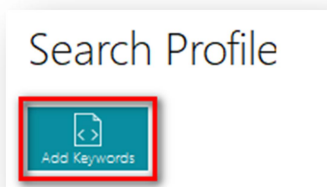
It is possible to supply a label for each device within the label field below the scan time field. This will allow easier identification of devices within the scan results.



Adding Keywords

Prior to commencing a Boot Scan it is possible to add additional keywords to both predefined and created on-the-fly Search Profiles. Only substring keywords can be entered.

1. Within the Captures/Search Profile pane, click the Add Keywords button.



2. A new section will appear, a default Capture Group Name will be entered along with a default Capture Name, it is possible to change these values.


A screenshot of a 'New Keyword Search Capture' dialog box. It contains fields for 'Capture Group Name' (with a dropdown set to 'ON THE FLY') and 'Capture Name' (with a text value 'Keyword Set 2020.01.06-12.55.36'). Below these is a table with three columns: 'Search Expression', 'Auto-Tag', and 'Auto-Comment'. The 'Search Expression' column has a text input with 'Enter value...'. The 'Auto-Tag' column has a dropdown with 'No tag'. The 'Auto-Comment' column has a text input with 'Enter comment...'. Below the table are radio buttons for 'Search' options: 'file names and artifacts (faster)' (selected) and 'file names, artifacts and file contents (slower)'. At the bottom are three buttons: 'SAVE', 'DELETE', and 'CANCEL'.

3. The keyword should be entered in the Search Expression column, an Auto-Tag and Auto-Comment value can be assigned to each keyword. A row for further keywords will appear when a keyword has been added.

Search Expression	Auto-Tag	Auto-Comment
Keyword 1	1	a comment for Keyword 1
Enter value...	No tag	Enter comment...

4. To remove a keyword highlight it by moving the mouse pointer over the keyword and press the Delete button that appears.

Search Expression	Auto-Tag	Auto-Comment
Keyword 1	1	ent for Keyword 1
Enter value...	No tag	Enter comment...

A small red square button with a white trash can icon and the word 'Delete' in white text, positioned at the bottom right of the table.

5. Select the Search Options, searching file names and artifacts will not search within file contents.

Search ☒ file names and artifacts (faster) ☐ file names, artifacts and file contents (slower)

6. Clicking the radio button to search file names, artifacts and file contents (slower) will provide further search options to choose between:
Search documents only or documents, internet files and text files.
Search user profiles only or the entire drive and deleted files.
Fast file identification (identifies files using the file extension) or thorough file identification (will check file signatures for all files).

A description showing which option is faster or slower will be present by each choice.

Search ☐ file names and artifacts (faster) ☒ file names, artifacts and file contents (slower)

Search ☒ documents (faster) ☐ documents, internet files, text files (slow...)

Search ☒ user profiles (faster) ☐ entire drive and deleted files (slower)

File identification method ☒ fast identification (fast...) ☐ thorough identification (slower)

7. Clicking the Save button will save the keyword Capture.
Clicking the Delete button will close the keyword window and not add the keyword Capture.
Clicking the Cancel button will disregard any current changes made on a keyword Capture that had been previously created.

SAVE

DELETE

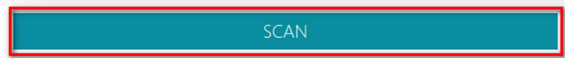
CANCEL

Starting a Scan

When a Target Device(s) has been selected, a Search Profile created or selected and appropriate Scan Information details have been entered, clicking on the Scan button will start the scan.

If an Authentication Key is not inserted the message *No license file found to run the scan* is displayed. Please insert the Authentication Key.

Start Scan Button



Scan Progress

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

Progress bar - Current area and files being scanned.

Matches Log - 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.

View Results button –View results currently collected by the scan. The scan will continue to run in the background.

Image button –Stops the scan and allows devices to be imaged.

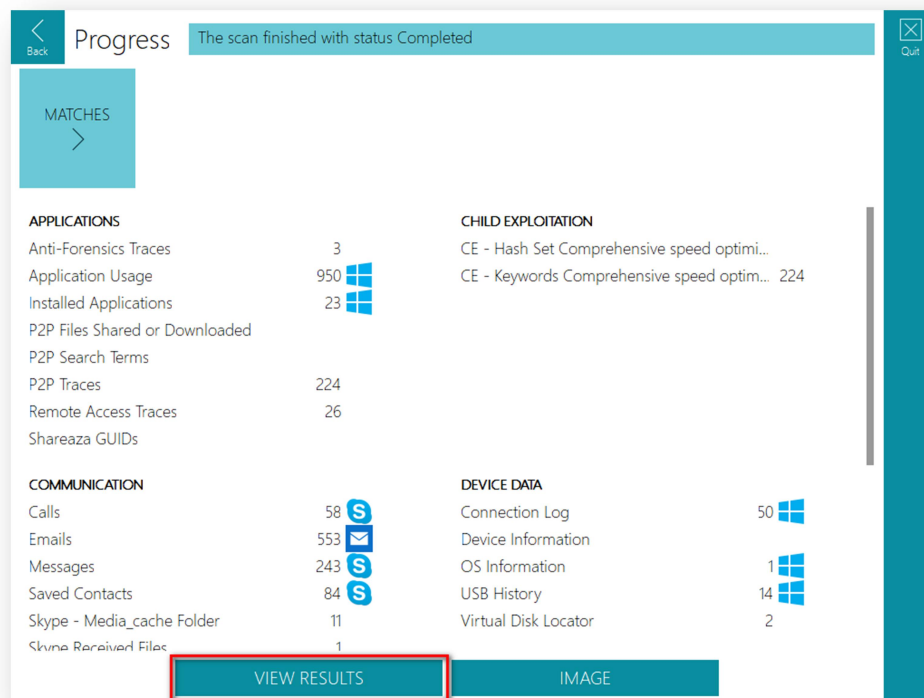
Pause button –Pauses the current scan. To resume a scan click on the Resume button that has replaced the Pause button.



2. Once the scan has completed the results can be viewed by clicking OK and then clicking View Results.

The scan finished with status Completed

OK



3. 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 Triage-G2 software used to prepare the Collection Key or on any other computer where Triage-G2 is installed.

Further help on Reviewing Scan Results and Reporting can be found in sections 11 and 12 of this guide.

Matches Log

During a scan the Matches Log pane will be populated with keyword hits and previews of files identified during the scan. It should be noted that approximately only one in every seven pictures encountered will be displayed while the scan is running.

1. While the Matches Log is active clicking the Matches button will disable file previews.



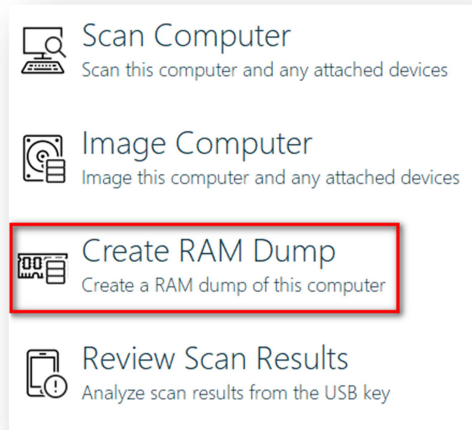
2. When the Matches Log has been switched off, clicking the Matches button will re-enable file previews.



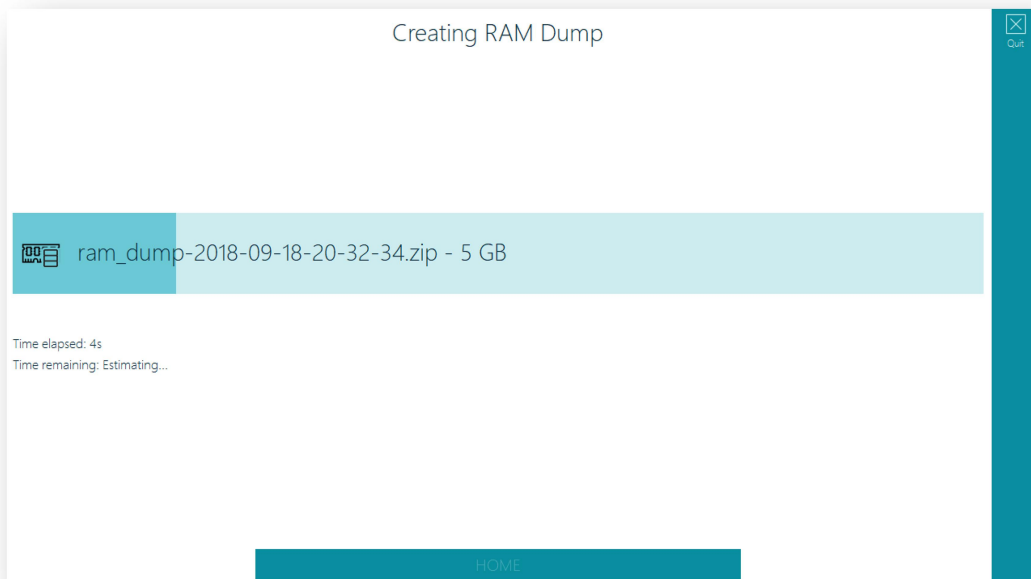
8. RAM Dump

When running a live scan from a Collection Key it is possible to create a RAM dump of the computer. RAM dumps can then be analyzed with appropriate software (e.g. Volatility).

1. From the main menu click on Create RAM Dump.



2. The RAM dump will be saved to the collection key within a zip file.

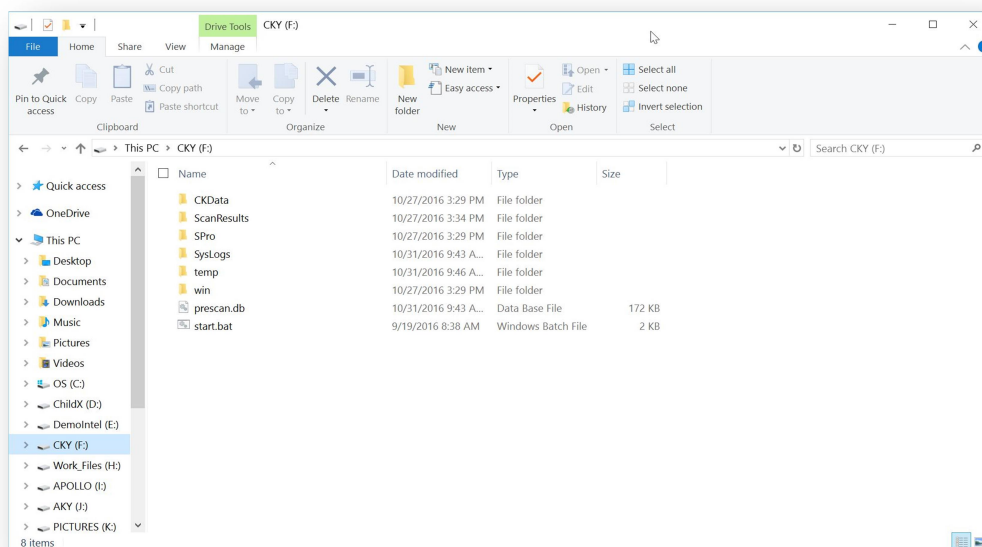


9. Live Scan

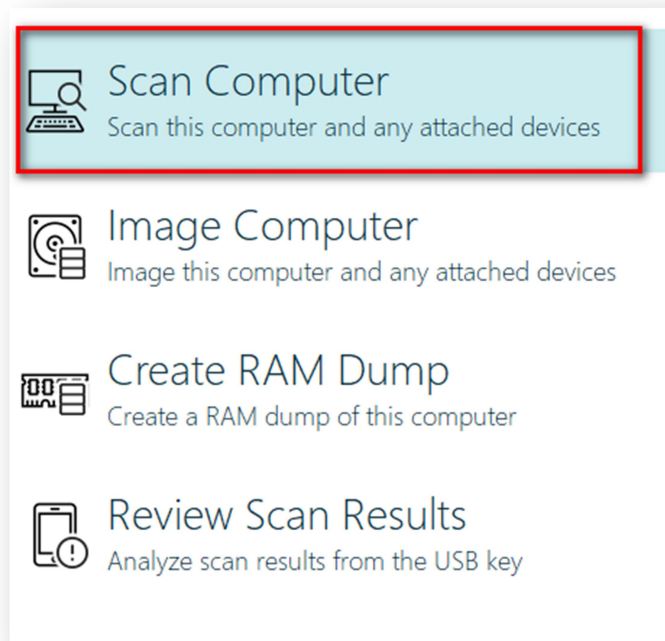
Triage-G2 accesses files on the target computer without modifying their timestamps. However, it should be expected that running Triage-G2 on a live system will leave traces related to the insertion of both the Collection Key and Authentication Key and the execution of the Triage-G2 application.

To run a Live Scan:

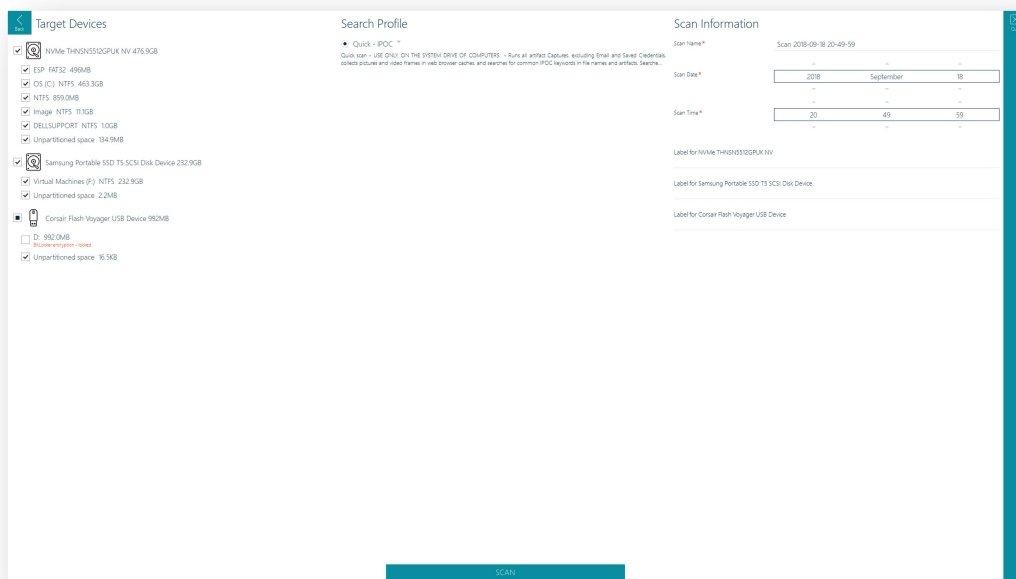
1. Insert the Collection Key into a USB port on the target computer and execute the Start.bat file stored on the Collection Key by double clicking on it



2. A main menu is presented, to continue with a Live Scan click on Scan Computer.



3. Target devices, a Search Profile and Scan Information details can now be selected. Clicking the Scan button will start the live scan



The rest of the process is identical to that described in the section 6 - BIOS/UEFI

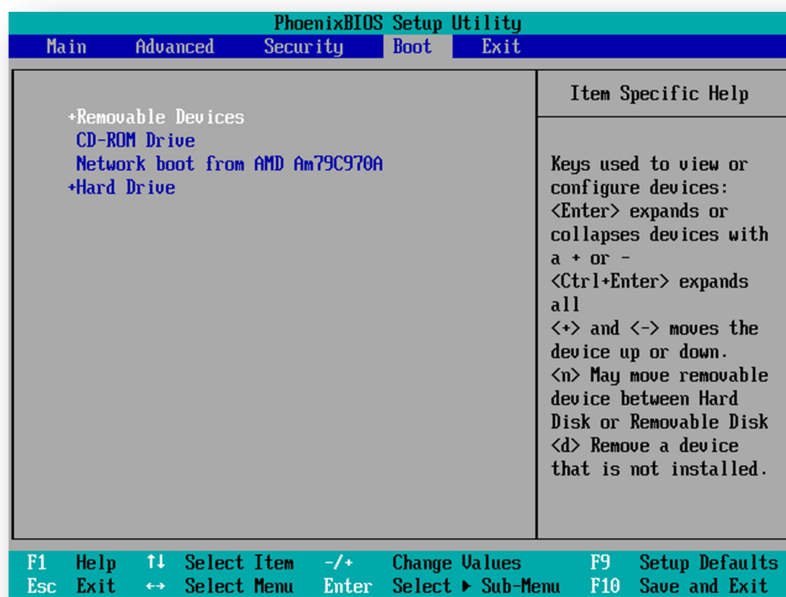
Most target computers will have to be configured to boot from the Collection Key. Computer manufacturers facilitate two ways to do this. Within the BIOS or UEFI firmware setup there is generally a boot sequence area where the computer may be configured to boot from a removable device first or alternatively 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 start up. The precise hotkey needed varies from manufacturer to manufacturer and model to model. Prior to booting, operators should research the appropriate manufacturers website to establish how to boot from a removable device.

Triage-G2 will boot computers with UEFI Secure Boot enabled.

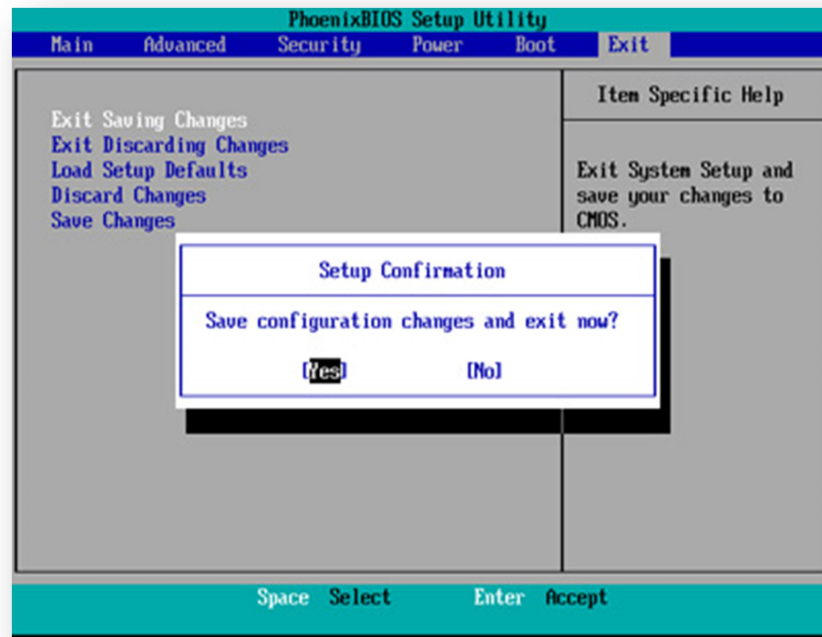
Steps to take control of the target computer BIOS/UEFI

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

5. Locate the boot menu and reorder to boot from:
Removable Device (sometimes referred to USB HDD or similar)
CD-ROM Drive
Hard Drive



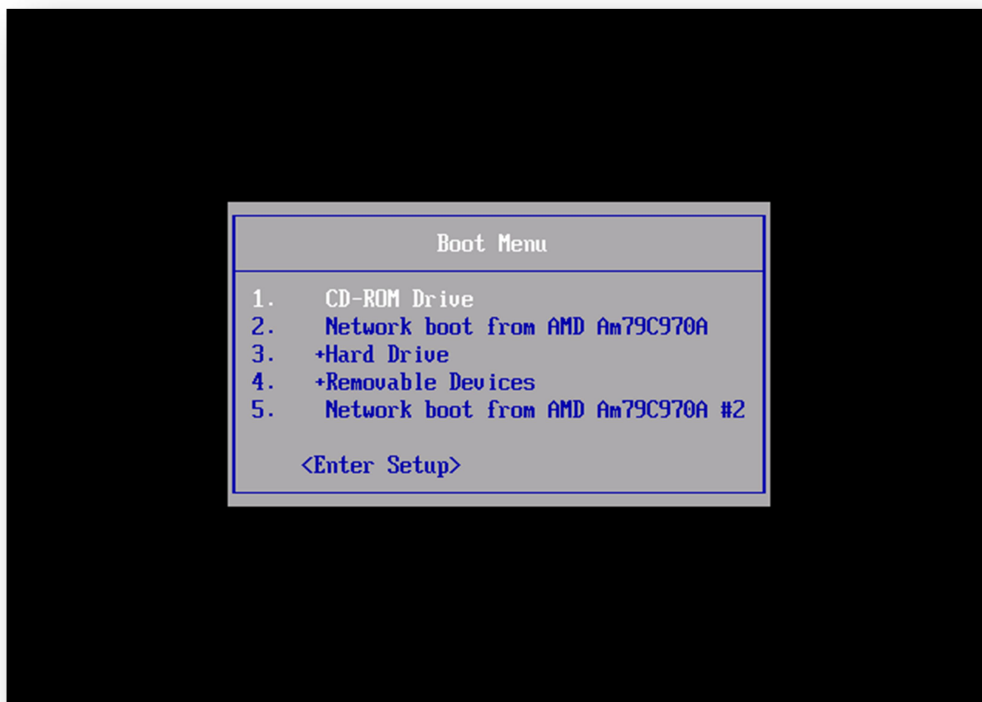
6. Save the changes and exit.
Boot to USB.



NOTE: the USB Collection Key might have to be connected in order for the removable devices option to appear.

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

2. 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 the Collection Key from the list.



NOTE: the USB Collection Key may have to be connected in order 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:

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

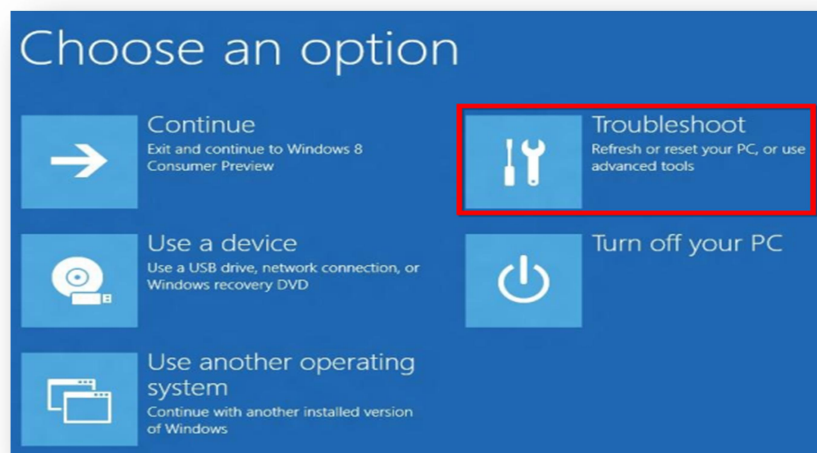
Fast Boot can be turned off by accessing the UEFI firmware via the appropriate hotkey and modifying the Fast Boot configuration. Please consult the relevant computer manufacturers web site for details on how to modify this setting.

Inadvertent boot to Windows 8/10

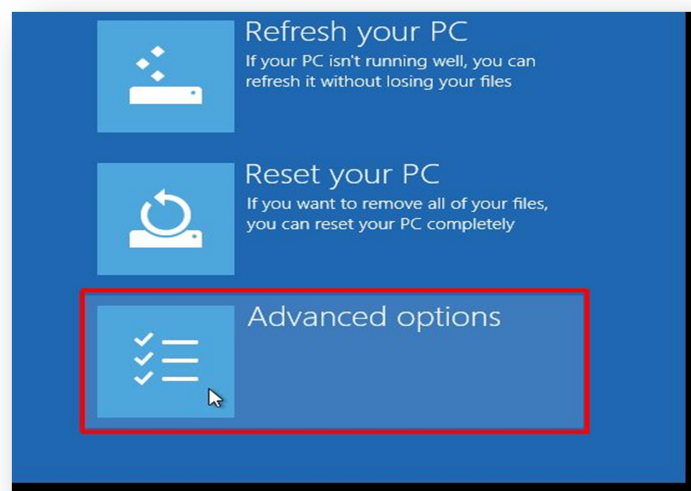
If the UEFI firmware settings cannot be accessed or Windows has been inadvertently booted here are the steps to restart automatically and access UEFI Firmware settings.

6. Hold down the shift key and select restart computer. This method also works if Windows 8/10 is not signed into, and the login screen is displayed allowing access to the restart menu option. If the computer signed in automatically click the Restart option from the Start menu while holding the shift key down.

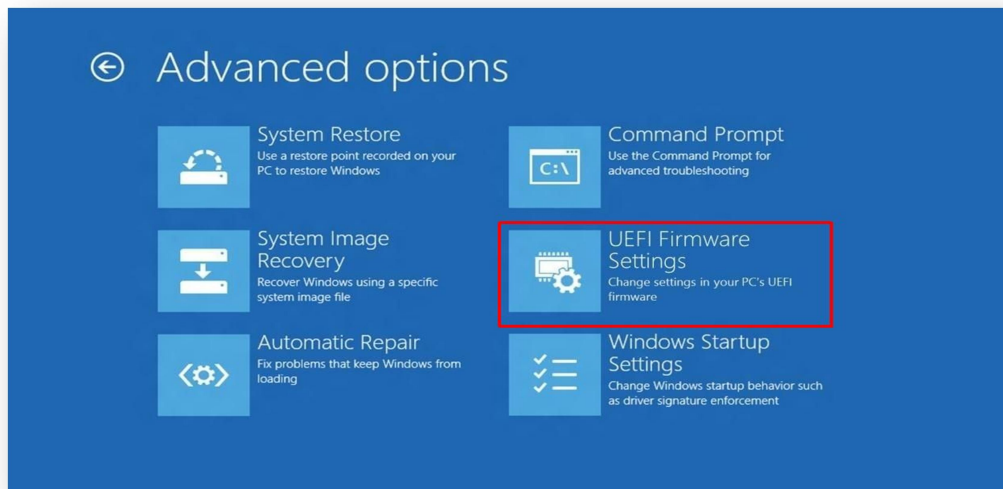
7. While shutting down Choose Troubleshoot from the menu options.



8. Choose Advanced Options.



9. Select UEFI Firmware Settings.



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

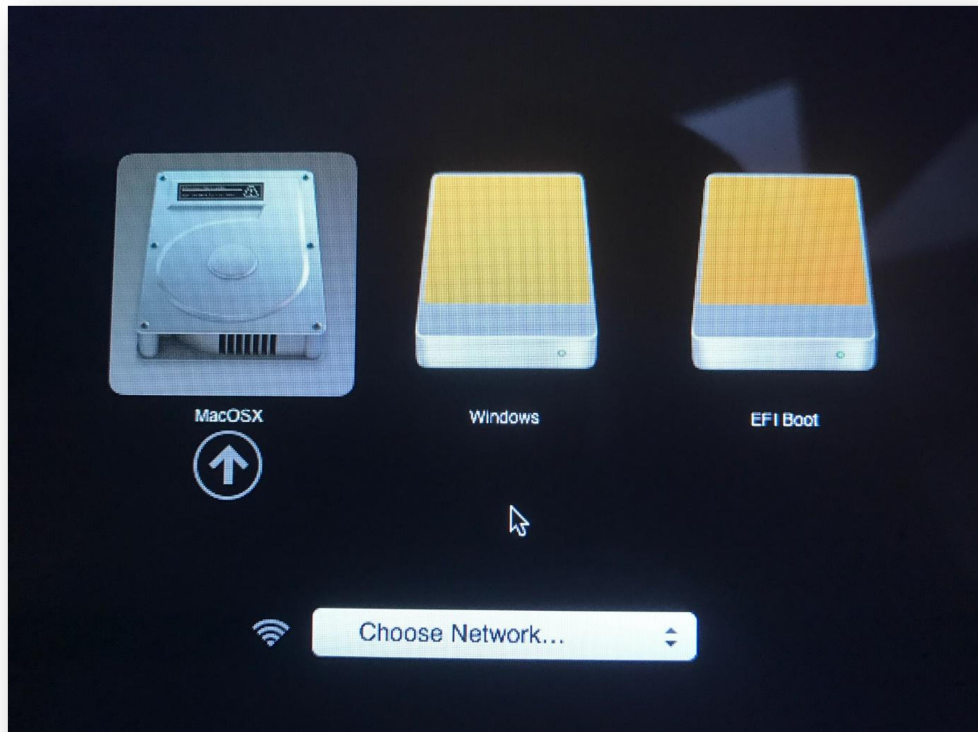


Apple Mac Computers

3. 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.



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



Boot Scan.

10. Desktop Scan

Triag-G2, when installed upon a 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), the contents of folders (can be a network shared folder), connected mobile devices and mobile device backups. To access the scan screen select the Scan Devices and Images option from the Home Screen.

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.



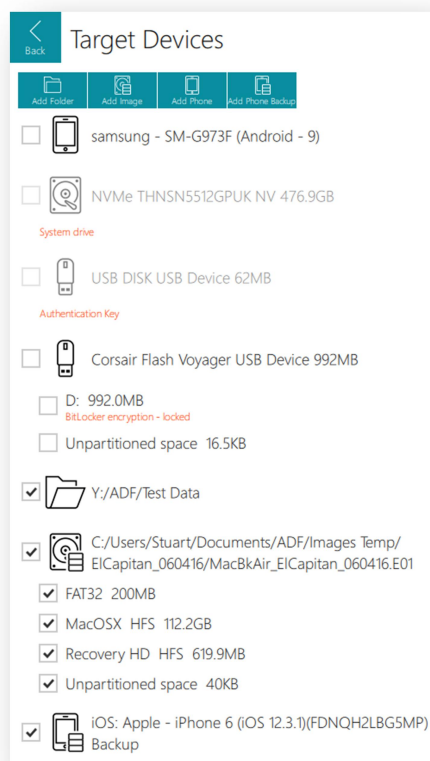
Adding Target Devices

The Target Devices section displays devices connected to the workstation that can be scanned. Devices such as the System drive and the Authentication key will be disabled; scanning these will not be possible.

The Target Devices section has a row of buttons allowing the user to add specific devices:

Option	Function
Add Folder	Allows the selection of a Folder (including Root) or network drive and adds it to the Target Devices List.
Add Image	Allows the selection of an E01 or dd image to the Target Devices List.
Add Phone (Pro Version Only)	Starts the process of adding an Android or iOS device.
Add Phone Backup (Pro Version Only)	Opens a folder browser dialog window to select an Android or iOS backup.

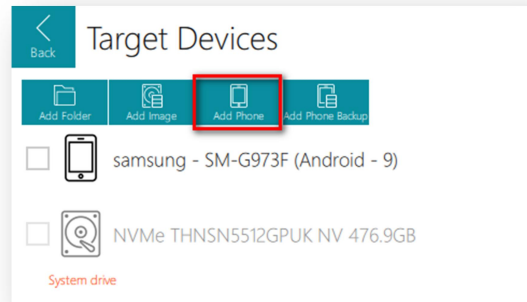
Target Devices Section



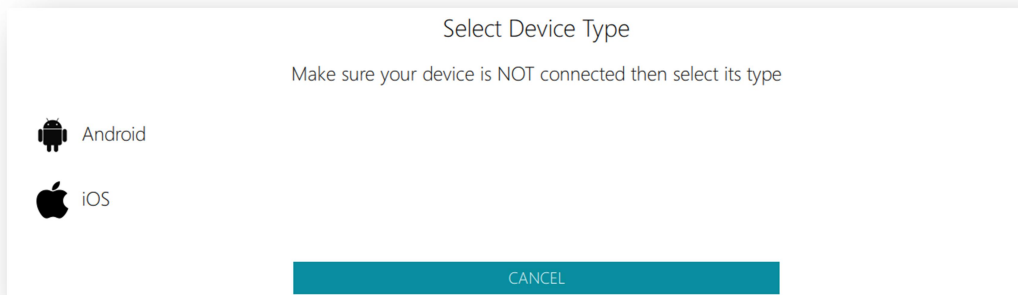
Adding a Phone (Pro Version Only)

Clicking on the Add Phone button will start the process of adding an Android or iOS device to allow it to be scanned.

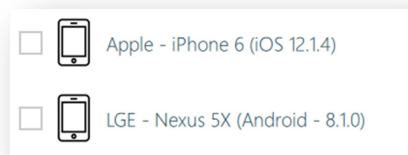
1. Click the Add Phone button



2. Select the type of the phone you wish to add. Clicking the Cancel button will stop the phone addition process and return to the Desktop Scan view



3. Follow the on screen instructions to add your device. When the mobile device has been successfully added it will appear in the Target Devices list



Adding an Android Device

In order to properly scan an Android device some actions are required for the device to be scanned by the application:

- The device must be unlocked, if it is password protected you will need to obtain this
- Developer mode must be activated, the method to do so can differ depending on the make/model of your Android device
- USB debugging mode must be activated
- Authorize the execution of apps from unknown sources
- It is recommended to prevent the device from auto-locking, this can disrupt the backup process
- It is recommended to place the device in airplane mode
- When the device is connected, ensure the USB connection is set to file transfer

Adding an iOS Device

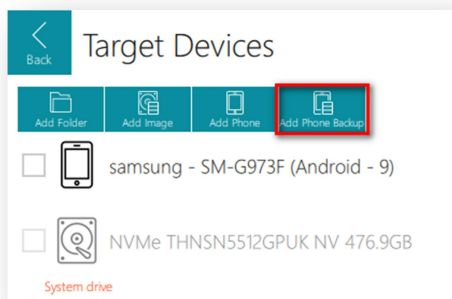
In order to properly scan an iOS device some actions are required for the device to be scanned by the application:

- The device must be unlocked, if it is password protected you will need to obtain this
- If a dialog appears on the device regarding trusting the computer, accept this

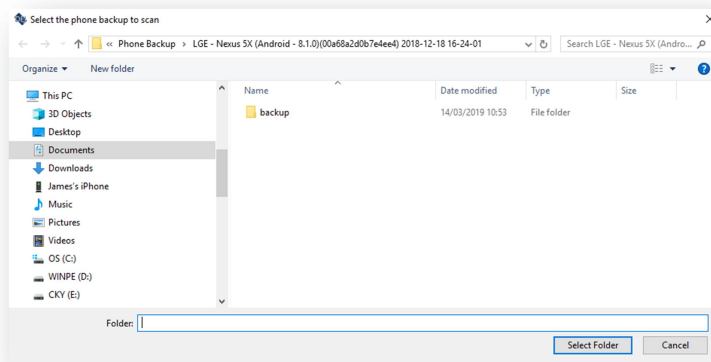
Adding a Phone Backup (Pro Version Only)

Clicking on the Add Phone Backup button will start the process of adding an ADF generated Android or iOS backup to the Target Devices allowing it to be scanned.

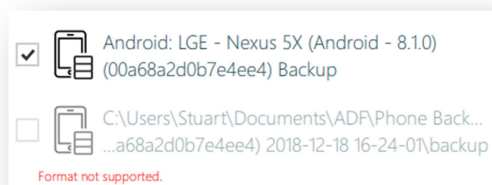
1. Click the Add Phone Backup button



2. A folder browser dialog window will open allowing you to select the root folder of an Android or iOS backup

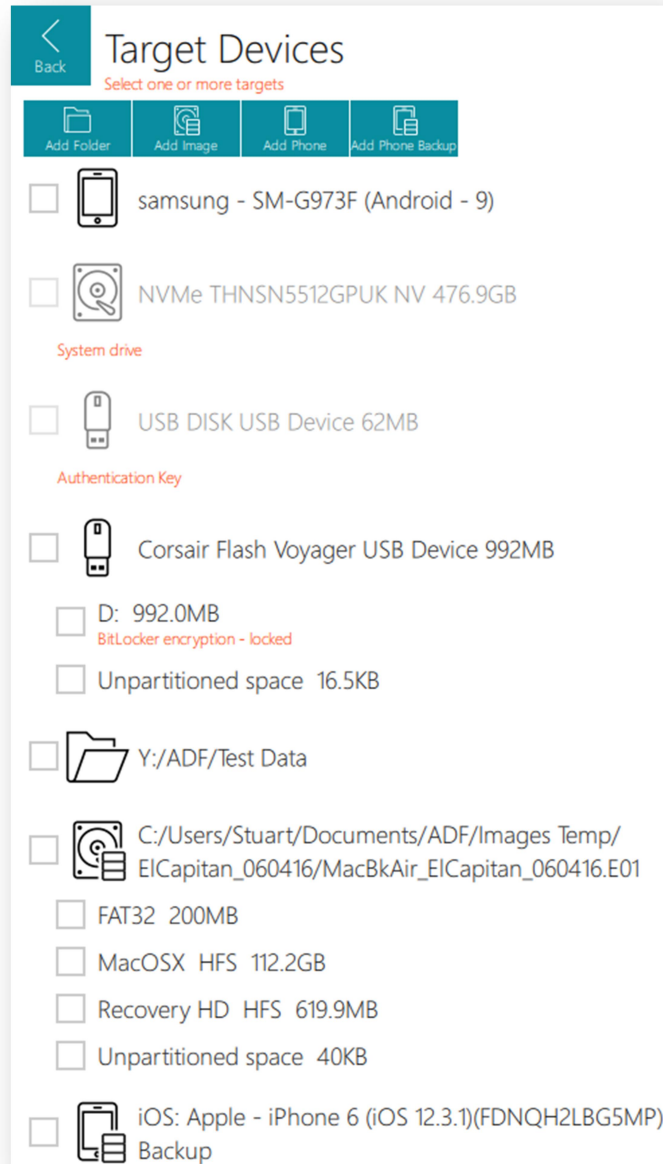


3. A correctly formatted backup will be added to the list, incorrectly formatted backups will display an error message. It should be noted that some Android artifacts, such as calls, messages and contacts, will not be recovered as they require the phone to be connected



Running a Desktop Scan

1. Select the target device(s)
Physical Drives are denoted by a hard disk icon (System drive is disabled)
Logical volumes are listed beneath the physical drive entry
Attached devices are denoted by a flash drive icon (Collection key is disabled)
Bitlocker / FileVault 2 volumes are flagged
Specific targeted folders are denoted by a folder icon
Image Files - E01 or .dd are denoted by an image icon.



2. Select the Search Profile
All Search Profiles will be available including custom profiles.

Search Profile

- ☐ Quick - Saved Credentials
USE ONLY ON THE SYSTEM DRIVE OF COMPUTERS in LIVE SCANS -
DISABLE ANTI-VIRUS BEFORE RUNNING. Runs Saved Credentials captu...
- ☐ Quick - General Profiling
USE ONLY ON THE SYSTEM DRIVE OF COMPUTERS - Runs all Artifact
Captures, excluding Email, P2P and Saved Credentials, searches for ant...
- ☒ Quick - G2
USE ONLY ON THE SYSTEM DRIVE OF COMPUTERS - Runs all Artifact
Captures, excluding emails, P2P captures and Saved Credentials, collect...
- ☐ Quick - Collection - iOS Backup
USE ONLY ON THE SYSTEM DRIVE OF COMPUTERS - Collects all files
from an iOS backup.
- ☐ Mobile Devices - General Profiling
Comprehensive scan - Runs all relevant mobile device artifact Captures,
collects allocated, and embedded pictures, videos and frames fro...
- ☐ Mobile Devices - G2
Comprehensive scan - Runs all relevant mobile device artifact Captures,
collects allocated, and embedded pictures, videos and frames fro...
- ☐ Intermediate - General Profiling
USE ONLY ON THE SYSTEM DRIVE OF COMPUTERS - Runs all Artifact
Captures, excluding P2P captures and Saved Credentials, collect...
- ☐ Intermediate - G2
USE ONLY ON THE SYSTEM DRIVE OF COMPUTERS - Runs all Artifact
Captures except P2P captures and Saved Credentials, collects picture...

3. Enter the 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 computer running Triage-G2 and can be modified to reflect the actual time if the system clock is incorrect.

It is possible to supply a label for each device within the label field below the scan time field. This will allow easier identification of devices within the scan results.

The screenshot shows a web-based form titled "Scan Information". It contains the following fields:

- Scan Name ***: A text input field containing "Scan 2018-02-22 11-40-40".
- Scan Date ***: A date picker with three columns: Year (2018), Month (February), and Day (22). Up and down arrows are visible above and below each column.
- Scan Time ***: A time picker with three columns: Hour (11), Minute (40), and Second (40). Up and down arrows are visible above and below each column.
- Label for hp v285w USB Device**: A text input field containing "Silver HP 64GB USB stick".

4. To start a scan insert the Authentication Key and then click on the scan button. If the Authentication Key is not inserted, the message *No license file found to run the scan* is displayed. Please insert the 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).

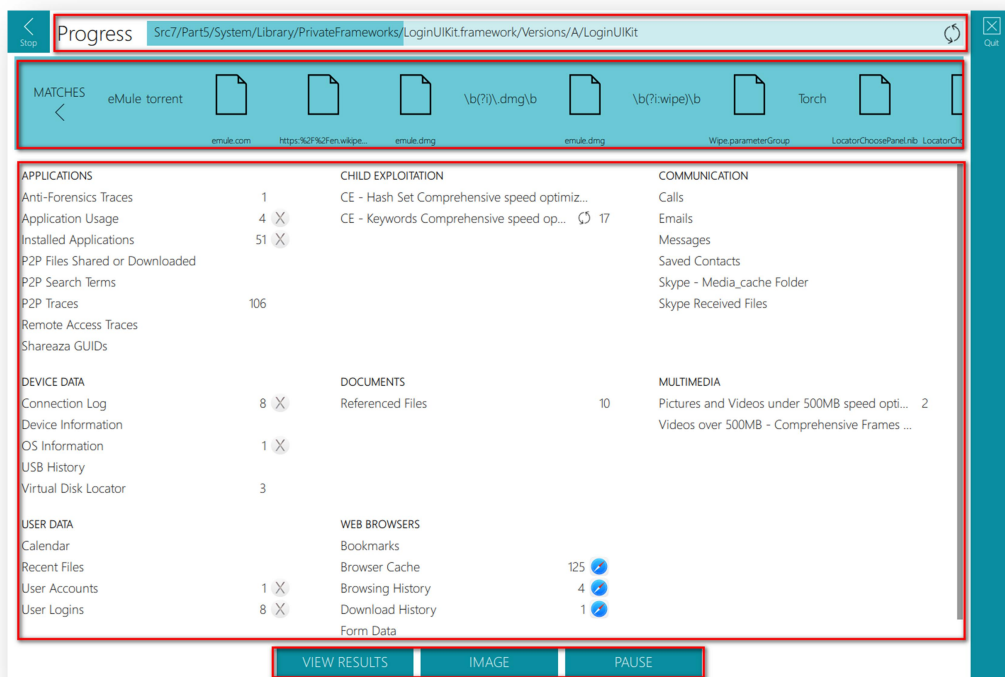
Matches Log - Real time preview (thumbnail) of File Capture matches collected. Images and Video files are represented by thumbnail images, keyword matches will show the keyword found, all other matches will be represented by an associated icon.

Capture results - Cumulative count of capture results.

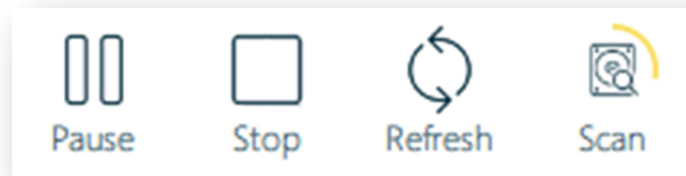
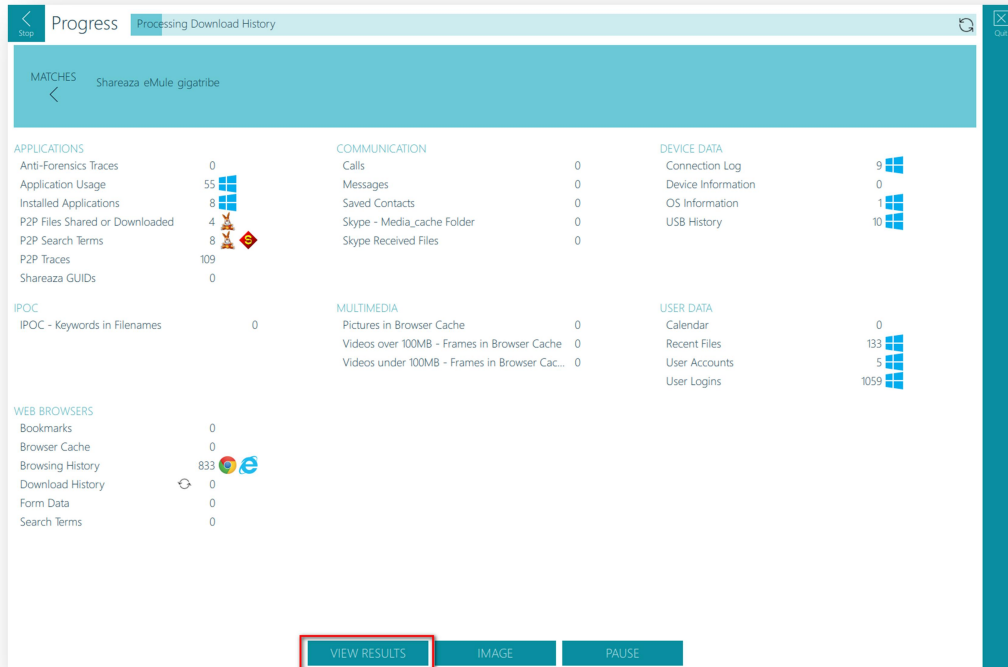
View Results button –View results currently collected by the scan. The scan will continue to run in the background.

Image button –Stops the scan and allows devices to be imaged.

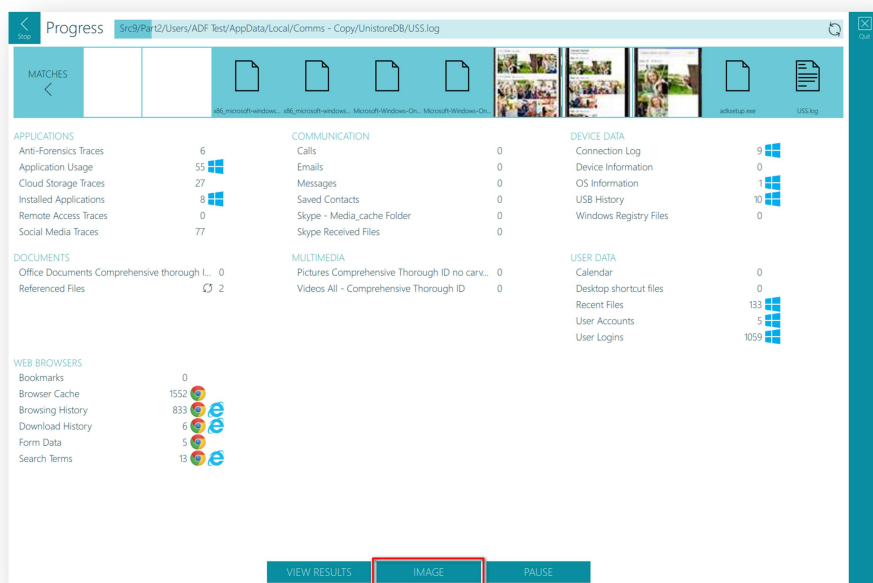
Pause button –Pauses the current scan. To resume a scan click on the Resume button that has replaced the Pause button.



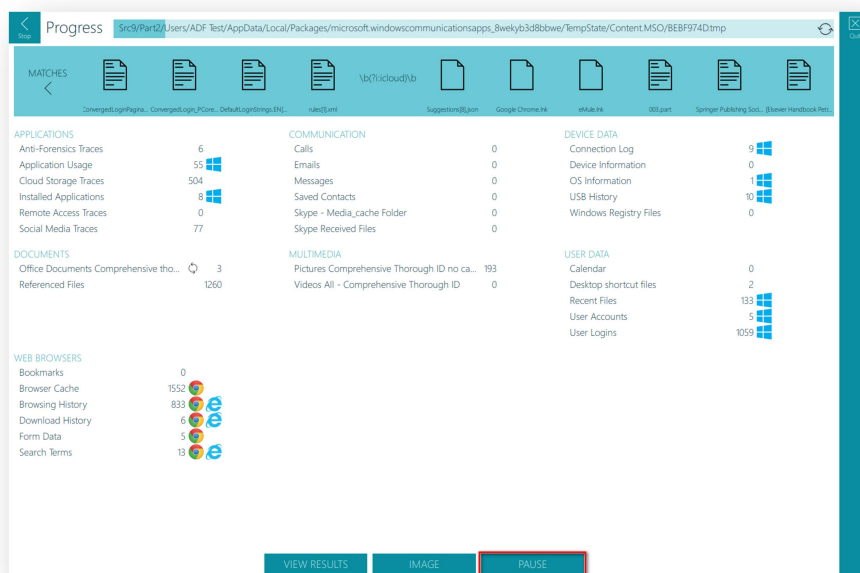
6. When running a scan, clicking the View Results button allows any records currently identified to be reviewed. The scan will continue in the background. When viewing results while a scan is running in the background, a scan button will appear in the function toolbar, clicking this produces buttons to Pause (pause the scan), Stop (stop the scan) or Refresh (refresh the current results).



7. Clicking the Image button will prompt the user to stop the scan: clicking the No button will resume the scan, clicking the Yes button will display the Imaging screen (see section 15 for further details on imaging devices).



8. Clicking the Pause button will pause the scan. To resume the scan press the Resume button that replaces the Pause button while the scan has been paused.

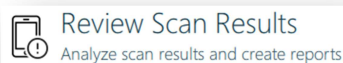


9. Once the scan has completed the user is prompted to view the results. Scan results are stored in the Scan Results folder (\\ProgramData\\ADF Solutions Inc\\v4\\ScanResults by default).

11. Review Scan Results

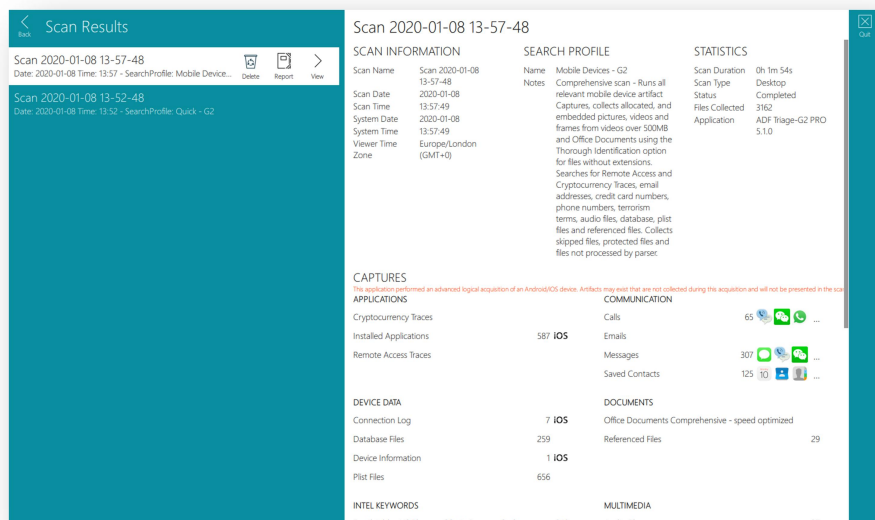
The Review Scan Results view allows the user to review the results of a scan, filter, sort, analyze, tag, and prepare a comprehensive report. Click the Review Scan Results from the Home Screen.

Review Scan Results Button



The Scan Results view is then displayed:

Scan Results View

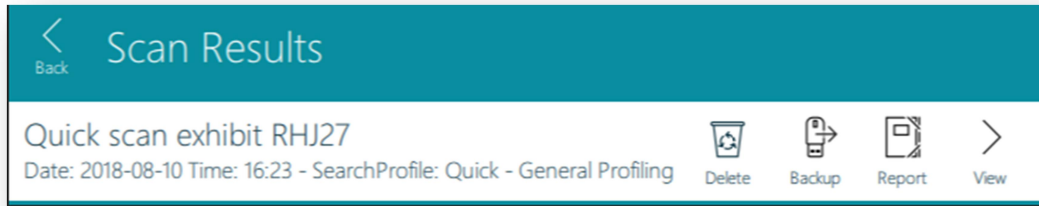


The Scan Name, Date and the Search Profile used are displayed on the left-hand side of the screen with the corresponding Scan Summary details shown on the right-hand side of the screen.

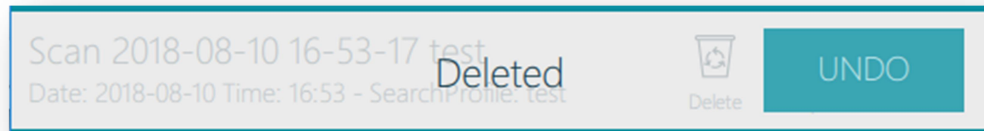
The Scan Results are listed in scan date and time order with the most recent scan at the top of the list.

For Scan Results that have been backed up onto the computer there are 3 options – Delete, Report and View. If the Scan Results are being accessed from a Collection Key then there is a 4th option – Backup – to the computer.

1. The following options are available for scan results, the picture shows a scan result being accessed from a collection key as the Backup option is available

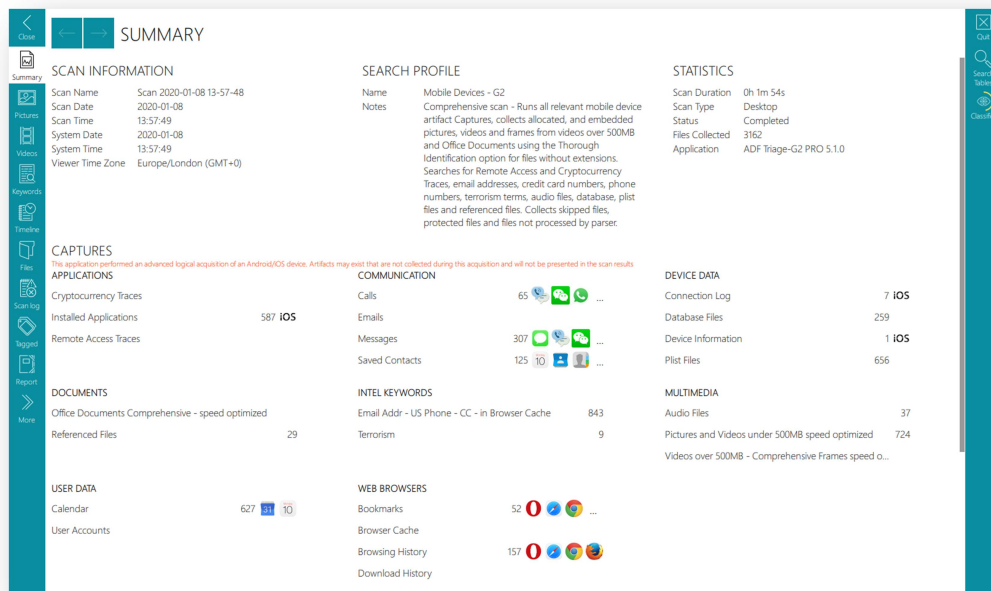


2. Clicking the Delete button will delete the report but there is a brief opportunity to undo this if the report has been deleted in error.



The summary view comprises five main sections: Scan Information, Search Profile, Statistics, Captures and Target Devices.

Summary View



The Scan Information section details the Scan Name, Scan Date and Scan Time, the System Date and System Time and the Viewer Time Zone.

The Search Profile section shows the Search Profile used to generate the Scan Results and any associated Notes on the Search Profile.

The Statistics section shows the Scan Duration, the Scan Type (Boot/Live/Desktop), the Status, the number of Files Collected and the application and version number used. The Tags Statistics are also shown if any exist.

The Scan Status can be one of 7 outcomes as shown in the table below. Any status other than Completed is shown in red:

Scan Status	Event	Scan Log Message (in scan log)
Completed	Scan completed successfully	NA
Interrupted	User stopped the scan	Scan was paused by the user.
Crashed	Application crashed during the scan	NA

Scan Status	Event	Scan Log Message (in scan log)
Out of Storage	No space left on destination drive during scan	Destination drive ran out of storage space.
Incomplete	Not all files can be cached	File system metadata is corrupted for source or partition. Setting scan status as Incomplete as not all files could be cached.
Incomplete	No memory left	System ran out of memory, so the scan cannot complete.
Incomplete	Target device no longer accessible	Target device no longer accessible so the scan cannot complete.

The Captures section lists the Captures used in the Search Profile and alongside each capture the number of results found. Each of the Capture names are hyperlinks and by clicking them the individual Capture results are displayed. Captures where no results were identified during the scan will not have a result number next to them.

The Target Devices section shows the details of the target devices that were scanned. If the device being scanned was an Android or iOS device acquired at the time of the scan, the backup duration and backup status details are displayed here. Where a mobile device backup was not fully completed this will be noted here:

Incomplete Mobile Device Backup

Backup Duration 0h 3m 31s
Backup Status Incomplete (missing Shared data)








At the top left side of the screen are the Backward and Forward buttons. These allow navigation backwards and forwards between screens.





Backward and Forward Buttons



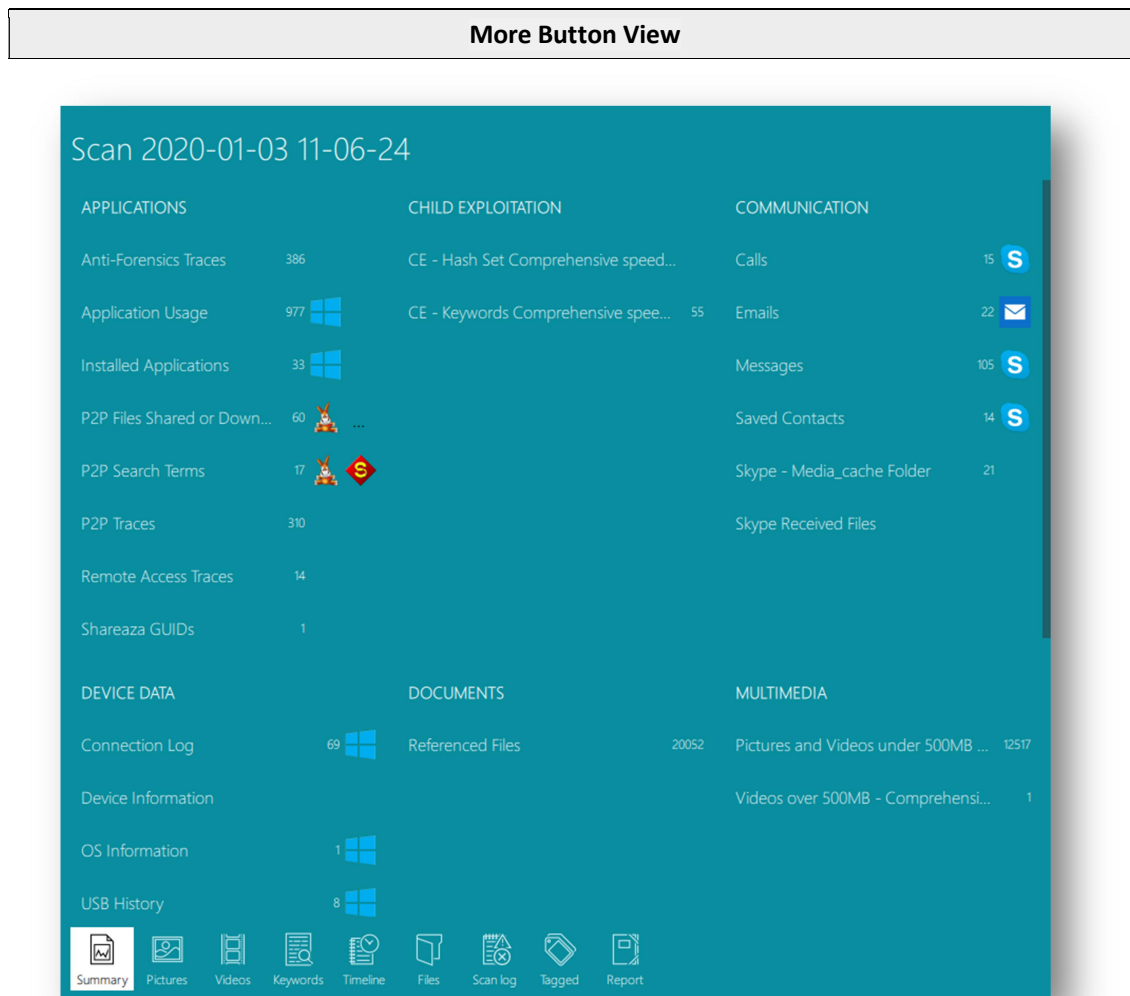
Capture and Navigation Toolbar

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
	Closes the currently viewed Scan Results and returns to the list of all stored Scan Results
	Access the Summary view.
	Access the Pictures view. This shows a gallery view of all pictures identified by the Captures in the Search Profile
	Access the Videos view where it is also possible to access the frame view and video player functionality
	Access the Keywords view showing keyword hits from keyword searches
	Access the Timeline view showing a listing of all Artifact and File Capture records in a single timeline
	Access the Files View which lists all files and folders upon the target devices

Option	Function
	A log of encountered protected files and parsing or scanning events
	Access the Tagged View which lists all tagged items
	Access the Report creation view
	Access to individual Capture results

When clicking the More button, the following panel is displayed:






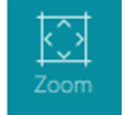







This shows at a glance all the captures and their results which are hyperlinked, clicking on a capture name will open the relevant capture.

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.

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
Search the scan result tables for specific Keywords	 Search Tables
Add, remove or reorder columns from view. Changes made to column display also modify columns displayed within reports. Adjust sort order of displayed results	 Columns
Deselects (unchecks) any selected records within the current view	 Deselect All
Allows the application of context specific filters to the displayed records	 Filter
Zoom function allows for resizing of preview thumbnails	 Zoom
Apply Tags for selected record(s) in the current view. Renaming of Tags is available here.	 Tags
Apply a Comment to selected record(s) in the current view	 Comments
Displays Classifier progress and allows the Classifier to be paused and resumed. Facilitates access to the Pictures view, filtered by a Visual Class	 Classifier




Function	Option
Only visible in the Files view. Toggles the path filter displayed as a hierarchical view of folders	 Folders Tree
Toggles the display of the Details Pane which provides further information and functionality for the selected record	 Details

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 lists 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 up to 1000 keyword hits highlighted in yellow with surrounding text visible
Frames	Displays 50 frames taken at regular intervals from a video file
Preview	Pictures are viewable in this pane at their actual size, "other files may be viewed by clicking the Undock button on the Details Pane Function Toolbar. Videos are playable via an internal player subject to installed codecs
Duplicates	Displays a list of duplicate files which can be clicked in to see data relating to the duplicate file

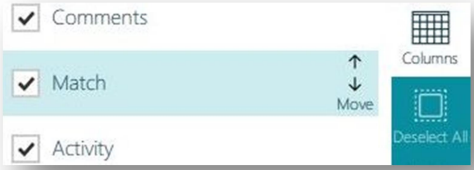
Function Toolbar of Details Pane

Function	Option
Undocks the Preview window	
Open the file with an external application	
Save the file to a chosen location	


Column controls




Left click and hold in between columns will allow the resizing column widths



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 header to sort Ascending or Descending (not all columns are sortable)





Preview Window

The Preview tab in the details pane shows a preview of pictures and documents. On occasion it is not possible to display the file within the details pane, a warning message of “Please undock to view content” will be displayed in such cases. Clicking on the Undock button will open a Preview window.



Preview Window



Function Toolbar of Preview Window

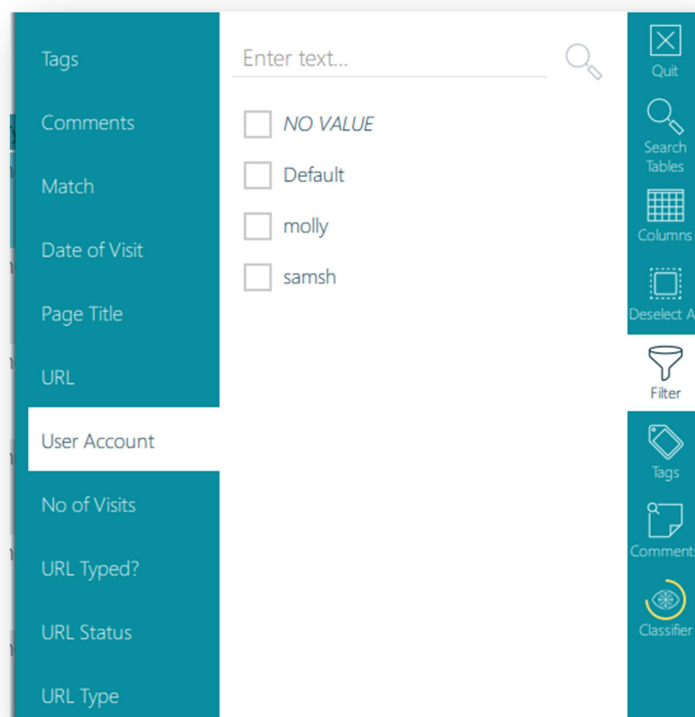
Function	Option
Docks the Preview window	 Dock
Open the file with an external application	 Open with
Save the file to a chosen location	 Save as
Print the contents of the Preview window	 Print

Filtering

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

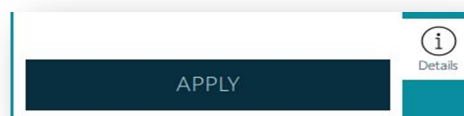
Some fields can be filtered by pre-set values or by entering text. If text is entered into the “Enter text” field the magnifying glass button within the field must be clicked.


Filter Options



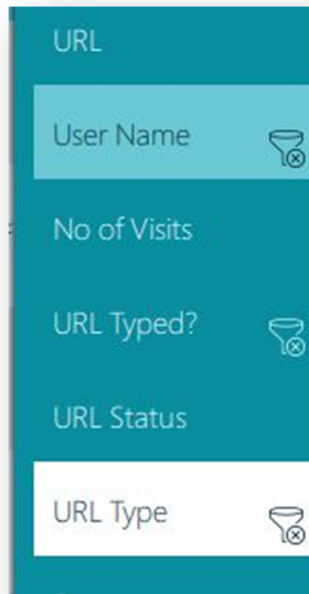
Click the Apply button to apply the filter.


Filter Apply Button



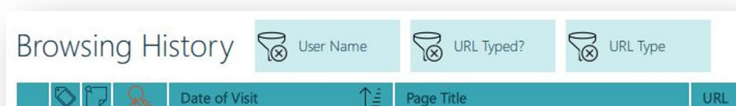
Active Filters are shown next to the column name that has been filtered (represented by the  icon). The filter can be removed by clicking on that icon.

Active Filters



Active filters are also shown on the top of the columns with the  icon. These filters can be removed by clicking on that icon.

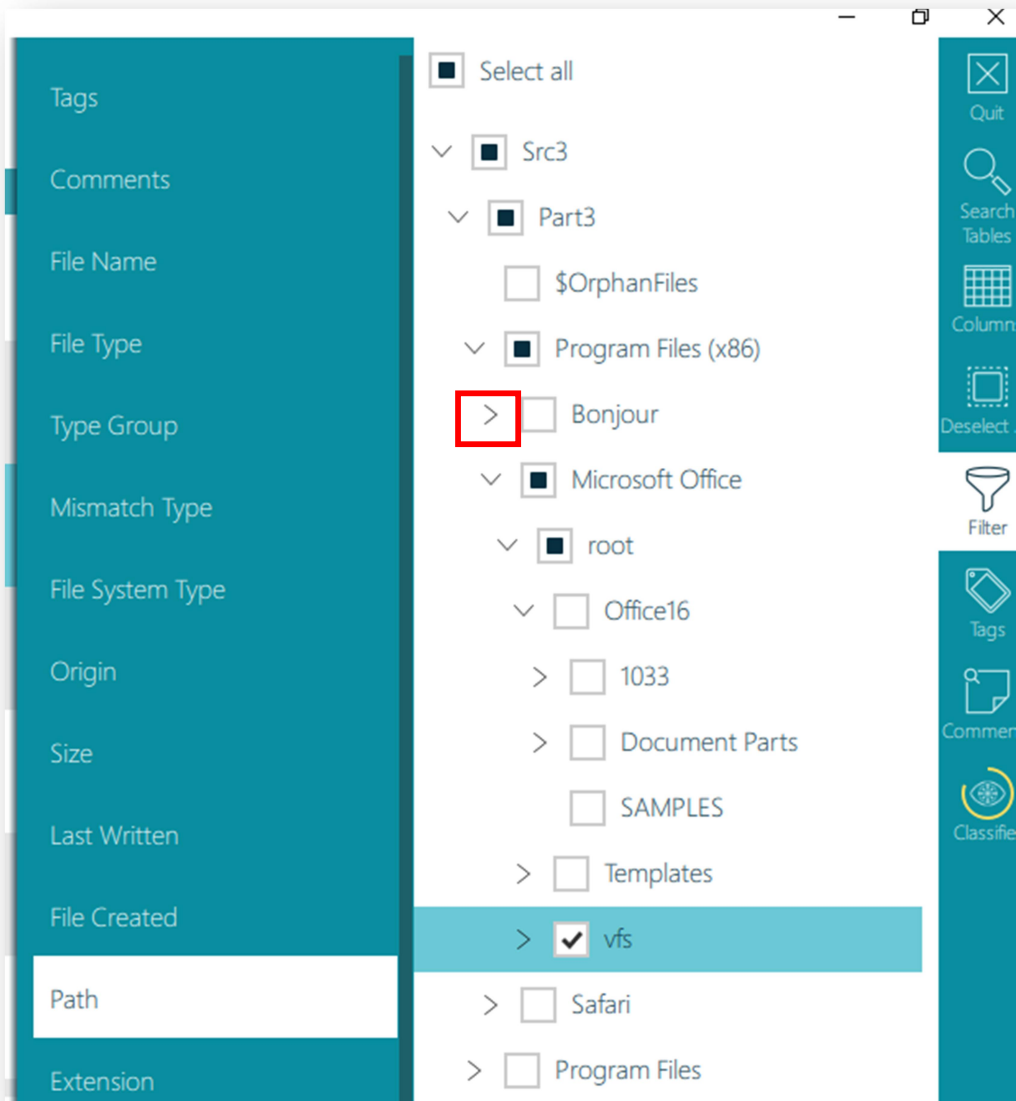
Active Filters



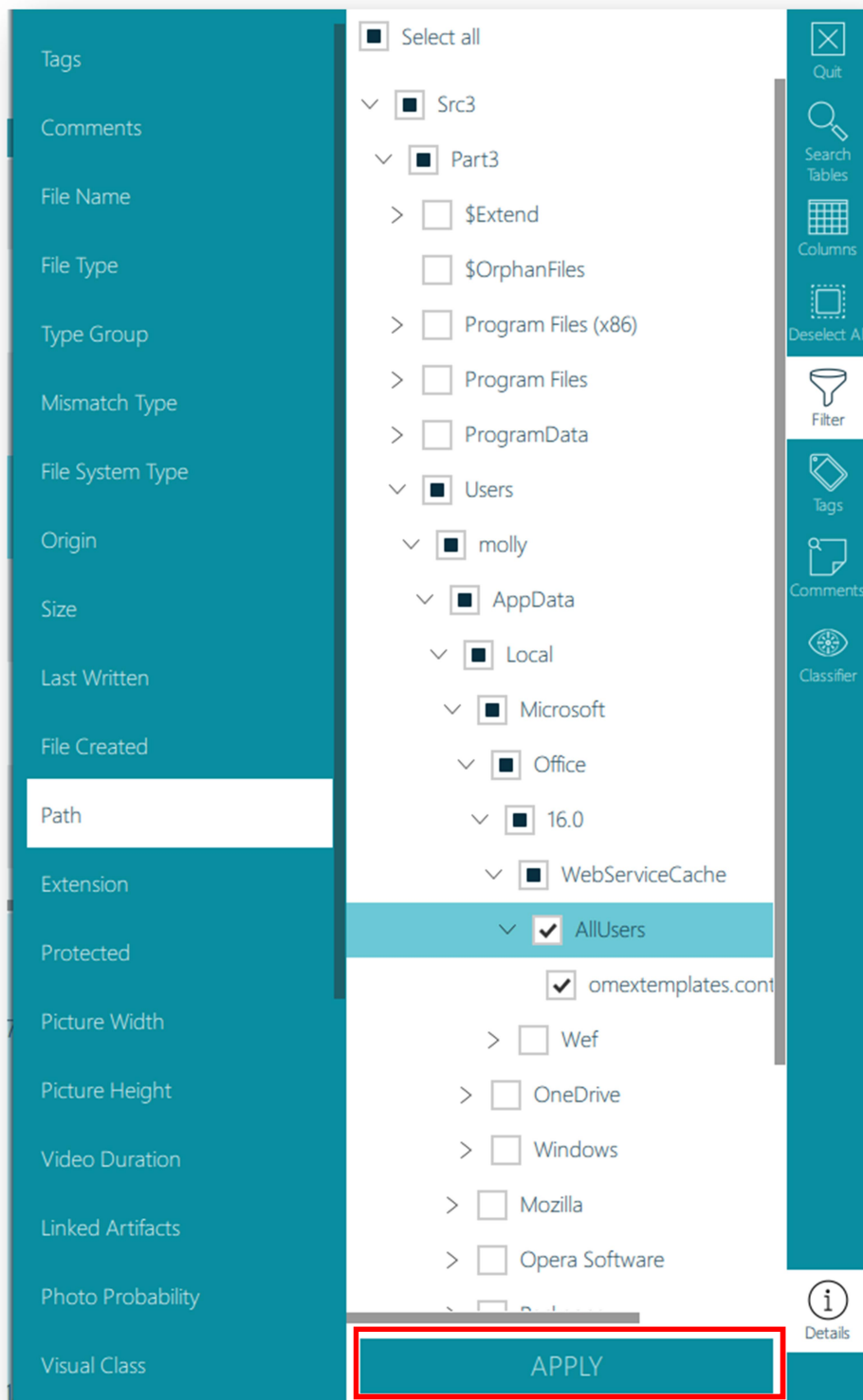
Filtering by Path

Enables the filtering of displayed files by path.

1. Clicking the Path option allows the results to be filtered by path. A selected folder indicates that all the items within that folder and any sub folders are selected. A black check box indicates a partial selection. Clicking the > icon will display sub folders.



2. When the desired folders have been selected click on Apply



Enhanced Filtering Pictures & Videos

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

EXIF data such as Make, Model, Camera Serial Number, Date/Time and GPS Coordinates can also be filtered here.

Picture and Video Filter Options

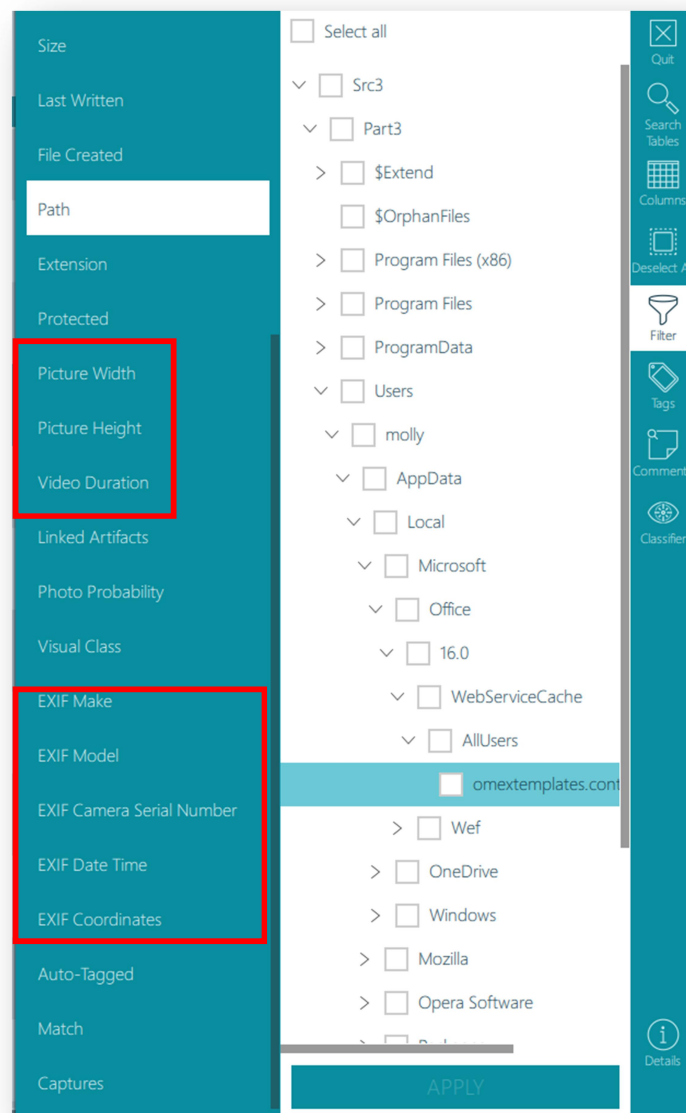


Photo Probability

Photo Probability filtering is applicable to all pictures within the Picture File Types group. The Photo Probability score indicates how likely it is that the file is a photograph. Files with a score of 70% or more are highly likely to be a photograph as opposed to other graphic file types such as icons and clipart or similar.

The Picture and Capture views can be sorted based on the Photo Probability score, allowing non photographic graphic files to be quickly removed from the displayed results. High (80% and above), medium (70% and above) and low (50% and above) pre-set options are available.

Photo Probability Filter Options

The screenshot shows a dialog box titled "Photo Probability Filter Options". On the left is a list of filter categories: Protected, Picture Width, Picture Height, Video Duration, Linked Artifacts, Photo Probability (highlighted), Visual Class, Entities, EXIF Make, EXIF Model, EXIF Camera Serial Number, EXIF Date Time, EXIF Coordinates, Auto-Tagged, and Captures. The main area is titled "Preset probability values" and contains three radio buttons: Low, Medium, and High. Below these are two input fields: "Greater than or equal to..." and "Lower than or equal to...". At the bottom of the main area is a large "APPLY" button. On the right side of the dialog is a vertical toolbar with icons and labels: Quit (X icon), Search Tables (magnifying glass icon), Columns (grid icon), Deselect All (dashed box icon), Filter (funnel icon), Zoom (double arrows icon), Tags (tag icon), Comments (speech bubble icon), Classifier (network icon), and Details (info icon).

Visual Class

If the scan results have been partially or entirely processed by the Classifier, picture file types may be filtered by one or more of 11 visual classes. The visual classes are:

Bestiality, Child Abuse, Others (various innocuous class types), People, Pornography, Portrait, Scanned Doc, US Currency, Vehicle, Weapon, Upskirting.

Visual Class Filter Options

The interface displays the following visual classes and their filter options:

Visual Class	Filter Type	Slider Range
Bestiality	<input type="checkbox"/>	0 to 100 (set at 85)
Child Abuse	<input type="checkbox"/>	0 to 100 (set at 85)
Others	<input type="checkbox"/>	0 to 100 (set at 85)
People	<input type="checkbox"/>	0 to 100 (set at 85)
Pornography	<input type="checkbox"/>	0 to 100 (set at 85)
Portrait	<input type="checkbox"/>	0 to 100 (set at 85)
Scanned Doc	<input type="checkbox"/>	0 to 100 (set at 85)
US Currency	<input type="checkbox"/>	0 to 100 (set at 85)
Upskirting	<input type="checkbox"/>	0 to 100 (set at 85)
Vehicle	<input type="checkbox"/>	0 to 100 (set at 85)
Weapon	<input type="checkbox"/>	0 to 100 (set at 85)
NO VALUE	<input type="checkbox"/>	-

Left sidebar (filters):

- Comments
- Match
- File Name
- File Type
- Type Group
- Mismatch Type
- File System Type
- Origin
- Size
- Last Written
- File Created
- Path
- Extension
- Protected
- Picture Width
- Picture Height
- Video Duration
- Linked Artifacts
- Photo Probability
- Visual Class

Right sidebar (actions):

- Quit
- Search Tables
- Columns
- Deselect All
- Filter
- Zoom
- Tags
- Comments
- Classifier
- Details

Bottom: APPLY

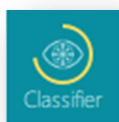
Each picture is processed by the Classifier in order to determine how likely it is to feature within a particular class and is given a probability score. A high visual class probability score indicates that the picture concerned is more likely to fall within that visual class.

Assigning a visual class score is not an exact science and some pictures may appear to be misclassified. However if the scan results include pictures that would correctly fall within a particular class, in most tests, filtering that class to show the top 15% would result in the filter displaying pictures belonging to that class.

Visual class scores filters can be adjusted in 5% increments.

The Classifier classifies automatically in the background as soon as the scan completes. Classifier progress is shown by the Yellow line around the Classifier icon.

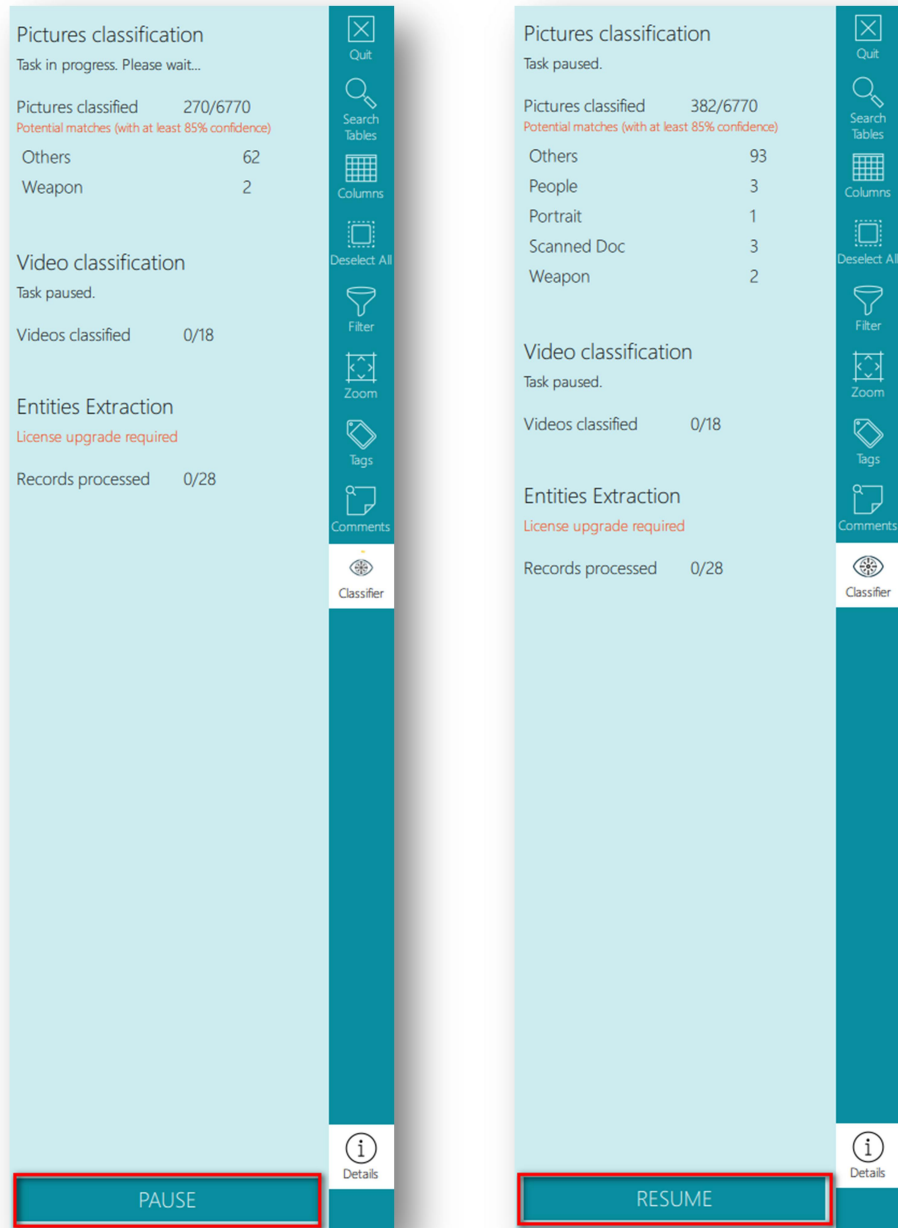
Visual Class Filter Options



Pausing the Classifier

The Classifier can be paused and will not start again until the Resume button is clicked.

Visual Class Filter Options



If the Classifier is running whilst the Scan results are closed then it will resume automatically the next time the Scan Results are opened.

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. Only one column can be sorted in each view.

Ascending	Descending
	

Records Selection and Navigation

There are several options for selecting records to be tagged or commented:

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 or by pressing the space bar
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 number keypad) or Page Down key. Moves the selected view a page at a time
4. Page Up - * (Star on number keypad) or Page Up key. Moves the selected view a page at a time

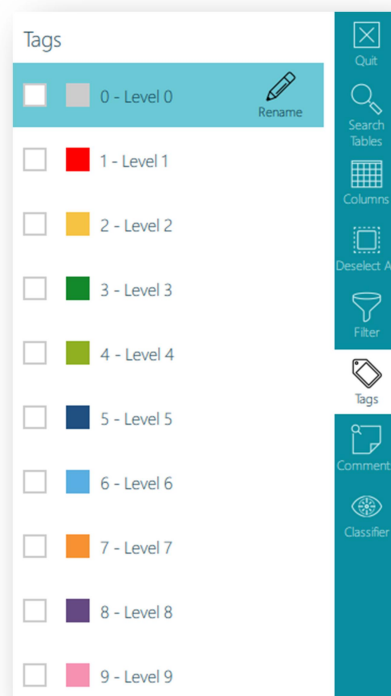
5. Navigation between records can also be achieved using:
Arrow keys (left -right-up-down)
Scroll bar
Mouse scroll wheel

Tagging

After selecting records there are ten (10) tags available that can be customized to suit the report. The default tags are named Level 0 through Level 9 and can be customized in the Settings view or by selecting Rename in the Tags function. Renamed Tags will be applied to the current scan results and do not apply to previous scan results.

1. To tag records with a specific tag:
Select record(s) then select the appropriate tag in the Tags function
Or select record(s) then press number key 0-9 as appropriate
Records can have multiple tags

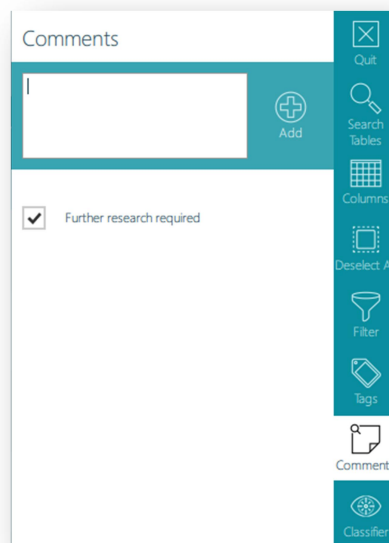
To un-tag a record
Select record(s) to be untagged then select the tag to be removed from the Tags function
Or select record(s) to be untagged then press number key of the tag to be untagged



Comments

Comments can be added to individual or multiple selected records by clicking the comments button on the function toolbar. 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.

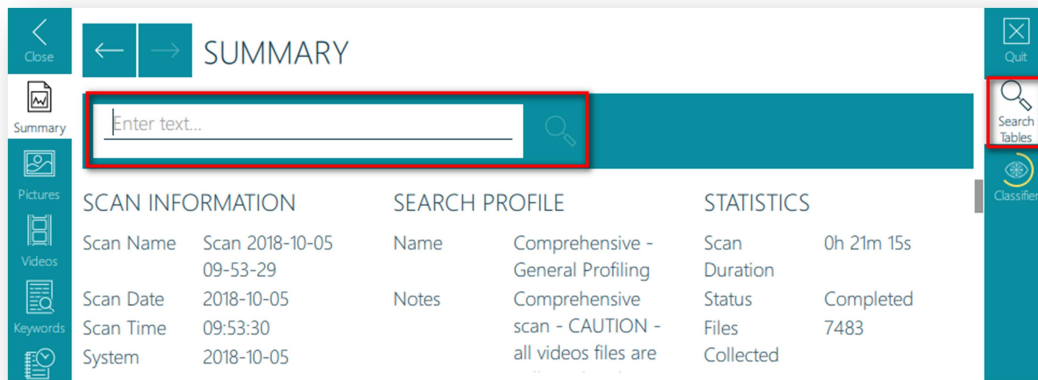
1. To add a comment to record(s):
Type the comment in the text box and click add
The comment will be added to the selected records
2. To remove/edit/delete a comment from record(s):
Select records with comment(s)
Open Comment function
Deselect comment - Affects selected records only
Edit Comment - Affects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



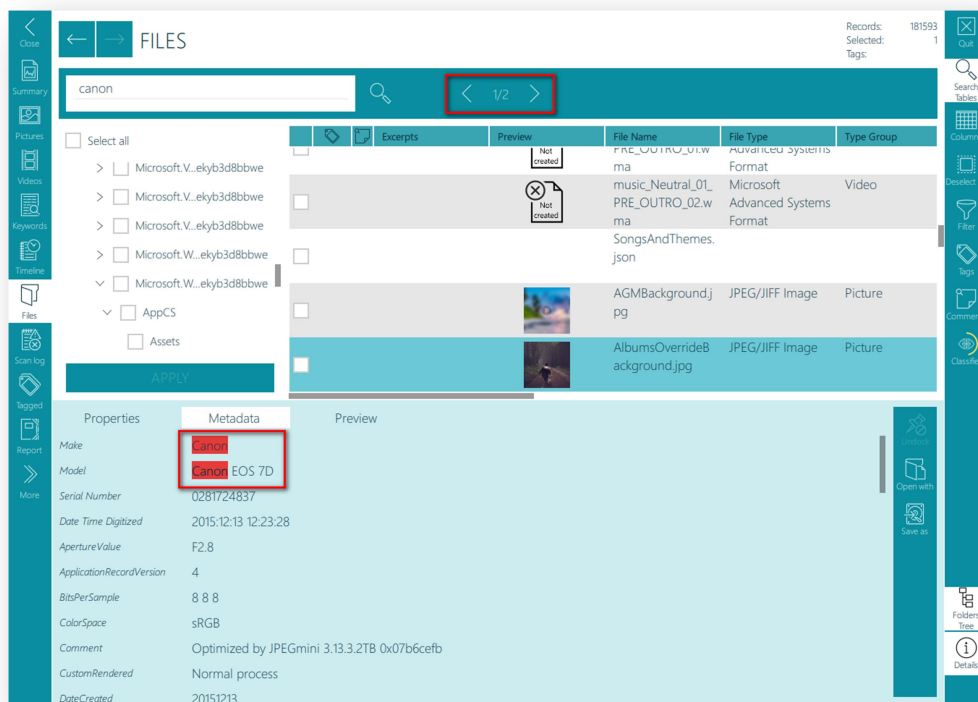
Search Scan Results

A keyword search can be carried out within the data contained in capture result tables. This keyword search is searching **only** the textual data within the results of Artifact Captures and the Files view.

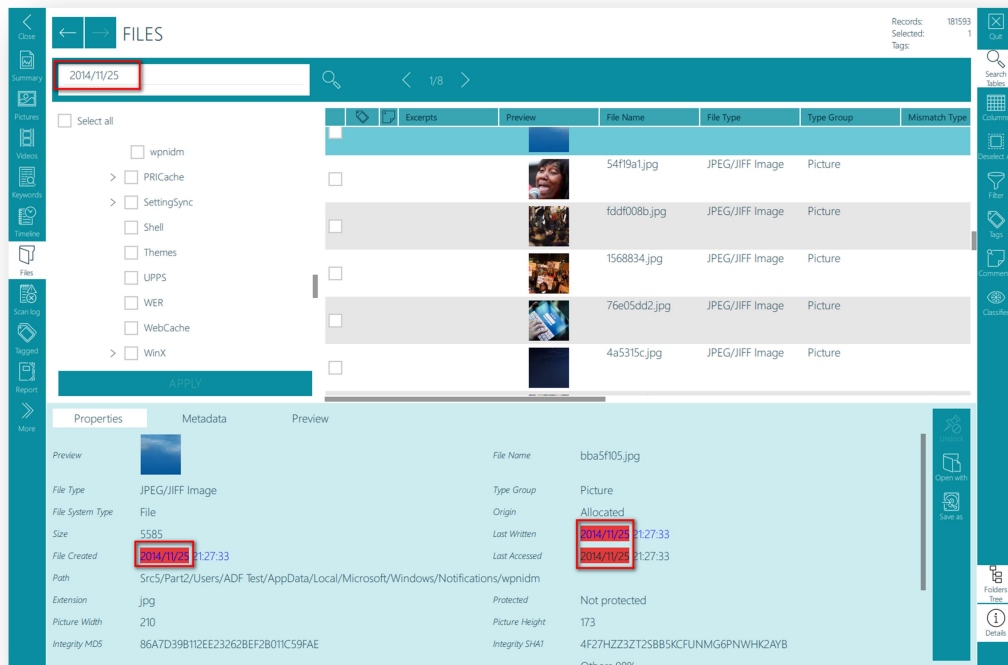
1. To carry out a search click the Search Tables button. This opens up a text box for the search term, clicking the magnifying glass button alongside will carry out the search.



2. The search bar will identify how many search results there are and allow navigation between them using the < and > buttons. The search term will be highlighted in red. The location of search hits is indicated above the search bar.



3. To conduct a search for dates, enter the date in the format yyyy/mm/dd where yyyy is the year, mm is the month and dd is the day (e.g. 2014/11/25), any dates matching this will be identified as a search hit.



Timeline

The Timeline view lists all file and artifact records that have timestamp information. The contents of the Activity, Info and Virtual Location columns are context specific and contain data relevant to the type of record displayed.

Timeline View

The screenshot displays the ADF Digital Evidence Investigator application in the Timeline View. The main window shows a list of records with the following columns: Timestamp, Activity, Info, and Preview. The records are as follows:

Timestamp	Activity	Info	Preview
16:26:15 (L)	visited		
2018/01/24 16:26:15	Recent access	catalan-sheepdog-2.jpg	
2018/01/24 16:26:15	File created	catalan-sheepdog-2.jpg	
2018/01/24 16:26:15	Last written	catalan-sheepdog-2.jpg	
2018/01/24 16:26:06	Browser URL visited		
2018/01/24 16:26:06	Recent access	catalan-sheepdog-3.jpg	

The 'Properties' panel at the bottom provides detailed information for the selected file 'catalan-sheepdog-2.jpg':

Properties	
Target	catalan-sheepdog-2.jpg
Extension	jpg
User Account	samsh
Drive Type	Fixed
Date Accessed	2018/01/24 16:26:15
Candidate	Src21/Part3/Users/samsh/OneDrive/Gospix/catalan-sheepdog-2.jpg [Referenced Files] [Pictures Comprehensive Thorough ID no carving]
Source	Microsoft Windows
Source File	Src21/Part3/Users/samsh/AppData/Roaming/Microsoft/Windows/Recent/catalan-sheepdog-2.lnk
Source Details	No details
Auto-Tagged	No

File Collection capture records list, within the File Created and Last Written columns, timestamps that hyperlink to the appropriate point within the Timeline View. Artifact Capture records may contain timestamps. Where these timestamps exist they hyperlink to the appropriate point within the Timeline View.

Timeline records that relate to a file may contain, within the Details view of that file, a hyperlink to the Files View filtered by the path of the file concerned.

Files

The Files view lists all files and folders encountered on the target device(s). The Files view is accessed by clicking the Files button on the navigation toolbar. The Files view may also be accessible via hyperlinks from several differing artifact captures (e.g. Download History, Recent Files). File Collection capture records contain hyperlinks to the file path of the file concerned. When these hyperlinks are clicked the appropriate record is shown within the Files View filtered by the path of the containing folder.

The Files view can be viewed with or without the Folders Tree displayed. This view is toggled by the Folders Tree button on the Function Toolbar.

Files View

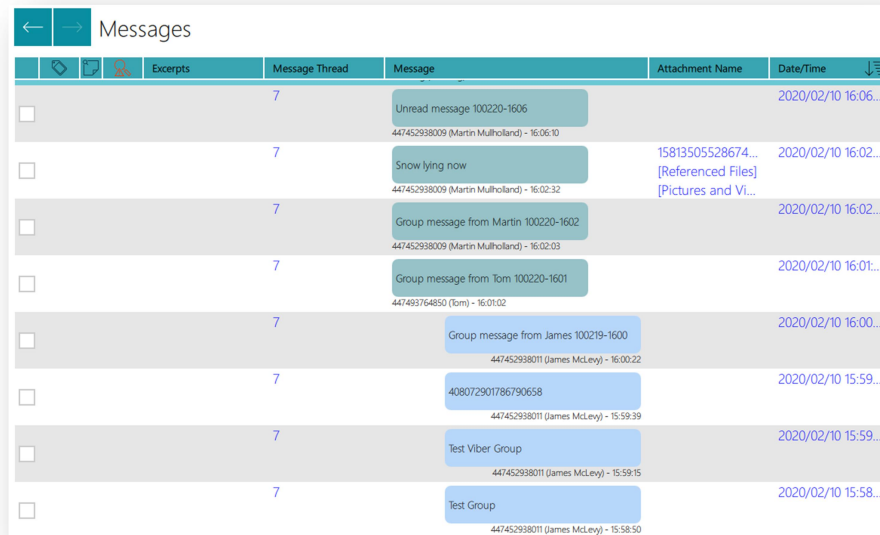
File Name	Origin	Size	File Created	Last Written	Linked Artifacts	Path
f_000140	Allocated	55806	2016/09/23 14:53...	2016/09/23 14:53...	Browser Cache	Src9/Part2/Users/ADF Test/AppData/Local/...
f_0000bc	Allocated	33783	2016/09/23 14:49...	2016/09/23 14:49...	Browser Cache	Src9/Part2/Users/ADF Test/AppData/Local/...
f_0000b5	Allocated	22148	2016/09/23 14:49...	2016/09/23 14:49...	Browser Cache	Src9/Part2/Users/ADF Test/AppData/Local/...
f_0000ba	Allocated	24209	2016/09/23 14:49...	2016/09/23 14:49...	Browser Cache	Src9/Part2/Users/ADF Test/AppData/Local/...
f_0000bb	Allocated	42861	2016/09/23 14:49...	2016/09/23 14:49...	Browser Cache	Src9/Part2/Users/ADF Test/AppData/Local/...
f_0000d7	Allocated	35461	2016/09/23 14:49...	2016/09/23 14:49...	Browser Cache	Src9/Part2/Users/ADF Test/AppData/Local/...
f_0000c2	Allocated	29960	2016/09/23 14:49...	2016/09/23 14:49...	Browser Cache	Src9/Part2/Users/ADF Test/AppData/Local/...
f_0000d4	Allocated	43303	2016/09/23 14:49...	2016/09/23 14:49...	Browser Cache	Src9/Part2/Users/ADF Test/AppData/Local/...
f_0000d5	Allocated	34429	2016/09/23 14:49...	2016/09/23 14:49...	Browser Cache	Src9/Part2/Users/ADF Test/AppData/Local/...
f_0000d8	Allocated	23015	2016/09/23 14:49...	2016/09/23 14:49...	Browser Cache	Src9/Part2/Users/ADF Test/AppData/Local/...

Files View records list, within the File Created and Last Written columns, timestamps that hyperlink to the appropriate point within the Timeline View. Files View records list, within the Linked Artifacts column, hyperlinks to any Artifact Captures that references the file shown.

Messages

Artifact Captures that result in the identification of messages are displayed in the Messages view.

Messages View



	Message Thread	Message	Attachment Name	Date/Time
<input type="checkbox"/>	7	Unread message 100220-1606 447452938009 (Martin Mulholland) - 16:06:10		2020/02/10 16:06...
<input type="checkbox"/>	7	Snow lying now 447452938009 (Martin Mulholland) - 16:02:32	15813505528674... [Referenced Files] [Pictures and Vi...	2020/02/10 16:02...
<input type="checkbox"/>	7	Group message from Martin 100220-1602 447452938009 (Martin Mulholland) - 16:02:03		2020/02/10 16:02...
<input type="checkbox"/>	7	Group message from Tom 100220-1601 447493764850 (Tom) - 16:01:02		2020/02/10 16:01...
<input type="checkbox"/>	7	Group message from James 100219-1600 447452938011 (James McLevy) - 16:00:22		2020/02/10 16:00...
<input type="checkbox"/>	7	408072901786790658 447452938011 (James McLevy) - 15:59:39		2020/02/10 15:59...
<input type="checkbox"/>	7	Test Viber Group 447452938011 (James McLevy) - 15:59:15		2020/02/10 15:59...
<input type="checkbox"/>	7	Test Group 447452938011 (James McLevy) - 15:58:50		2020/02/10 15:58...

The Messages view will display the message content in the Message column. Messages sent by the local user, known as Outgoing messages, will be displayed in a blue message bubble that is right aligned in the Message column. Messages sent from others to the local user, known as Incoming messages, will be displayed in a green message bubble and left aligned in the Message column.

The Message Thread column indicates if messages are part of a single conversation, clicking on a hyperlink in this column will filter the view to only show messages from that conversation. It is not possible to determine a message thread for all message applications.

Tagged View

The Tagged view lists all tagged records.

Tagged View

The screenshot displays the 'Tagged View' interface for 'File Records tagged with Level 5'. The interface includes a sidebar on the left with navigation options like Summary, Pictures, Videos, Keywords, Timeline, Maps, Scan Log, Tagged, Report, and More. The main area shows a table of records with columns: File Name, File Type, Type Group, Mismatch Type, and Origin. Below the table, there is a 'Properties' pane showing details for the selected record, 'Scenario5RTL.png'.

File Name	File Type	Type Group	Mismatch Type	Origin
Scenario5RTL.png	Portable Network Graphic	Picture		Allocated
7e61214d.jpg	JPEG/JIFF Image	Picture		Allocated
43206eb7.jpg	JPEG/JIFF Image	Picture		Allocated

Properties for Scenario5RTL.png:

- Tags: 5 - Level 5
- File Name: Scenario5RTL.png
- Type Group: Picture
- Origin: Allocated
- Last Written: 2017/10/13 10:52:08
- Last Accessed: 2017/10/13 10:51:08
- Path: Src5\Part2\Program Files\WindowsApps\Microsoft3DBuilder_14.11302.0_x86_8wekyb3d8bbwe\Assets\HeroHelp
- Extension: png
- Picture Width: 832
- Picture Height: 608
- Integrity MD5: 2B1D9CB8EAC58987E968C8CEC8CB68AB
- Integrity SHA1: 75B16YNID74HDLIISYD4464253RKNQEVCP

All tagged records are accessible from this view. Each tag where appropriate will indicate the Artifact and File records associated with it.

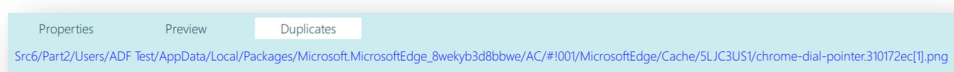
Duplicate Files

Files with matching hash values and file size identified during a scan are considered duplicate files. It is possible to identify duplicates of a file within the Files view and the Pictures view will display an icon to show a picture has duplicates.

Files View

Within the Files view, duplicate files are displayed in the details pane. Duplicate files are shown as a hyperlink which, when clicked, will display details for the duplicate file.

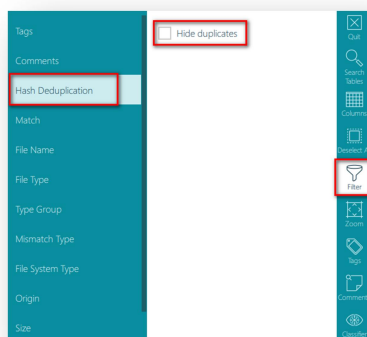
Duplicate Files in Details Pane



Pictures View

The Duplicates tab appears within the Pictures view. A Hash Deduplication option is also available within the Filter options. Selecting the Hide duplicates option will only display one picture in the gallery view if duplicates of the picture are identified.

Hash Deduplication Filter



Pictures that have duplicates will display an icon showing that duplicate pictures were identified:

Duplicate Picture Icon



Referenced File Functionality

The following Artifact Capture results contain records that may reference files on the target device(s) or files embedded within files on the target device(s). We refer to these files as Referenced Files.

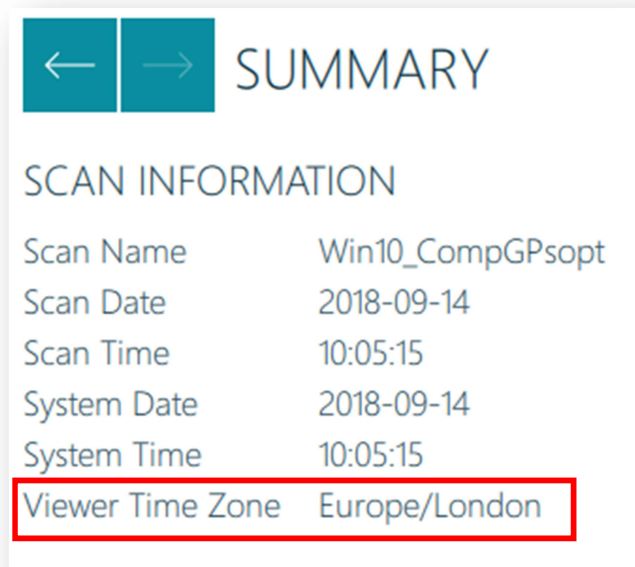
Artifact Capture	Notes
Recent Files	This Artifact Capture identifies recently accessed files. Recently accessed files that can be located upon the target device(s) are treated as Referenced Files and are accessible by a hyperlink in the Candidate column to the relevant file record in the Files View. Candidate files are identified by matching their File Name and File Path with the information within the Artifact Capture record.
Download History	This Artifact Capture recovers information relating to downloaded files. Downloaded files that can be located upon the target device(s) are treated as Referenced Files and are accessible by a hyperlink in the File Name column. Hyperlinks will exist to the Files View record for the downloaded file and to any File Collections Captures that have collected the file concerned.
P2P Files Shared or Downloaded	This Artifact Capture recovers information relating to files downloaded or shared by P2P applications. If these files can be located upon the target device(s) they are treated as Referenced Files and are accessible by a hyperlink in the Candidate column to the relevant file record in the Files View. The Candidate column can also contain details of other Captures that reference the file.
Browser Cache	This Artifact Capture extracts cached files from containers used by the Google Chrome, Safari, Edge, Opera and Firefox browsers. The extracted cached files are listed within the Files View and shown as embedded files. We also treat these files as referenced files. These referenced files are accessible by a hyperlink in the Referenced File column. Hyperlinks will exist to the Files View record for the cached file and to any File Collection Captures that have collected the file concerned.
Messages	This Artifact Capture recovers messaging client messages. These messages may have associated attachments. These attachments are treated as referenced files. These referenced files are accessible by a hyperlink in the Attachment Name column. Hyperlinks will exist to the Files View record for the attached file and to any File Collection Captures that have collected the file concerned. The Attachment Name column can also contain details of other Captures that reference the file.

Artifact Capture	Notes
Emails	This Artifact Capture recovers email client messages. These messages may have associated attachments. These attachments are treated as referenced files. These referenced files are accessible by a hyperlink in the Attachment Names column. Hyperlinks will exist to the Files View record for the attached file and to any File Collection Captures that have collected the file concerned. The Attachment Names column can also contain details of other Captures that reference the file.

File Collection capture records list, within the Linked Artifacts column, hyperlinks to any Artifact Captures that references the file shown.

Time Zone Section

Viewer Time Zone in Summary View



When scans are carried out upon system drives the scanner tries to establish the configured time zone. If a time zone is established all timestamps that are displayed within the results viewer are adjusted where necessary to reflect the configured time zone. Within the Summary view the Viewer Time Zone value will reflect the established time zone.

When scans are carried out on multiple target devices in one scan the scanner searches for a system drive and if one is found establishes the configured time zone. If a time zone is established all timestamps that are displayed within the results viewer for all target devices are adjusted where necessary to reflect the configured time zone. If multiple system drives are located the most recently used system drive takes precedence and all timestamps that are displayed within the results viewer are adjusted in accordance with the time zone discovered on this device. In these cases, within the Summary view the Viewer Time Zone value will reflect the established time zone.

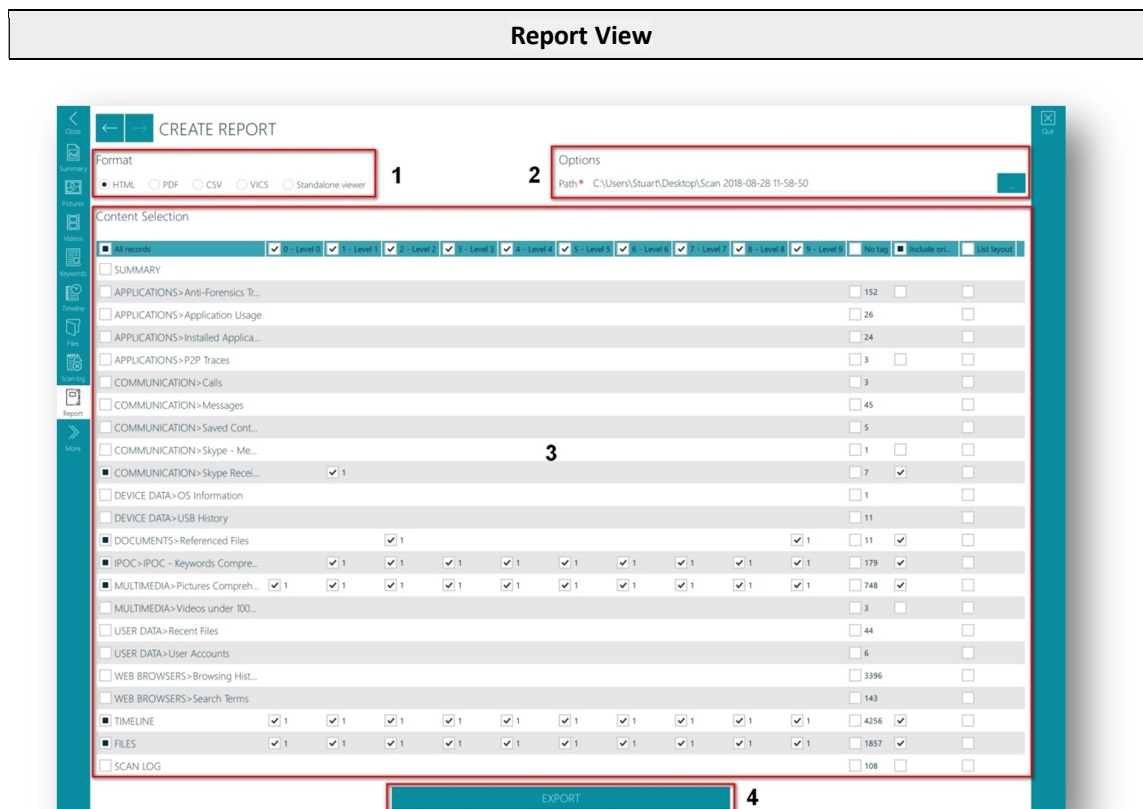
When scans are carried out upon target devices that are non-system drives (without an operating system) no timestamp adjustment is carried out. In this case within the Summary view the Viewer Time Zone will reflect the time zone used by the viewing computer.

In cases where the scanner cannot establish the time zone on system drives no timestamp adjustment is carried out. In this case within the Summary view the Viewer Time Zone will reflect the time zone used by the viewing computer.

12. Reporting

The Report view allows the creation of reports in various formats (HTML, PDF and CSV), the creation of a Project VIC JSON file (and an export of the associated files) or the creation of a Standalone Viewer report. The Report view can be accessed from the Navigation toolbar.

Reports can only be created when Triage-G2 is running as a desktop application or when using the Standalone Viewer functionality. Reports cannot be created during live or boot mode scans.



The Create Report view has 4 main sections:

Section	Functionality
1 - Format	Select the desired report output
2 - Options	Choose the desired output location for the report and define orientation for PDF reports
3 - Content Selection	Select the records/files desired within the report
4 - Export Button	Create the report

HTML Report

HTML reports are viewable with a web browser. The HTML report is customizable allowing the choice of specific Captures and tagged items to show in the 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 can be opened directly from the HTML report providing there are associated applications on the computer used to view the report.

1. Click Report button.

CREATE REPORT

Format: ☒ HTML ☐ PDF ☐ CSV ☐ VICS ☐ Standalone viewer

Options: Path: C:\Users\Stuart\Desktop\Scan 2018-08-28 11:58:50

Content Selection

Category	Sub-category	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5	Level 6	Level 7	Level 8	Level 9	No tag	Include pri	List layout
<input checked="" type="checkbox"/> All records		<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"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> SUMMARY														
<input type="checkbox"/> APPLICATIONS>Anti-Forensics Tr...														
<input type="checkbox"/> APPLICATIONS>Application Usage														
<input type="checkbox"/> APPLICATIONS>Installed Applica...														
<input type="checkbox"/> APPLICATIONS>P2P Traces														
<input type="checkbox"/> COMMUNICATION>Calls														
<input type="checkbox"/> COMMUNICATION>Messages														
<input type="checkbox"/> COMMUNICATION>Saved Cont...														
<input type="checkbox"/> COMMUNICATION>Skype - Me...														
<input checked="" type="checkbox"/> COMMUNICATION>Skype Rece...		<input checked="" type="checkbox"/>												
<input type="checkbox"/> DEVICE DATA>OS Information														
<input type="checkbox"/> DEVICE DATA>USB History														
<input checked="" type="checkbox"/> DOCUMENTS>Referenced Files			<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"/>	<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"/> 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"/>			
<input type="checkbox"/> MULTIMEDIA>Videos under 100...														
<input type="checkbox"/> USER DATA>Recent Files														
<input type="checkbox"/> USER DATA>User Accounts														
<input type="checkbox"/> WEB BROWSERS>Browsing Hist...														
<input type="checkbox"/> WEB BROWSERS>Search Terms														
<input checked="" 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"/>			
<input checked="" type="checkbox"/> FILES		<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"/>			
<input type="checkbox"/> SCAN LOG														

EXPORT

2. Select Format – HTML from the format section.

The screenshot shows the 'CREATE REPORT' window. In the 'Format' section, the 'HTML' radio button is selected and highlighted with a red box. Other options include PDF, CSV, VICS, and Standalone viewer. The 'Options' section shows a path: C:\Users\Stuart\Desktop\Scan 2018-08-28 11-58-50. The 'Content Selection' section is visible below, showing a list of categories and their associated counts.

Category	Count
APPLICATIONS>Anti-Forensics Tr...	152
APPLICATIONS>Application Usage	26
APPLICATIONS>Installed Applica...	24
APPLICATIONS>P2P Traces	3
COMMUNICATION>Calls	3
COMMUNICATION>Messages	45
COMMUNICATION>Saved Cont...	5
COMMUNICATION>Skype - Me...	1
COMMUNICATION>Skype Recei...	7
DEVICE DATA>OS Information	1
DEVICE DATA>USB History	11
DOCUMENTS>Referenced Files	11
IPOC>IPOC - Keywords Compre...	179
MULTIMEDIA>Pictures Compreh...	748
MULTIMEDIA>Videos under 100...	3
USER DATA>Recent Files	44
USER DATA>User Accounts	6
WEB BROWSERS>Browsing Hist...	3396
WEB BROWSERS>Search Terms	143
TIMELINE	4256
FILES	1857
SCAN LOG	108

3. By default, all tagged records are selected in the Content Selection section.

The screenshot shows the 'CREATE REPORT' window. In the 'Content Selection' section, the 'All records' checkbox is selected, and all individual record checkboxes are also selected, indicating that all tagged records are selected by default. The 'Format' section shows 'HTML' selected. The 'Options' section shows the same path: C:\Users\Stuart\Desktop\Scan 2018-08-28 11-58-50.

Category	Count
APPLICATIONS>Anti-Forensics Tr...	152
APPLICATIONS>Application Usage	26
APPLICATIONS>Installed Applica...	24
APPLICATIONS>P2P Traces	3
COMMUNICATION>Calls	3
COMMUNICATION>Messages	45
COMMUNICATION>Saved Cont...	5
COMMUNICATION>Skype - Me...	1
COMMUNICATION>Skype Recei...	7
DEVICE DATA>OS Information	1
DEVICE DATA>USB History	11
DOCUMENTS>Referenced Files	11
IPOC>IPOC - Keywords Compre...	179
MULTIMEDIA>Pictures Compreh...	748
MULTIMEDIA>Videos under 100...	3
USER DATA>Recent Files	44
USER DATA>User Accounts	6
WEB BROWSERS>Browsing Hist...	3396
WEB BROWSERS>Search Terms	143
TIMELINE	4256
FILES	1857
SCAN LOG	108

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

The screenshot shows the 'CREATE REPORT' dialog with the 'Content Selection' tab active. The 'All records' checkbox is highlighted with a red box. The 'Format' section shows 'HTML' selected. The 'Options' section shows the path 'C:\Users\Stuart\Desktop\Scan 2018-08-28 11-58-50'. The 'Content Selection' table lists various categories and their record counts.

Category	0 - Level 0	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 checked="" type="checkbox"/> SUMMARY													
<input checked="" type="checkbox"/> APPLICATIONS>Anti-Forensics Tr...											152		
<input checked="" type="checkbox"/> APPLICATIONS>Application Usage											26		
<input checked="" type="checkbox"/> APPLICATIONS>Installed Applica...											24		
<input checked="" type="checkbox"/> APPLICATIONS>P2P Traces											3		
<input checked="" type="checkbox"/> COMMUNICATION>Calls											3		
<input checked="" type="checkbox"/> COMMUNICATION>Messages											45		
<input checked="" type="checkbox"/> COMMUNICATION>Saved Cont...											5		
<input checked="" type="checkbox"/> COMMUNICATION>Skype - Me...											1		
<input checked="" type="checkbox"/> COMMUNICATION>Skype Recl...											7		
<input checked="" type="checkbox"/> DEVICE DATA>OS Information											1		
<input checked="" type="checkbox"/> DEVICE DATA>USB History											11		
<input checked="" type="checkbox"/> DOCUMENTS>Referenced Files											11		
<input checked="" type="checkbox"/> IIOC>IIOC - Keywords Compre...											179		
<input checked="" type="checkbox"/> MULTIMEDIA>Pictures Compreh...											748		
<input checked="" type="checkbox"/> MULTIMEDIA>Videos under 100...											3		
<input checked="" type="checkbox"/> USER DATA>Recent Files											44		
<input checked="" type="checkbox"/> USER DATA>User Accounts											6		
<input checked="" type="checkbox"/> WEB BROWSERS>Browsing Hist...											3396		
<input checked="" type="checkbox"/> WEB BROWSERS>Search Terms											143		
<input checked="" type="checkbox"/> TIMELINE											4256		
<input checked="" type="checkbox"/> FILES											1857		
<input checked="" type="checkbox"/> SCAN LOG											108		

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

The screenshot shows the 'CREATE REPORT' dialog with the 'Content Selection' tab active. The 'All records' checkbox is highlighted with a red box. The 'Format' section shows 'HTML' selected. The 'Options' section shows the path 'C:\Users\Stuart\Desktop\Scan 2018-08-28 11-58-50'. The 'Content Selection' table lists various categories and their record counts.

Category	0 - Level 0	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 checked="" type="checkbox"/> SUMMARY													
<input type="checkbox"/> APPLICATIONS>Anti-Forensics Tr...											152		
<input type="checkbox"/> APPLICATIONS>Application Usage											26		
<input type="checkbox"/> APPLICATIONS>Installed Applica...											24		
<input type="checkbox"/> APPLICATIONS>P2P Traces											3		
<input type="checkbox"/> COMMUNICATION>Calls											3		
<input type="checkbox"/> COMMUNICATION>Messages											45		
<input type="checkbox"/> COMMUNICATION>Saved Cont...											5		
<input type="checkbox"/> COMMUNICATION>Skype - Me...											1		
<input type="checkbox"/> COMMUNICATION>Skype Recl...											7		
<input type="checkbox"/> DEVICE DATA>OS Information											1		
<input type="checkbox"/> DEVICE DATA>USB History											11		
<input type="checkbox"/> DOCUMENTS>Referenced Files											11		
<input type="checkbox"/> IIOC>IIOC - Keywords Compre...											179		
<input checked="" type="checkbox"/> MULTIMEDIA>Pictures Compreh...											748		
<input type="checkbox"/> MULTIMEDIA>Videos under 100...											3		
<input type="checkbox"/> USER DATA>Recent Files											44		
<input type="checkbox"/> USER DATA>User Accounts											6		
<input type="checkbox"/> WEB BROWSERS>Browsing Hist...											3396		
<input type="checkbox"/> WEB BROWSERS>Search Terms											143		
<input type="checkbox"/> TIMELINE											4256		
<input type="checkbox"/> FILES											1857		
<input type="checkbox"/> SCAN LOG											108		

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

CREATE REPORT

Format: ☒ HTML ☐ PDF ☐ CSV ☐ VICS ☐ Standalone viewer

Options: Path: C:\Users\Stuart\Desktop\Scan 2018-08-28 11-58-50

Content Selection

☒ All records ☒ 0 - Level 0 ☐ 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 ori... ☐ List layout

☐ SUMMARY

☐ APPLICATIONS>Anti-Forensics Tr... 152 ☐

☐ APPLICATIONS>Application Usage 26 ☐

☐ APPLICATIONS>Installed Applica... 24 ☐

☐ APPLICATIONS>P2P Traces 3 ☐

☐ COMMUNICATION>Calls 3 ☐

☐ COMMUNICATION>Messages 45 ☐

☐ COMMUNICATION>Saved Cont... 5 ☐

☐ COMMUNICATION>Skype - Me... 1 ☐

☐ COMMUNICATION>Skype Recei... 7 ☐

☐ DEVICE DATA>OS Information 1 ☐

☐ DEVICE DATA>USB History 11 ☐

☐ DOCUMENTS>Referenced Files 1 ☐

☐ IIOC>IIOC - Keywords Compre... 1 ☐

☒ MULTIMEDIA>Pictures Compreh... 1 ☐

☐ MULTIMEDIA>Videos under 100... 3 ☐

☐ USER DATA>Recent Files 44 ☐

☐ USER DATA>User Accounts 6 ☐

☐ WEB BROWSERS>Browsing Hist... 3396 ☐

☐ WEB BROWSERS>Search Terms 143 ☐

☒ TIMELINE 1 ☐

☒ FILES 1 ☐

☐ SCAN LOG 108 ☐

EXPORT

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

CREATE REPORT

Format: ☒ HTML ☐ PDF ☐ CSV ☐ VICS ☐ Standalone viewer

Options: Path: C:\Users\Stuart\Desktop\Scan 2018-08-28 11-58-50

Content Selection

☐ All records ☐ 0 - Level 0 ☐ 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 ori... ☐ List layout

☐ SUMMARY

☐ APPLICATIONS>Anti-Forensics Tr... 152 ☒

☐ APPLICATIONS>Application Usage 26 ☐

☐ APPLICATIONS>Installed Applica... 24 ☐

☐ APPLICATIONS>P2P Traces 3 ☒

☐ COMMUNICATION>Calls 3 ☐

☐ COMMUNICATION>Messages 45 ☐

☐ COMMUNICATION>Saved Cont... 5 ☐

☐ COMMUNICATION>Skype - Me... 1 ☒

☐ COMMUNICATION>Skype Recei... 7 ☒

☐ DEVICE DATA>OS Information 1 ☐

☐ DEVICE DATA>USB History 11 ☐

☐ DOCUMENTS>Referenced Files 1 ☐

☐ IIOC>IIOC - Keywords Compre... 1 ☐

☐ MULTIMEDIA>Pictures Compreh... 1 ☐

☐ MULTIMEDIA>Videos under 100... 3 ☒

☐ USER DATA>Recent Files 44 ☐

☐ USER DATA>User Accounts 6 ☐

☐ WEB BROWSERS>Browsing Hist... 3396 ☐

☐ WEB BROWSERS>Search Terms 143 ☐

☐ TIMELINE 1 ☐

☐ FILES 1 ☒

☐ SCAN LOG 108 ☒

EXPORT

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

The screenshot shows the 'CREATE REPORT' dialog box. In the 'Content Selection' section, the 'List layout' checkbox is checked and highlighted with a red box. The 'Format' section shows 'HTML' selected. The 'Options' section shows the path 'C:\Users\Stuart\Desktop\Scan 2018-08-28 11-58-50'. The 'Content Selection' table lists various categories and their counts, with checkboxes for selection.

Category	Count	Selected
SUMMARY		<input checked="" type="checkbox"/>
APPLICATIONS>Anti-Forensics Tr...	152	<input checked="" type="checkbox"/>
APPLICATIONS>Application Usage	26	<input checked="" type="checkbox"/>
APPLICATIONS>Installed Applica...	24	<input checked="" type="checkbox"/>
APPLICATIONS>P2P Traces	3	<input checked="" type="checkbox"/>
COMMUNICATION>Calls	3	<input checked="" type="checkbox"/>
COMMUNICATION>Messages	45	<input checked="" type="checkbox"/>
COMMUNICATION>Saved Cont...	5	<input checked="" type="checkbox"/>
COMMUNICATION>Skype - Me...	1	<input checked="" type="checkbox"/>
COMMUNICATION>Skype Recei...	7	<input checked="" type="checkbox"/>
DEVICE DATA>OS Information	1	<input checked="" type="checkbox"/>
DEVICE DATA>USB History	11	<input checked="" type="checkbox"/>
DOCUMENTS>Referenced Files	11	<input checked="" type="checkbox"/>
IPOC>IPOC - Keywords Compre...	179	<input checked="" type="checkbox"/>
MULTIMEDIA>Pictures Compreh...	748	<input checked="" type="checkbox"/>
MULTIMEDIA>Videos under 100...	3	<input checked="" type="checkbox"/>
USER DATA>Recent Files	44	<input checked="" type="checkbox"/>
USER DATA>User Accounts	6	<input checked="" type="checkbox"/>
WEB BROWSERS>Browsing Hist...	3396	<input checked="" type="checkbox"/>
WEB BROWSERS>Search Terms	143	<input checked="" type="checkbox"/>
TIMELINE	4256	<input checked="" type="checkbox"/>
FILES	1857	<input checked="" type="checkbox"/>
SCAN LOG	108	<input checked="" type="checkbox"/>

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

The screenshot shows the 'CREATE REPORT' dialog box. In the 'Content Selection' section, the 'SUMMARY' checkbox is checked and highlighted with a red box. The 'Format' section shows 'HTML' selected. The 'Options' section shows the path 'C:\Users\Stuart\Desktop\Scan 2018-08-28 11-58-50'. The 'Content Selection' table lists various categories and their counts, with checkboxes for selection.

Category	Count	Selected
SUMMARY		<input checked="" type="checkbox"/>
APPLICATIONS>Anti-Forensics Tr...	152	<input type="checkbox"/>
APPLICATIONS>Application Usage	26	<input type="checkbox"/>
APPLICATIONS>Installed Applica...	24	<input type="checkbox"/>
APPLICATIONS>P2P Traces	3	<input type="checkbox"/>
COMMUNICATION>Calls	3	<input type="checkbox"/>
COMMUNICATION>Messages	45	<input type="checkbox"/>
COMMUNICATION>Saved Cont...	5	<input type="checkbox"/>
COMMUNICATION>Skype - Me...	1	<input type="checkbox"/>
COMMUNICATION>Skype Recei...	7	<input type="checkbox"/>
DEVICE DATA>OS Information	1	<input type="checkbox"/>
DEVICE DATA>USB History	11	<input type="checkbox"/>
DOCUMENTS>Referenced Files	11	<input type="checkbox"/>
IPOC>IPOC - Keywords Compre...	179	<input type="checkbox"/>
MULTIMEDIA>Pictures Compreh...	748	<input type="checkbox"/>
MULTIMEDIA>Videos under 100...	3	<input type="checkbox"/>
USER DATA>Recent Files	44	<input type="checkbox"/>
USER DATA>User Accounts	6	<input type="checkbox"/>
WEB BROWSERS>Browsing Hist...	3396	<input type="checkbox"/>
WEB BROWSERS>Search Terms	143	<input type="checkbox"/>
TIMELINE	4256	<input type="checkbox"/>
FILES	1857	<input type="checkbox"/>
SCAN LOG	108	<input type="checkbox"/>

10. Optional - Choose path to save report to (default value is the Desktop of the currently logged in user, the default location can be changed in the Settings view).

CREATE REPORT

Format: ☒ HTML ☐ PDF ☐ CSV ☐ VICS ☐ Standalone viewer

Options: Path * C:\Users\Stuart\Desktop\Scan 2018-08-28 11-58-50

Content Selection

All records	0 - Level 0	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 checked="" type="checkbox"/> SUMMARY													
<input type="checkbox"/> APPLICATIONS>Anti-Forensics Tr...													
<input type="checkbox"/> APPLICATIONS>Application Usage													
<input type="checkbox"/> APPLICATIONS>Installed Applica...													
<input type="checkbox"/> APPLICATIONS>P2P Traces													
<input type="checkbox"/> COMMUNICATION>Calls													
<input type="checkbox"/> COMMUNICATION>Messages													
<input type="checkbox"/> COMMUNICATION>Saved Cont...													
<input type="checkbox"/> COMMUNICATION>Skype - Me...													
<input type="checkbox"/> COMMUNICATION>Skype Recei...													
<input type="checkbox"/> DEVICE DATA>OS Information													
<input type="checkbox"/> DEVICE DATA>USB History													
<input type="checkbox"/> DOCUMENTS>Referenced Files													
<input checked="" type="checkbox"/> IPOC>IPOC - Keywords Compre...	<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"/>	<input checked="" type="checkbox"/>	<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"/>	<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"/>
<input type="checkbox"/> MULTIMEDIA>Videos under 100...													
<input type="checkbox"/> USER DATA>Recent Files													
<input type="checkbox"/> USER DATA>User Accounts													
<input type="checkbox"/> WEB BROWSERS>Browsing Hist...													
<input type="checkbox"/> WEB BROWSERS>Search Terms													
<input type="checkbox"/> TIMELINE													
<input type="checkbox"/> FILES													
<input type="checkbox"/> SCAN LOG													

EXPORT

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

CREATE REPORT

Format: ☒ HTML ☐ PDF ☐ CSV ☐ VICS ☐ Standalone viewer

Options: Path * C:\Users\Stuart\Desktop\Scan 2018-08-28 11-58-50

Content Selection

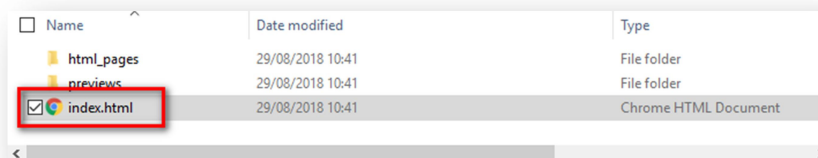
All records	0 - Level 0	1 - Level 1	2 - Level 2	3 - Level 3	4 - Level 4	5 - Level 5	6 - Level 6	7 - Level 7	8 - Level 8	9 - Level 9	No tag	Include on...	List layout
<input checked="" type="checkbox"/> SUMMARY													
<input type="checkbox"/> APPLICATIONS>Anti-Forensics Tr...													
<input type="checkbox"/> APPLICATIONS>Application Usage													
<input type="checkbox"/> APPLICATIONS>Installed Applica...													
<input type="checkbox"/> APPLICATIONS>P2P Traces													
<input type="checkbox"/> COMMUNICATION>Calls													
<input type="checkbox"/> COMMUNICATION>Messages													
<input type="checkbox"/> COMMUNICATION>Saved Cont...													
<input type="checkbox"/> COMMUNICATION>Skype - Me...													
<input type="checkbox"/> COMMUNICATION>Skype Recei...													
<input type="checkbox"/> DEVICE DATA>OS Information													
<input type="checkbox"/> DEVICE DATA>USB History													
<input type="checkbox"/> DOCUMENTS>Referenced Files													
<input checked="" type="checkbox"/> IPOC>IPOC - Keywords Compre...	<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"/>	<input checked="" type="checkbox"/>	<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"/>	<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"/>
<input type="checkbox"/> MULTIMEDIA>Videos under 100...													
<input type="checkbox"/> USER DATA>Recent Files													
<input type="checkbox"/> USER DATA>User Accounts													
<input type="checkbox"/> WEB BROWSERS>Browsing Hist...													
<input type="checkbox"/> WEB BROWSERS>Search Terms													
<input type="checkbox"/> TIMELINE													
<input type="checkbox"/> FILES													
<input type="checkbox"/> SCAN LOG													

EXPORT

Opening HTML Report

HTML reports are stored within a folder as specified within the Option path field. To open an HTML report, browse to the location where the folder was created, open the folder and double click on the *index.html* file therein:

Opening HTML Report



When viewing an HTML report it will open within the default web browser.

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 hide them within the viewer prior to creating the report. A navigation bar appears when moving the cursor over the turquoise section at the left-hand side of the report containing the >> symbol.

HTML Report Navigation



PDF Report

The PDF report is customizable allowing the choice of specific Captures and tags to show in the report, all records can also be shown in the report. Where files have been collected with a scan these can be exported with the report, these can then be opened directly from the PDF report providing there are associated applications on the computer viewing the report.

PDF Report

CREATE REPORT

Format

☐ HTML:
 ☒ PDF
 ☐ CSV
 ☐ VICS
 ☐ Standalone viewer

Content Selection

All records	0 - Level 0	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
SUMMARY													
<input type="checkbox"/> APPLICATIONS>Anti-Forensics Tr...											152	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> APPLICATIONS>Application Usage											26	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> APPLICATIONS>Installed Applica...											24	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> APPLICATIONS>P2P Traces											3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> COMMUNICATION>Calls											3	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> COMMUNICATION>Messages											45	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> COMMUNICATION>Saved Cont...											5	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> COMMUNICATION>Skype - Me...											1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> COMMUNICATION>Skype Recei...	<input type="checkbox"/>	1									7	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> DEVICE DATA>OS Information											1	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> DEVICE DATA>USB History											11	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> DOCUMENTS>Referenced Files			<input type="checkbox"/>	1						<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> IIOC>IIOC - Keywords Compre...	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	179	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> MULTIMEDIA>Pictures Compreh...	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	748	<input checked="" type="checkbox"/>
<input type="checkbox"/> MULTIMEDIA>Videos under 100...											3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> USER DATA>Recent Files											44	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> USER DATA>User Accounts											6	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> WEB BROWSERS>Browsing Hist...											3396	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> WEB BROWSERS>Search Terms											143	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> TIMELINE	<input type="checkbox"/>	1	<input type="checkbox"/>	1	<input type="checkbox"/>	1	<input type="checkbox"/>	1	<input type="checkbox"/>	1	<input type="checkbox"/>	4256	<input checked="" type="checkbox"/>
<input type="checkbox"/> FILES	<input type="checkbox"/>	1	<input type="checkbox"/>	1	<input type="checkbox"/>	1	<input type="checkbox"/>	1	<input type="checkbox"/>	1	<input type="checkbox"/>	1857	<input checked="" type="checkbox"/>
<input type="checkbox"/> SCAN LOG											108	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Options

Path * C:\Users\Stuart\Desktop\Scan 2018-08-28 11:58-50 PDF

Orientation: ☒ Landscape ☐ Portrait

When creating a PDF report Landscape or Portrait orientation can be selected. Reports containing a large number of columns are best produced in Landscape as some columns may not be displayed in Portrait orientation due to the limited page space available.

PDF Orientation

Options


Path* C:\Users\Stuart\Desktop\Scan 2018-08-28 11-58-50 - PDF 3

Orientation: ☒ Landscape ☐ Portrait

Opening PDF Report

PDF reports are stored within a folder as specified within the Option path field. To open a PDF report, browse to the location where the folder was created, open the folder and double click on the *<scan name>.pdf* file therein:

Opening PDF Report

<input type="checkbox"/> Name	Date modified	Type	Size
 Scan 2018-08-28 11-58-50.pdf	29/08/2018 14:01	PDF File	3,300 KB

When viewing a PDF report it will open within the default application used to open PDF files.

The PDF report displays the same columns that were visible in the viewer in the order they were displayed. To remove columns from the PDF report hide them within the viewer prior to creating the report. With limited page space it is recommended to remove columns irrelevant to the report prior to creating a PDF report.

PDF Report

Scan 2018-08-28 11-58-50

SUMMARY

SCAN INFORMATION	
Scan Name	Scan 2018-08-28 11-58-50
Scan Date	2018-08-28
Scan Time	11:58:51
System Date	2018-08-28
System Time	11:58:51
Viewer Time	Europe/London
Zone	

STATISTICS	
Scan Duration	0h 0m 29s
Status	Completed
Files Collected	805
Application	ADF Digital Evidence Investigator 0.0.0

SEARCH PROFILE	
Name	Comprehensive - IPOC speed optimized
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 using the Thorough Identification for Files Without Extension option. Searches for anti-forensics traces, remote access traces, P2P traces and files from Skype caches. Collects protected files and files not processed by parser

TAGS STATISTICS	
0 - Level 0	1
1 - Level 1	1
2 - Level 2	1
3 - Level 3	1
4 - Level 4	1
5 - Level 5	1
6 - Level 6	1
7 - Level 7	1
8 - Level 8	1
9 - Level 9	1

CAPTURES

APPLICATIONS	
Anti-Forensics Traces	201
Application Usage	26
Installed Applications	24
P2P Files Shared or Downloaded	0
P2P Search Terms	0
P2P Traces	3
Remote Access Traces	0
Sharemeta GUIDs	0

COMMUNICATION	
Calls	3
Emails	0
Messages	45
Saved Contacts	5
Skype - Media cache Folder	1
Skype Received Files	8

DOCUMENTS	
Referenced Files	13

SUMMARY 1 / 199

Opening CSV Report

CSV reports are stored within a folder as specified within the Option path field. To open a CSV report, browse to the location where the folder was created, open the folder and double click on the desired <capture>.csv file therein:

Opening CSV Report

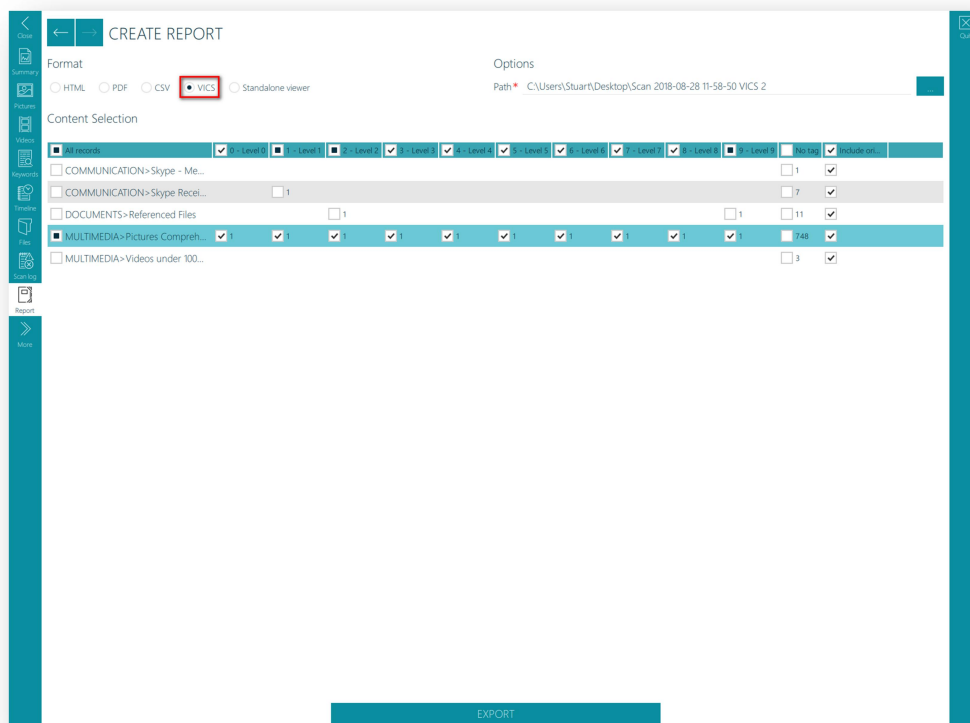
Name	Date modified	Type	Size
original_files	20/09/2018 10:26	File folder	
APPLICATIONS-Anti-Forensics Traces-FILES.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	6 KB
APPLICATIONS-Application Usage.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	21 KB
APPLICATIONS-Cloud Storage Traces-FILES.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	30 KB
APPLICATIONS-Installed Applications.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	3 KB
APPLICATIONS-Social Media Traces-Browser Cache.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	12 KB
APPLICATIONS-Social Media Traces-Browsing History.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	16 KB
APPLICATIONS-Social Media Traces-FILES.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	8 KB
DEVICE DATA-Connection Log.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	3 KB
DEVICE DATA-OS Information.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	2 KB
DEVICE DATA-USB History.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	4 KB
DEVICE DATA-Windows Registry Files.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	8 KB
DOCUMENTS-Office Documents Comprehensive thorough ID .csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	13 KB
DOCUMENTS-Referenced Files.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	627 KB
FILES.csv	20/09/2018 10:27	Microsoft Excel Comma Separated ...	62,939 KB
MULTIMEDIA-Pictures Comprehensive Thorough ID no carving.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	3,348 KB
MULTIMEDIA-Videos All - Comprehensive Thorough ID.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	215 KB
SCAN LOG.csv	20/09/2018 10:27	Microsoft Excel Comma Separated ...	91 KB
TIMELINE.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	4,596 KB
USER DATA-Desktop shortcut files.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	2 KB
USER DATA-Recent Files.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	46 KB
USER DATA-User Accounts.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	3 KB
USER DATA-User Logins.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	199 KB
WEB BROWSERS-Browser Cache.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	965 KB
WEB BROWSERS-Browsing History.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	302 KB
WEB BROWSERS-Download History.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	4 KB
WEB BROWSERS-Form Data.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	2 KB
WEB BROWSERS-Search Terms.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	5 KB

When viewing a CSV report it will open within the default application used to open CSV files.

VICS Report

The VICS report option allows the creation of a Project VICS compatible output folder. This folder contains selected picture and video files together with a Project VICS compatible JSON file. This report is compatible with and can be imported into other applications that support Project VICS including Griffeye. The output Project VICS JSON file can also be used to create Triage-G2 hash captures for use in other cases.

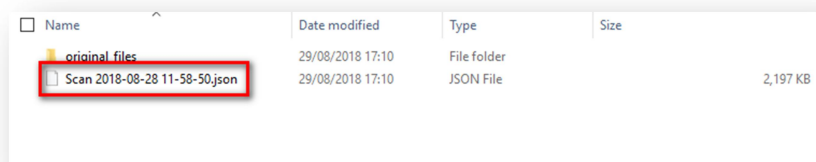
VICS Report



Using VICS Report Output

The Project VICS output is stored within a folder as specified within the Option path field. When asked to import a Project VICS JSON file within another application, browse to this location and select the <scan name>.json file:

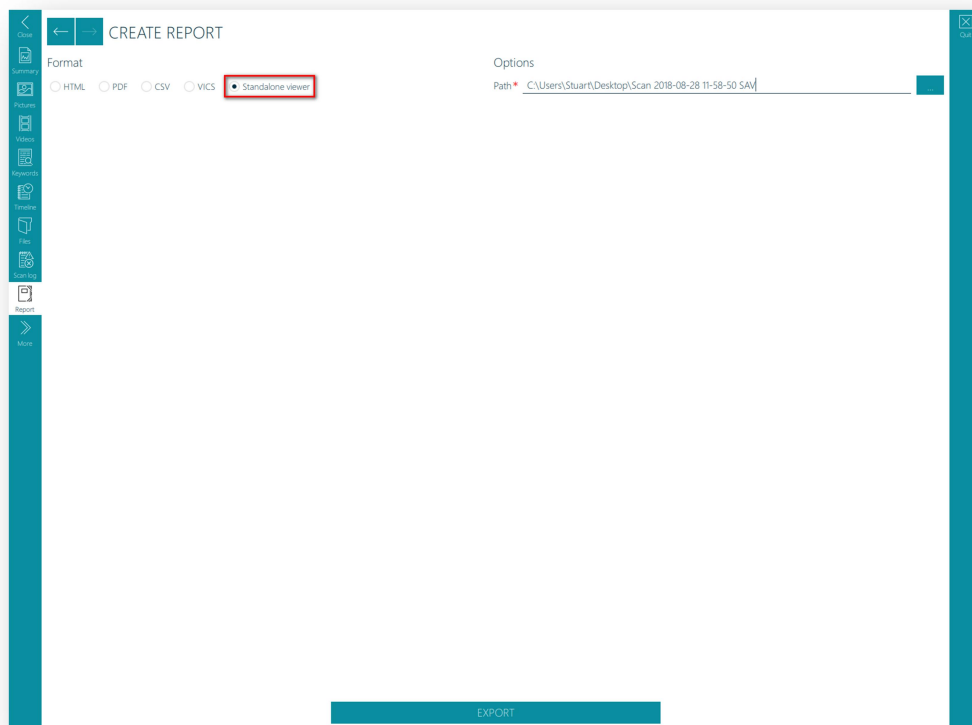
Project VICS JSON File



Standalone Viewer

The Standalone Viewer option outputs all of the scan results into a self-contained folder that includes a built in standalone application that can view the results. This standalone application runs independently of Triage-G2 and can be run on any Windows computer where the user has sufficient privileges. No license is required to view these reports. All Tags and Comments that have been created during the review are included in the output. The Standalone Viewer cannot be run from read-only storage devices such as CDs or DVDs. Standalone Viewer reports allow easy collaboration with other investigators and provide a good method of archiving Scan Results.

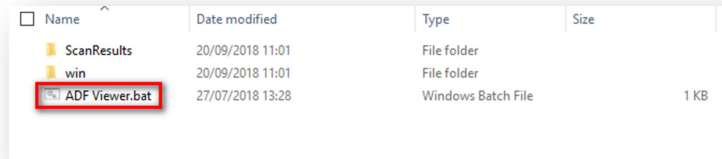
Standalone Viewer



Opening Standalone Viewer

The Standalone Viewer is stored within a folder as specified within the Option path field. To open the Standalone Viewer, browse to the location where the folder was created, open the folder and double click on the *ADF Viewer.bat* file therein:

Opening Standalone Viewer



<input type="checkbox"/> Name	Date modified	Type	Size
ScanResults	20/09/2018 11:01	File folder	
win	20/09/2018 11:01	File folder	
ADF Viewer.bat	27/07/2018 13:28	Windows Batch File	1 KB

The Standalone Viewer will operate as Triage-G2 does when reviewing scan results, see section 11 for further details.

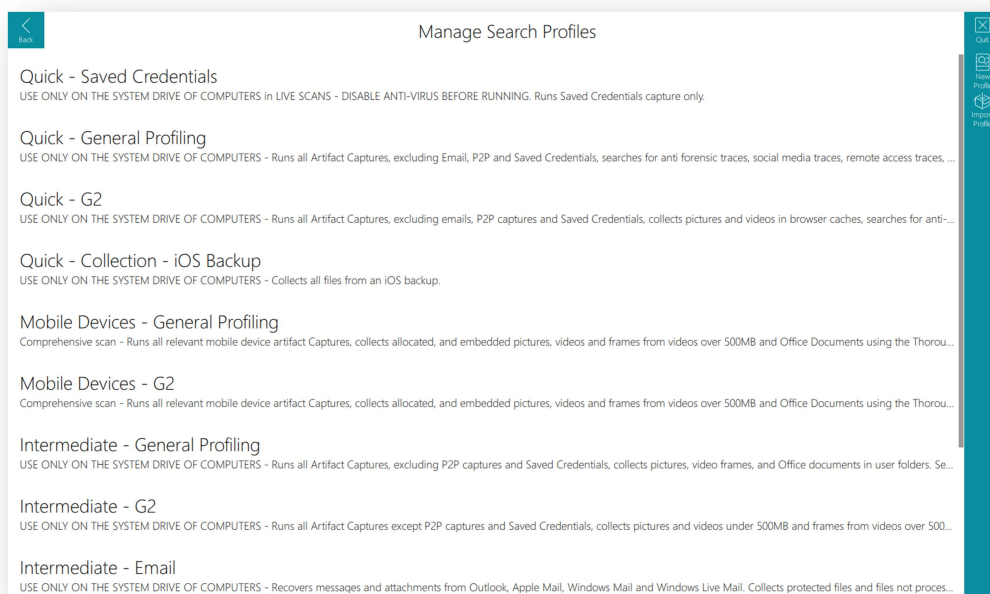
13. Managing and creating Search Profiles

Triage-G2 comes with thirteen 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 Collection Captures recover files matching certain criteria such as file properties, inclusion of keywords or matching hash values. File Collection Captures are supplied with the program and can also be user created.

Triage-G2 allows the creation of custom Search Profiles containing a combination of default and user created Captures. Copies of the default Search Profiles may also be modified to suit operational requirements.

To create a Search Profile, select Setup Scans from the Home screen which will display the Manage Search Profiles view. From here it is possible to create, edit, or delete profiles. The default Search Profiles cannot be edited or deleted, these can only be copied allowing the copy to be edited.

Manage Search Profiles View



Hiding Default Profiles

To hide a Default Search Profile a file entitled config.json file must be edited, this is located by default at “\Users\\AppData\Local\ADF Solutions Inc\ADF Triage-G2\config.json”.

1. Whilst the ADF DEI program is not running open the JSON file in an editor of your choice (notepad will suffice)

```
{
  "Display Default Captures": [
    {
      "name": "OS Information",
      "show": true
    },
    {
      "name": "User Accounts",
      "show": true
    },
    {
      "name": "USB History",
      "show": true
    },
    {
      "name": "Calls",
      "show": true
    },
    {
      "name": "Saved Contacts",
      "show": true
    }
  ]
}
```

2. Scroll to the “Display Default Search Profiles” section and change the “show” value to “false” for the Search Profile to hide

```

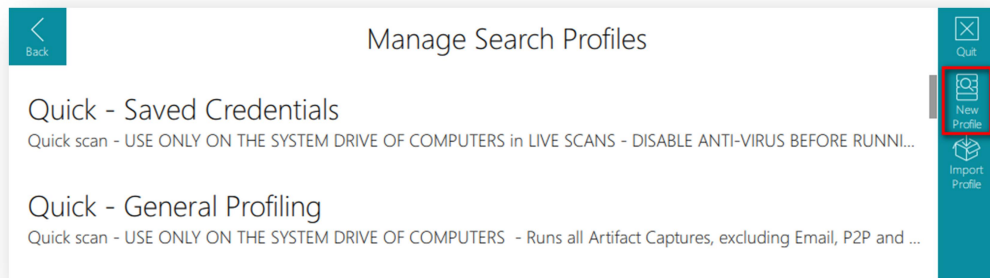
  "Display Default Search Profiles": [
    {
      "name": "Comprehensive - Collect Pictures from Free Space",
      "show": true
    },
    {
      "name": "Comprehensive - General Profiling speed optimized",
      "show": true
    },
    {
      "name": "Comprehensive - General Profiling",
      "show": false
    },
    {
      "name": "Comprehensive - IPOC speed optimized",
      "show": true
    },
    {
      "name": "Comprehensive - IPOC",
      "show": true
    }
  ]
}
```

3. Save the edited file

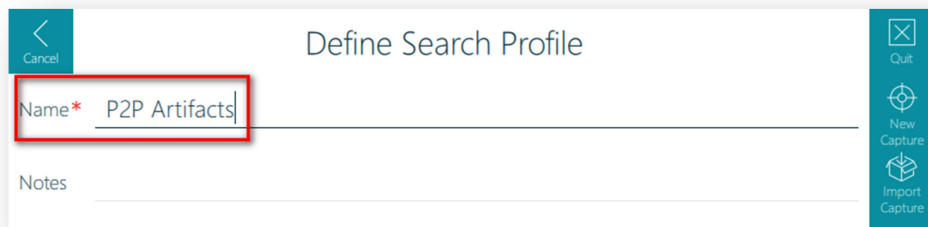
4. To display hidden Default Search Profiles change the “show” value from “false” to “true”

Creating a new Search Profile

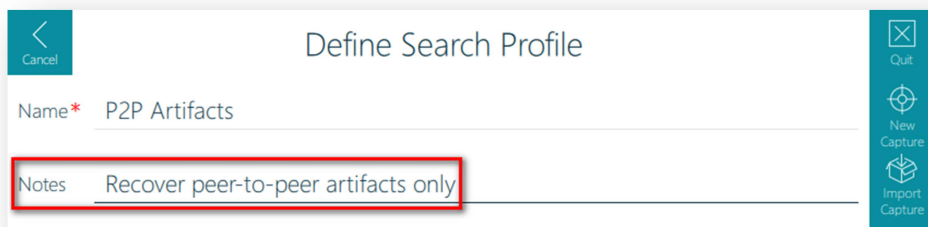
1. Click on the New Profile button in the Function Toolbar



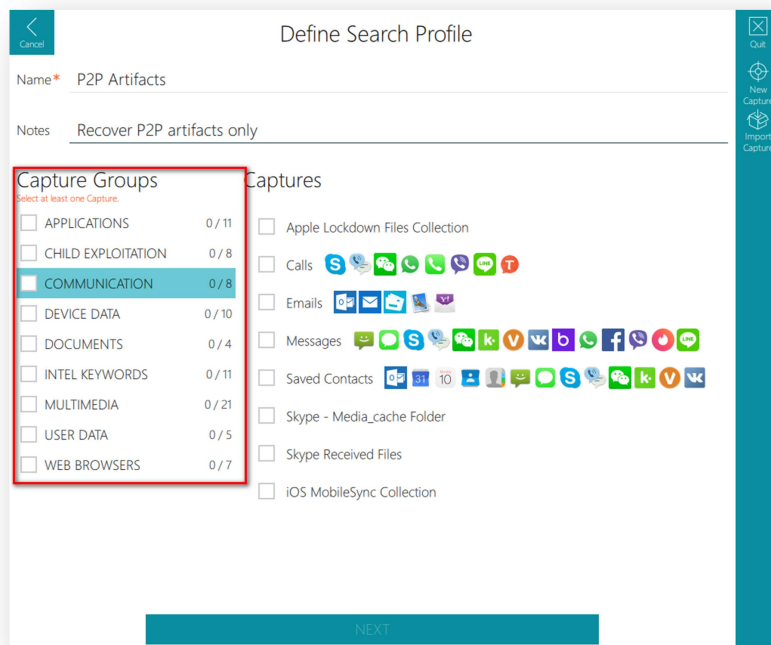
2. Enter a unique name for the profile



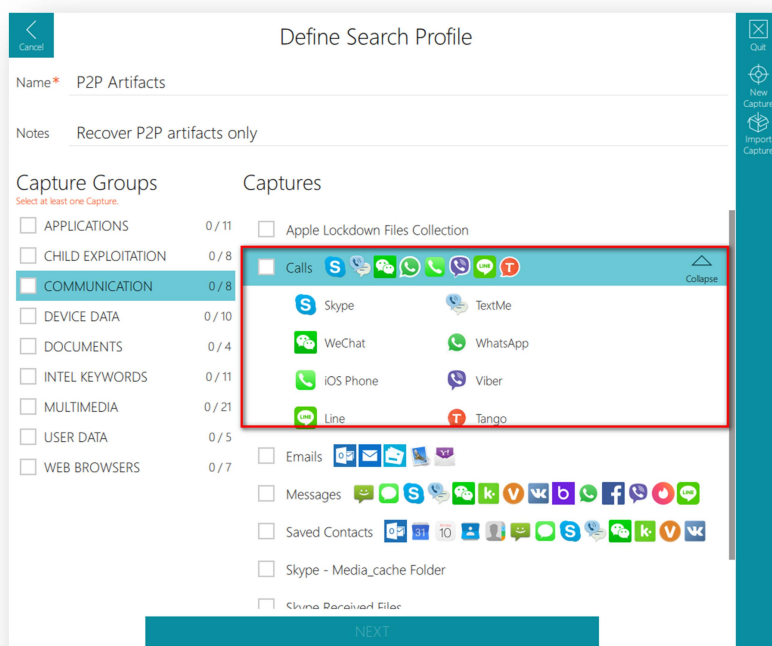
3. Optional - Enter notes describing what the search profile will do



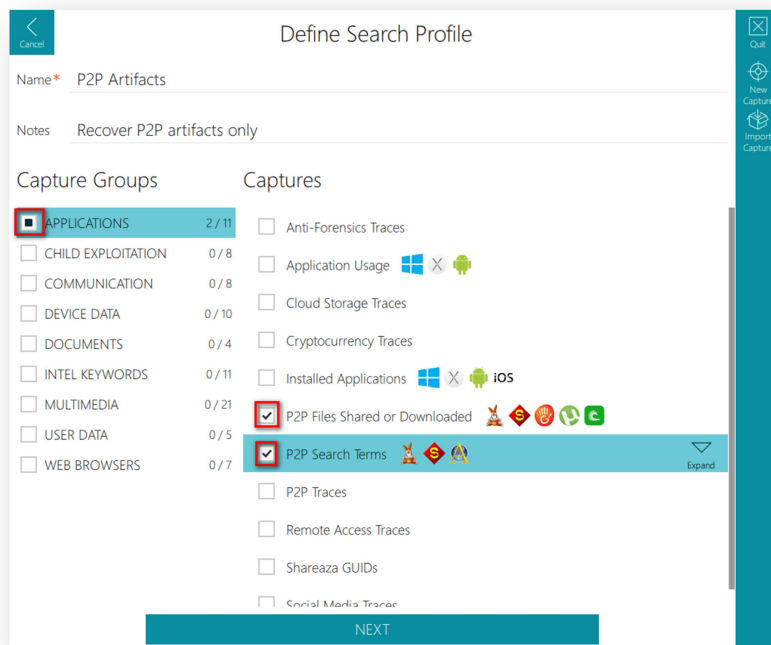
4. The left hand side of the Define Search Profile view contains groups of Captures available. Clicking on a Capture Group displays the Captures on the right hand side



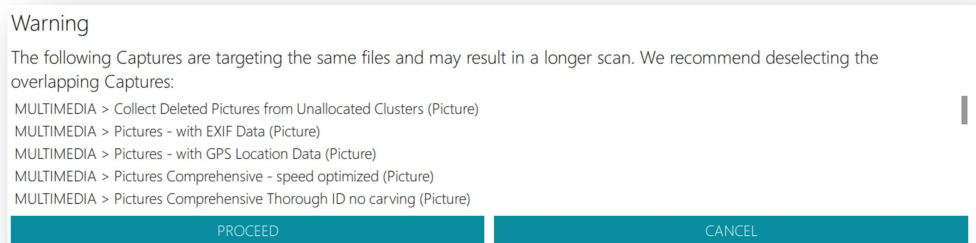
5. Clicking on an Artifact Capture allows the option to Expand: this shows further details for the type of data the Artifact Capture will collect. Clicking Collapse will return to the Capture selection view



6. To select a Capture click on the check box next to it and a tick will appear. To select all Captures within a Category, Click on the check box next to the Category



7. When the desired Captures for the Search Profile have been selected, click the Next button to continue. If any overlapping Captures have been detected a warning dialog will be presented showing them. Clicking Proceed here will continue creating the Search Profile with overlapping Captures, clicking Cancel will allow these to be amended



8. It is possible to add or delete custom fields of information that the user enters at the point of starting a scan or to use scan information fields setup in the Settings view. By default there are three mandatory fields: Scan Name, Scan Date, and Scan Time. Additional fields can be added to prompt for more information by typing in the “enter new field name” text box. It is possible to include a default value and make this new field mandatory. To delete a custom field, click on the Delete button alongside it

Scan Information Fields

☐ Use the fields defined in the application settings
☒ Use the following fields

Field Name	Default Value	Mandatory (*)
Scan Name	NA	<input checked="" type="checkbox"/>
Scan Date	NA	<input checked="" type="checkbox"/>
Scan Time	NA	<input checked="" type="checkbox"/>
Custom Field		<input type="checkbox"/>

Enter new field name...

Delete

9. There are five Scan Options:

Skip files processed for more than X min – set a time value for when files that are taking too long to process are skipped. This feature is useful if corrupt files are stopping scans from completing quickly. Type a numerical value and select minutes or seconds

Collect skipped files – collects files less than 2GB that were skipped during a scan

Collect protected files – this copies any password protected files detected by Captures to the Scan Results.

Collect files that crashed parser – this copies any files that Captures cannot read to the Scan Results.

Activate BitLocker on Collection Key – this will encrypt any Scan Results written to the key securing the data against loss or theft

Scan Options

Skip files processed for more than min ☐ Collect skipped files (max 2GB)

☐ Collect protected files encountered by the Captures (max 2GB)

☐ Collect files that crashed the parsers (max 2GB)

☐ Activate BitLocker on Collection Key (it is impossible to recover the data if the password is lost)

10. Select the post-scan options. Selecting a tick box will automatically start that task when the scan is finished. Highlighting a task shows an order button, clicking this and dragging the mouse allows the task to be ordered above or below the other tasks determining the order these tasks are ran upon scan completion. The Entity Extraction task requires the Rosoka module add-on to be purchased

Post-Scan Options

Select which tasks should start automatically when the scan finishes and move them to define their order of execution.

<input checked="" type="checkbox"/>	Video classification	<div>↑ ↓ Order</div>
<input checked="" type="checkbox"/>	Picture classification	
<input checked="" type="checkbox"/>	Entity extraction	

11. Add a Whitelist. This can be added based on a folder of files, a CSV file containing hash values or a JSON file of hash values. See the section on Whitelists for further details

Whitelists

Add Files

Import CSV

Import JSON

No whitelist

12. Click on the Save button and the new Search Profile will be listed on the Manage Search Profiles screen and can edited or deleted

SAVE

Captures with Saved Contacts

When creating a Search Profile that contains Captures with user details (such as Messages for message Principal or message Recipient) the Saved Contacts Capture should be selected in order to resolve the user names. Failure to select the Saved Contacts will result in a User ID being displayed but no Friendly Name.

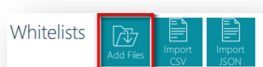
Whitelists

Whitelists are a list of files to be ignored during a scan. There are three ways to add a whitelist: selecting a folder of files, adding a CSV file containing hash values or adding a JSON file containing hash values.

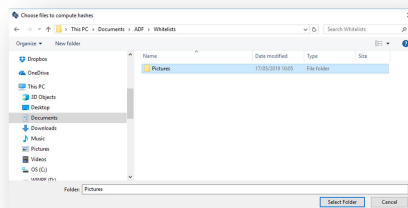
The location where whitelists are saved can be changed in the Settings view. Whitelists created in one Search Profile will be available for use in all user created Search Profiles.

Add Folder of Files

1. Click on the Add Files button in the Whitelists section



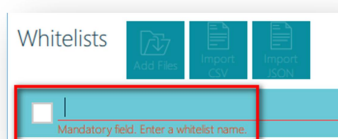
2. Select the folder containing the files to add to the whitelist



3. A message will be displayed showing the status of the whitelist creation. Any errors that occurred during the whitelist creation are displayed, these can include duplicate files or files locked by other applications such as database files. Click the OK button to continue

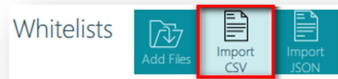
Computation completed
Hash values computed: 3
Warnings/errors: 0

4. Give the whitelist a name, this is mandatory and must differ from other whitelist names, pressing the enter/return key will complete the naming of the whitelist

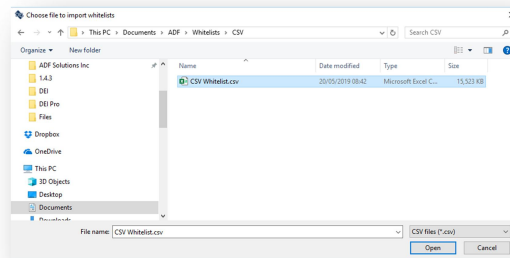


Add Files from CSV

1. Click on the Import CSV button in the Whitelists section



2. Select the CSV file. The CSV file must contain one hash value column (titled "sha-1", "sha1" or "md5") and an optional file size column (titled "filesize" or "file size")



3. A message will be displayed showing the status of the whitelist creation. Any errors that occurred during the whitelist creation are displayed, such as duplicate hash values. Click the OK button to continue

Importing Hash Values

Import completed

Hash values imported: 467491

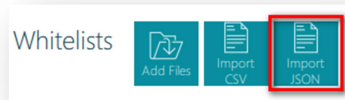
Warnings/errors: 0

4. Give the whitelist a name, this is mandatory and must differ from other whitelist names, pressing the enter/return key will complete the naming of the whitelist

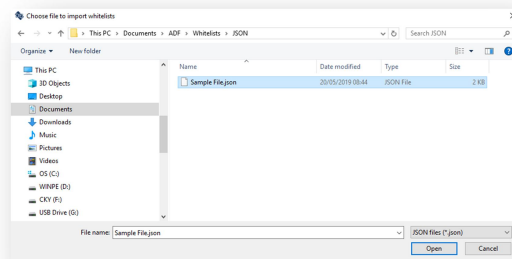


Add Files from JSON

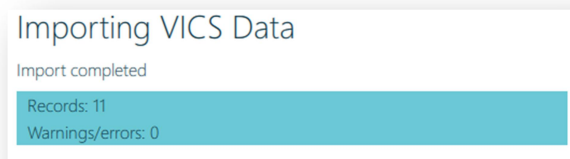
1. Click on the Add Files button in the Whitelists section



2. Select the project VIC formatted JSON file to add as a whitelist



3. A message will be displayed showing the status of the whitelist creation. Any errors that occurred during the whitelist creation are displayed, such as duplicate hash values. Click the OK button to continue



4. Give the whitelist a name, this is mandatory and must differ from other whitelist names, pressing the enter/return key will complete the naming of the whitelist

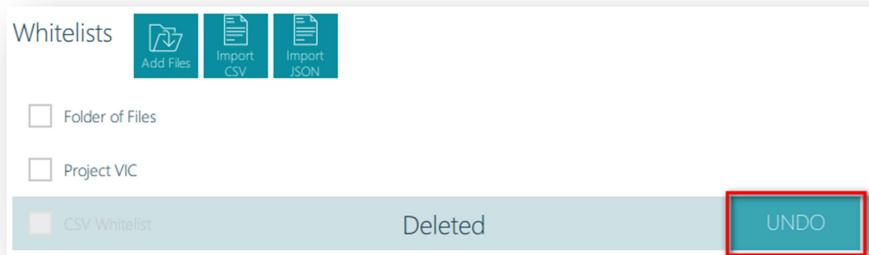


Deleting Whitelists

1. Highlight the whitelist to delete, a delete button will appear, clicking on this will start the deletion process

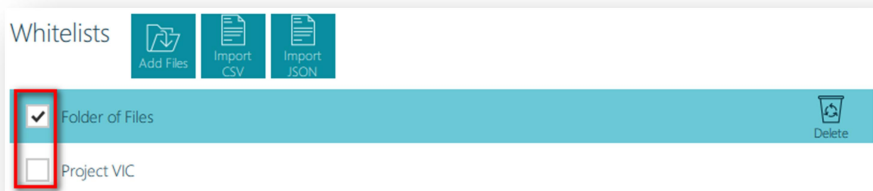


2. The whitelist will not be deleted instantly, a short time delay allows the option to undo the deletion by clicking on the UNDO button that appears



Selecting Whitelists

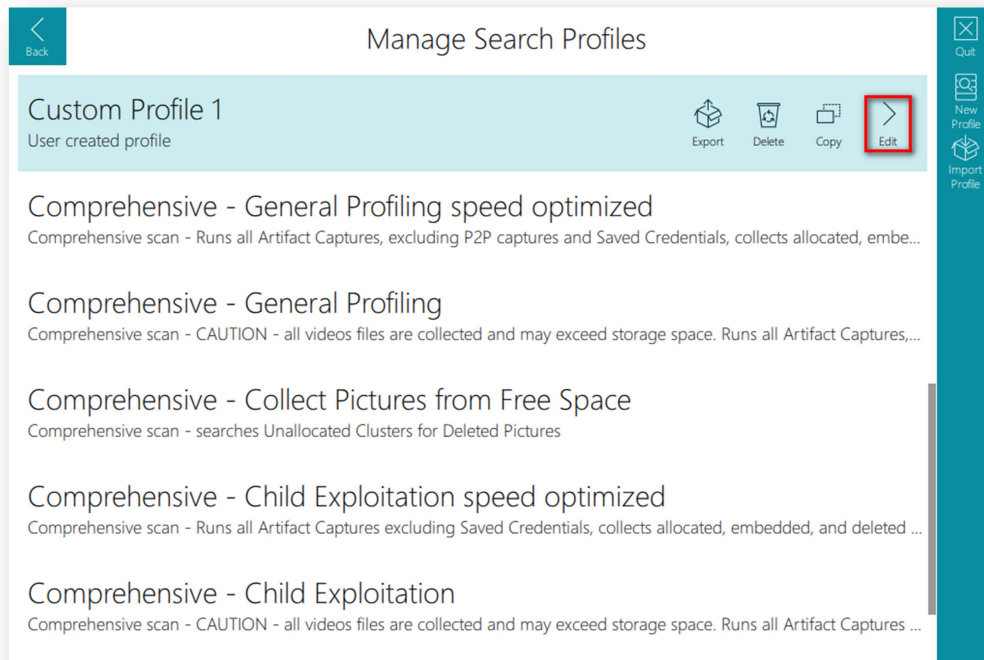
1. To add a whitelist to a search profile, click on the check box next to the whitelists required



Editing a Search Profile

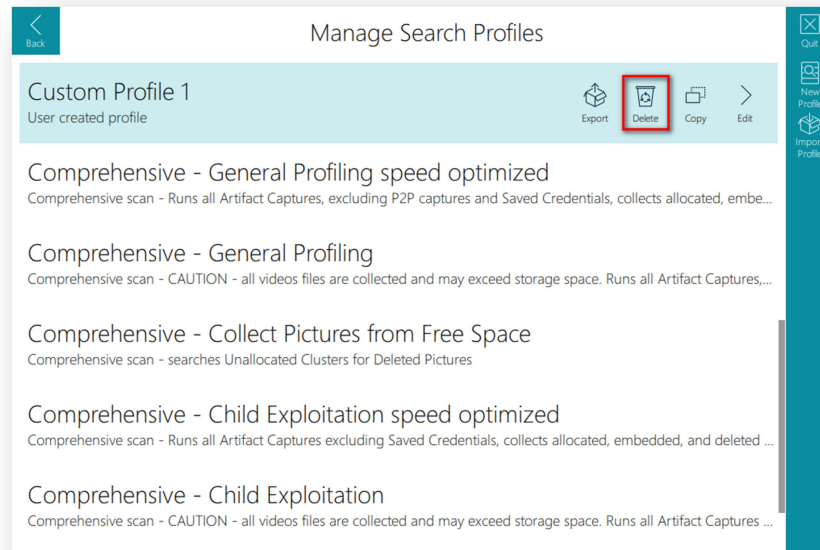
It is possible to edit any user created Search Profile, it is not possible to edit any default Search Profiles, however, default Search Profiles can be copied and the copies edited.

1. To edit a Search Profile, click on Setup Scans on the Home screen and then highlight the Search Profile to edit, this will reveal an edit button that when clicked allows the editing of the Search Profile

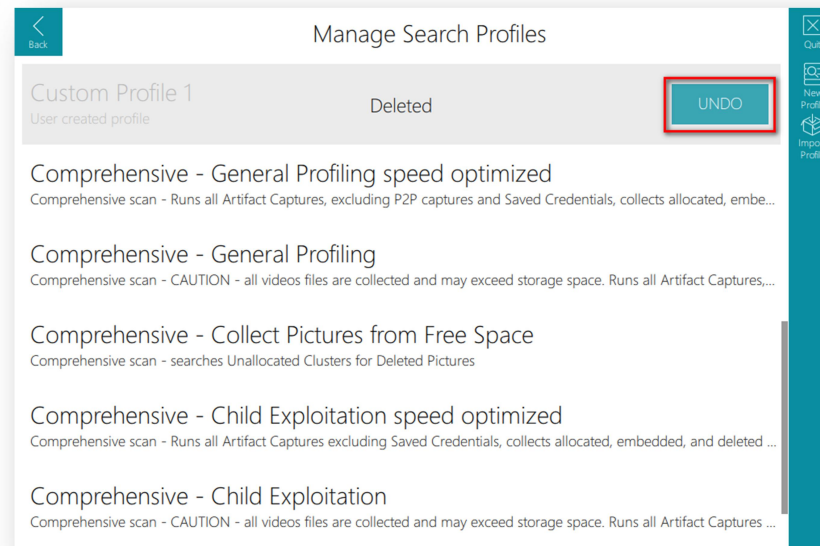


Deleting a Search Profile

1. To delete a Search Profile, click on Setup Scans on the Home screen and then highlight the Search Profile to delete, this will reveal a Delete button that when clicked deletes that Search Profile



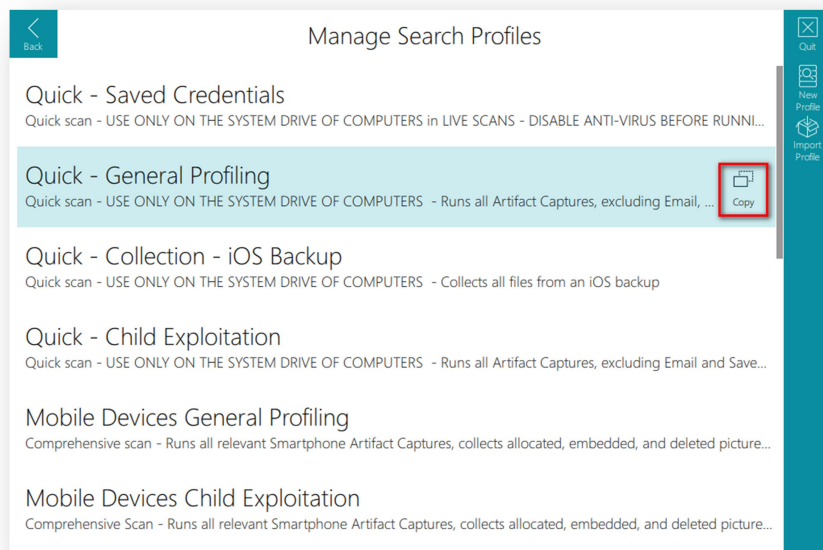
2. When a Search Profile is deleted there will an opportunity to undo the deletion for a small period of time. To undo the deletion, click on the Undo button



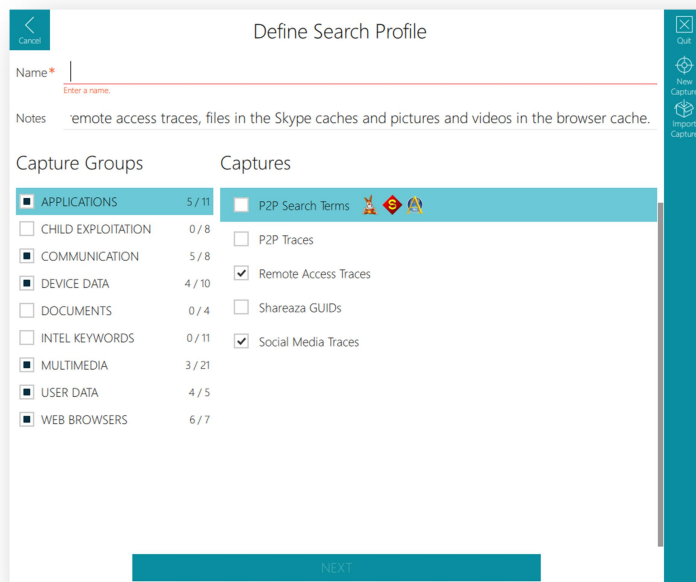
Copying a Search Profile

Copies of the default Search Profiles may be modified to suit operational requirements.

1. To copy a Search Profile, click on Setup Scans on the Home screen and then highlight the Search Profile to copy, this will reveal a Copy button that when clicked creates a copy of that Search Profile



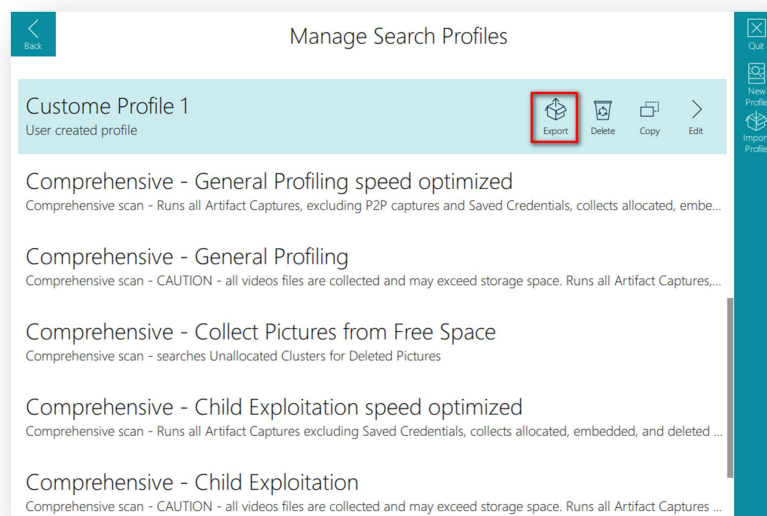
2. Copying a profile will present the Define Search Profile screen. From here captures may be added/deleted or modified



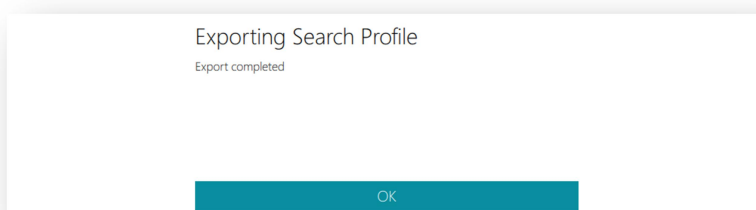
Exporting a Search Profile

It is possible to create a Search Profile on one computer and export it so that it is available to be used in another computer. This allows the creation of a Search Profile and share it with other team members or create a profile in the office to provide to staff who are conducting onsite examinations. An exported Search Profile can only be imported within the same version of Digital Evidence Investigator and Triage Investigator.

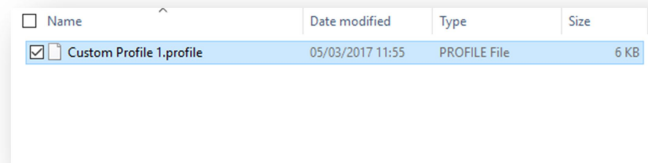
1. To export a Search Profile, click on Setup Scans on the Home screen and then highlight the Search Profile to export and click the Export button that is revealed.



2. When the Export button is clicked, a folder browser dialog window will appear to select the location the exported profile will be saved. After a folder has been selected a message will be displayed when the exporting process is complete.



3. Exported Search Profiles will be named after the Search Profile and contain a .profile file extension.

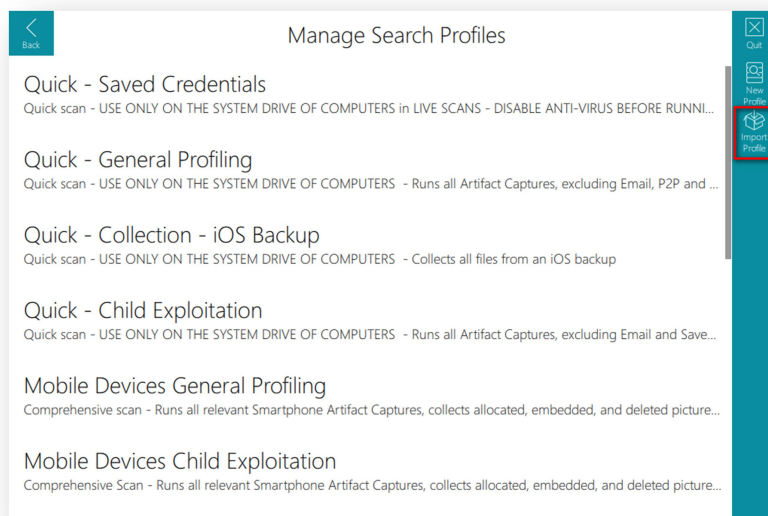


A screenshot of a file explorer window. The window displays a table with columns: Name, Date modified, Type, and Size. A single file is listed: 'Custom Profile 1.profile', which is a 'PROFILE File' and is 6 KB in size. The file is selected, indicated by a blue highlight and a checkmark in the selection column.

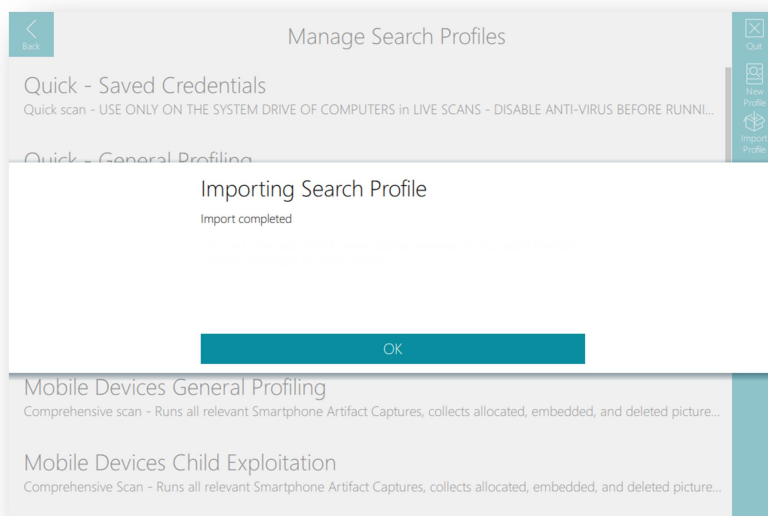
<input type="checkbox"/>	Name	Date modified	Type	Size
<input checked="" type="checkbox"/>	Custom Profile 1.profile	05/03/2017 11:55	PROFILE File	6 KB

Importing a Search Profile

1. To import a Search Profile, click on Setup Scans on the Home screen and then click on the Import Profile button.



2. Clicking on the import button will open a file browser dialog window; from here the profile to import can be selected. After the profile has been imported a message will be displayed to show the process has completed.



14. Managing and Creating File Captures

File Captures can locate and collect files based on their File Properties, included Keyword(s) or their Hash Value.

Captures are grouped within nine default Capture Groups:

Applications, Communication, Device Data, Documents, Intel Keywords, IPOC, Multimedia, User Data and Web Browsers.

Hiding Default File Captures

To hide a Default Search Profile a file entitled config.json file must be edited, this is located by default at “\Users\\AppData\Local\ADF Solutions Inc\ADF Triage-G2\config.json”.

1. Whilst the ADF DEI program is not running open the JSON file in an editor of your choice (notepad will suffice)

```
{
  "Display Default Captures": [
    {
      "name": "OS Information",
      "show": true
    },
    {
      "name": "User Accounts",
      "show": true
    },
    {
      "name": "USB History",
      "show": true
    },
    {
      "name": "Calls",
      "show": true
    },
    {
      "name": "Saved Contacts",
      "show": true
    },
  ],
}
```

2. Scroll to the “Display Default Captures” section and change the “show” value to “false” for the Capture to hide



```
{
  "Display Default Captures": [
    {
      "name": "OS Information",
      "show": true
    },
    {
      "name": "User Accounts",
      "show": true
    },
    {
      "name": "USB History",
      "show": true
    },
    {
      "name": "Calls",
      "show": false
    },
    {
      "name": "Saved Contacts",
      "show": true
    },
    {

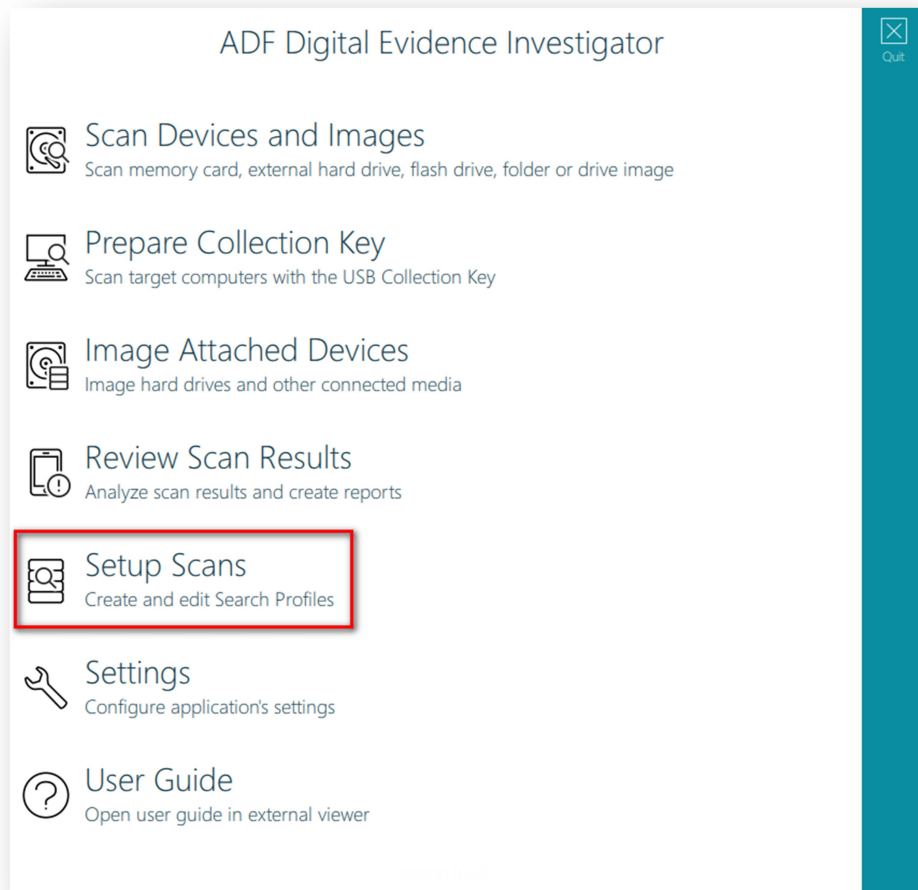
```

3. Save the edited file

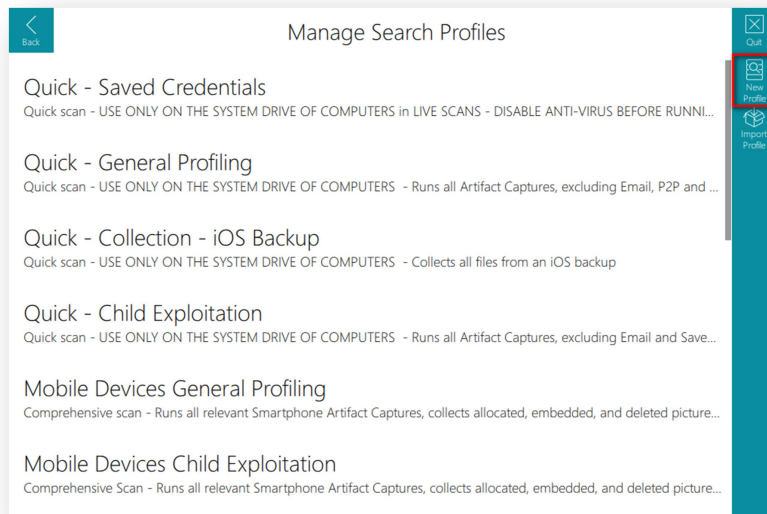
4. To display hidden Default Search Profiles change the “show” value from “false” to “true”

Creating a New File Capture

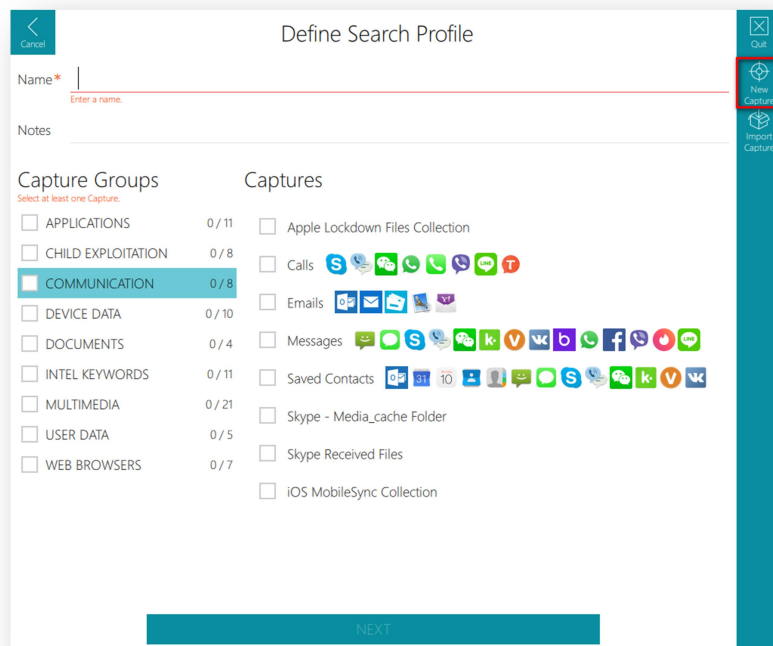
1. Select Setup Scans from the Home screen.



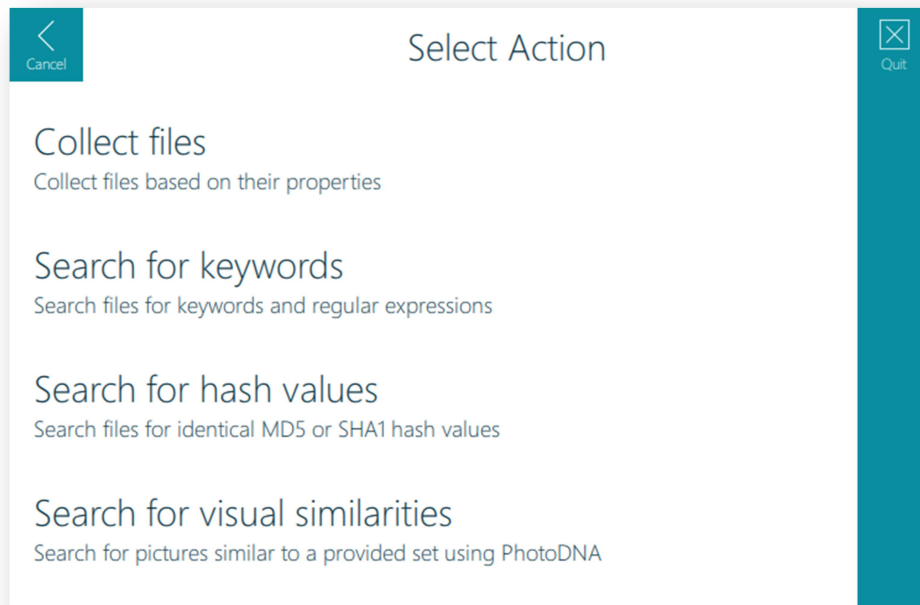
2. Click on the New Profile button in the Function Toolbar.



3. Click on the New Capture button from the Function Toolbar.



4. Choose one of the four options below:



Option	Note
Collect files	Search for and collect files based on their file type, properties and location.
Search for keywords	Search for files by keyword(s) using substrings or regular expressions.
Search for hash values	Search for files using MD5 or SHA1 hash values.
Search for visual similarities	Searches for visually similar pictures to ones provided by the user and groups visually similar pictures together.

Collect Files

1. Type an existing Capture Group name or a new Capture Group name appropriate to the Capture.

The screenshot shows the 'Define Files to Collect' dialog box. The 'Capture Group Name' field is highlighted with a red box and contains the text 'APPLICATIONS'. The 'Capture Name' field is empty. The dialog is divided into three main sections: File Types, Options, and File Sources. The File Types section has a list of file types with checkboxes, including 'All Files', 'Specific Files', 'Archive', 'Audio File', 'Binary File', 'Database File', 'Disk Image', 'Document', 'Email File', 'Internet File', 'Mac OS Artifact', 'Misc Artifact', 'P2P File', 'Picture', 'Picture DB File', 'Text File', 'Video', and 'Windows Registry'. The Options section has checkboxes for 'Only detect files (no collection)', 'File identification method' (Fast, Thorough for files without extensions, Thorough for all files), and 'Search selected file types in' (Archive, Document, Picture DB File). The File Sources section has checkboxes for 'Entire file system', 'Targeted folders', 'Files referenced by artifact records', 'Deleted files', and 'Carve pictures from Unallocated space'. The File Properties section has fields for 'Include files when size is within boundaries' (B, FILE SIZE, 100, MB), 'Include pictures with width and height greater than' (pixels), 'Include files when created timestamp is within boundaries' (YYYY / MM / DD, FILE CREATED (UTC), YYYY / MM / DD), and 'Include files when modified timestamp is within boundaries' (YYYY / MM / DD, LAST WRITTEN (UTC), YYYY / MM / DD). A blue button at the bottom says 'ENTER ALL REQUIRED INFORMATION'.

2. Type in a Capture Name which is not already in use.

The screenshot shows the 'Define Files to Collect' dialog box. The 'Capture Name' field is highlighted with a red box and contains the text 'W7 Prefetch Files'. The 'Capture Group Name' field contains the text 'APPLICATIONS'. The dialog is divided into three main sections: File Types, Options, and File Sources. The File Types section has a list of file types with checkboxes, including 'All Files', 'Specific Files', 'Archive', 'Audio File', 'Binary File', 'Database File', 'Disk Image', 'Document', 'Email File', 'Internet File', 'Mac OS Artifact', 'Misc Artifact', 'P2P File', 'Picture', 'Picture DB File', 'Text File', 'Video', and 'Windows Registry'. The Options section has checkboxes for 'Only detect files (no collection)', 'File identification method' (Fast, Thorough for files without extensions, Thorough for all files), and 'Search selected file types in' (Archive, Document, Picture DB File). The File Sources section has checkboxes for 'Entire file system', 'Targeted folders', 'Files referenced by artifact records', 'Deleted files', and 'Carve pictures from Unallocated space'. The File Properties section has fields for 'Include files when size is within boundaries' (B, FILE SIZE, 100, MB), 'Include pictures with width and height greater than' (pixels), 'Include files when created timestamp is within boundaries' (YYYY / MM / DD, FILE CREATED (UTC), YYYY / MM / DD), and 'Include files when modified timestamp is within boundaries' (YYYY / MM / DD, LAST WRITTEN (UTC), YYYY / MM / DD). A blue button at the bottom says 'ENTER ALL REQUIRED INFORMATION'.

3. Pick a File Type: it is possible to specify which file types to include in the search. Searches for All Files or Specific Files are available. It is possible to add multiple specific file types. If the file type required does not exist it is possible to create one by clicking on View on any File Type group and then following the instructions within the Adding a Custom File Type section.

Define Files to Collect

Capture Group Name * APPLICATIONS Capture Name * W7 Prefetch Files

File types

- ☐ All Files
- ☒ Specific Files
- ☐ Archive
- ☐ Audio File
- ☒ Binary File [View](#)
- ☐ Database File
- ☐ Disk Image
- ☐ Document
- ☐ Email File
- ☐ Internet File
- ☐ Mac Os Artifact
- ☐ Misc Artifact
- ☐ P2P File
- ☐ Picture
- ☐ Picture DB File
- ☐ Text File
- ☐ Video
- ☐ Windows Registry

Options

☐ Only detect files (no collection)

File identification method

- ☒ Fast identification
- ☐ Thorough identification for files without extensions
- ☐ Thorough identification for all files

☐ Search selected file types in

- ☐ Archive
- ☐ Document
- ☐ Picture DB File

File Sources

Select a source:

- ☐ Entire file system
- ☐ Targeted folders
- ☐ Files referenced by artifact records
- ☐ Deleted files
- ☐ Carve pictures from Unallocated space

File Properties

Include files when size is within boundaries

4 B > < FILE SIZE < 100 < MB >

Include pictures with width and height greater than _____ pixels

Include files when created timestamp is within boundaries

YYYY / MM / DD < FILE CREATED (UTC) < YYYY / MM / DD

Include files when modified timestamp is within boundaries

YYYY / MM / DD < LAST WRITTEN (UTC) < YYYY / MM / DD

ENTER ALL REQUIRED INFORMATION

4. Select the Capture Options:
- Only detect files (no collection)** The original files will not be collected but preview thumbnails of images are created.
- File identification method –**
- Fast identification** identifies file types using the file extension only
- Thorough identification for files without extensions** uses file signature analysis to identify files that have no file extension and fast identification on those that do
- Thorough identification for all files** uses file signature analysis to identify all files. This will increase the time the scan takes to run
- Search selected file types in -**
- Archives** Searches for all selected file types within archives
- Documents** Searches for all selected file types embedded within Document file types
- Picture DB files** Searches for all selected Picture file types within Windows thumbcache and thumbs.db files and Apple itmb files

Options

☐ Only detect files (no collection)

File identification method

☒ Fast identification

☐ Thorough identification for files without extensions

☐ Thorough identification for all files

☐ Search selected file types in

☐ Archive

☐ Document

☐ Picture DB File

5. Select the File Properties for the File Collection:
- File Size** The left hand size specifies the minimum file size whilst the right hand size specifies the maximum file size. It is possible to specify Bytes, Kilobytes, Megabytes and Gigabytes by clicking on the arrows next to the size unit
 - Pixel size** Limit the pictures collected by setting the minimum pixel width and height
 - Created Date** Specifies a UTC created date range for the selected file types
 - Modified Date** Specifies a UTC modified date range for the selected file types

The screenshot shows the 'File Properties' dialog box. It has four sections for filtering files:

- Include files when size is within boundaries:** A range from 100 MB to 100 MB.
- Include pictures with width and height greater than:** A range from 100 pixels to 100 pixels.
- Include files when created timestamp is within boundaries:** A range from YYYY / MM / DD to YYYY / MM / DD.
- Include files when modified timestamp is within boundaries:** A range from YYYY / MM / DD to YYYY / MM / DD.

6. Select the File Source options:
- Entire file system** Searches all live files
 - Targeted folders** May be used to limit the extent of the scan making it run quicker. These can be used to limit the search to areas where evidential material is likely to exist. In addition, Targeted folders are searched before other folders and are not searched again if both Targeted folders and Entire file system are selected. See the Targeted Folder section for more details
 - Files referenced by artifact records** Used to target files referenced by Artifact Captures (e.g. email attachments)
 - Carve pictures from Unallocated space** This searches unallocated space and collects any picture files where the file header starts at a sector boundary. When the original size of the picture cannot be determined the following occurs:
 - JPG files: the end of file is searched for in the following 30 MB after the header, if the end of the file cannot be detected the first 5MB is collected
 - PNG and GIF files: the end of file is searched for in the following 5 MB after the header, if the end of file cannot be located no file is carvedBMP files are fully identified as the file size is in the header

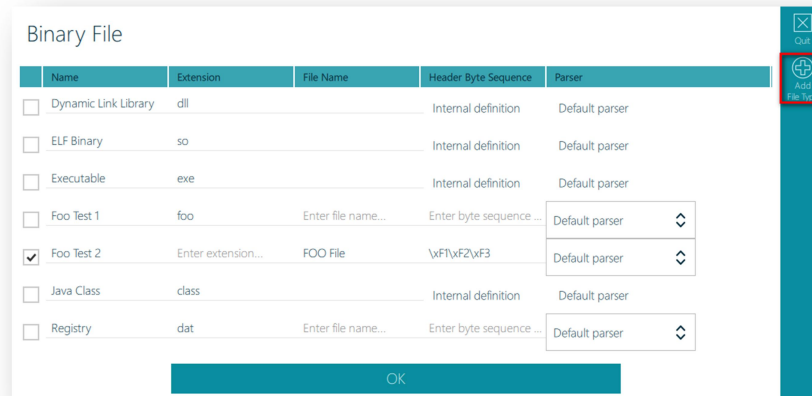
The screenshot shows the 'File Sources' dialog box. It has a title 'File Sources' and a subtitle 'Select a source.' Below the subtitle are five checkboxes:

- ☐ Entire file system
- ☐ Targeted folders
- ☐ Files referenced by artifact records
- ☐ Deleted files
- ☐ Carve pictures from Unallocated space

7. When the required options are selected click the Save button.

Adding a Custom File Type

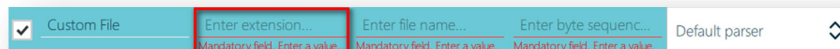
1. Within the File Types section click on View on any File Type group and then click the Add File Type button to add a new file type.



Name	Extension	File Name	Header Byte Sequence	Parser
<input type="checkbox"/> Dynamic Link Library	dll		Internal definition	Default parser
<input type="checkbox"/> ELF Binary	so		Internal definition	Default parser
<input type="checkbox"/> Executable	exe		Internal definition	Default parser
<input type="checkbox"/> Foo Test 1	foo	Enter file name...	Enter byte sequence...	Default parser
<input checked="" type="checkbox"/> Foo Test 2	Enter extension...	FOO File	\xF1xF2xF3	Default parser
<input type="checkbox"/> Java Class	class		Internal definition	Default parser
<input type="checkbox"/> Registry	dat	Enter file name...	Enter byte sequence...	Default parser

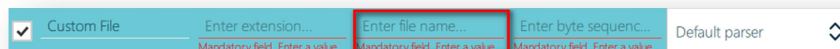
2. There are three options available to identify a file: Extension, File Name and Header Byte Sequence. It is a requirement to enter at least one of these options and when searching for a custom file by file name a header byte sequence has to be added.

3. Add the file extension by clicking on the Enter extension text box and adding the extension, it is not required to add a dot prior to the extension



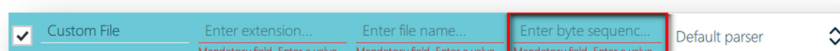
<input checked="" type="checkbox"/> Custom File	Enter extension... Mandatory field. Enter a value.	Enter file name... Mandatory field. Enter a value.	Enter byte sequence... Mandatory field. Enter a value.	Default parser
---	---	---	---	----------------

4. Add the file name by clicking on the Enter file name text box and adding the file name. A header byte sequence also needs to be entered when searching for files using this criteria. This allows the addition of custom files that have no file extension, differing names but the same header byte sequence such as Windows registry files.



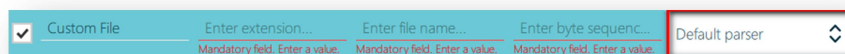
<input checked="" type="checkbox"/> Custom File	Enter extension... Mandatory field. Enter a value.	Enter file name... Mandatory field. Enter a value.	Enter byte sequence... Mandatory field. Enter a value.	Default parser
---	---	---	---	----------------

5. Add the header byte sequence by clicking on the Enter byte sequence text box and entering it as a regular expression e.g.- \x17\x00\x00\x00\x53\x43\x41).



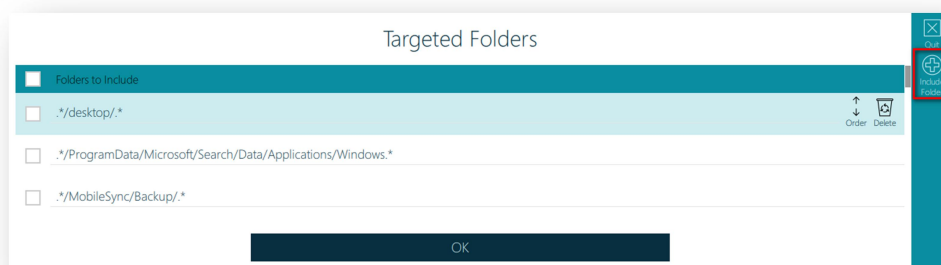
<input checked="" type="checkbox"/> Custom File	Enter extension... Mandatory field. Enter a value.	Enter file name... Mandatory field. Enter a value.	Enter byte sequence... Mandatory field. Enter a value.	Default parser
---	---	---	---	----------------

6. Add Parser type (document, image, text or video). If unknown - select Default Parser.



Adding Targeted Folders

1. Within the File Sources section highlight Targeted folders and click on View >. From here click the Include Folder button on the Function Toolbar.



2. Add the desired folder path represented by a regular expression. It is possible to use .* characters to substitute for parts of the path that may vary or be unknown.
Example ./desktop/*
Example ./users/*
Example /users/*\ntuser\dat

When desired paths have been added click OK.

Search for Keywords

When creating any Capture, a Capture Group and name must be provided for the Capture. See the Collect Files section for further details.

Adding Keywords

Define Keyword Capture

Cancel

Capture Group Name* Enter a name.

Capture Name* Enter a name.

Search Expressions
Enter search expressions.

Search Expression	Auto-Tag	Auto-Comment
Enter value...	No tag	Enter comment...

Search Scope
Select a scope.

☒ File and folder names

☐ Files content and metadata

☐ Artifact records from other Captures

Options

Search type: ☒ Substring ☐ Regular Expression

☒ Collect matching files

SAVE

Out

Import

Clear Table

There are two ways to add keywords. They can be typed in individually or imported from a CSV file or text file, both of which can contain multiple keywords. See the section Importing a list of keywords for further help with importing keyword lists.

Adding a keyword manually

1. Keywords can be typed into the Search Expression field. A tag value (0-9) can be assigned and a comment (1000 characters maximum) for hits resulting from this keyword.

Adding a keyword will automatically add a new line for further keywords.

Define Keyword Capture

Cancel

Capture Group Name* Enter a name.

Capture Name* Enter a name.

Search Expressions

Search Expression	Auto-Tag	Auto-Comment
New Keyword	1	Comment for new keyword
Enter value...	No tag	Enter comment...

Delete

Search Scope
Select a scope.

☐ File and folder names

☐ Files content and metadata

☐ Artifact records from other Captures

Options

Search type: ☒ Substring ☐ Regular Expression

☒ Collect matching files

SAVE

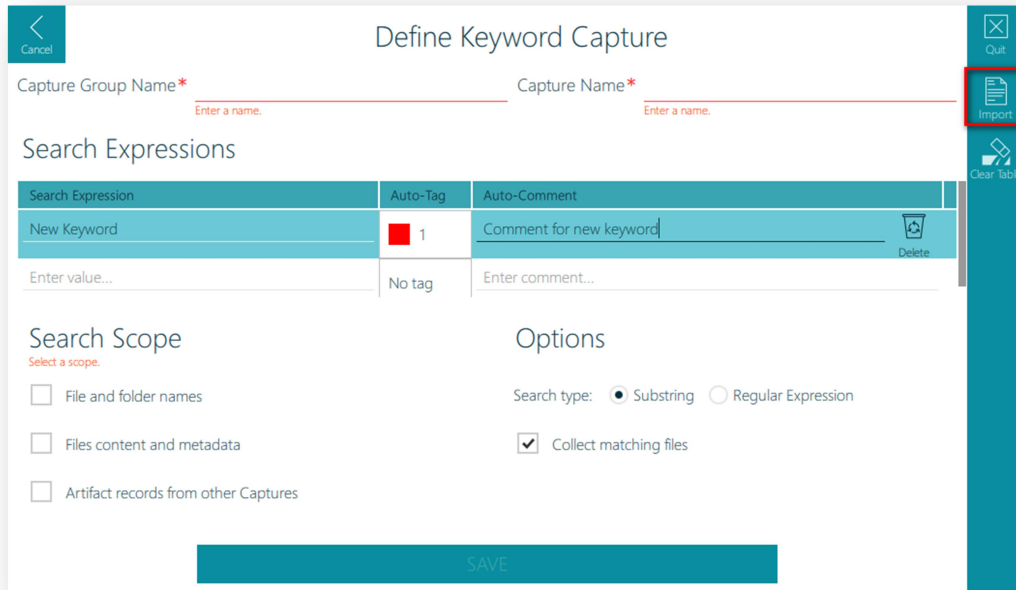
Quit

Import

Clear table

Importing a list of keywords

1. It is possible to import a CSV file containing keywords and optional information about those keywords and it is also possible to import a list of keywords from a text file. Within the Define Keyword Capture screen press the Import button. This will open a file browser dialog.

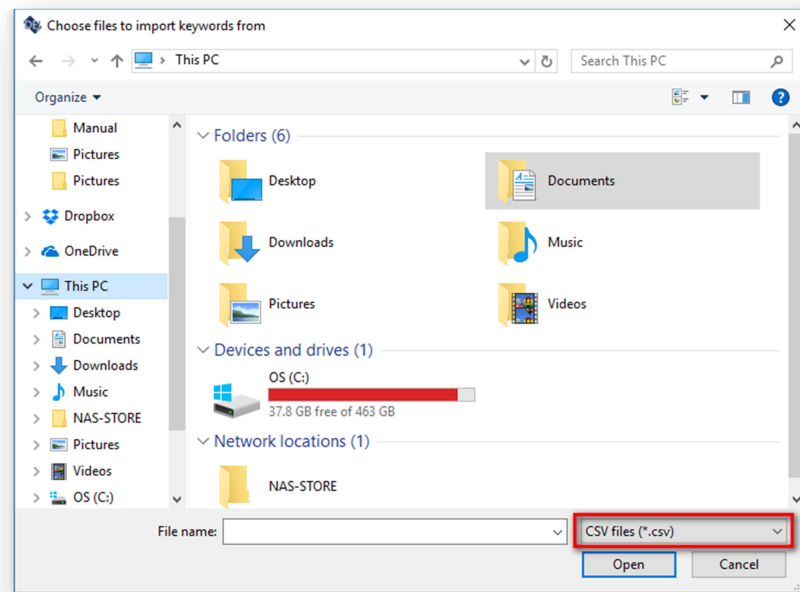


The 'Define Keyword Capture' screen features a teal header with a back arrow and 'Cancel' button on the left, and 'Quit', 'Import', and 'Clear table' buttons on the right. The 'Import' button is highlighted with a red box. The main area contains two input fields: 'Capture Group Name*' and 'Capture Name*', both with red error text 'Enter a name.'. Below these is the 'Search Expressions' section with a table:

Search Expression	Auto-Tag	Auto-Comment
New Keyword	1	Comment for new keyword
Enter value...	No tag	Enter comment...

The table has a 'Delete' icon in the 'Auto-Comment' column. Below the table is the 'Search Scope' section with three checkboxes: 'File and folder names', 'Files content and metadata', and 'Artifact records from other Captures'. To the right is the 'Options' section with 'Search type' (radio buttons for 'Substring' and 'Regular Expression') and a checked checkbox for 'Collect matching files'. A large teal 'SAVE' button is at the bottom.

2. Within the file browser dialog select the keyword CSV file and click Open.



3. The CSV file must be in the following format:

The following column is required:

keyword: the keyword to add

The following columns are optional:

auto-tag: the tag to automatically assign to keyword hits (numbers 1-9 to only)

auto-comment: the comment to assign to keyword hits (1000 characters maximum)

	A	B	C
1	keyword	auto-tag	auto-comment
2	test	1	keyword comment

4. The text file must be in the following format:

The text **keyword** must be on the first row of the text file, one keyword per row thereafter.

```
keyword
kw1
kw2
kw3
kw4
kw5|
```

5. Once imported the table is populated with the keywords, and a dialog box is displayed showing the number of keywords imported, and if there were any errors, such as duplication or improper formatting.

The screenshot shows a dialog box titled "Define Keyword Capture". At the top, there are two input fields: "Capture Group Name*" and "Capture Name*", both with a red asterisk and a placeholder "Enter a name.". To the right of the "Capture Name*" field is an "Import" button with a document icon. Below the input fields, the text "Import completed." is displayed. Underneath, a blue bar shows the number "1" and "0 error(s)". At the bottom of the dialog is a large "OK" button. At the very bottom, there is a checkbox labeled "Artifact records from other Captures" and a button labeled "ENTER ALL REQUIRED INFORMATION".

Deleting and Clearing Keywords

1. To delete a single keyword, highlight the keyword to delete and click the Delete button.

The screenshot shows the 'Define Keyword Capture' dialog box. At the top, there are fields for 'Capture Group Name*' and 'Capture Name*', both with a red asterisk and a placeholder 'Enter a name.'. Below these is the 'Search Expressions' section, which contains a table with three columns: 'Search Expression', 'Auto-Tag', and 'Auto-Comment'. The first row is highlighted in blue and contains 'New Keyword', a red square with the number '1', and 'Comment for new keyword'. To the right of this row is a 'Delete' button with a trash icon. Below the table are input fields for 'Enter value...', 'No tag', and 'Enter comment...'. To the left of the 'Options' section is the 'Search Scope' section with three checkboxes: 'File and folder names', 'Files content and metadata', and 'Artifact records from other Captures'. The 'Options' section has two radio buttons for 'Search type:' (Substring and Regular Expression) and a checked checkbox for 'Collect matching files'. At the bottom is a large blue 'SAVE' button. On the right side of the dialog is a vertical toolbar with icons for 'Quit', 'Import', and 'Clear Table'.

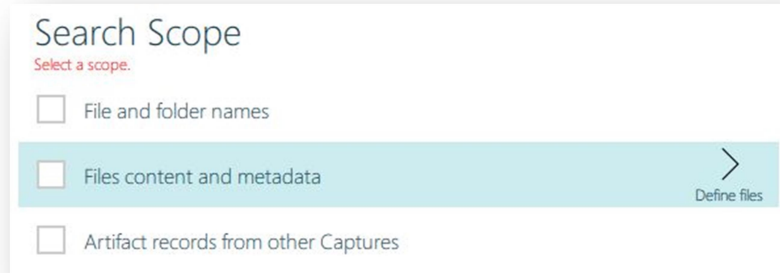
2. To delete all keywords click the Clear Table button on the function toolbar.

This screenshot is identical to the one above, showing the 'Define Keyword Capture' dialog box. However, in this version, the 'Clear Table' button on the right-hand vertical toolbar is highlighted with a red box, indicating the action to delete all keywords.

Search Scope

The Search Scope options detail where the capture searches for keywords.

Keyword Search Scope Options

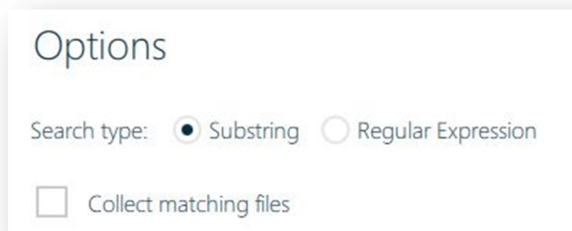


Option	Function
File and Folder Names	Keywords are searched for in file and folder names
File Content and Metadata	Keywords are searched for within the content of each file and any associated file metadata. The user must define the files to be searched by clicking on the Define Files button (see Collect Files section)
Artifact records from other Captures	Keywords are searched for in other Capture results e.g. browsing history

Options

The Keyword Options allows the selection of Substring or Regular Expression keyword search types and the option to collect matching files.

Keyword Search Options



Options

Search type: ☒ Substring ☐ Regular Expression

☐ Collect matching files

Option	Function
Substring	The keyword is searched for exactly as it is shown in the keyword list and can be part of a longer string of data i.e. Searching for the character string <i>pot</i> would find any text string containing those three (3) letters in that order for example <i>pot</i> , <i>pots</i> , <i>potting</i> , <i>potter</i> , <i>spot</i> , <i>spots</i> , <i>spotting</i> , <i>spotter</i> , <i>spotted</i> , <i>potent</i> , <i>potentate</i> , <i>teapot</i> , <i>tinpot</i> , etc.
Regular Expression	Allows for complex search terms using the Regular Expression search pattern language (See Appendix B - RegEx Cheat Sheet) to be entered into the Search Expression field.
Collect Matching Files	Selecting this will collect the file in which the keyword was found.

Search for Hash Values

Search for Hash Values Screen

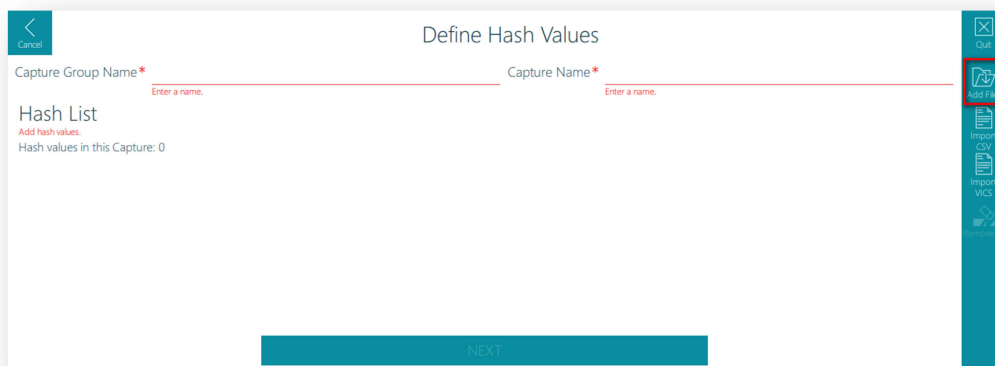
The screenshot shows the 'Define Hash Values' screen. At the top, there is a title bar with a back arrow and 'Cancel' on the left, and 'Define Hash Values' in the center. Below the title bar, there are two input fields: 'Capture Group Name*' and 'Capture Name*', both with red error text 'Enter a name.' below them. To the left of the main content area, there is a 'Hash List' section with the text 'Add hash values.' and 'Hash values in this Capture: 0'. On the right side, there is a vertical toolbar with icons for 'Quit', 'Add Files', 'Import CSV', 'Import VCS', and 'Import List'. At the bottom center, there is a large blue button labeled 'NEXT'.

There are three (3) ways to add Hash Values to a Hash Capture. It is possible to hash files located in a folder; import a CSV format or text file containing multiple hash values; or import a project VIC formatted JSON file. The CSV/text file must contain at least 1 column header entitled either md5 or sha1. The CSV file can optionally include columns for file size, category, auto-tag and auto-comment (see Import List section for further details).

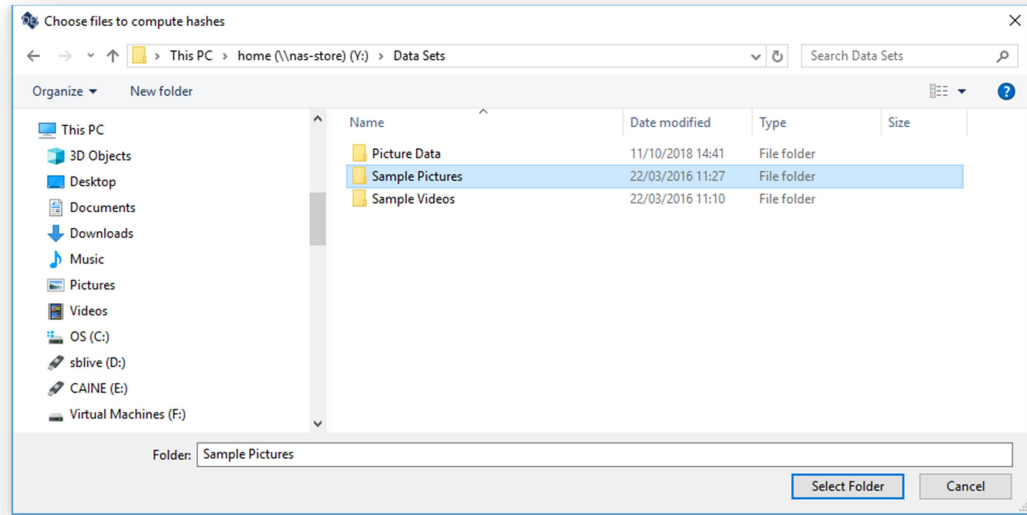
Add Files

Triage-G2 can create a hash set from all files in a folder by clicking on the Add Files button on the Function Toolbar and navigating to and selecting the folder containing the files.

1. Within the search for hash files screen click the Add Files button.



2. This will bring up a folder browser dialog, selecting a folder will hash all of the files within that folder and any sub folders.



3. After selecting a folder it is possible to automatically assign a tag and comment to all files identified during a scan that have hash values matching the files in the folder. Clicking the OK button will hash the files in the selected folder.

Define Hash Values

Assign Tags and Comments

Assign a tag automatically to this hash set?

☒ No tag ☐ 0 - Level 0 ☐ 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

Assign a comment automatically to this hash set?

OK

NEXT

4. When all files have been hashed a message will be displayed showing the result of the file hashing.

Define Hash Values

Capture Group Name* DOCUMENTS Capture Name* IP Theft Documents

Computation completed.

2/2

0 error(s)

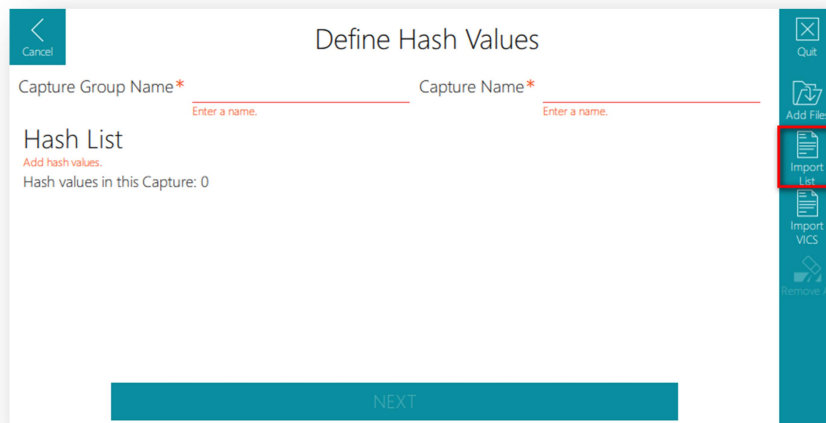
OK

NEXT

Import List

Click on the Import List button on the Function Toolbar and navigate to the csv or text file.

1. Within the search for hash files screen click the Import List button.



2. The CSV file must be in the following format:

One of the following columns are required:

md5: hash value as a 32 character hexadecimal string

sha1: hash value as a 40 character hexadecimal string (base-16 SHA-1) or a 32 character string (base-32 SHA-1)

The following columns are optional:

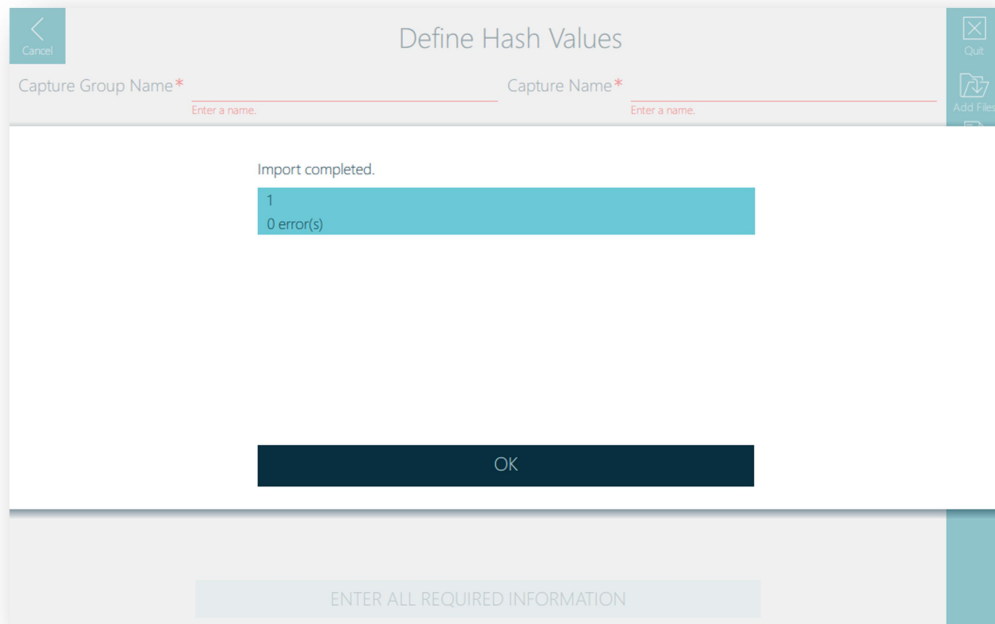
file size: the size of the file in bytes

auto-tag: the tag to automatically assign (numbers 1-9 to only)

auto-comment: the comment to assign to the file (1000 characters maximum)

	A	B	C	D
1	md5	file size	auto-tag	auto-comment
2	146826FB97638B6B3ADFA628CAD89C19	1438	1	Text file containing IP

3. When a CSV file is selected, a message will be displayed if the import has been successful. A warning message will be displayed if the CSV file is incorrectly formatted.



Import VICs

It is possible to import Project Vic formatted JSON files containing hash values. Project VIC JSON files containing category information will auto-tag matching files during a scan with that category number.

1. Within the search for hash files screen press the Import VICs button. This will open a file browser dialog window for selection of the JSON file.

Define Hash Values

Capture Group Name* Enter a name. Capture Name* Enter a name.

Hash List

Add hash values.

Hash values in this Capture: 0

NEXT

2. A message will be displayed showing the outcome of the import. If the JSON format is unsupported a warning will appear here.

Define Hash Values

Capture Group Name* Enter a name. Capture Name* Enter a name.

Import completed.

11

0 error(s)

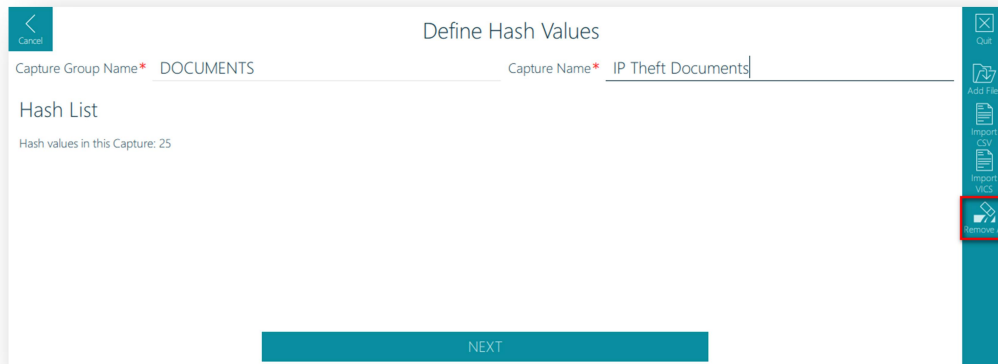
OK

ENTER ALL REQUIRED INFORMATION

Remove Hash Values

It is possible to remove all of the hash values stored within a hash value file capture.

1. Within the search for hash files screen click the Remove All button.



Search for Visual Similarities

The search for visual similarities Capture allows the identification of visually similar images to ones already possessed. When reviewing the output of this Capture pictures will be sorted based on how similar they are to the set of pictures possessed, this also has the effect of roughly grouping together pictures that are themselves similar even if they do not match any of the pictures in the Capture

Search for Visual Similarities Screen

The screenshot shows a dialog box titled "Define PhotoDNA set". It has a teal header bar with a "Cancel" button on the left and a "Quit" button on the right. The main area is divided into three sections: "PhotoDNA Set", "File Types", and "File Sources".

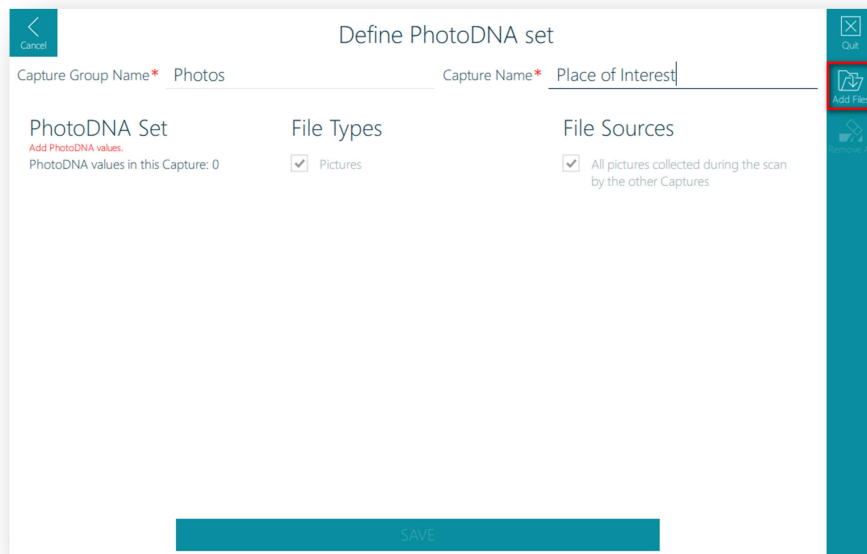
- PhotoDNA Set:** Contains the text "Add PhotoDNA values." and "PhotoDNA values in this Capture: 0".
- File Types:** Contains a checkbox labeled "Pictures" which is checked.
- File Sources:** Contains a checkbox labeled "All pictures collected during the scan by the other Captures" which is checked.

At the bottom of the dialog is a large teal "SAVE" button. On the right side of the dialog, there is a vertical teal bar with three icons: "Quit", "Add Files", and "Remove All".

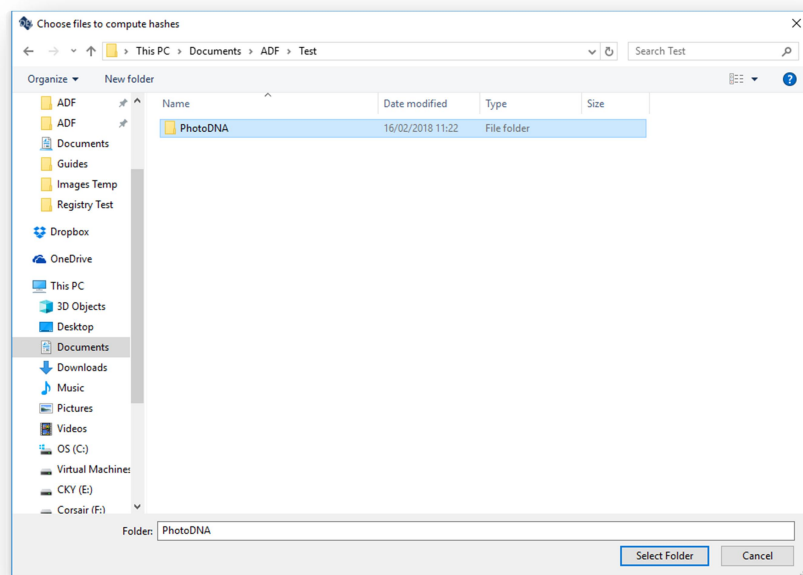
Add Files

The Capture requires that at least one picture be added. There is no limit on how many pictures can be added but it will significantly slow down the scan if a large number of pictures are added.

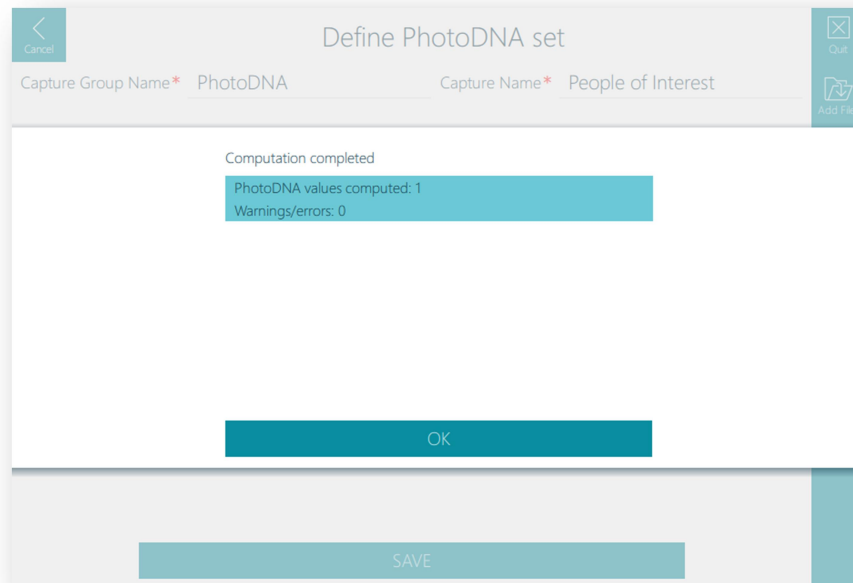
1. After providing a Capture Group Name and a Capture Name press the Add Files button.



2. This will bring up a folder browser dialog, selecting a folder will add any picture files contained within it to the Capture, non-picture files are ignored.

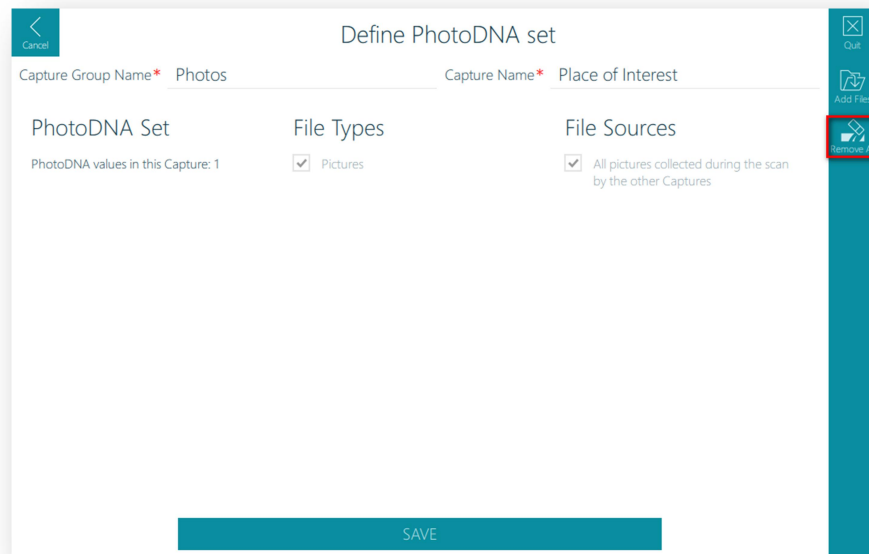


3. After selecting a folder a results screen will show how many pictures have been added and if there are any errors or warnings (such as a file not being a picture).



Remove All Files

1. To remove pictures from the Capture press the Remove All button.



Reviewing Visual Similarity Results

1. The following picture was added to a Search for Visual Similarities Capture.



2. The folder that was scanned contained an exact copy of this picture, slightly edited versions of the picture, pictures of the same building from slightly different angles and pictures of the same building downloaded from the Internet.



3. When reviewing the results of this capture the pictures displayed are sorted by PhotoDNA score. Pictures that have the highest PhotoDNA score are presented first.

In this example the Capture identified the exact picture as the first result followed by the edited picture and those from slightly different angles. Pictures containing similar buildings scored highly followed by pictures which scored lower on visual similarity.

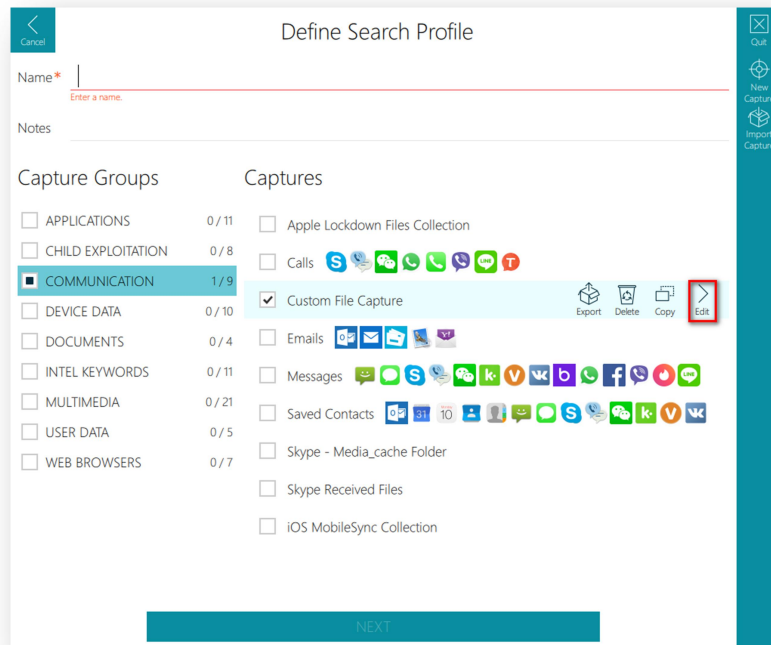
The screenshot displays the ADF Triage-G2 interface. At the top, a navigation bar includes a 'Close' button, a 'Place of Interest' title, and a 'Records: 21' indicator. Below the title is a grid of 21 image thumbnails. The left sidebar contains navigation icons for Summary, Pictures, Videos, Keywords, Timeline, Files, Scan log, Report, and More. The right sidebar contains icons for Out, Search, Tables, Columns, Deselect All, Filter, Tags, Comments, and Classifier. The bottom section is divided into three tabs: Properties, Metadata, and Preview. The Properties tab is active, showing details for the selected image.

Properties	Metadata	Preview
Preview		File Name
File Type	JPEG/JIFF Image	Type Group
File System Type	File	Origin
Size	3764863	Last Written
File Created	2018/08/30 15:26:36	Last Accessed
Path	Src11	Extension
Protected	Not protected	Picture Width
Picture Height	2268	
Integrity MDS	99EC1DDA43AFFFC7359679A25A8AE55C	

Editing a File Capture

It is possible to edit any user created File Capture, it is not possible to edit any default File Captures, however, default File Captures can be copied and the copies edited.

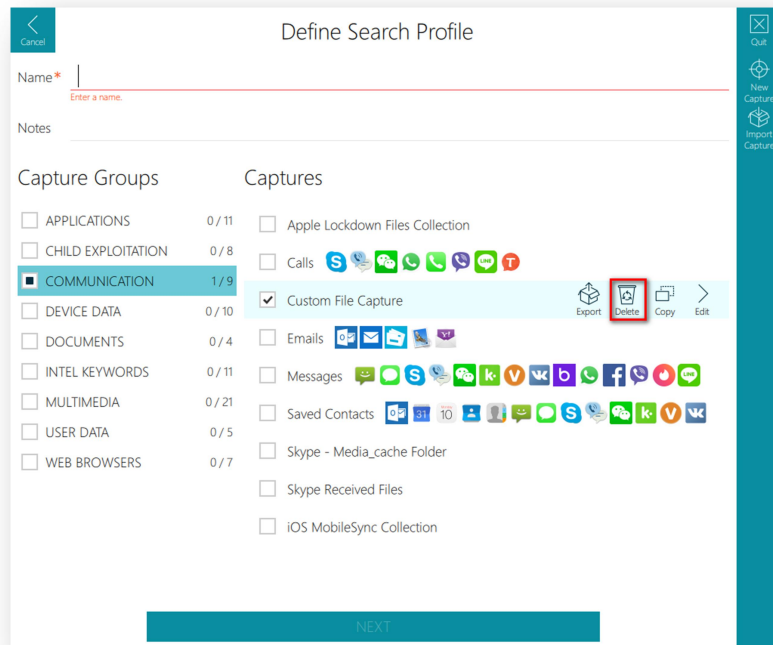
1. To edit a File Capture, click on Setup Scans on the Home screen and then edit any user created Search Profile. Highlighting the File Capture to be edited will reveal an Edit button that when clicked allows editing of the File Capture.



Deleting a File Capture

It is possible to delete any user created File Capture, it is not possible to delete any default File Captures.

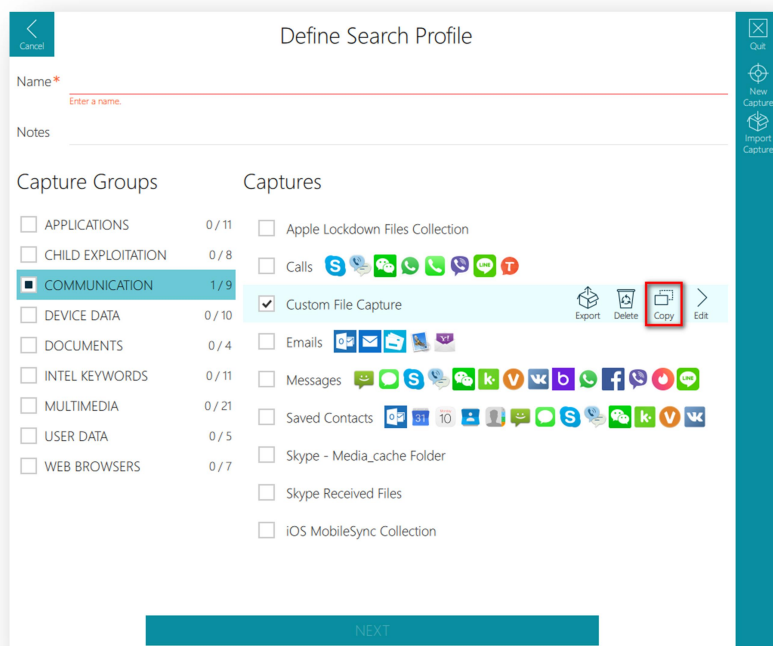
1. To delete a File Capture, click on Setup Scans on the Home screen and then edit any user created Search Profile. Highlighting the File Capture to delete will reveal a Delete button that when clicked deletes the File Capture.



Copying a File Capture

It is possible to copy any user created File Capture and any default File Captures.

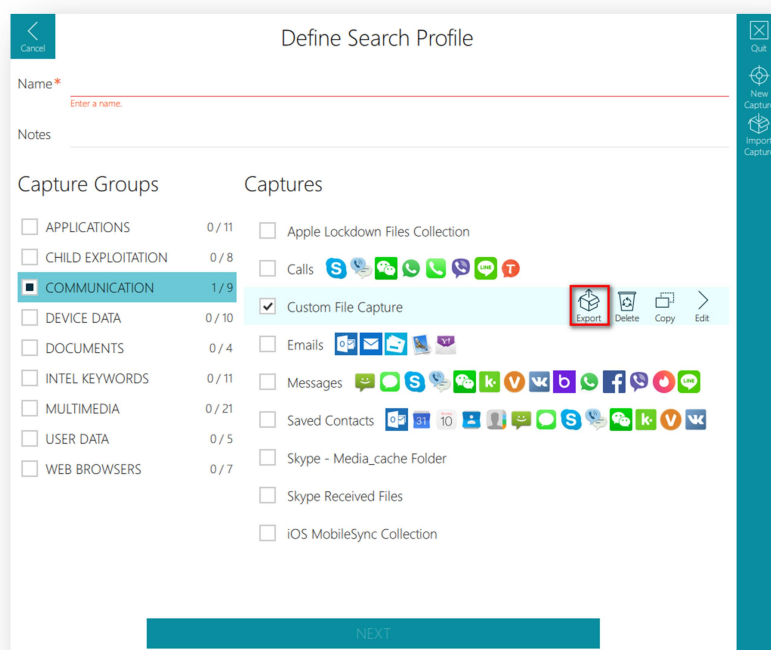
1. To copy a File Capture, click on Setup Scans on the Home screen and then edit any user created Search Profile or create a new Search Profile. Highlighting the File Capture to copy will reveal a Copy button that when clicked creates a copy of the File Capture. The appropriate File Capture definition view will appear with all of the File Captures current settings selected, a new name has to be provided for this File Capture.



Exporting a File Capture

It is possible to export any user created File Capture, it is not possible to export default file captures. Exporting a File Capture creates a file with a CAPTURE file extension. This can then be imported into another instance of Triage-G2, this must be the same version as the instance used to export the File Capture.

1. To export a File Capture, highlight the user created capture to export then click on the Export button. This will open a folder browser dialog window to select the location where the exported capture will be saved.



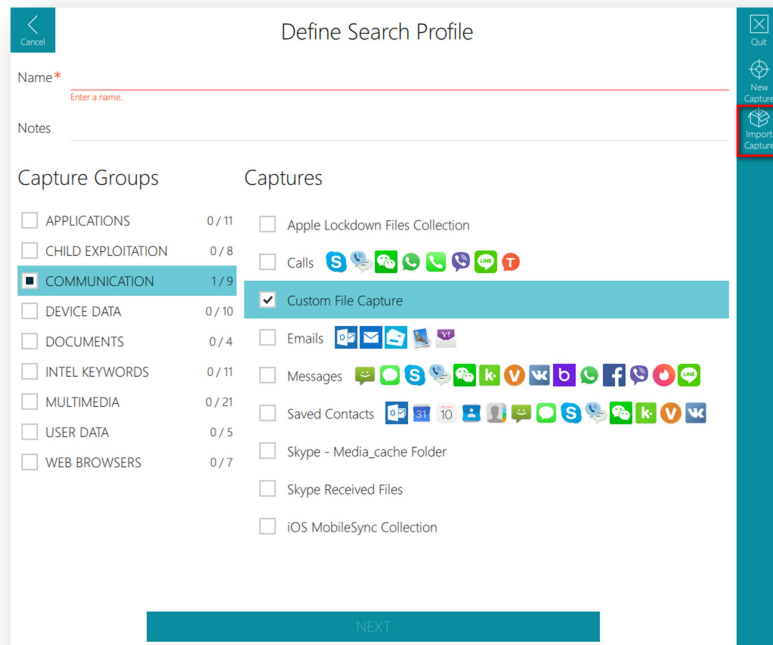
2. After selecting a folder for the capture to be saved to a message will be displayed showing the outcome of the File Capture export.



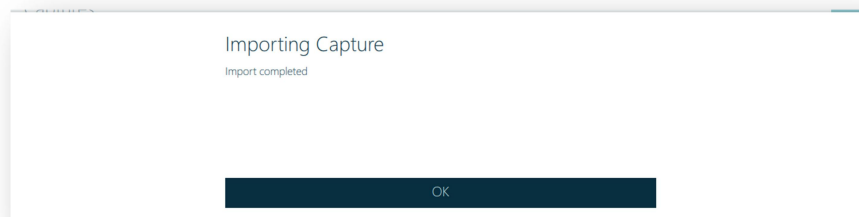
Importing a File Capture

Exported File Captures can be shared and imported into Search Profiles in other instances of Triage-G2, provided the same version of Triage-G2 is used.

1. To import a File Capture, click on the Import Capture button within the function toolbar of the Define Search Profile screen. This will open a file browser dialog window to select the File Capture to import.



2. After selecting the File Capture to import a message will be displayed showing the outcome of the File Capture import.



Saved Credentials Capture

The Saved Credentials Capture recovers usernames and passwords saved by the Firefox, Google Chrome, Opera and Internet Explorer web browsers. This capture only runs during a live scan (see section 9) on a target computer that has had any anti-virus or Operating System file protection (such as Windows Defender) settings disabled. It is also possible to run a live scan within a virtualised representation of a target computer.

This Capture is located in the Web Browsers file captures group.

Saved Credentials Capture

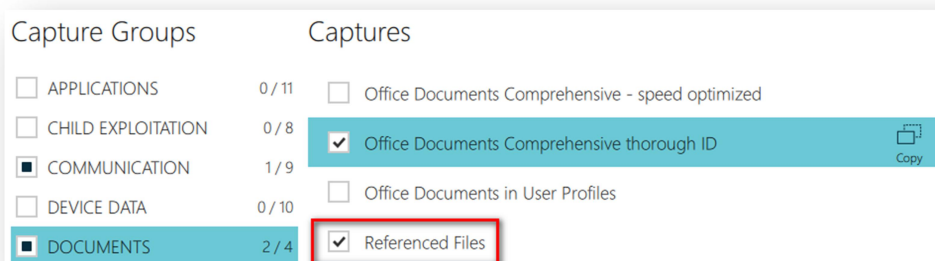


Referenced Files Capture

The Referenced Files Capture targets files referenced by the P2P, Email, Messages, Recent files, Browser Cache and Download History captures.

This Capture is located in the Documents file capture group.

Referenced Files Capture

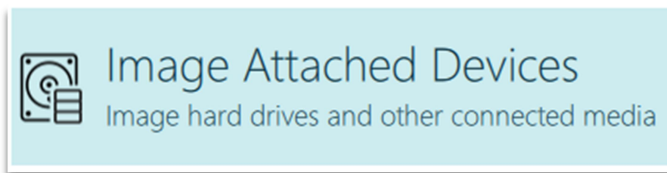


15. Imaging Computers and Other Storage Devices

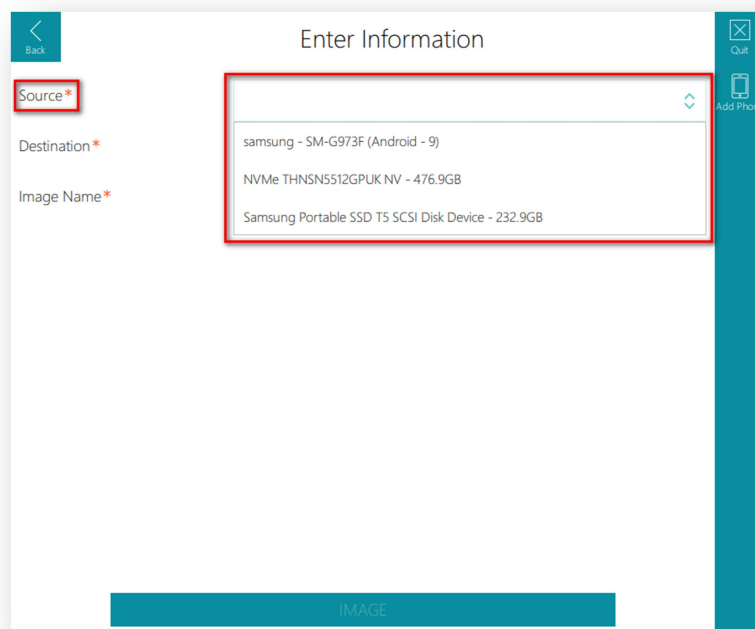
Using the Desktop Application to Image Attached Devices

The application can be used to create forensic images of attached devices. Suitable write blocking measures must be used to achieve forensically sound images.

1. Click on the Image Attached Devices button on the Home screen.



2. Select the device to be imaged, clicking on the Source combo box will display a list of attached devices. If the selected device is not an Android or iOS device further imaging options will be revealed.



3. Enter a destination for the image. Clicking on the “...” button will show a folder browser dialog box to select a destination folder. A default destination is entered when a source device is selected.

The screenshot shows the 'Enter Information' form in the ADF Triage-G2 application. The 'Source' field is set to 'Samsung Portable SSD T5 SCSI Disk Device - 232.9GB'. The 'Destination' field is highlighted with a red box and contains the path 'C:\Users\Stuart\Documents\ADF\Phone Backup'. The 'Image Name' field contains 'Samsung Portable SSD T5 SCSI Disk Device 2019-11-21 10-49-01'. The 'Image Format' is set to 'EWF'. The 'Case Number', 'Evidence Number', 'Unique Description', 'Examiner', and 'Notes' fields are empty. A checkbox for 'Verify image after it is created (doubles imaging time)' is unchecked. A large blue 'IMAGE' button is at the bottom.

4. Add the name for the forensic image; a default name is supplied on selecting a device.

The screenshot shows the 'Enter Information' form in the ADF Triage-G2 application. The 'Source' field is set to 'Samsung Portable SSD T5 SCSI Disk Device - 232.9GB'. The 'Destination' field contains the path 'C:\Users\Stuart\Documents\ADF\Phone Backup'. The 'Image Name' field is highlighted with a red box and contains the default name 'Samsung Portable SSD T5 SCSI Disk Device 2019-11-21 10-51-13'. The 'Image Format' is set to 'EWF'. The 'Case Number', 'Evidence Number', 'Unique Description', 'Examiner', and 'Notes' fields are empty. A checkbox for 'Verify image after it is created (doubles imaging time)' is unchecked. A large blue 'IMAGE' button is at the bottom.

5. Select the desired image format by clicking the appropriate radio button. The choices are Expert Witness Disk Image Format (EWF) or DD.

The screenshot shows the 'Enter Information' form in the Triage-G2 application. The form has a teal header with a 'Back' button on the left and 'Quit' and 'Add Phone' buttons on the right. The form fields are as follows:

- Source*: Samsung Portable SSD T5 SCSI Disk Device - 232.9GB
- Destination*: C:\Users\Stuart\Documents\ADF\Phone Backup
- Image Name*: Samsung Portable SSD T5 SCSI Disk Device 2019-11-21 10-54-15
- Image Format: ☒ EWF ☐ DD (This field is highlighted with a red box)
- Case Number: (empty text field)
- Evidence Number: (empty text field)
- Unique Description: (empty text field)
- Examiner: (empty text field)
- Notes: (empty text field)
- ☐ Verify image after it is created (doubles imaging time)

At the bottom of the form is a large teal button labeled 'IMAGE'.

6. Additional details such as Case Number, Evidence Number, Unique Description, Examiner and Notes can be added. These fields are not mandatory.

This screenshot shows the same 'Enter Information' form as the previous one, but with a different set of fields highlighted. The 'Image Format' field is no longer highlighted. Instead, the following fields are grouped together and highlighted with a red box:

- Case Number
- Evidence Number
- Unique Description
- Examiner
- Notes

The other fields in the form remain the same as in the previous screenshot.

7. Clicking on the verification check box will verify the image after acquisition has completed.

Enter Information

Source * Samsung Portable SSD T5 SCSI Disk Device - 232.9GB

Destination * C:\Users\Stuart\Documents\ADF\Phone Backup

Image Name * Samsung Portable SSD T5 SCSI Disk Device 2019-11-21 11-41-55

Image Format ☒ EWF ☐ DD

Case Number

Evidence Number

Unique Description

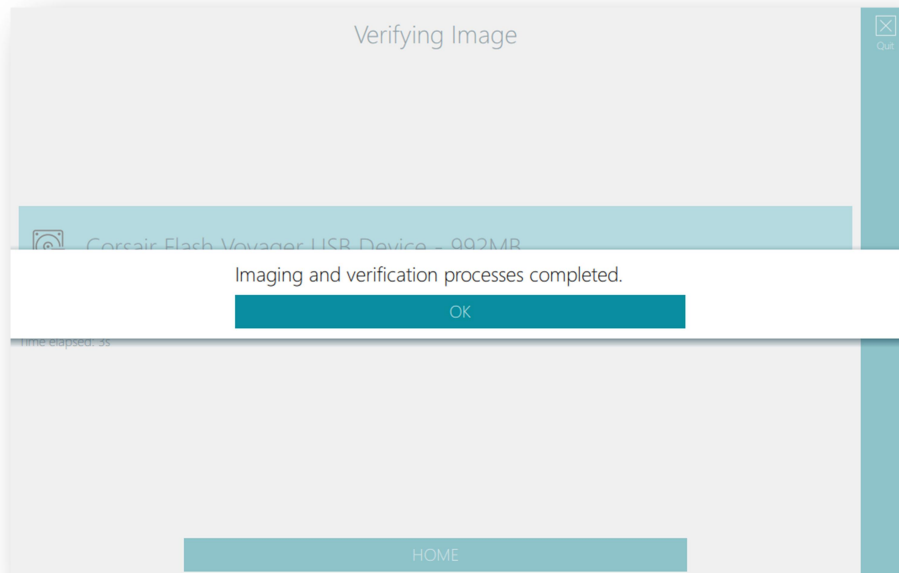
Examiner

Notes

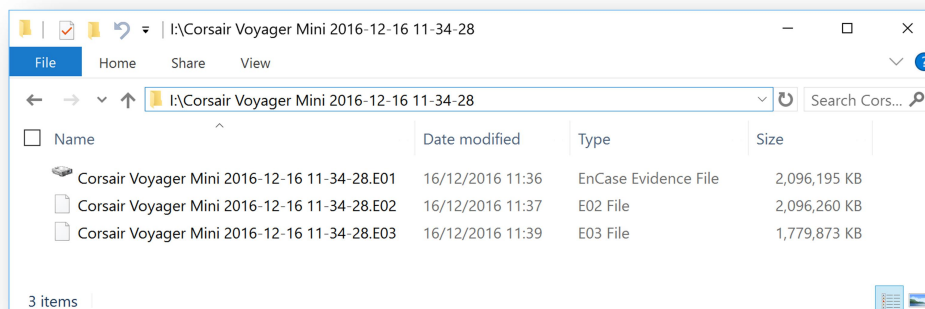
☒ Verify image after it is created (doubles imaging time)

IMAGE

8. Clicking the Image button will start the imaging process. A progress bar will be displayed and a notification shown when the imaging process has completed. If the image is to be verified this will occur after the imaging process and a new progress bar will be displayed



9. The forensic image will be created in the format selected in step 5. Verification results will be found in an accompanying .log file.



```
Created By ADF Triage-G2 5.1.0

Case Information:
Case Number: ADF/2020/001
Evidence Number: SBE/001
Unique Description: USB device found on kitchen table
Examiner: A. Examiner
Notes:

Physical Drive Information:
Drive Model: Corsair Flash Voyager USB Device
Drive Serial Number: 8
Drive Interface Type: USB
Removable drive: True
Source data size: 992 MB
Sector size: 0 B
Sector count: -

Image Information:
Imaging started : Wed Jan  8 14:10:38 2020
Imaging finished : Wed Jan  8 14:11:33 2020
Format: EWF (e01)
Segment size: 4.0GB max
Compression level: LIBEWF_COMPRESSION_FAST

Segment list:
C:\Users\Stuart\Documents\ADF\Phone Backup\Corsair Flash Voyager
USB Device 2020-01-08 14-10-38\Corsair Flash Voyager USB Device
2020-01-08 14-10-38.E01

Physical Drive Hash Values:
MD5 checksum: 360cf72980cbefa30fb5db8345042151
SHA1 checksum: c6e730c0c909ed0c53e73021075b69fad091ea91

Image Verification Results:
Verification started : Wed Jan  8 14:11:33 2020
Verification finished : Wed Jan  8 14:11:36 2020

Image MD5 checksum: 360cf72980cbefa30fb5db8345042151 - verified
Image SHA1 checksum: c6e730c0c909ed0c53e73021075b69fad091ea91 -
verified
```

Adding Mobile Device (Pro Version Only)

If a mobile device is connected but not showing in the source list it is possible to add it by clicking on the Add Phone button:

1. Click the Add Phone button

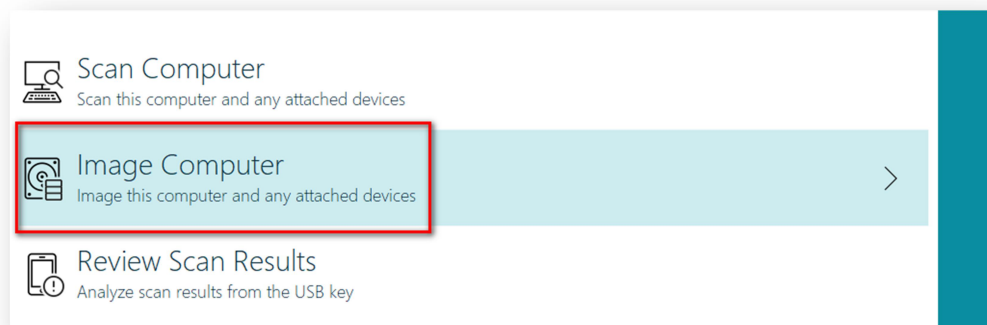
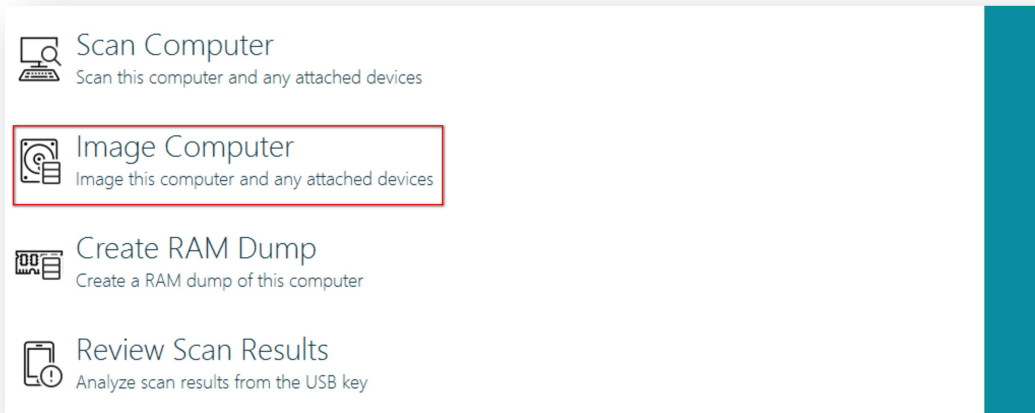
2. Select the type of the phone to add. Clicking the Cancel button will stop the phone addition process and return to the Image Information view

3. Follow the on screen instructions to add the device. When the mobile device has been successfully added it will appear in the Source combo box

Imaging Computers and Devices via Boot or Live Scans

Imaging functionality can be accessed during Boot and Live Scans.

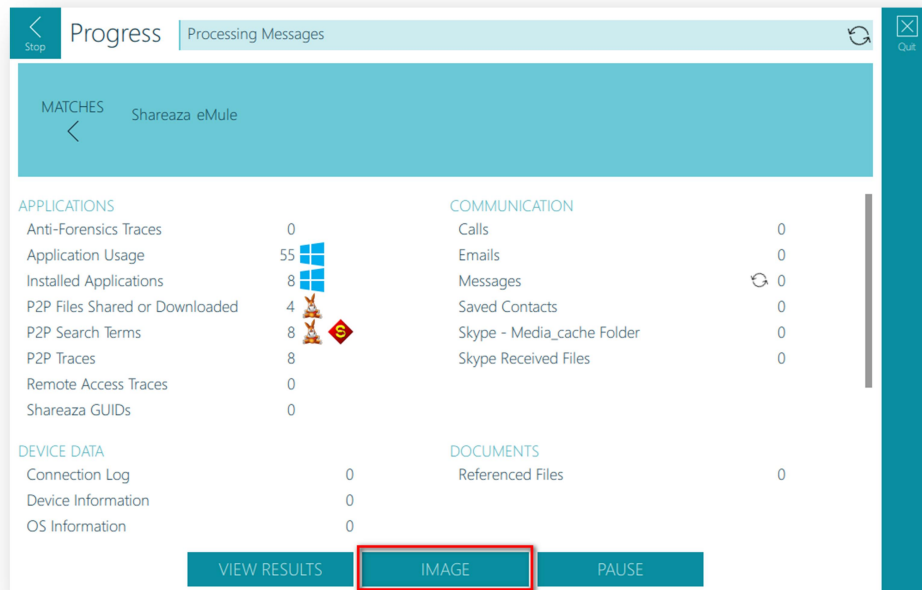
1. Click on the Image Computer button to create a forensic image of the current computer or attached device. The first screenshot shows a live scan and the second shows a boot scan.



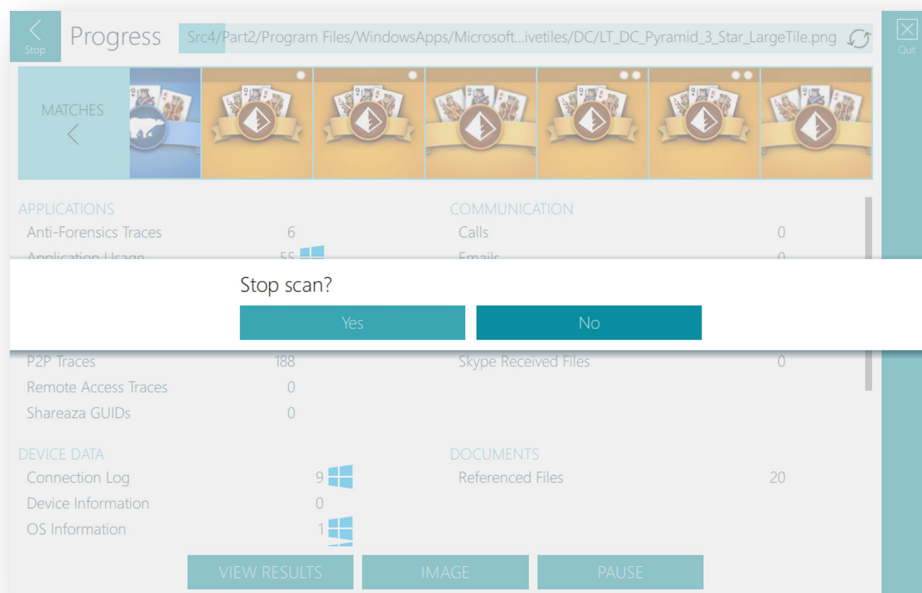
Imaging Devices During a Scan

Imaging functionality can also be accessed during a scan.

1. During the scan, click on the Image button.



2. A prompt will appear to stop the scan. Clicking Yes opens the Image Information view, clicking No will continue the scan.



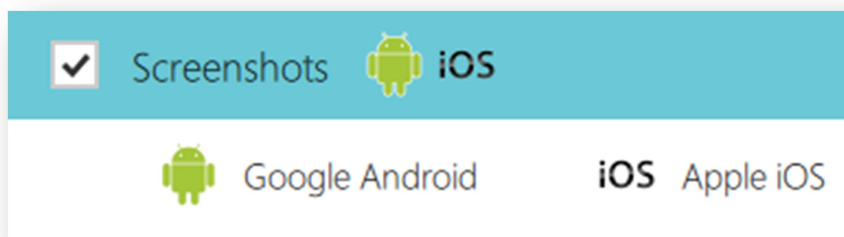
16. Mobile Device Screenshots

PRO

Screenshots of iOS and Android mobile devices can be taken when creating a backup or scanning a mobile device with a Search Profile containing the Screenshot Capture. Screenshots can have user notes associated with them and text identified within the screenshot will be extracted.

The Screenshots Capture is located in the Applications Capture Group:

Screenshots Capture



Screenshots During Backup Creation

1. Click the Image Attached Devices button on the Home Screen

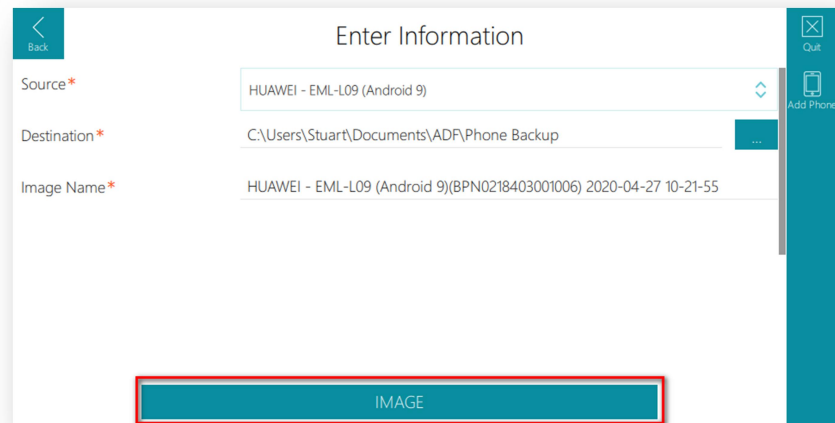


Image Attached Devices

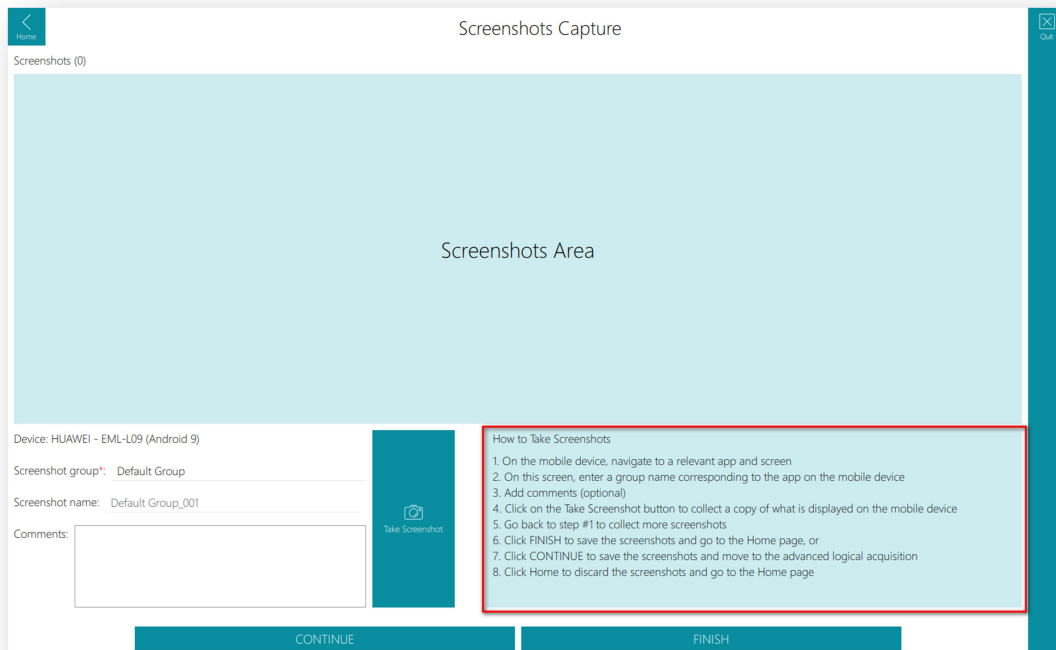
Image hard drives, connected media and perform an advanced logical acquisition of an Android/iOS device

2. Add the mobile device by clicking on the Add Phone button and following the wizard (see adding Mobile Devices section) and selecting it from the Source combo box

3. Enter a Destination for the backup and an Image Name and click the Image button



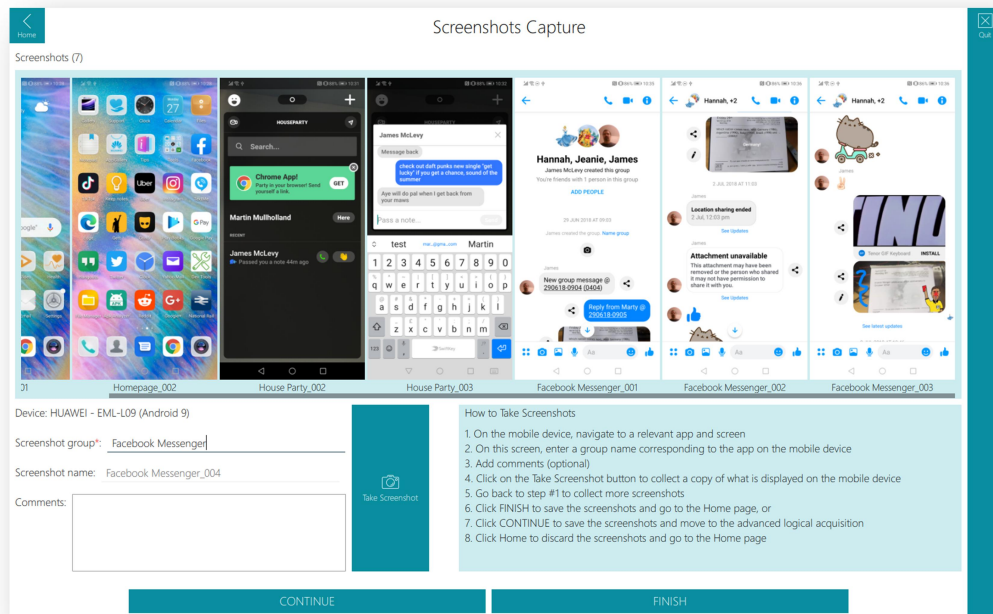
4. The Screenshots Capture view is presented, instructions for taking screenshots are present within this screen



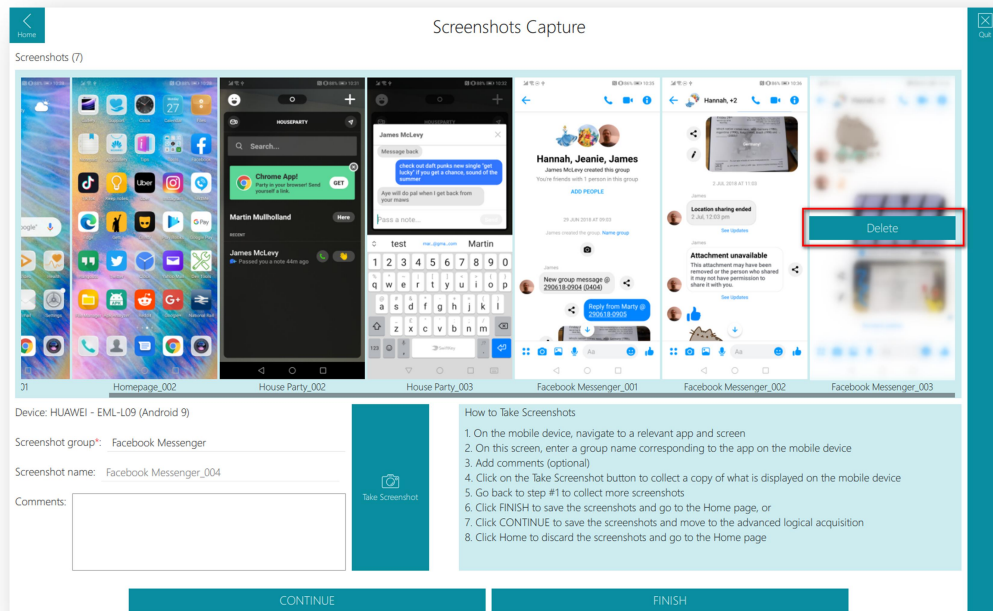
How to Take Screenshots

1. On the mobile device, navigate to a relevant app and screen
2. On this screen, enter a group name corresponding to the app on the mobile device
3. Add comments (optional)
4. Click on the Take Screenshot button to collect a copy of what is displayed on the mobile device
5. Go back to step #1 to collect more screenshots
6. Click FINISH to save the screenshots and go to the Home page, or
7. Click CONTINUE to save the screenshots and move to the advanced logical acquisition
8. Click Home to discard the screenshots and go to the Home page

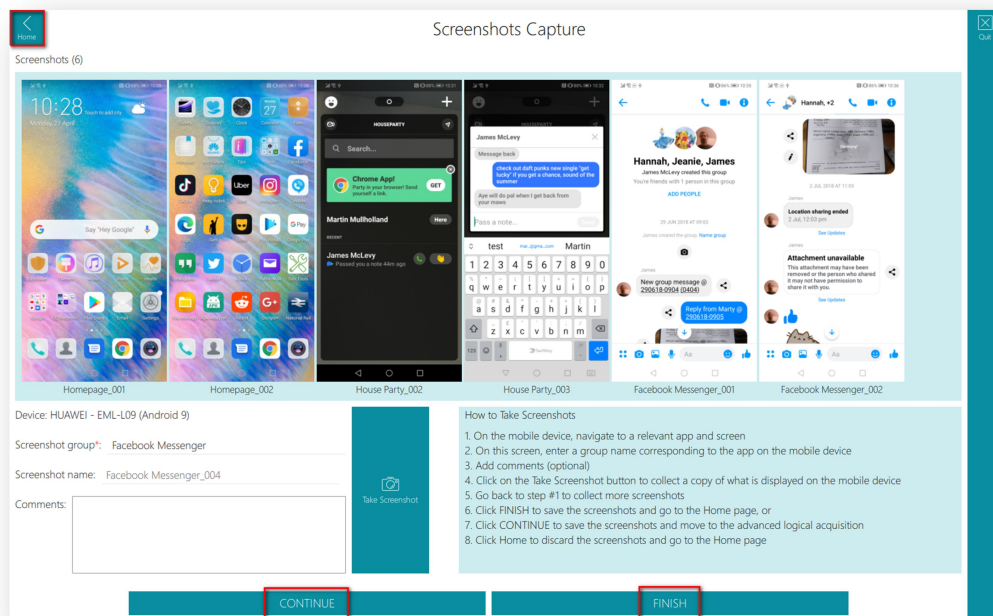
- When taking a screenshot by clicking the Take Screenshot button, whatever is displayed on your mobile device is captured, the screenshot taken is displayed in the Screenshots Area. The name of the screenshot is the value entered in the Screenshot group with an auto-incremented number appended to the end



- To delete a screenshot highlight it in the Screenshots Area and click the Delete button that appears



7. Clicking the Home button will return to the Home screen and discard all screenshots. Clicking the CONTINUE button will carry out the logical extraction of the mobile device. Clicking the FINISH button will save the Screenshots; these can then be processed to extract text content



Screenshots During Scan Device

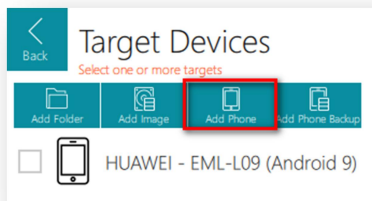
1. Click the Scan Devices and Images button on the Home Screen



Scan Devices and Images

Scan Android/iOS devices, memory cards, external hard drive, flash drive, folder or drive image

2. Add the mobile device by clicking on the Add Phone button and following the wizard (see adding Mobile Devices section) and selecting it from the Target Devices list



3. Select a Search Profile containing the Screenshots Capture. All default Mobile Devices Search Profiles contain the Screenshots Capture

Search Profile

☒ Mobile Devices - Screenshots

Manually collect screenshots from the mobile device then process the screenshots to extract textual information that can be used for keyword searching and entity extraction/translation (with Rosoka add-on).

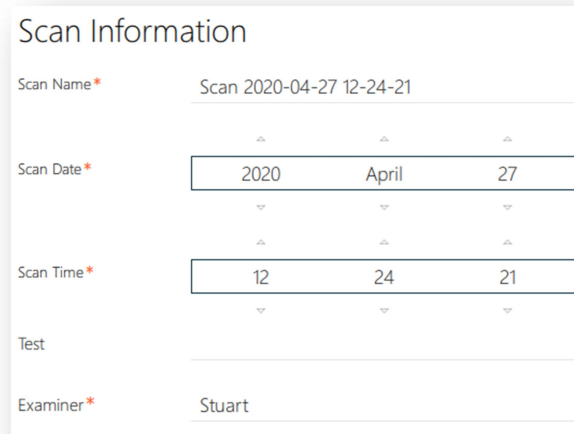
☐ Mobile Devices - General Profiling

Comprehensive scan - Runs all relevant mobile device artifact Captures, collects allocated, and embedded pictures, videos and frames from videos over 500M...

☐ Mobile Devices - Child Exploitation

Comprehensive scan - Runs all relevant mobile device artifact Captures, collects allocated, and embedded pictures and videos and frames from videos ove...

4. Enter the Scan Information then click the Scan button to bring up the Screenshots view



Scan Information

Scan Name* Scan 2020-04-27 12-24-21

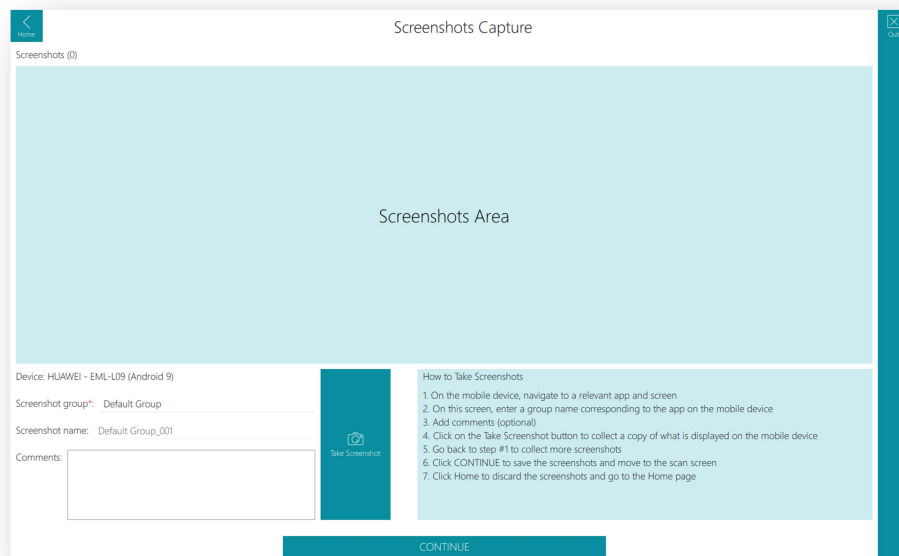
Scan Date* 2020 April 27

Scan Time* 12 24 21

Test

Examiner* Stuart

5. Taking screenshots uses the same procedure described in the Screenshots During Backup Creation section. There is no Finish button, clicking the Continue button will run the selected Search Profile on the mobile device



Screenshots Capture

Screenshots (0)

Screenshots Area

Device: HUAWEI - EML-L09 (Android 9)

Screenshot group*: Default Group

Screenshot name: Default Group_001

Comments:

Take Screenshot

How to Take Screenshots

1. On the mobile device, navigate to a relevant app and screen
2. On this screen, enter a group name corresponding to the app on the mobile device
3. Add comments (optional)
4. Click on the Take Screenshot button to collect a copy of what is displayed on the mobile device
5. Go back to step #1 to collect more screenshots
6. Click CONTINUE to save the screenshots and move to the scan screen
7. Click Home to discard the screenshots and go to the Home page

CONTINUE

Reviewing Screenshots

Clicking on Screenshots within the Summary screen will load the Screenshots view.

Screenshots View

The screenshot displays the 'Screenshots' view in the ADF Triage-G2 application. The interface includes a left sidebar with navigation options: Close, Summary, Pictures, Videos, Keywords, Timeline, Files, Scan log, Tagged, Report, and More. The main content area is titled 'Screenshots' and shows a list of items on the left and a detailed view on the right.

Records: 1
Selected: 1
Tags:

Item	Count
Chatous	1
Instagram	1
Kik	2
Line	1
LivU	1
Messages	2

Properties

Property	Value
Preview	
Group	Instagram
Textual Content	e oda Oo V View all...
Origin	Allocated
Auto-Tagged	No

Entities

Entity	Value
Name	Instagram_001
Timestamp	2020/04/28 13:34:41
Entities	PLACE>aa (1) PLACE>ny (1)
Source	Apple iOS
Captures	Screenshots

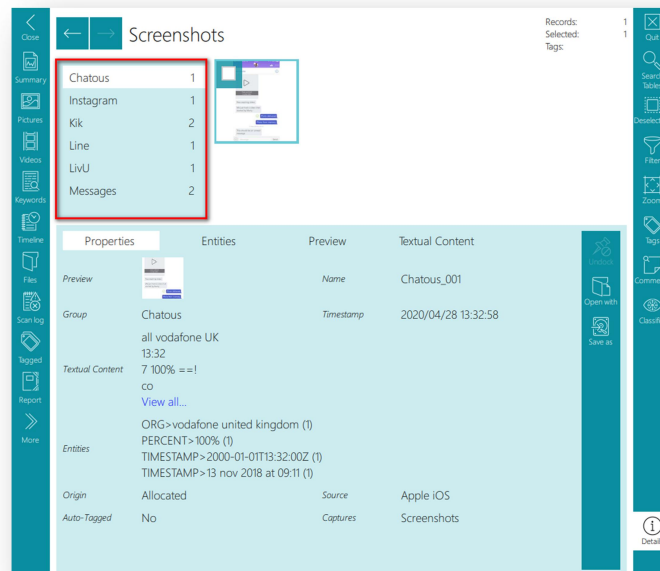
Preview

Textual Content

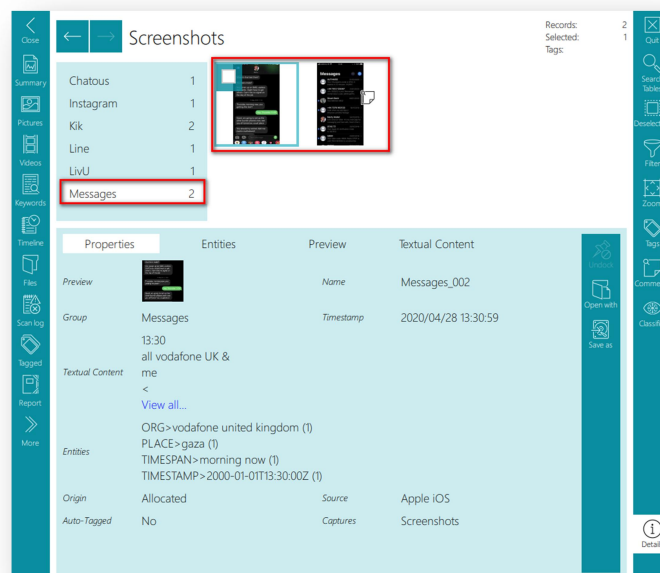
Actions: Undo, Open with, Save as

Right Sidebar: Out, Search Tables, Deselect All, Filter, Zoom, Tags, Comments, Classifier, Details

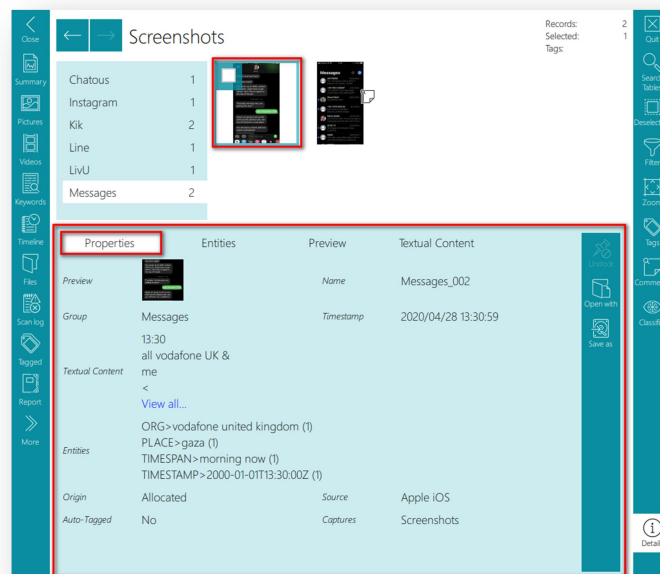
1. The left hand pane shows the Screenshot Group names entered when the screenshots were taken



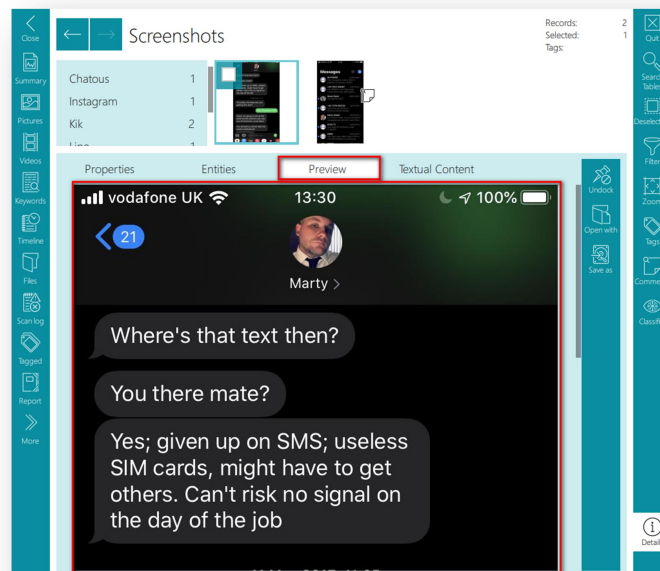
2. Clicking on a Screenshot Group name will show a gallery of screenshots taken under that name



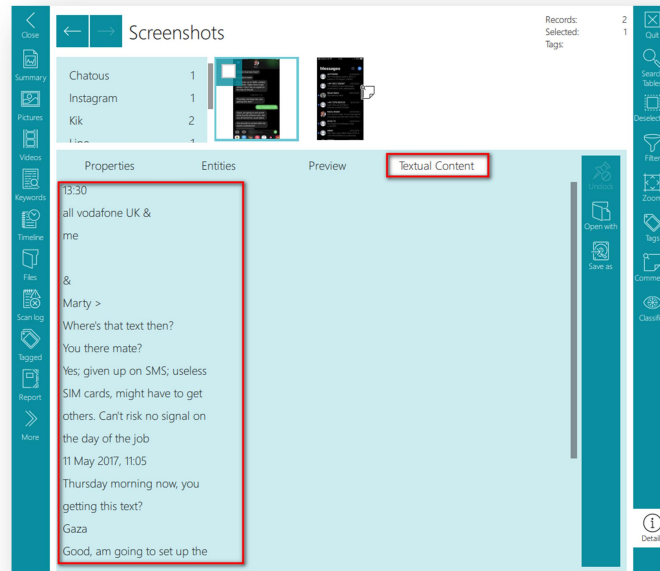
3. Clicking on a screenshot in the gallery will update the Details pane. The Properties tab will show details associated with the screenshot such as the name, the date/time the screenshot was taken and any user entered comments



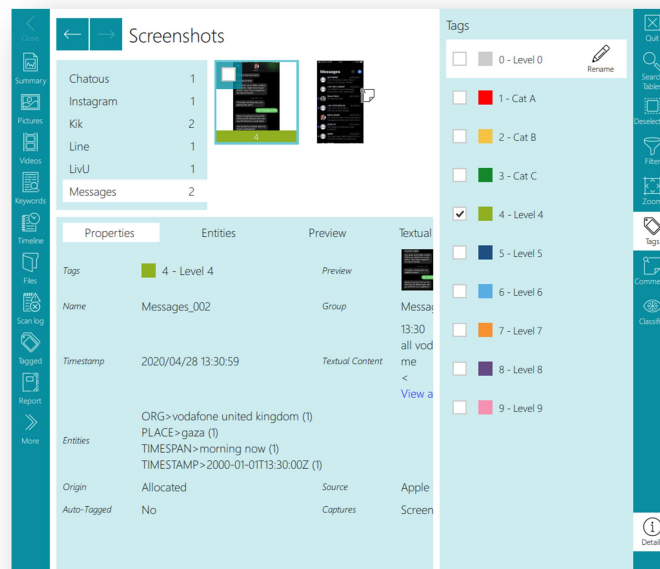
4. The Preview tab will show a full size image of the screenshot



5. The Textual Content tab will show any text information that was extracted from the screenshot. The textual content may not accurately reflect the text that was present on screen at the time and some text may not have been identified. It is possible to use the Search Tables function to search for any text that has been extracted from screenshots. Keyword search captures can also search extracted text within screenshots if Artifact records from other Captures is selected within the Keyword search capture's Search Scope



6. Screenshots can be tagged like any file or record



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.
BIOS	BIOS (basic input/output system) is the program a personal computer's microprocessor uses to get the computer system started after it is powered 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-G2'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.

Term	Meaning
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: 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: 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	(\<\/?[^\>]+\>)	HTML Tags
Character Classes		Note	
\c	Control character	These patterns are intended for reference purposes and have not been extensively tested. Please use with caution and test thoroughly before use.	
\s	White space		
\S	Not white space		
\d	Digit		
\D	Not digit		
\w	Word		
\W	Not word		
\hhh	Hexadecimal character hh		
\Oxxx	Octal character xxx		
POSIX Character Classes		Quantifiers	Ranges
[[:upper:]]	Upper case letters	*	0 or more +
[[:lower:]]	Lower case letters	*?	0 or more, ungreedy +
[[:alpha:]]	All letters	+	1 or more +
[[:alnum:]]	Digits and letters	+?	1 or more, ungreedy +
[[:digit:]]	Digits	?	0 or 1 +
[[:xdigit:]]	Hexadecimal digits	??	0 or 1, ungreedy +
[[:punct:]]	Punctuation	{3}	Exactly 3 +
[[:blank:]]	Space and tab	{3,}	3 or more +
[[:space:]]	Blank characters	{3,5}	3, 4 or 5 +
[[:cntrl:]]	Control characters	{3,5}?	3, 4 or 5, ungreedy +
[[:graph:]]	Printed characters	Special Characters	
[[:print:]]	Printed characters and spaces	\	Escape Character +
[[:word:]]	Digits, letters and underscore	\n	New line +
		\r	Carriage return +
		\t	Tab +
		\v	Vertical tab +
		\f	Form feed +
		\a	Alarm
		[\b]	Backspace
		\e	Escape
		\N{name}	Named Character
Assertions		String Replacement (Backreferences)	
?=	Lookahead assertion +	\$n	nth non-passive group
?!	Negative lookahead +	\$2	"xyz" in /^(abc(xyz))\$/
?<=	Lookbehind assertion +	\$1	"xyz" in /^(?:abc)(xyz)\$/
?!= or ?<!	Negative lookbehind +	\$`	Before matched string
?>	Once-only Subexpression	\$'	After matched string
?()	Condition [if then]	\$+	Last matched string
?()	Condition [if then else]	\$&	Entire matched string
?#	Comment	\$_	Entire input string
		\$&	Literal "\$"
Note		Available free from AddedBytes.com	
Items marked + should work in most regular expression implementations.			
Pattern Modifiers		Metacharacters (must be escaped)	
g	Global match	^	[
i	Case-insensitive	\$	{
m	Multiple lines	(\
s	Treat string as single line)	
x	Allow comments and white space in pattern	<	>
e	Evaluate replacement		
U	Ungreedy pattern		