

Introduction

This guide covers how to prepare the search criteria to use in a scan by saving them in a Search Profile and Captures.

This document applies to the following applications

ADF PRO



Digital Evidence Investigator



Mobile Device Investigator



Why Setup a Scan?

The search criteria used to collect information from the target devices are defined in a Search Profile. Creating Search Profiles prior to a scan has two main benefits:

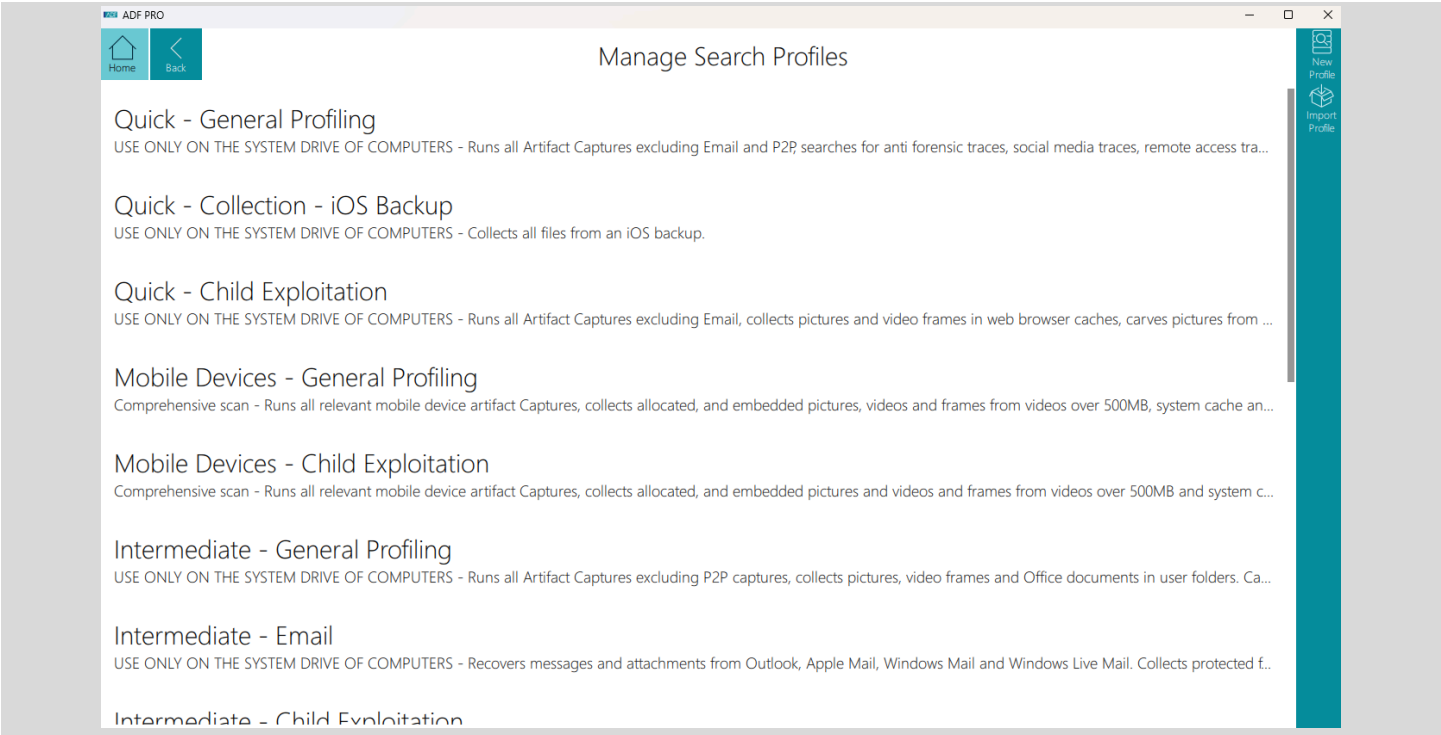
1. It makes starting a scan simple and fast.
2. It makes it possible to share the Search Profiles with other users who need to work on similar investigations. The same Search Profiles can be shared across all the ADF products.

A Search Profile is a combination of data collection modules called Captures, and settings, and whitelists. There are two types of Captures. Artifact Captures are designed to recover information created by applications and Operating Systems. Users cannot create or edit artifact Captures. File Captures recover files matching precise criteria such as file properties, keywords in their names or contents, and identical or similar digital signatures. Users can create and edit file Captures. Search Profiles can be generic or case-specific. For example, a generic Search Profile would focus on collecting information generally relevant to a type of investigation such as common keywords and all pictures. A case-specific Search Profile would search for precise information such as names, account numbers, locations, etc.



Managing and Creating Search Profiles


To manage or create Search Profiles, navigate to **Home > Setup Scans & Key Management > Manage Search Profiles**.

This screen lists the Search Profiles and offers a function toolbar. The default Search Profiles are described in this [Default Search Profiles](#) paragraph.







The right-hand side function toolbar offers the following actions:

 New Profile	To create a new Search Profile.
 Import Profile	To import a Search Profile. Select the “.profile” file to import in the Windows File Selector.



It is only possible to import a Search Profile that was created by the same version of the ADF application.

The following actions are offered on the selected Search Profile:

 Export	<p>To export the user-created Search Profile and all its Captures into a profile file. Select the folder where the Search Profile will be exported in the Windows Folder Selector. Note that if a Whitelist is used it is not exported as Whitelists have to be managed independently of the Search Profiles.</p>
 Delete	<p>To delete the user-created Search Profile. It is possible to undo this action for 30 seconds. This action does not delete that Search Profile's Captures.</p>
 Copy	<p>To copy the Search Profile and immediately edit it.</p>
 Edit	<p>To edit the user-created Search Profile. It is not possible to edit a default Search Profile but it can be copied then edited.</p>

Creating a New Search Profile

Here are the instructions to create a new Search Profile:

1. Click on the **New Profile** button in the function toolbar.
2. In the **Define Search Profile** screen
 - a. Enter a unique name for the profile.
 - b. Enter some notes describing the profile. This is optional but recommended.
 - c. The left-hand side panel contains groups of Captures available. Clicking on a Capture Group displays the Captures on the right-hand side.
 - d. Select the Captures to be used in the Search Profile. To manage Captures see the [Managing and Creating File Captures](#) paragraph. Additional information about the default Captures can be found in the [Default Captures](#) paragraph.
 - e. For Captures that collect app artifacts, it is possible to precisely select which apps should be processed by expanding the Capture block to reveal the individual apps.



Captures are independent from each other, except for the Saved Contacts Capture which should be selected when the Messages or Calls Captures are selected. Doing so resolves the communication participants' names to display their saved contact names.

- f. When the desired Captures for the Search Profile have been selected, click the **NEXT** button to continue.



If any overlapping file 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.

The overlapping Capture detection is only based on these rules:

- Capture A and B belong to the same Capture Group, AND
- Capture A and B have the same action (file collection, hash search, kw search), AND
- Capture A and B have at least one file type group in common (the "All files" is ignored), AND
- The max file size of Capture A is greater than the min file size of Capture B

3. In the Options screen




- a. The **Scan Information Fields** section offers to use the information fields defined in the [global Settings](#) or define new fields specific to this Search Profile. Defining new fields is identical to doing it in the [global Settings](#).
- b. The **Scan Options** section offers the following:
 - i. **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. By default files are skipped after one hour.
 - ii. **Collect skipped files:** collects files less than 2GB that were skipped for taking too long to process.
 - iii. **Collect protected files encountered by the Captures (max 2GB):** this copies any password protected files detected by the Captures. These files can be found in the [Scan Log view](#) of the scan result by filtering records with Type="password protected".
 - iv. **Collect files that crashed parser (max 2GB):** this copies any corrupted files that couldn't be processed by the Captures. These files can be found in the [Scan Log view](#) of the scan result by filtering records with Type="parsing error".
 - v. **Activate BitLocker on Collection Key (it is impossible to recover the data if the password is lost):** this activates the BitLocker encryption when preparing the Collection Key so all data saved on it (Search Profiles, Captures, Scan Results, etc) is fully encrypted securing the data against loss or theft.
 - vi. **Run live scans in stealth mode:** this makes traces left by the execution of the live Scanner application difficult to detect. More details can be found [here](#) (**PRO** **DEI**).
 - vii. **Automatically start picture and video classification tasks during the scan:** to enable [picture classification](#), [video classification](#), simply check this checkbox. Additional options are then available to **Prioritize scan speed** (to limit the time spent classifying files during the scan) or **Prioritize picture and video classification speed** (to classify as many files as possible during the scan, hence slowing down the overall scan).
 - viii. **Automatically start entity extraction when scan finishes:** to enable [entity extraction](#), simply check this checkbox.
- c. The **Whitelists** section shows the whitelists that can be used by the Search Profile. It is possible to select one or more whitelists. Deselecting a whitelist does not delete it.
- d. Click on the **SAVE** button to finish the Search Profile creation.

Managing Whitelists



A whitelist is a list of files that can be safely ignored during a scan so they do not create records in the scan result. There are three ways to create a whitelist: selecting the files to be added to the whitelist, adding a CSV file containing hash values, or adding a JSON file containing hash values.

Whitelists created in one Search Profile will be available for use in all user-created Search Profiles.

The following actions are offered in the **Whitelists** section of the Search Profile **Options** screen:

 Add Files	To select a folder containing the files to be added to the whitelist.
 Import CSV	To create a whitelist with hash values contained in a CSV file.
 Import VICS	To create a whitelist with hash values contained in a VICS file (JSON format).

The following actions are offered on the selected whitelist:

 Rename	To rename the whitelist.
 Delete	To delete the whitelist. A deleted whitelist affects all the Search Profiles using it. It is possible to undo this action for 30 seconds.

Creating a Whilelist from Files

To create a whitelist from files:

1. Click on the **Add Files** button.

2. Select the folder where the safe files are located in the Windows Folder Selector.
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.
4. A default name is given to the whitelist which can be modified immediately or later. Make sure the whitelist name is unique if renaming it.

Creating a Whilelist from CSV

To create a whitelist from a CSV files:

1. Click on the **Import CSV** button.
2. Select the CSV file from the Windows File Selector. The UTF-8 formatted CSV file must contain:
 - a. Hash value column: titled "md5" for 32 character hexadecimal MD5 values, or "sha1" or "sha-1" for either 40 character hexadecimal SHA1 values or 32 character base-32 RFC 4648 SHA1 values.
 - b. Optional file size column: titled "file size" or "filesize" for file size in bytes.
 - c. Example:

```
md5, file size
01e21b88109af7348797f4b06b888445, 3342
311b395d4d8f86c38cf054cb3b28a02a, 875234
```
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. A default name is given to the whitelist which can be modified immediately or later. Make sure the whitelist name is unique if renaming it.



Proving the file size greatly improves the performance when using whitelists.

Creating a Whilelist from a VICS File

To create a whitelist from a VICS file (JSON format):

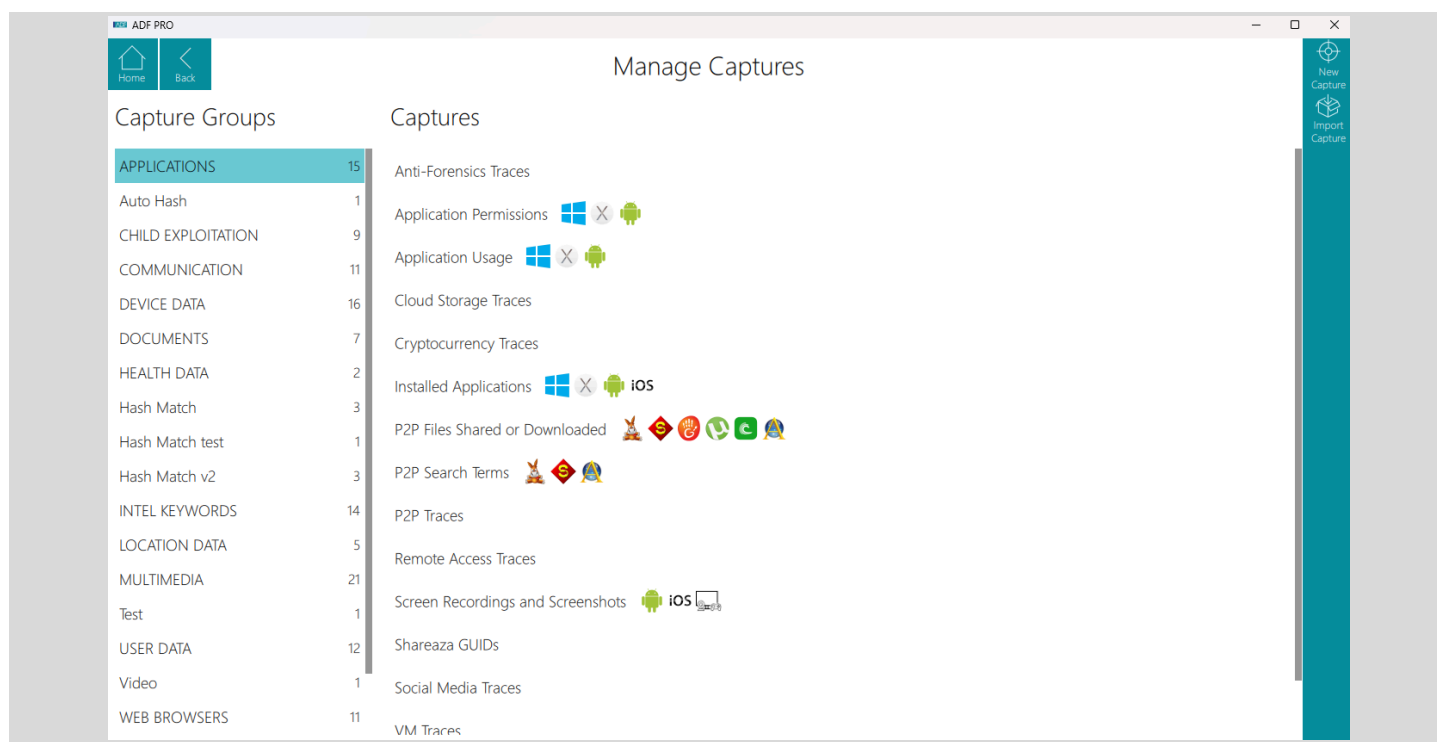
1. Click on the **Import VICS** button.
2. Select the VICS file from the Windows File Selector.
3. Select which categories identified in the VICS file should be imported and click on the **OK** button.
4. A message will be displayed showing the status of the whitelist creation. Any errors that occurred during the whitelist creation are displayed, such as duplicate hash values. Click the **OK** button to continue.
5. A default name is given to the whitelist which can be modified immediately or later. Make sure the whitelist name is unique if renaming it.

Importing and Exporting Whitelists

To export a whitelist, its database file has to be copied to the new destination. The location where the whitelists are saved is defined in the [Settings](#) screen. The whitelist database file name is based on the whitelist name with the “db” extension.

Managing and Creating File Captures



To manage or create Captures, navigate to **Home > Scan Setup & Key Management > Manage Captures**. This screen lists all the Captures organized by groups and offers a function toolbar.



To view the description of a capture, hover your mouse over its name.

Alternatively, the [Define Search Profile](#) screen lists all the Captures organized by groups so they can be added to a Search Profile. From this screen it is also possible to manage the file Captures.






The right-hand side function toolbar offers the following actions:

 New Capture	To create a new file Capture. See the Creating a new Capture paragraph below for details.
 Import Capture	To import a file Capture. Select the “.capture” file to import in the Windows File Selector.



It is only possible to import a Capture that was created by the same version of the ADF application.

The following actions are offered on the selected Capture:

 Export	To export the user-created file Capture into a capture file. Select the folder where the Capture will be exported in the Windows Folder Selector.
 Delete	To delete the user-created file Capture. Deleting a file Capture affects all the Search Profiles using it. It is possible to undo this action for 30 seconds. Default Captures cannot be deleted but they can be hidden (see the Display Default Captures paragraph of the Configuring the ADF Application guide).
 Copy	To copy the file Capture and immediately edit it.
 Edit	To edit the user-created file Capture. It is not possible to edit a default file Capture but it can be copied then edited.
 	To show all the applications supported by the Capture. Note that a detailed list of supported applications can be found here .

Expand	
--------	--

Creating a new Capture

To create a new file Capture follow these instructions:

1. Click on the **New Capture** button.
2. Choose the type of file Capture to create:
 - a. [Search for files by properties](#): Search for and collect files based on their file type, properties and location.
 - b. [Search for keywords](#): Search for files by keyword(s) using substrings or regular expressions.
 - c. [Search for hash values](#): Search for files using MD5 or SHA1 hash values.
 - d. [Search for visual similarities](#): Searches for visually similar pictures to ones provided by the user and groups visually similar pictures together.
3. Read the paragraphs below that describe how to continue the creation of each type of file Capture.
4. Once the file Capture is created, it is automatically added to the Search Profile. It is possible to uncheck the Capture so that it is not used by the Search Profile.

Search for Files by Properties

On the **Define Files to Collect** screen it is possible to define the type of files to collect and the scope of collection.

ADF PRO

Define Files to Collect

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

File Types
Select a file type

☐ 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

Options

☒ Collect matching files

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

☐ Excluded folders

File Sources
Select a source

☐ Entire file system

☐ Targeted folders

☐ Files referenced by artifact records

☐ Deleted files

☐ Carve pictures from Unallocated space

☐ Carve pictures in

☐ System Cache

File Properties

Include files when size is within boundaries

MB

Include pictures with width and height greater than pixels

SAVE

The following information has to be entered:

- **Capture Group Name:** the group name is used to organize the Captures and is visible in the Viewer and in the reports. Type a new name or use an existing one.

- **Capture Name:** enter a unique Capture name that describes what the Capture does.
- **File Types:** 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 from the [Adding a Custom File Type](#) paragraph. Note that when selecting **All Files**, all files including those that are not defined under **Specific Files** will be identified and processed.
- **Options:**
 - a. **Collect matching files:** the original files will be collected and processed (thumbnails are created, video frames are extracted, metadata is extracted, etc).
 - b. **File identification method:**
 - i. **Fast identification:** identifies file types using the file extension only. This method is the fastest but it will not identify files without extensions or files with an incorrect extension.
 - ii. **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. This method is useful for applications that save data in files without extensions such as the Google Chrome cache.
 - iii. **Thorough identification for all files:** uses file signature analysis to identify all files. This will increase the time the scan takes to run but it is the most accurate file identification method.
 - c. **Search selected file types in:**
 - i. **Archives:** searches for all selected file types within archives such as zip, tar and other containers.
 - ii. **Documents:** searches for all selected file types embedded within Document file types.
 - iii. **Picture DB File:** searches for all selected file types within Windows thumbcache and thumbs.db files and Apple itmb files.
 - d. **Excluded folders:** to exclude some folders from the file Capture search. The path of these folders has to be entered as a regular expression. For example:
 - i. To exclude any folder named "desktop", type exactly `*/desktop/*`.
 - ii. To exclude any folder with the word "image" in it, type exactly `*image*`.
- **File Properties:**
 - a. **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.
 - b. **Pixel size:** limits the pictures collected by setting the minimum pixel width and height.
 - c. **File created:** specifies a UTC created date range for the selected file types.
 - d. **Last written:** specifies a UTC modified date range for the selected file types.
- **File Sources:**
 - a. **Entire file system:** searches all allocated files.
 - b. **Targeted folders:** may be used to limit or focus the extent of the scan. 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
 - c. **Files referenced by artifact records:** used to target files referenced by artifact records (e.g. email attachments, recent files, etc). More details about referenced files can be found in this [Referenced Files](#) paragraph of the [Reviewing Scan Results](#) guide.

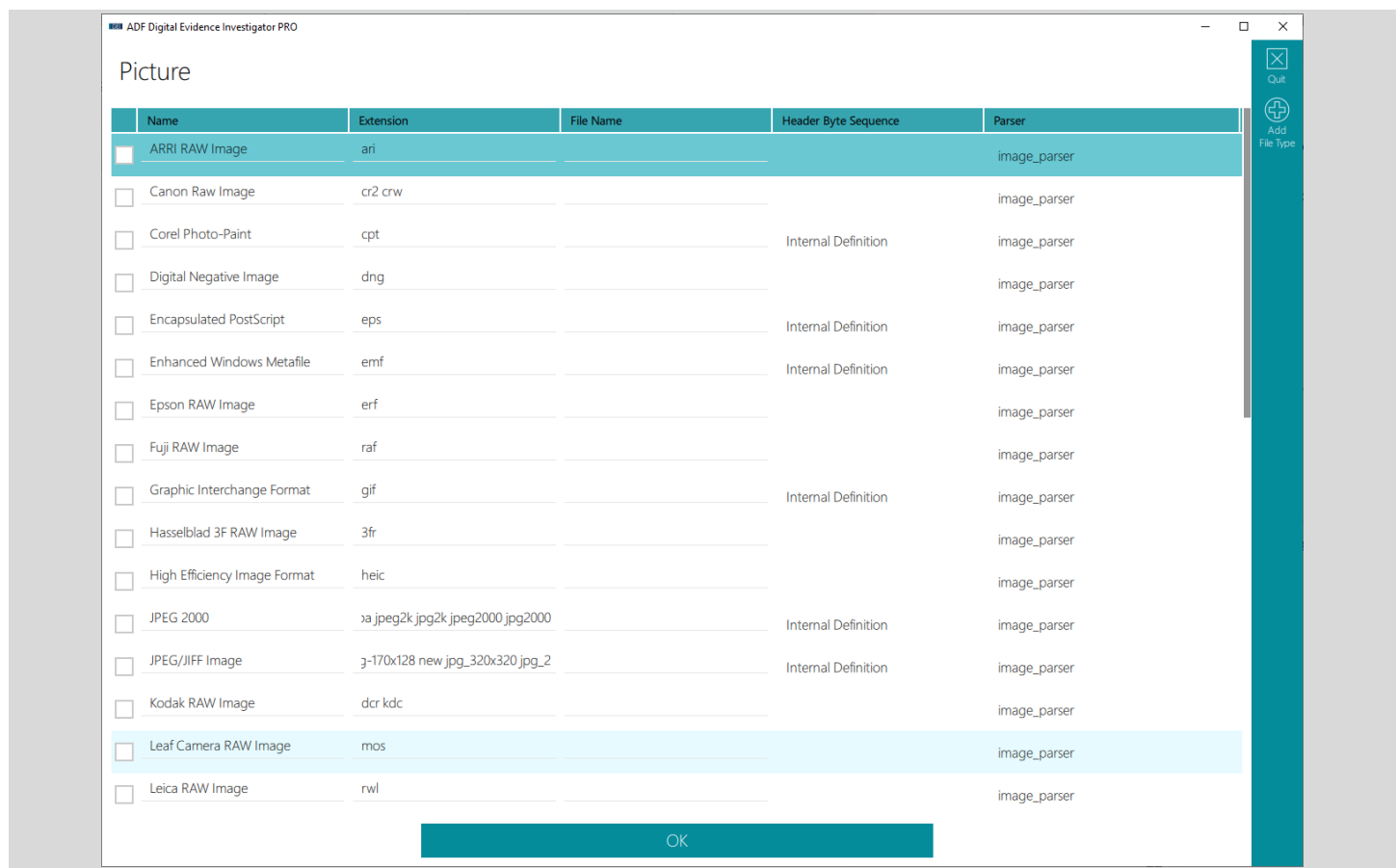
- d. **Deleted files:** used to recover files that have been deleted if a reference can still be found in the file system directory index and if the file content has not been overwritten.
- e. **Carve pictures from unallocated space:** this searches unallocated space and collects any picture files when their header signature is identified.
- f. **Carve pictures in:** this carves pictures from the allocated files defined in the groups listed in this option.
- When the required options are selected click the **SAVE** button.

The picture formats that can be carved are listed [here](#). The following rules are used to identify the file size:

- **JPG:** the algorithm tries to identify the End of File (EoF) byte sequence by reading consecutive sectors up to 30 MB. If the EoF is not found, then the entire 30 MB of data is carved.
- **PNG, GIF:** the algorithm tries to identify the End of File byte sequence by reading consecutive sectors up to 30 MB. If the EoF is not found, then the data is not carved.
- **TIFF, PSD:** the algorithm tries to identify the End of File byte sequence by reading consecutive sectors without limitations.
- **BMP, WEBP:** the algorithm locates the exact file size in the file header.

Adding a Custom File Type

It is possible to create new file types to be processed during a scan.



Here are the instructions to create a new file type:

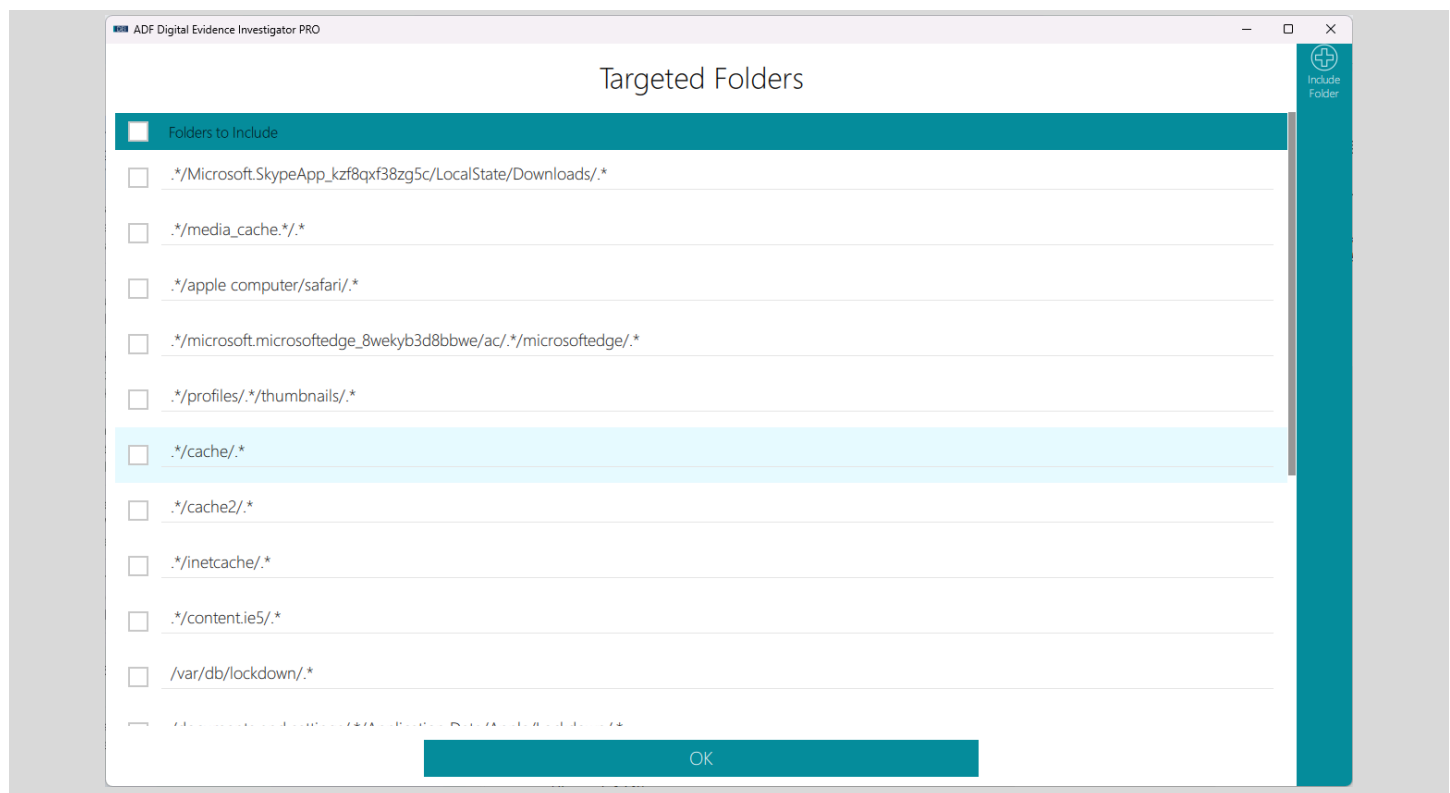
1. Within the **File Types** section click on the **View** button on any file type group.
2. On the file type screen click the **Add File Type** button of the functional toolbar to add a new file type.
3. There are three options available to identify a file: **Extension**, **File Name** and **Header Byte Sequence**. It is a requirement to enter at least one of these options.
 - a. Add the file extension by clicking in the **Extension** cell. Do not add a dot prior to the extension. It is possible to add multiple extensions by separating them by a space.
 - b. Add the file name by clicking in the **File Name** cell.
 - c. Add the header byte sequence by clicking in the **Header Byte Sequence** cell. The byte sequence has to be entered as a regular expression. For example `\x12\x4e.{2}\x2b` or `\x17\x00\x00\x00\x53\x43\x43\x41`.
4. Add Parser type to help process these files (document, image, text or video). If unknown, select **Default Parser**.
5. When finished click on the **OK** button.



The file types are common to all the Captures and modifying a file type modifies it for all the Captures using it.

Adding a Targeted Folder

It is possible to create new targeted folders to narrow the scope of a search or prioritize folders of interest.



Here are the instructions to create a new targeted folder:

1. Within the **File Sources** section mouse-over the **Targeted folders** and click on the **View** button.
2. On the **Targeted Folders** screen click the **Include Folder** button of the functional toolbar to add a new folder.
3. Add the desired folder path. The path has to be entered as a regular expression. For example:
 - a. To search any folder named "desktop", type exactly `./desktop/.*`
 - b. To search any folder with the word "image" in it, type exactly `.*image.*`
 - c. To search the "users" folder but not its sub-folders, type exactly `./users/[^/]*`
4. When finished click on the **OK** button.



The targeted folders are common to all the Captures and modifying a targeted folder path modifies it for all the Captures using it.

Search for Keywords

On the **Define Keyword Capture** screen it is possible to define the keywords (a.k.a. search expressions) to search for, and define the scope of search.

Define Keyword Capture

Capture Group Name* Enter a name.

Capture Name* Enter a name.

Search Expressions

Enter search expressions.

Selected Search Type: Substring Case Insensitive

Search Expression	Expression Name	Search Type	Auto-Tag	Auto-Comment
<input type="text"/> Enter value...	<input type="text"/> Enter name...	Substring Case Insensitive	No tag	<input type="text"/> Enter comment...

Search Scope

Select a scope.

☐ File and folder names

☐ Files content and metadata

☐ Artifact records from other Captures



Options

☒ Collect matching files

Import List

Clear Table

The right-hand side function toolbar offers the following actions:

 Import List	To import search expressions from a CSV file.
 Clear Table	To remove all the search expressions from the table.

The following information has to be entered:

1. **Capture Group Name:** the group name is used to organize the Captures and is visible in the Viewer and in the reports. Type a new name or use an existing one.
2. **Capture Name:** enter a unique Capture name that describes what the Capture does.
3. **Selected Search Type:** Choose a default search type from the dropdown menu. Keywords manually entered into the Search Expression table will inherit this setting. The available search types are:
 - a. Substring - Case Insensitive (selected by default)
 - b. Substring - Case Sensitive
 - c. Whole Word - Case Insensitive
 - d. Whole Word - Case Sensitive
 - e. Regular Expression
4. **Search Expressions:**
 - a. Keywords can be entered manually in the Search Expression cell. Use the Search Type column to modify the search type for each keyword. For bulk changes, use the table checkboxes to select the keywords, choose a search type from the Select Search Type dropdown, and click the Apply button. Optionally, tags and comments can be automatically assigned to the matching records. Adding a search expression will automatically create a new line for additional entries.
 - b. The keywords can also be imported by using the **Import List** button in the functional toolbar. Clicking this button opens a Windows File Selector to select the CSV file. The UTF-8 formatted CSV file must contain:
 - i. Search expression column: titled "keyword".
 - ii. Optional tag column: titled "auto-tag" with values from 0 to 9.
 - iii. Optional comment column: titled "auto-comment" with text no longer than 1000 characters.
 - iv. Optional search type column: titled "search-type" with values 0 to 4:
 - 0 = Substring - Case Insensitive
 - 1 = Substring - Case Sensitive
 - 2 = Whole Word - Case Insensitive
 - 3 = Whole Word - Case Sensitive
 - 4 = Regular Expression
 - v. Example:
 keyword, auto-tag, auto-comment, search type
 kw1

```
kw2, 5, Related to case 123, 3
kw3 kw31, 5, Related to case 123, 2
```

Note, if the selected CSV file does not contain the columns titled “auto-tag” and “auto-comment”, the **Assign Tags and Comments** dialog is displayed to manually associate tags and comments with all the search expressions from the CSV file.

If the selected CSV file does not contain the "search-type" column or contains empty values within it, search expressions will inherit the search type selected from the **Select Search Type** dropdown.

- c. Use the Expression Name column to assign a user-friendly label to each keyword. This is especially helpful when working with regular expressions, as the assigned name will be shown in place of the regular expression when viewing keywords in the Scan Results.
- d. To delete a search expression, mouse-over it to see the **Delete** button.

5. Search Scope:

- a. **File and folder names:** search expressions are searched for in file and folder names. Note that it is not possible to use an expression that should match both a folder and file names.
- b. **File content and metadata:** search expressions are searched for within the content of each file and its metadata. To define which files to search, mouse-over this option and click on the **View** button which opens the **Define Files to Search** screen. This screen offers the same options as the [Define Files to Collect](#) screen described above except for:
 - i. The **Carve pictures from unallocated space** option is not offered.
- c. **Artifact records from other Captures:** search expressions are searched for in other Capture results e.g. browsing history, chat messages, etc.

6. Options:



- a. **Collect matching files:** selecting this will collect the file in which at least one keyword was found.




7. Click on the **SAVE** button to finish the Capture creation.

Search for Files by Hash Value

On the **Define Hash Values** screen it is possible to define the hash values to search for and the scope of search.

The right-hand side function toolbar offers the following actions:

 Add Files	To compute the hash values from local files.
 Import List	To import hash values from a CSV file.

 Import VICS	To import hash values from a VICS file (JSON format).
 Import CAID	To import hash values from a CAID file (JSON format).
 Remove All	To remove all the hash values.

The following information has to be entered:

1. **Capture Group Name:** the group name is used to organize the Captures and is visible in the Viewer and in the reports. Type a new name or use an existing one.
2. **Capture Name:** enter a unique Capture name that describes what the Capture does.
3. **Hash List:** shows the number of hash values in the Capture. To add hash values to the ones already present, use the function toolbar buttons:
 - a. **Add Files:** this will bring up a Windows Folder Selector and selecting a folder will hash all of the files within that folder and any sub-folders. It is also possible to automatically assign a tag and a comment to the matching record by setting those up in the **Assign Tags and Comments** dialog. Note that if hash values were already present in the Capture, the tag and comment are not assigned to them.
 - b. **Import List:** this will bring up a Windows File Selector to select the CSV file. The UTF-8 formatted CSV file must contain:
 - i. Hash value column: titled “md5” for 32 character hexadecimal MD5 values, or “sha1” or “sha-1” for either 40 character hexadecimal SHA1 values or 32 character base-32 RFC 4648 SHA1 values.
 - ii. Optional file size column: titled “file size” or “filesize” for file size in bytes.
 - iii. Optional tag column: titled “auto-tag” with values from 0 to 9.
 - iv. Optional comment column: titled “auto-comment” with text no longer than 1000 characters.
 - v. Example:


```
sha1, file size, auto-tag, auto-comment
5219e8be8201c9f90ddef72144797582d97c0016, 69223, 1, Related to
case 122
f2965b27cd2d0e5ebb3d48afa9b904152b42f0b7, 6659
d22cfd4ed85d7b90f145b98a28397970cffa6987, 923120, , Related to
case 122
```

Note, if the selected CSV file does not contain the columns titled “auto-tag” and “auto-comment”, the **Assign Tags and Comments** dialog is displayed to manually associate tags and comments with all the hash values from the CSV file.
 - c. **Import VICS:** this will bring up a Windows File Selector to select the VICS file. Then select which VICS categories should be imported (note that these categories may not all be present in the selected file).

Each hash value from that category is assigned a tag with the same number and it is possible to enter a comment that will be assigned automatically to the matching file. Finally, select "Include Hash Comments" to also assign comments found in the VICS file..

- d. **Import CAID:** this will bring up a Windows File Selector to select the CAID file. Then select which CAID categories should be imported (note that these categories may not all be present in the selected file). Each hash value from that category is assigned a tag with the same number and it is possible to enter a comment that will be assigned automatically to the matching file. Finally, select "Include Hash Comments" to also assign comments found in the CAID file.
- e. When all the hash values have been added, click on the **NEXT** button.
- f. The **Define Files to Hash** screen offers the same options as the [Define Files to Collect](#) screen described above.
- g. Click on the **SAVE** button to finish the Capture creation.





Proving the file size greatly improves the performance of hash value searches.

Search for Visual Similarities

On the **Define PhotoDNA Set** screen it is possible to define the PhotoDNA values to search for but the scope of search is always set to all the pictures that other file Captures processed during the scan. To better understand what to expect from such a Capture, see how the results are presented in the [Visual Similarity \(PhotoDNA\) Capture View](#) paragraph of the [Reviewing Scan Results](#) guide.

The right-hand side function toolbar offers the following actions:

 Add Files	To compute the PhotoDNA values from local files.
 Remove All	To remove all the PhotoDNA values.

The following information has to be entered:

4. **Capture Group Name:** the group name is used to organize the Captures and is visible in the Viewer and in the reports. Type a new name or use an existing one.
5. **Capture Name:** enter a unique Capture name that describes what the Capture does.
6. **PhotoDNA Set:** shows the number of PhotoDNA values in the Capture. To add PhotoDNA values to the ones already present, use the function toolbar:

- a. **Add Files:** this will bring up a Windows Folder Selector and selecting a folder will compute the PhotoDNA of all the files within that folder and any sub-folders. Only the jpg, png, gif, bmp file types are processed.
7. Click on the **SAVE** button to finish the Capture creation.



A Visual Similarities (PhotoDNA) Capture only works on pictures collected by other file Captures so make sure such Capture is part of the same Search Profile.

Default Search Profiles

The table below lists the Search Profiles that are available out-of-the-box.

Search Profile	Description
Quick - General Profiling	USE ONLY ON THE SYSTEM DRIVE OF COMPUTERS - Runs all Artifact Captures excluding Email and P2P, searches for anti forensic traces, social media traces, remote access traces, files in the Skype caches and pictures and videos in the browser cache and carves pictures from system cache files.
Quick - Collection - iOS Backup	USE ONLY ON THE SYSTEM DRIVE OF COMPUTERS - Collects all files from an iOS backup.
Quick - Child Exploitation	USE ONLY ON THE SYSTEM DRIVE OF COMPUTERS - Runs all Artifact Captures excluding Email, collects pictures and video frames in web browser caches, carves pictures from system cache files and searches for common Child Exploitation keywords in file names and artifacts. Searches for P2P traces, anti-forensic traces and files in the Skype caches.
Mobile Devices - General Profiling	Comprehensive scan - Runs all relevant mobile device artifact Captures, collects allocated, and embedded pictures, videos and frames from videos over 500MB, system cache and Office Documents using the Thorough Identification option for files without extensions. Searches for Remote Access and Cryptocurrency Traces, audio files, database, plist files and referenced files. Collects skipped files, protected files and files not processed by parser.
Mobile Devices - Child Exploitation	Comprehensive scan - Runs all relevant mobile device artifact Captures, collects allocated, and embedded pictures and videos and frames from videos over 500MB and system cache, searches for common Child Exploitation keywords, and searches for known hash values using the Thorough Identification option for files without extensions. Searches for Remote Access Traces, audio files, database, plist files and referenced files. Collects skipped files, protected files and files not processed by parser.
Intermediate - General Profiling	USE ONLY ON THE SYSTEM DRIVE OF COMPUTERS - Runs all Artifact Captures excluding P2P captures, collects pictures, video frames and Office documents in user folders. Carves pictures from system cache files. Searches for anti-forensic traces, remote access traces, cloud storage traces, social media traces and files in the Skype caches. Collects protected files and files not processed by parser.
Intermediate - Email	USE ONLY ON THE SYSTEM DRIVE OF COMPUTERS - Recovers messages and attachments from Outlook, Apple Mail, Windows Mail and Windows Live Mail. Collects protected files and files not processed by parser.

Intermediate - Child Exploitation	USE ONLY ON THE SYSTEM DRIVE OF COMPUTERS - Runs all Artifact Captures, collects pictures and video frames in user folders, carves pictures from system cache files, searches for common Child Exploitation keywords in user folders, and searches user folders for known hash values. Searches for anti-forensics traces, remote access traces, P2P traces and files in Skype caches. Collects protected files and files not processed by parser.
External Devices - General Profiling	Runs all Artifact Captures, excluding P2P captures and Saved Credentials, collects allocated, embedded, and deleted pictures, videos, and frames from videos over 500MB and Office Documents using the Thorough Identification for Files Without Extensions. Collects Registry files, searches for anti-forensics applications, remote access traces, social media traces, files in the Skype caches and collects user Desktop shortcuts. Collects protected files and files not processed by parser.
External Devices - Collection - iOS Backup	USE ONLY ON THE SYSTEM DRIVE OF COMPUTERS - Collects all files from an iOS backup.
External Devices - Child Exploitation	Runs all Artifact Captures, collects allocated, embedded, and deleted pictures and videos and frames from videos over 500MB, carves pictures from system cache files, searches for common Child Exploitation 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.
Device - Screen Casting	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).
Comprehensive - Intel	Runs all Artifact Captures, collects allocated, embedded, and deleted pictures, videos and frames from videos over 500MB and Office documents. Collects Registry files, searches for anti-forensics applications, remote access traces, cloud storage traces, social media traces, files in Skype caches and terrorism keywords, and collects user Desktop shortcuts. Searches for email addresses, phone and credit cards numbers in browser caches. Carves pictures from system cache files. Collects files that are protected or not processed by parser.
Comprehensive - General Profiling speed optimized	Runs all Artifact Captures, collects allocated, embedded, and deleted pictures, videos, and frames from videos over 500MB and Office Documents using the Thorough Identification for Files Without Extensions. Carves pictures from system cache files. Collects Registry files, searches for anti-forensics applications, remote access traces, social media traces, files in the Skype caches and collects user Desktop shortcuts. Collects protected files and files not processed by parser.
Comprehensive - General Profiling	Runs all Artifact Captures, collects allocated, embedded, and deleted pictures and videos and frames from videos over 500MB and Office documents, carves pictures from system cache files. Collects Registry files, searches for anti-forensics applications, remote access traces, social media traces, files in the Skype caches and collects user Desktop shortcuts. Collects protected files and files not processed by parser.
Comprehensive - Collect Pictures from Free Space	Searches Unallocated Clusters for Deleted Pictures.

Comprehensive - Child Exploitation speed optimized	Runs all Artifact Captures, collects allocated, embedded, and deleted pictures and videos and frames from videos over 500MB, carves pictures from system cache files, searches for common Child Exploitation 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.
Comprehensive - Child Exploitation	Runs all Artifact Captures, collects allocated, embedded, and deleted pictures and videos and frames from videos over 500MB, carves pictures from system cache files. Searches for common Child Exploitation keywords, and searches for known hash values. Searches for anti-forensics traces, remote access traces, P2P traces and files from Skype caches. Collects protected files and files not processed by parser.

Default Captures

The table below lists the Captures that are available out-of-the-box.

Capture	Notes
APPLICATIONS > Anti-Forensics Traces	Identifies installed applications that can be used to conceal user's activity.
APPLICATIONS > Application Permissions	Identifies permissions used by installed applications
APPLICATIONS > Application Usage	Collects applications' usage information for all the users of the targeted Operating Systems.
APPLICATIONS > Cloud Storage Traces	Keyword search (Regex) for traces of Cloud storage and installations.
APPLICATIONS > Cryptocurrency Traces	Keyword search (Regex) for traces of cryptocurrency installations and wallets.
APPLICATIONS > Installed Applications	Collects the list of installed applications on the targeted Operating Systems.
APPLICATIONS > P2P Files Shared or Downloaded	Collects the list of files shared and downloaded on Peer-to-Peer networks.
APPLICATIONS > P2P Search Terms	Collects the list of search terms found in Peer-to-Peer applications.
APPLICATIONS > P2P Traces	Keyword search (substring) for installations of P2P applications.
APPLICATIONS > Remote Access Traces	Keyword search (substring) for installations of remote computer access applications.
APPLICATIONS > Screen Recordings and Screenshots	Offers an interface to collect screenshots from mobile devices and process them for text extraction.
APPLICATIONS > Shareaza GUID's	Keyword search (Regex) for Shareaza GUID's. Max file size 100MB.

APPLICATIONS > Social Media Traces	Keyword search (RegEx) for traces of the most popular social media sites and activity.
APPLICATIONS > VM Traces	Keyword search (RegEx) for traces of virtual machine applications
APPLICATIONS > VPN Traces	Keyword search (RegEx) for traces of VPNs
CHILD EXPLOITATION > CE Encrypted Archive Hash Set	A targeted search for password-protected archive files matching hashes of known CSAM material
CHILD EXPLOITATION > CE Hash Set Comprehensive speed optimized	A targeted search for Child Exploitation (CE) pictures and videos based on a predetermined hash set. This search will identify and collect files from the entire file system including deleted files. Uses the thorough file identification method on files without extension only. Max files size 1GB.
CHILD EXPLOITATION > CE Hash Set Comprehensive Thorough ID	A targeted search for Child Exploitation (CE) pictures and videos based on a predetermined hash set. This search will identify and collect files from the entire file system including deleted files. Max files size 1GB.
CHILD EXPLOITATION > CE Hash Set In User Profiles	A targeted search for Child Exploitation (CE) pictures and videos based on a predetermined hash set. This search will identify and collect files from the User profiles. Max files size 1GB.
CHILD EXPLOITATION > CE Hash Set without File Sizes	A targeted search for Child Exploitation (CE) pictures and videos based on a predetermined hash set. This search will identify and collect files from the entire file system including deleted files. Note that this set is different from the “CE Hash Set Comprehensive” Capture and it does not contain file sizes so it takes longer to scan. Max files size 1GB.
CHILD EXPLOITATION > Keywords Comprehensive speed optimized	A targeted keyword search (RegEx) of documents, internet files, and text files that will identify terms associated with Child Exploitation (CE) and collect the files that contain them. Uses the thorough file identification method on files without extension only. Max files size 250MB.
CHILD EXPLOITATION > Keywords Comprehensive Thorough ID	A targeted keyword search (RegEx) of documents, internet files, and text files that will identify terms associated with Child Exploitation (CE) and collect the files that contain them. Max files size 250MB.
CHILD EXPLOITATION > Keywords in Filenames	A targeted keyword search (substring) of file and folder names and artifacts from other captures, that will identify terms associated with Child Exploitation (CE) and collect the files that contain them.
CHILD EXPLOITATION > Keywords in User Profiles	A targeted keyword search (RegEx) of documents, internet files, and text files in the users profiles, that will identify terms associated with Child Exploitation (CE) and collect the files that contain them. Max files size 250MB.

COMMUNICATION > Apple Lockdown Files collection	Collects iOS devices lockdown files to allow pairing with devices from a different computer. Max files size 100MB.
COMMUNICATION > Calls	Collects calls metadata from a variety of applications.
COMMUNICATION > Emails	Collects individual emails from a variety of email client applications.
COMMUNICATION > iOS MobileSync Collection	A Targeted search that collects all the files in the “MobileSyncBackup” directory if present.
COMMUNICATION > Message Board Subscriptions	Collects list of Message Board Subscriptions from Reddit.
COMMUNICATION > Messages	Collects chat and other short messages from a variety of applications. Principals and recipients will contain more information when the Saved Contacts Capture is also selected.
COMMUNICATION > Saved Contacts	Collects saved contact information from a variety of applications.
COMMUNICATION > Skype - Media_Cache Folder	A targeted search to collect all files in the Skype “Media_Cache” directory if present. Max files size 500MB.
COMMUNICATION > Skype - Received Files	A targeted search to collect all files in the Skype “my skype received files” directory if present. Max files size 500MB.
COMMUNICATION > Voicemail	Collects voicemail information
DEVICE DATA > Database Files	Collects database files between 1KB and 300MB in size including those in archives.
DEVICE DATA > Device Information	Collects general information about the connected target device.
DEVICE DATA > Encrypted Drive	Collects data from drives encrypted by Bitlocker. All drives from the target device are analyzed regardless of whether they are selected as a target or not.
DEVICE DATA > Large File Locator	A search to detect all files with a size over 1GB.
DEVICE DATA > Network Interfaces	Collects a list of network interfaces
DEVICE DATA > Network Usage	Collects recent network data
DEVICE DATA > Saved Networks	Collects a list of saved networks
DEVICE DATA > Networks Connection Activity	Collects network connection information from the targeted system.
DEVICE DATA > OS Information	Collects general information about the targeted Operating Systems.
DEVICE DATA > Paired Bluetooth Devices	Collects list of Paired Bluetooth Devices.
DEVICE DATA > Plist Files	Collects plist files between 1KB and 100MB in size including those in archives.

DEVICE DATA > Terminal History	Collects the history of recent terminal commands on Mac and Windows
DEVICE DATA > USB History	Collects the history of all USB devices plugged into the targeted system.
DEVICE DATA > Virtual Disk Locator	Keyword targeted search (RegEx) that identifies Virtual Machine files.
DEVICE DATA > Windows Registry Files	Collects NTUSER.DAT, SYSTEM, SOFTWARE, SAM and SECURITY Registry files. This may also capture files with the same file names from the MAC OS.
DEVICE DATA > Windows.edb Search Database	Collects the Windows.edb file with a file size of 1MB -10GB.
DOCUMENTS > Office Documents Comprehensive - speed optimized	A comprehensive search that will identify and collect documents between 10KB and 50MB, including those in archives and those recently deleted. Uses the thorough file identification method on files without extension only.
DOCUMENTS > Office Documents Comprehensive thorough ID	A comprehensive search that will thoroughly identify and collect documents between 10KB and 50MB, including those in archives and those recently deleted.
DOCUMENTS > Office Documents in User Profiles	A targeted search of the user profiles that will identify and collect documents between 10KB and 50MB, including those in archives.
DOCUMENTS > Referenced Files	Collects all files referenced by another artifact such as email attachments, files shared via chat messages, downloaded files, downloaded P2P files, and recently accessed files.
HEALTH DATA > Health Metrics	Collects health metric data stored on target device
HEALTH DATA > Health Profiles	Collects a list of health profile data stored on target device
INTEL KEYWORDS > BIN Numbers in Browser Cache	A targeted keyword search (RegEx) of potential credit/debit card numbers with common US BIN numbers
INTEL KEYWORDS > Chemical and Biological	A targeted keyword search (RegEx) of documents, internet files, and text files that will identify chemical and biological terms and collect those files. Max file size 250MB.
INTEL KEYWORDS > Chemical and Biological - Arabic	A targeted Arabic keyword search (RegEx) of documents, internet files, and text files that will identify chemical and biological terms and collect those files. Max file size 250MB.
INTEL KEYWORDS > Chemical and Biological - Russian	A targeted Russian keyword search (RegEx) of documents, internet files, and text files that will identify chemical and biological terms and collect those files. Max file size 250MB.
INTEL KEYWORDS > Chemical and Biological - Urdu	A targeted Urdu keyword search (RegEx) of documents, internet files, and text files that will identify chemical and biological terms and collect those files. Max file size 250MB.

INTEL KEYWORDS > Domestic Security	A targeted keyword search (RegEx) of documents, internet files, and text files that will identify domestic security terms and collect the files that contain them. Max file size 250MB.
INTEL KEYWORDS > Email Addr-US Phone-CC in Browser Cache	A targeted keyword search (RegEx) of documents, internet files, and text files in the browser cache that will identify email addresses, US phone numbers, and CC numbers and collect the files that contain them. Max file size 250MB.
INTEL KEYWORDS > Explosive Precursors	A targeted keyword search (RegEx) of documents, internet files, and text files that will identify Explosive Precursor terms and collect the files that contain them. Max file size 250MB.
INTEL KEYWORDS > Financial Fraud Traces	A targeted keyword search (RegEx) of documents, internet files, and text files that will identify financial fraud terms and collect the files that contain them. Max file size 250MB.
INTEL KEYWORDS > Infrastructure Security	A targeted keyword search (RegEx) of documents, internet files, and text files that will identify infrastructure security terms and collect the files that contain them. Max file size 250MB.
INTEL KEYWORDS > Terrorism	A targeted keyword search (RegEx) of documents, internet files, and text files that will identify terrorism terms and collect the files that contain them.
INTEL KEYWORDS > US Agencies	A targeted keyword search (RegEx) of documents, internet files, and text files that will identify US agencies and collect the files that contain them. Max file size 250MB.
LOCATION DATA > Location History	Collects a timeline of locations a device was detected
LOCATION DATA > Saved Locations	Collects a list of saved locations on devices
LOCATION DATA > Searched Locations	Collects locations searched on maps applications
LOCATION DATA > Trip History	Collects trips created on maps applications
LOCATION DATA > Wi-Fi Locations	Collects wifi locations seen by a target device
MULTIMEDIA > Audio Files	Collects audio files, between 1KB and 2GB in size from all locations on the target including from within containers.

MULTIMEDIA > Collect Deleted Pictures from Unallocated Clusters	Collects picture files after carving them from the unallocated space of the targeted systems. Carves pictures from system cache files. Max file size 250MB.
MULTIMEDIA > Pictures - with EXIF Data	A targeted search that collects picture files containing camera brand in their EXIF data. Carves pictures from system cache files. Max file size 250MB.
MULTIMEDIA > Pictures - with GPS Location Data	A targeted search that collects picture files containing GPS location data. Carves pictures from system cache files. Max file size 250MB.
MULTIMEDIA > Pictures Comprehensive - speed optimized	Collects picture files from common picture storage folders and the rest of the drive. It collects allocated, recently deleted and pictures from within containers. Carves pictures from system cache files. Uses the thorough file identification method on files without extension only. Max file size 250MB.
MULTIMEDIA > Pictures Comprehensive Thorough ID no carving	Collects picture files from common picture storage folders and the rest of the drive. It collects allocated, recently deleted and pictures from within containers. Carves pictures from system cache files. Max file size 250MB.
MULTIMEDIA > Pictures comprehensive Thorough ID with carving	Collects picture files from common picture storage folders and the rest of the drive. It collects allocated, recently deleted, carved from unallocated and pictures from within containers. Carves pictures from system cache files. Max file size 250MB.
MULTIMEDIA > Pictures and Videos under 500MB Thorough ID	Collects picture files and video files (under 500MB) from common picture storage folders and the rest of the drive. It collects allocated, recently deleted and pictures/videos from within containers using thorough file identification. Carves pictures from system cache files.
MULTIMEDIA > Pictures and Videos under 500MB in User Profiles	A targeted search that collects picture files and video files (under 500MB) from user profiles. It collects allocated, recently deleted and pictures/videos from within containers using thorough file identification on files without extension only. Carves pictures from system cache files.
MULTIMEDIA > Pictures and Videos under 500MB speed optimized	Collects picture files and video files (under 500MB) from common picture storage folders and the rest of the drive. It collects allocated, recently deleted and pictures/videos from within containers using thorough file identification on files without extension only. Carves pictures from system cache files.
MULTIMEDIA > Pictures in Cache	A targeted search that collects pictures files from browser cache, including archives, using thorough file identification. Carves pictures from system cache files. Max file size 250MB.
MULTIMEDIA > Pictures in User Profiles	A targeted search that collects pictures files from user profiles, including archives, using thorough file identification. Carves pictures from system cache files. Max file size 250MB.
MULTIMEDIA > Videos All - Comprehensive Thorough ID	Collects all videos irrespective of size, using thorough file identification. It collects video files from archives, the entire file system, and recently deleted files.
MULTIMEDIA > Videos over 500MB - Comprehensive Frames speed opt	Collects frames from videos over 500MB, using thorough file identification on files without extension only. It processes video files from archives, the entire file system, and recently deleted files.

MULTIMEDIA > Videos over 500MB - Comprehensive Frames Thorough	Collects frames from videos over 500MB, using thorough file identification. It processes video files from archives, the entire file system, and recently deleted files.
MULTIMEDIA > Videos over 500MB - Frames in Browser Cache	A targeted search that collects frames from videos over 500MB, using thorough file identification on files without extension only. It processes video files from archives that are located in common Browser cache folders.
MULTIMEDIA > Videos over 500MB - Frames in User Profiles	A targeted search that collects frames from videos over 500MB, using thorough file identification on files without extension only. It processes video files from archives that are located in user profiles folders.
MULTIMEDIA > Videos under 500MB - Comprehensive speed optimized	A targeted search that collects allocated and recently deleted videos, less than 500MB, using thorough file identification on files without extension only.
MULTIMEDIA > Videos under 500MB - Comprehensive Thorough ID	A targeted search that collects allocated and recently deleted videos, less than 500MB, using thorough file identification.
MULTIMEDIA > Videos under 500MB - Frames in Browser Cache	A targeted search that collects frames from videos in the browser cache, less than 500MB, using thorough file identification on files without extension only.
MULTIMEDIA > Videos under 500MB - Frames in User Profiles	A targeted search that collects frames from videos in the users profiles, less than 500MB, using thorough file identification on files without extension only.
USER DATA > Calendar	Collects calendar entries.
USER DATA > Clipboard History	Collects recent clipboard content found on a target device
USER DATA > Cloud Files	Collects records of files which exist(ed) on the filesystem that potentially have online backups via cloud storage solutions
USER DATA > Desktop Shortcut Files	Collects link (lnk) files found on the users' Desktops.
USER DATA > Financial Transactions	Collects financial transactions.
USER DATA > Notes	Collects individual notes.
USER DATA > Notifications	Collects notifications received on devices
USER DATA > Recent Files	Identifies files that have been accessed recently by the users from the targeted system.
USER DATA > Reminders	Collects reminders on devices
USER DATA > User Accounts	Collects user information and login data from the targeted Operating Systems.
USER DATA > User Logins	Collects user login and logoff events from the targeted Operating Systems.

USER DATA > Voice Memos	Collects voice memos saved on devices
WEB BROWSERS > Bookmarks	Collects bookmarks saved by various web browsers.
WEB BROWSERS > Browser Cache	Collects files from the various browser caches.
WEB BROWSERS > Browsing History	Collects the list of URLs saved by various web browsers.
WEB BROWSERS > Download History	Collects downloaded files metadata and tries to locate them on the targeted system.
WEB BROWSERS > Extensions	Collects extensions on web browsers
WEB BROWSERS > Form Data	Collects the form data saved by web browsers.
WEB BROWSERS > Saved Credentials	Collects logins and passwords saved by web browsers. This Capture can only run during a live Windows computer scan. It is highly recommended to disable the anti-virus for this Capture to work.
WEB BROWSERS > Search Terms	Extracts the search terms from saved URLs.
WEB BROWSERS > Top Sites	Collects top sites saved by web browsers.
WEB BROWSERS > Session	Collects the last state of tabs from a web browser session
WEB BROWSERS > Synced Tabs	Collects cloud tabs and browser tabs synced between devices

Regular Expression Cheat Sheet

Cheatography

Regular Expressions Cheat Sheet

by Dave Child (DaveChild) via cheatography.com/1/cs/5/

Anchors	Assertions	Groups and Ranges
<code>^</code> Start of string, or start of line in multi-line pattern	<code>?=</code> Lookahead assertion	<code>.</code> Any character except new line (<code>\n</code>)
<code>\A</code> Start of string	<code>?!</code> Negative lookahead	<code>(a b)</code> a or b
<code>\$</code> End of string, or end of line in multi-line pattern	<code>?<=</code> Lookbehind assertion	<code>(...)</code> Group
<code>\Z</code> End of string	<code>?!= or ?<!</code> Negative lookbehind	<code>(?....)</code> Passive (non-capturing) group
<code>\b</code> Word boundary	<code>?></code> Once-only Subexpression	<code>[abc]</code> Range (a or b or c)
<code>\B</code> Not word boundary	<code>?()</code> Condition [if then]	<code>[^abc]</code> Not (a or b or c)
<code>\<</code> Start of word	<code>?()</code> Condition [if then else]	<code>[a-q]</code> Lower case letter from a to q
<code>\></code> End of word	<code>?#</code> Comment	<code>[A-Q]</code> Upper case letter from A to Q
Character Classes	Quantifiers	<code>[0-7]</code> Digit from 0 to 7
<code>\c</code> Control character	<code>*</code> 0 or more {3} Exactly 3	<code>\x</code> Group/subpattern number "x"
<code>\s</code> White space	<code>+</code> 1 or more {3,} 3 or more	Ranges are inclusive.
<code>\S</code> Not white space	<code>?</code> 0 or 1 {3,5} 3, 4 or 5	Pattern Modifiers
<code>\d</code> Digit	Add a <code>?</code> to a quantifier to make it ungreedy.	<code>g</code> Global match
<code>\D</code> Not digit	Escape Sequences	<code>i *</code> Case-insensitive
<code>\w</code> Word	<code>\</code> Escape following character	<code>m *</code> Multiple lines
<code>\W</code> Not word	<code>\Q</code> Begin literal sequence	<code>s *</code> Treat string as single line
<code>\x</code> Hexadecimal digit	<code>\E</code> End literal sequence	<code>x *</code> Allow comments and whitespace in pattern
<code>\O</code> Octal digit	"Escaping" is a way of treating characters which have a special meaning in regular expressions literally, rather than as special characters.	<code>e *</code> Evaluate replacement
POSIX		<code>U *</code> Ungreedy pattern
<code>[[:upper:]]</code> Upper case letters	Common Metacharacters	<code>*</code> PCRE modifier
<code>[[:lower:]]</code> Lower case letters	<code>^</code> [. \$	String Replacement
<code>[[:alpha:]]</code> All letters	{ * (\	<code>\$n</code> nth non-passive group
<code>[[:alnum:]]</code> Digits and letters	+) ?	<code>\$2</code> "xyz" in <code>/^(abc(xyz))\$/</code>
<code>[[:digit:]]</code> Digits	< >	<code>\$1</code> "xyz" in <code>/^(?:abc)(xyz)\$/</code>
<code>[[:xdigit:]]</code> Hexadecimal digits	The escape character is usually <code>\</code>	<code>\$'</code> Before matched string
<code>[[:punct:]]</code> Punctuation	Special Characters	<code>\$'</code> After matched string
<code>[[:blank:]]</code> Space and tab	<code>\n</code> New line	<code>\$+</code> Last matched string
<code>[[:space:]]</code> Blank characters	<code>\r</code> Carriage return	<code>\$&</code> Entire matched string
<code>[[:cntrl:]]</code> Control characters	<code>\t</code> Tab	Some regex implementations use <code>\</code> instead of <code>\$</code> .
<code>[[:graph:]]</code> Printed characters	<code>\w</code> Vertical tab	
<code>[[:print:]]</code> Printed characters and spaces	<code>\f</code> Form feed	
<code>[[:word:]]</code> Digits, letters and underscore	<code>\xxx</code> Octal character xxx	
	<code>\xhh</code> Hex character hh	