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		
ADFPRO Mobile & Computer Triage	DEI Digital Evidence Investigator	MDI 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:

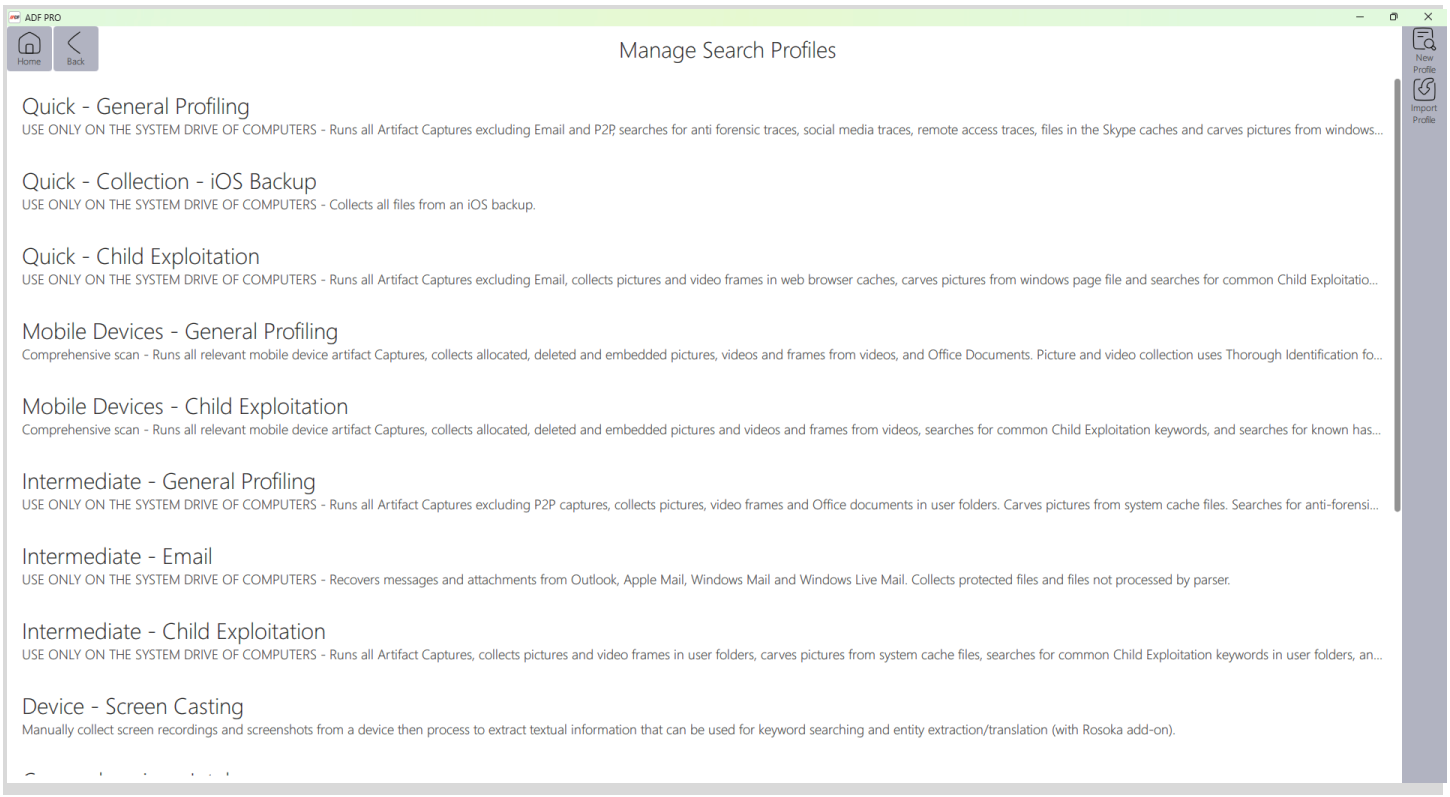
1. It makes starting a scan simple and fast.
2. It makes it possible to share the Search Profiles with other users who need to work on similar investigations. The same Search Profiles can be shared across all the ADF products.

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** > **Scan Setup & 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.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.



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.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

The following actions are offered on the selected Search Profile:

 Export	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. The exported profile keeps the name of the whitelist: where the profile is imported, a whitelist with the same name has to exist, otherwise the profile is shown as Invalid. References inconsistent whitelists.
 Delete	To delete the user-created Search Profile. It is possible to undo this action for 15 seconds. This action does not delete that Search Profile's Captures.
 Copy	To copy the Search Profile and immediately edit it.
 Edit	To edit the user-created Search Profile. It is not possible to edit a default Search Profile but it can be copied then edited.

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; and the Message Threads Capture, which needs the Messages Capture: selecting Message Threads also selects Messages, and deselecting Messages also deselects Message Threads. Selecting Saved Contacts resolves the communication participants' names

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

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 based on following 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 file size ranges of Capture A and B overlap, AND
- For keyword searches, both Captures search the file content and metadata.

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 between 10 seconds and 120 minutes and select minutes or seconds. By default files are skipped after one hour. Any value entered overrides default.
      ii. **Collect skipped files (max 2GB)**: collects files less than 2GB that were skipped for taking too long to process. These files can be found in the Scan Log view of the scan result by filtering records with Type=”Parser timeout”.
      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 the parsers (max 2GB)**: this copies the files whose processing crashed the parser. These files can be found in the Scan Log view of the scan result by filtering records with Type=”Parser crash”.
      v. **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 (ADFPRO Mobile & Computer Triage DEI).
      vi. **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).
      vii. **Automatically start Entity extraction when scan finishes:** to enable entity extraction**,** simply check this checkbox.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

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 3 seconds by pressing the UNDO button .

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

Creating a Whitelist 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 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 Whitelist from CSV

To create a whitelist from a CSV file:

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 40 character hexadecimal 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 incorrectly formatted lines. 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.



Providing the file size for every hash value greatly improves the performance when using whitelists.

Creating a Whitelist 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. In the Import Options dialog, select the categories (0 to 10) to import and click on the **OK** button. The hash values of the other categories, and those without a category, are not imported.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

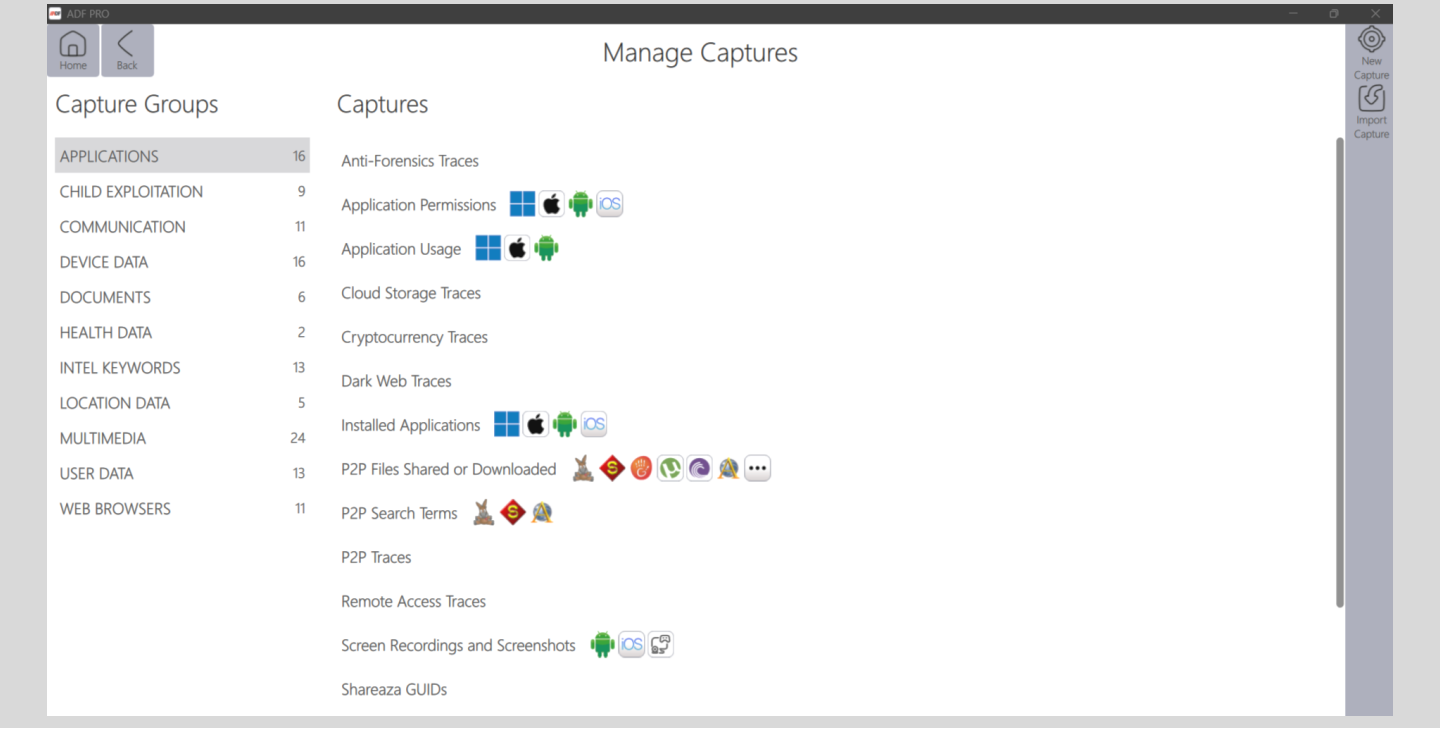
4. A message will be displayed showing the status of the whitelist creation. Any errors that occurred during the whitelist creation are displayed, such as incorrectly formatted records. Click the **OK** button to continue.
5. A default name is given to the whitelist which can be modified immediately 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. To import a whitelist, copy its database file into the whitelists folder: it is listed the next time the Options screen of a Search Profile is opened. The location where the whitelists are saved is defined in the Data Paths section of 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.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

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.

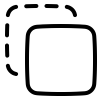
The right-hand side function toolbar offers the following actions:

 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: a confirmation lists them, and once it is confirmed the deletion cannot be undone. When no other Search Profile uses the Capture, it is possible to undo this action for 15 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.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

 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.
 Expand	To show the description of the Capture and all the applications it supports. Note that a detailed list of supported applications can be found in Technical Specifications.

Creating a new Capture

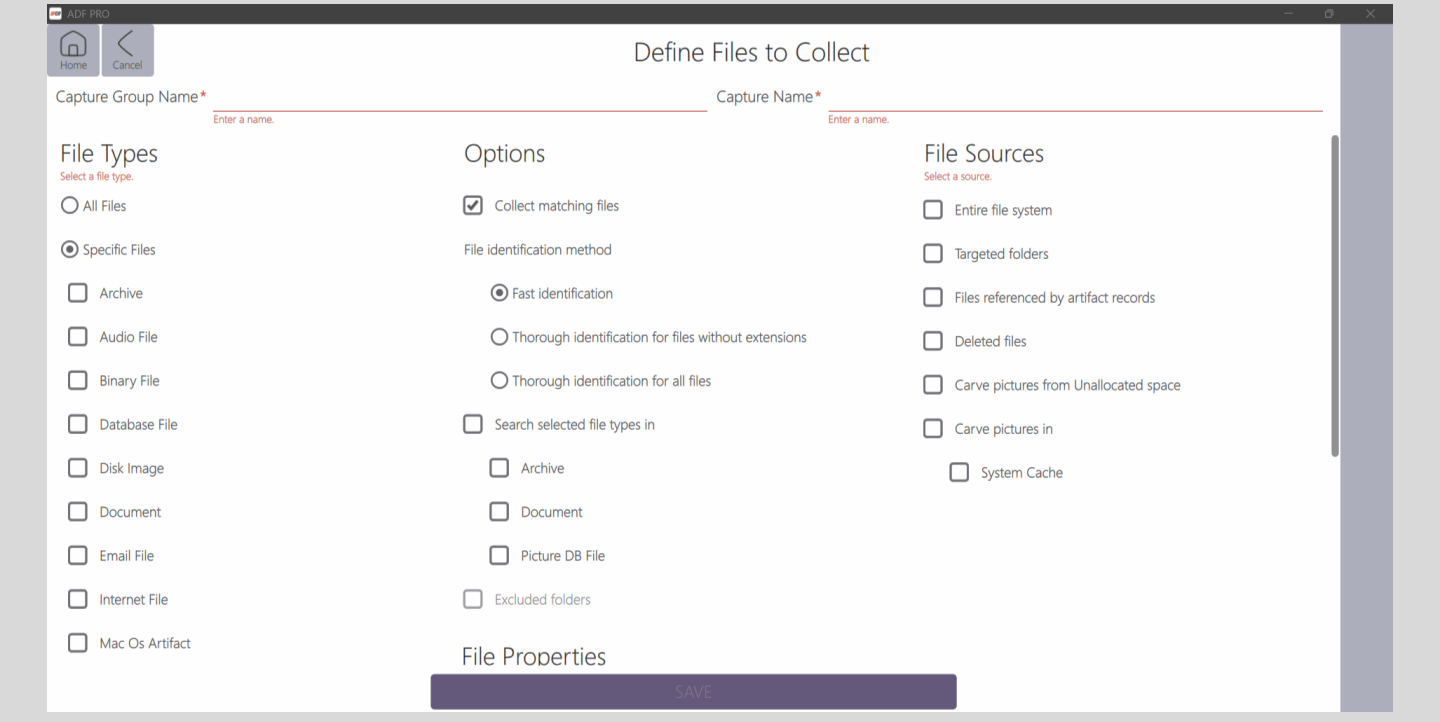
To create a new file Capture follow these instructions:

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 files by hash value: Search for files using MD5 or SHA1 hash values.
    d. Search for visual similarities: Searches for pictures visually similar to ones provided by the user, using PhotoDNA.
3. Read the paragraphs below that describe how to continue the creation of each type of file Capture.
4. When the file Capture is created from the Define Search Profile screen, 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.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.



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**: a copy of the original files is saved in the scan result. The matching files are processed whether this option is selected or not (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. **Archive**: searches for all selected file types within archives such as zip, tar and other containers.
        ii. **Document**: searches for all selected file types embedded within Document file types.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

iii. **Picture DB File**: searches for all selected file types within Windows thumbcache and thumbs.db files and Apple ithmb 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.
- **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.

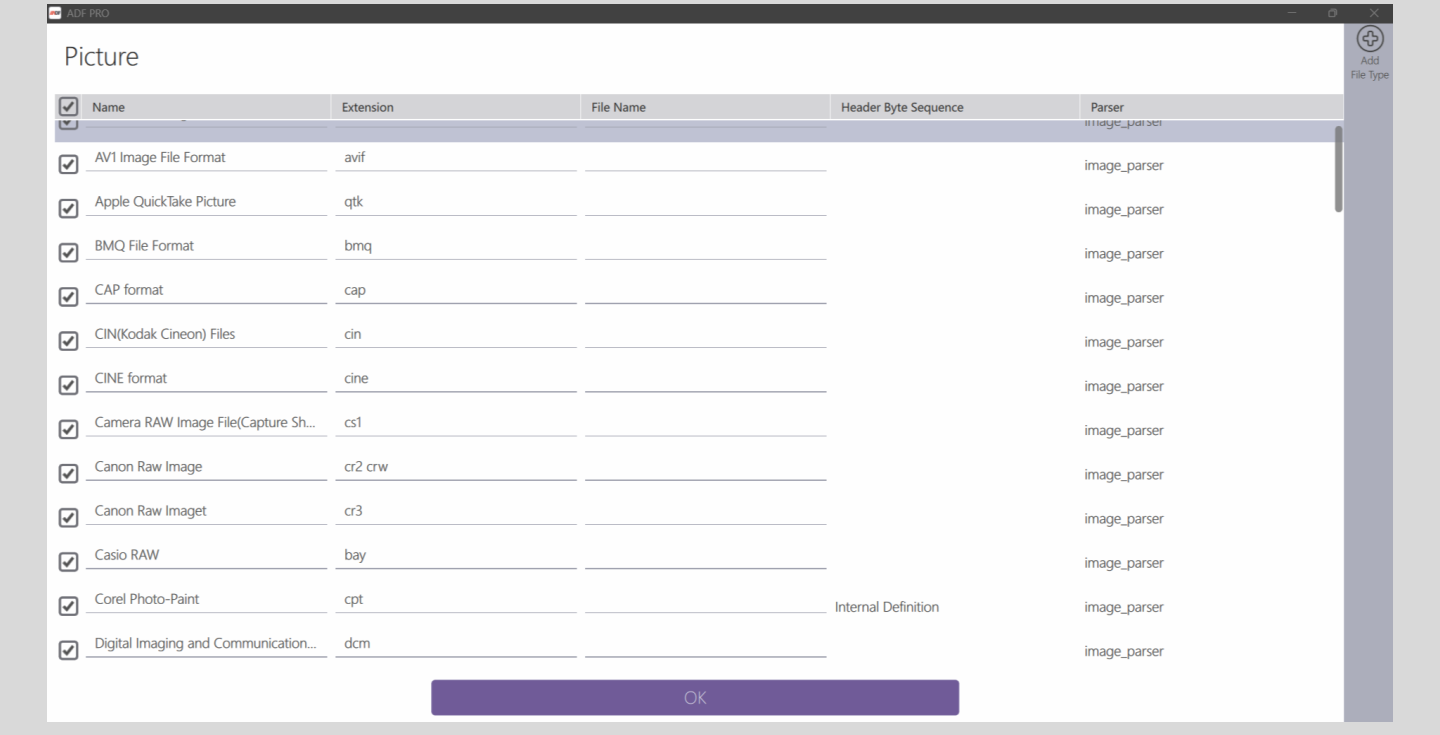
The picture formats that can be carved are listed here. The following rules are used to identify the file size:

- 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 computes the file size from the file structure (the farthest data referenced in a TIFF file, the lengths of the sections of a PSD file), without size limit. PSD files with ZIP-compressed image data are not carved.
- 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.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.



Here are the instructions to create a new file type:

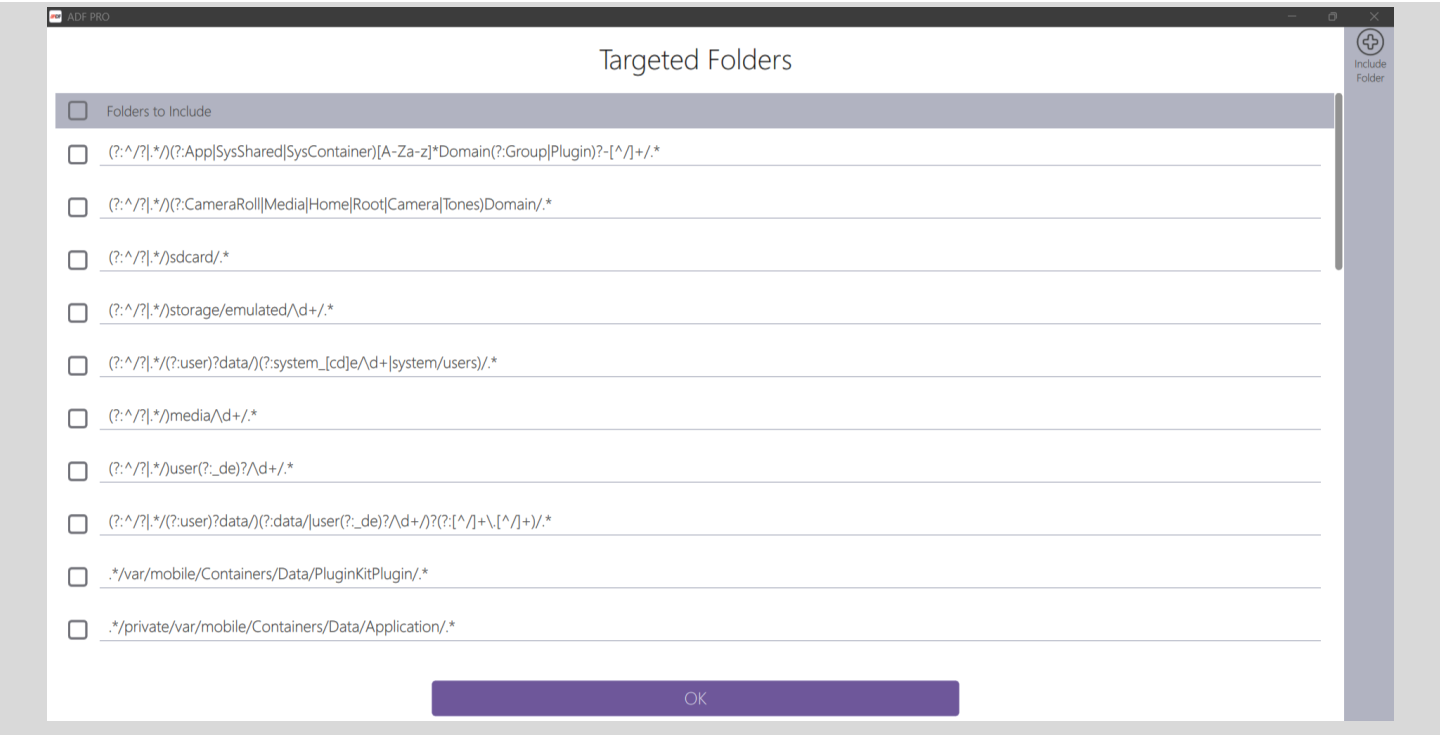
1. Within the **File Types** section click on the **View** button on any file type group.
2. On the file type screen click the **Add File Type** button of the functional toolbar to add a new file type.
3. There are three options available to identify a file: **Extension**, **File Name** and **Header 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: type the name without its extension and without wildcards. It is possible to add multiple file names by separating them by a space. A file matches when its name without the extension is the same (not case sensitive) and, if extensions are entered, its extension is one of them; without an extension entered, only files without an extension match. With a Thorough identification method, a file type recognized from the file content takes precedence.
    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. The header byte sequence is only checked by Thorough identification for all files, and by Thorough identification for files without extensions on the files that have no extension.
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.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

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.

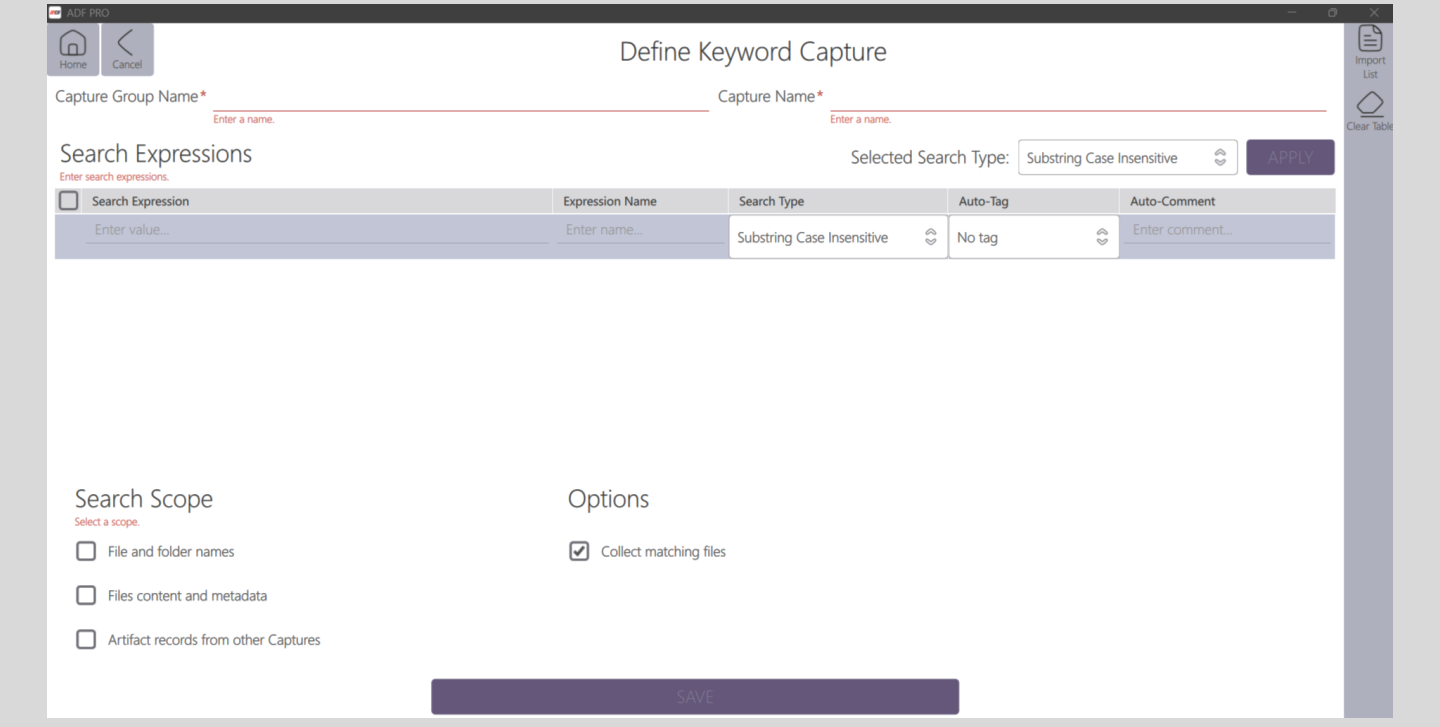


The targeted folders are common to all the Captures and modifying a targeted folder path modifies it for all the Captures using it.

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.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.



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

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

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 Selected 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 name column: titled “name” with the Expression Name of the keyword, no longer than 200 characters.
        v. 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
        vi. Example:

```
keyword, auto-tag, auto-comment, search type
kw1, , , 0
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, as Substring Case Insensitive, whatever the**Selected Search Type**. A line with an empty search type value is skipped.A value that contains a comma must be enclosed in double quotes, with no spaces between the quotes and the separating commas. For example, the regular expression a{2,3} is written as “a{2,3}”.
    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 the whole path of each file, as shown in the Path column, including its file name. An expression can therefore match both a folder and a file name, and a keyword found in a folder name matches that folder and every file below it.
    b. **Files 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:

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

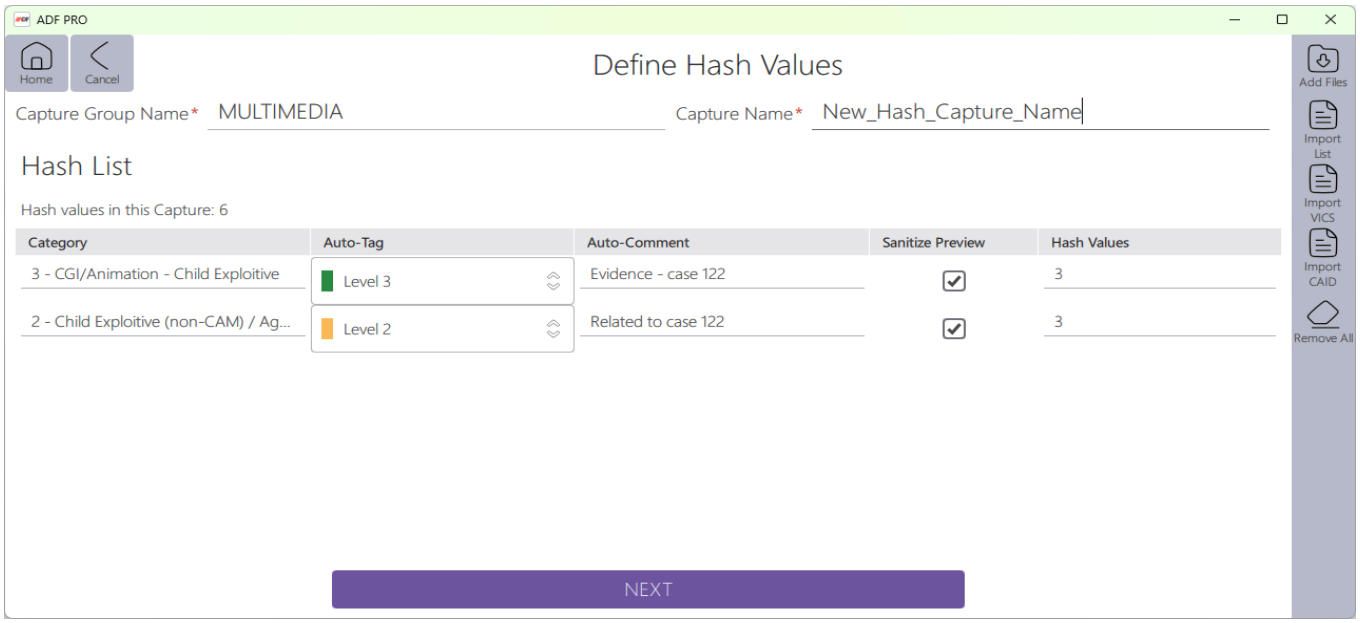
i. The **Carve pictures from unallocated space** and **Carve pictures in** options are not offered.
ii. The **Collect matching files** option is set on the **Define Keyword Capture** screen (see Options below).

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.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

 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, a comment and a category to the matching record by setting those up in the **Assign Tags and Comments** dialog. There is a **Sanitize Previews** option in the dialog; if checked, the previews of the matched records will be pixelated in the viewer. Note that if the hash value of a file is already in the Capture, its tag, comment and Sanitize Previews option are replaced with the new ones, even when these are left empty, and so is its category when one is entered.
    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” for 40 character hexadecimal SHA1 values.
        ii. Optional file size column: titled “file size” 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. Optional sanitize preview column: titled “sanitize preview” with values “true” or “false”.
        vi. Example:

```
sha1, file size, auto-tag, auto-comment, sanitize preview
5219e8be8201c9f90ddef72144797582d97c0016, 69223, 1, Related to case 122, true
f2965b27cd2d0e5ebb3d48afa9b904152b42f0b7, 6659, 1, Related to case 122, true
d22cfd4ed85d7b90f145b98a28397970cffa6987, 923120, 2, Related to case 122, false
```

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

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. There is a **Sanitize Previews** option in the dialog when the file has no “sanitize preview” column; if checked, the previews of the matched records will be pixelated in the viewer. If the file has an “auto-tag” or “auto-comment” column but no “sanitize preview” column, the application asks: “Do you want the file previews for hash-matched items to be sanitized in the viewer?” Click Yes to have the previews of the matched records pixelated in the viewer.

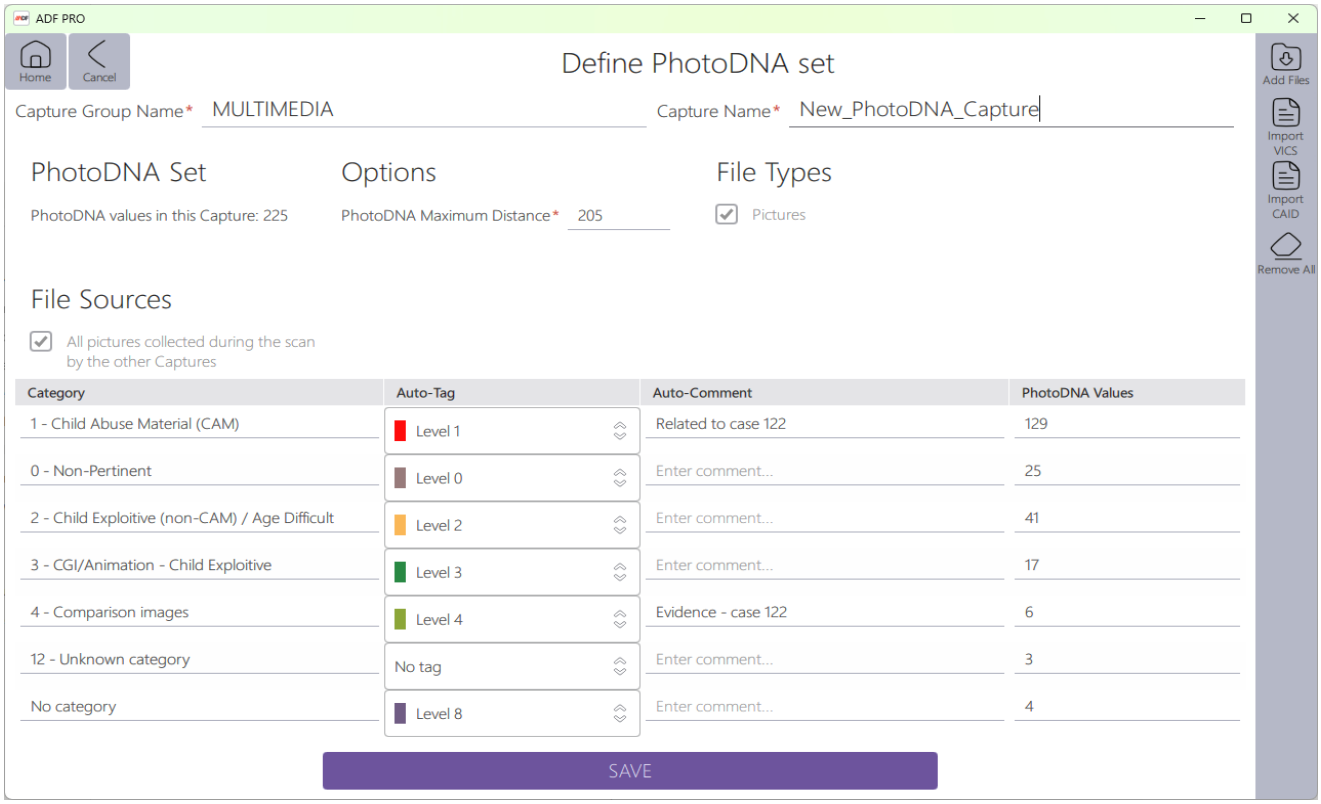
c. **Import VICS**: this will bring up a Windows File Selector to select the VICS file. The file is first scanned for the categories it contains: each category then shows its number of records, and the categories that are not in the file cannot be selected (SKIP SCAN stops the scan and keeps all the categories, without their numbers of records). Then select which VICS categories should be imported. Each hash value from that category is assigned a tag with the same number (for the records without a category, or with a category number above 9, choose the tag in the Auto-Tag column) and it is possible to enter a comment that will be assigned automatically to the matching file. Select "Include Hash Comments" to also assign comments found in the VICS file. The Sanitize Preview column is checked for every category by default, so the previews of the matched records are pixelated in the viewer; uncheck it to keep the previews unsanitized.
d. **Import CAID**: this will bring up a Windows File Selector to select the CAID file. The file is first scanned for the categories it contains: each category then shows its number of records, and the categories that are not in the file cannot be selected (SKIP SCAN stops the scan and keeps all the categories, without their numbers of records). Then select which CAID categories should be imported. Each hash value from that category is assigned a tag with the same number (for the records without a category, or with a category number above 9, choose the tag in the Auto-Tag column) and it is possible to enter a comment that will be assigned automatically to the matching file. Select "Include Hash Comments" to also assign comments found in the CAID file. The Sanitize Preview column is checked for every category by default, so the previews of the matched records are pixelated in the viewer; uncheck it to keep the previews unsanitized.
e. The table below the number of hash values has one row for each combination of Category, Auto-Tag, Auto-Comment and Sanitize Preview, with its number of Hash Values. Hash values added later with the same combination join its row. A change in a row applies to all its hash values: type a new category or comment and press Enter or click elsewhere, choose another tag from the drop-down list, or click the Sanitize Preview cell to switch it on or off. To delete a row with all its hash values, mouse-over it and click the **Delete** button at its right end: the row is deleted at once, without confirmation. The hash values added without a category, tag, comment or Sanitize Preview share the last row, which shows “No metadata” in its Auto-Comment column.
f. When all the hash values have been added, click on the **NEXT** button.
g. The **Define Files to Hash** screen offers the same options as the Define Files to Collect screen described above.
h. Click on the **SAVE** button to finish the Capture creation.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

Providing the file size for every hash value greatly improves the performance of hash value searches: a file whose size matches none of the hash values is then not hashed at all. Add Files records the sizes automatically; in a CSV file, use the “file size” column; VICS and CAID imports take the size from the MediaSize value of each record, when present. If even one hash value in the Search Profile has no file size, every file has to be hashed.

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.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

 Import VICS	To import PhotoDNA values from a VICS file (JSON format).
 Import CAID	To import PhotoDNA values from a CAID file (JSON format).
 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. It is also possible to automatically assign a tag, a comment and a category to the matching pictures by setting those up in the **Assign Tags and Comments** dialog. Only the pictures in the supported formats are processed: jpg, jpeg, jpe, jif, png, gif, bmp, tif and tiff (first page only), webp, psd, tga, targa, jp2, j2k, j2c, pcx and xpm.
    b. **Import VICS and Import CAID**: as for a hash value Capture, without the Sanitize Preview option. The records without a PhotoDNA value are skipped.
7. **PhotoDNA Maximum Distance**: the pictures with a PhotoDNA Distance at or below this value are included in the Capture, and receive the tag and comment of the closest PhotoDNA value, if it has any. Lower distances mean higher visual similarity: 0 is an exact match, and 205, the default and highest value, is the industry match threshold.
8. The table below the PhotoDNA Set, Options, File Types and File Sources sections has one row for each combination of Category, Auto-Tag and Auto-Comment, with its number of PhotoDNA Values. PhotoDNA values added later with the same combination join its row. A change in a row applies to all its PhotoDNA values: type a new category or comment and press Enter or click elsewhere, or choose another tag from the drop-down list. To delete a row with all its PhotoDNA values, mouse-over it and click the **Delete** button at its right end: the row is deleted at once, without confirmation. The PhotoDNA values added without a category, tag or comment share the last row, which shows “No metadata” in its Auto-Comment column.
9. Click on the **SAVE** button to finish the Capture creation.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.



A Visual Similarities (PhotoDNA) Capture only works on pictures processed 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 carves pictures from windows page file.
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 windows page file 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 - Logical	USE ON AN EXTRACTION TAKEN FROM THE PHONE, FROM iTUNES OR FROM AN ANDROID BACKUP - Comprehensive scan - Runs all relevant mobile device artifact Captures, collects allocated, deleted and embedded pictures, videos and frames from videos, and Office Documents. Pictures and videos up to 500MB are collected from across the whole extraction, and pictures are also carved from system cache files; for videos over 500MB only frames are extracted and the video itself is not collected. Searches for Remote Access, Cryptocurrency and Dark Web Traces, audio files, database, text files, plist files and referenced files. Collects protected files.
Mobile Devices - General Profiling - FFS	USE ON A FULL FILE SYSTEM OR PHYSICAL EXTRACTION - Comprehensive scan - Runs all relevant mobile device artifact Captures, collects allocated, deleted and embedded pictures and videos, and Office Documents. Picture and video collection uses Thorough Identification for all files, is targeted to the folders where user data is stored, and carves pictures from unallocated space. Operating system files, app install packages and the caches of streaming and music apps are skipped. Searches for Remote Access, Cryptocurrency and Dark Web Traces, audio files, database, text files, plist files and referenced files. Collects protected files. If the extraction came from the phone itself, from iTunes or from an Android backup, use the Logical profile instead or media will be missed.
Mobile Devices - Child Exploitation - Logical	USE ON AN EXTRACTION TAKEN FROM THE PHONE, FROM iTUNES OR FROM AN ANDROID BACKUP - Comprehensive scan - Runs all relevant mobile device artifact Captures, collects allocated, deleted and embedded pictures and videos and frames from videos, searches for common Child Exploitation keywords, and searches for known hash values using the Thorough Identification option for files without extensions. Pictures and videos up to 500MB are collected from across the whole extraction, and pictures are also carved from system cache files; for videos over 500MB only frames are extracted and the video itself is not collected.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

	Searches for Remote Access, Cryptocurrency and Dark Web Traces, audio files, database, plist files and referenced files. Collects protected files.
Mobile Devices - Child Exploitation - FFS	USE ON A FULL FILE SYSTEM OR PHYSICAL EXTRACTION - Comprehensive scan - Runs all relevant mobile device artifact Captures, collects allocated, deleted and embedded pictures and videos, searches for common Child Exploitation keywords, and searches for known hash values using the Thorough Identification option for files without extensions. Picture and video collection uses Thorough Identification for all files, is targeted to the folders where user data is stored, and carves pictures from unallocated space. Operating system files, app install packages and the caches of streaming and music apps are skipped. Searches for Remote Access, Cryptocurrency and Dark Web Traces, audio files, database, plist files and referenced files. Collects protected files. If the extraction came from the phone itself, from iTunes or from an Android backup, use the Logical profile instead or media will be missed.
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.
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.
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.
External Devices - General Profiling	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.
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.
Device - Screen Casting	Manually collect screen recordings and screenshots from a device then process to extract textual information that can be used for keyword searching and entity extraction/translation (with Rosoka add-on).

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

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.
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.
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.
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.
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.

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	This artifact capture collects the device permissions associated with applications on target devices (e.g. access to storage, photos, internet, etc.)
APPLICATIONS > Application Usage	This artifact capture collects the application usage event history by users on target devices. This can include the date/time the application was used as well as for how long
APPLICATIONS > Cloud Storage Traces	Keyword search (RegEx) for traces of Cloud storage and installations.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

APPLICATIONS > Dark Web Traces	Keyword search (RegEx) for traces of anonymity networks, dark web clients and on-disk Tor artifacts.
APPLICATIONS > Cryptocurrency Traces	Keyword search (RegEx) for traces of cryptocurrency installations and wallets.
APPLICATIONS > Installed Applications	This artifact capture collects a list of installed applications on target devices
APPLICATIONS > P2P Files Shared or Downloaded	This artifact capture collects a list of files shared and/or downloaded using Peer-to-Peer clients on target devices. (e.g. Bittorrent Classic, Bittorrent Web, uTorrent, Ares)
APPLICATIONS > P2P Search Terms	This artifact capture collects a list of search terms extracted from Peer-to-Peer clients on target devices. (e.g. Bittorrent Classic, Bittorrent Web, uTorrent, Ares)
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.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

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	This artifact capture collects the history of audio/video calls made on a variety of applications on target devices (e.g. iOS/Android Phone, WhatsApp, Telegram, etc.) It is best run in conjunction with Saved Contacts
COMMUNICATION > Emails	This artifact capture collects individual emails extracted from a variety of email clients on target devices
COMMUNICATION > iOS MobileSync Collection	A Targeted search that collects all the files in the “MobileSyncBackup” directory if present.
COMMUNICATION > Message Board Subscriptions	This artifact capture collects a list of subscriptions on message board applications on target devices (e.g. Reddit)
COMMUNICATION > Message Threads	This artifact capture collects message threads from a variety of messaging applications on target devices (e.g. Android/iOS Messages, WhatsApp, Line, Telegram, etc.) It is best run in conjunction with Saved Contacts. It will not produce any results without Messages capture being run as well
COMMUNICATION > Messages	This artifact capture collects messages/conversations from a variety of messaging applications on target devices (e.g. Android/iOS Messages, WhatsApp, Line, Telegram, etc.) It is best run in conjunction with Saved Contacts
COMMUNICATION > Saved Contacts	This artifact capture collects a list of known contact information found in a variety of applications on target devices (e.g. iOS Contacts, WhatsApp, Telegram, etc.)
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	This artifact capture collects information related to voicemails extracted from applications on target devices (e.g. iOS Voicemail)
DEVICE DATA > Database Files	Collects database files between 1KB and 300MB in size including those in archives.
DEVICE DATA > Device Information	This artifact capture collects general identifying information on target devices. This is information closely related to the physical device (e.g. phone numbers or the device model)
DEVICE DATA > Encrypted Drive	This artifact capture 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. Only run against a live windows system

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

DEVICE DATA > Large File Locator	A search to detect all files with a size over 1GB.
DEVICE DATA > Network Interfaces	This artifact capture collects a list of network interfaces and their associated data on target devices (e.g. the results of ipconfig /all)
DEVICE DATA > Network Usage	This artifact capture collects the recent data usage event statistics associated with applications on target devices. This includes the timestamps of the application's usage event as well as the amount of bytes in/out
DEVICE DATA > Saved Networks	This artifact capture collects a list of of networks that are saved on target devices
DEVICE DATA > Networks Connection Activity	This artifact capture collects the recent history of network connection events on target devices. This includes the name of the network as well as when the logged connection event took place
DEVICE DATA > OS Information	Collects general information about the targeted Operating Systems. This artifact capture collects general identifying information on the operating system installed on target devices (e.g. Windows, MacOS, Android, etc.) This information contains general properties such as the build and version of the operating system, as well as properties specific to the device such as a serial number and the user assigned name of the device
DEVICE DATA > Paired Bluetooth Devices	This artifact capture collects a list of Bluetooth devices that are either paired with or known to target devices
DEVICE DATA > Plist Files	Collects plist files between 1KB and 100MB in size including those in archives.
DEVICE DATA > Terminal History	This artifact capture collects a list of logged recently executed commands from the terminal on target devices
DEVICE DATA > USB History	This artifact capture collects a list of USB devices that were recently connected to target devices
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 250MB, 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 250MB, 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 250MB, 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.
DOCUMENTS > Text Documents Comprehensive - speed optimized	A comprehensive search that will identify and collect text files 50MB and smaller, including those in archives and those recently deleted. Uses the thorough file identification method on

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

	files without extension only.
DOCUMENTS > Text Documents Comprehensive thorough ID	A comprehensive search that will thoroughly identify and collect text files 50MB and smaller, including those in archives and those recently deleted.
HEALTH DATA > Health Metrics	This artifact capture collects recent health data of various types (e.g. Heart Rate [BPM], Step Count, Distance Walked [Meters], Flights of Stairs Climbed) including when this data was collected and the length of the collection period for each event on target devices
HEALTH DATA > Health Profiles	This artifact capture collects personally identifiable information related to health profiles on target devices (e.g. Name, Height, Weight, Sex, Birthday, Blood Type, etc.)
INTEL KEYWORDS > BIN Numbers	A targeted keyword search (RegEx) of potential credit/debit card numbers with common US BIN numbers
INTEL KEYWORDS > BIN Numbers in Browser Cache	A targeted keyword search (RegEx) in Browser Cache 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.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

LOCATION DATA > Location History	This artifact capture collects a historic list of geographical locations that target devices were located at specific times, allowing for the creation of a timeline
LOCATION DATA > Saved Locations	This artifact capture collects a list of geographical locations saved to target devices by the operating system, these are typically auto-saved as frequently visited or in other ways significant
LOCATION DATA > Searched Locations	This artifact capture collects a list of geographical locations searched on maps applications (e.g. Waze) found on target devices
LOCATION DATA > Trip History	This artifact capture collect a list of navigation trips created on maps applications (e.g. Waze trip navigating from Portland, OR, USA to Toronto, Ontario, Canada) on target devices
LOCATION DATA > Wi-Fi Locations	This artifact capture collects the geographical locations of wifi nodes detected by target devices
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.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

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 Page File	A targeted search that carves picture files from windows page 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 > Mobile Targeted Audio	Collects audio files, between 1KB and 2GB in size, from the folders on mobile devices where user data is stored, including from within containers. Excludes music and podcast applications.
MULTIMEDIA > Mobile Targeted Pictures and Videos - Thorough ID	Collects picture files and video files of any size from the folders on mobile devices where user data is stored, using thorough file identification on all files. It collects allocated, recently deleted, carved from unallocated and pictures/videos from within containers and documents. Minimum file size 4KB, minimum dimension 75 pixels. Excludes streaming, music and podcast applications.
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	This artifact capture collects entries found in calendar applications (e.g. Google Calendar, Apple Calendar) on target devices
USER DATA > Clipboard History	This artifact capture collects a list of recent clipboard content found on target devices
USER DATA > Cloud Files	This artifact capture collects records of files on target devices which exist(ed) on the filesystem

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

	that potentially have online backups via cloud storage solutions (e.g iCloud)
USER DATA > Desktop Shortcut Files	Collects link (lnk) files found on the users' Desktops.
USER DATA > Merchant Financial Transactions	This artifact capture collects records of merchant financial transactions from applications on target devices. This can assist when building a timeline of events of the user's activities and identify a user's pattern of behavior.
USER DATA > Peer Financial Transactions	This artifact capture collects peer-to-peer financial transaction records from payment applications on target devices, documenting money transfers between individuals. This can assist when building a timeline of events of the user's activities and identify a user's pattern of behaviour.
USER DATA > Notes	This artifact capture collects a list of notes from note taking applications (e.g. Apple Notes) found on target devices
USER DATA > Notifications	This artifact capture collects a list of recent notifications received on target devices
USER DATA > Recent Files	This artifact capture identifies files that have been accessed recently by the users on target devices
USER DATA > Reminders	This artifact capture collects a list of reminders from applications (e.g. Apple Reminders) on target devices
USER DATA > User Accounts	This artifact capture collects user account information (e.g. User Name, User ID, Profile Path, etc.) from target devices
USER DATA > User Logins	This artifact capture collects a list of historic user login and logoff events from the target devices
USER DATA > Voice Memos	This artifact capture collects voice memo data saved in voice memo applications (e.g. Apple Voice Memos) on target devices
WEB BROWSERS > Bookmarks	This artifact capture collects bookmarks saved by various web browsers (e.g. Chrome, Edge, Safari, Firefox, etc.) on target devices
WEB BROWSERS > Browser Cache	This artifact capture collects files from the various browser caches (e.g. Chrome, Edge, Safari, Firefox, etc.) on target devices
WEB BROWSERS > Browsing History	This artifact capture collects a list of records related to the websites previously visited by various web browsers (e.g. Chrome, Edge, Safari, Firefox, etc.) on target devices. These records contain properties such as the URL, the date of the navigation, and what browser profile was active during the navigation.
WEB BROWSERS > Download History	This artifact capture collects data related to downloaded files and their metadata from various web browsers (e.g. Chrome, Edge, Safari, Firefox, etc.) on target devices, and tries to locate them on the target devices if they are present
WEB BROWSERS > Extensions	This artifact capture collects a list of extensions found on various web browsers (e.g. Chrome, Edge, Safari, Firefox, etc.) on target devices
WEB BROWSERS > Form Data	This artifact capture collects the data saved on target devices by various web browsers (e.g. Chrome, Edge, Safari, Firefox, etc.) that is used for auto-filling forms. This data is often information that the user does not want to repeatedly type into forms such as home addresses and emails

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

WEB BROWSERS > Saved Credentials	This artifact capture collects logins and passwords saved by web browsers on target devices. 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	This artifact capture collects a list of terms that have been entered into search engines in various browsers (e.g. Chrome, Edge, Safari, Firefox, etc.) on target devices.
WEB BROWSERS > Top Sites	This artifact capture collects top sites saved by web browsers (e.g. Chrome, Edge, Safari, Firefox, etc.) on target devices. These are sites that the browser considers particularly notable, typically due to being frequently visited
WEB BROWSERS > Session	This artifact capture collects the last state of tabs from browser sessions extracted from various browsers (e.g. Chrome, Edge, Safari, Firefox, etc.) on target devices
WEB BROWSERS > Synced Tabs	This artifact capture collects data from browser tabs that are synced between devices with the same account logged in (e.g. logged in user with Chrome on a macOS device syncing tabs that are open on a separate iOS device). This is supported by various web browsers (e.g. Chrome, Edge, Safari, Firefox, etc.)

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

Regular Expression Cheat Sheet

Cheatography

Regular Expressions Cheat Sheet

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

Anchors

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

Character Classes

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

POSIX

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

Assertions

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

Quantifiers

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

Add a ? to a quantifier to make it ungreedy.

Escape Sequences

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

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

Common Metacharacters

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

The escape character is usually \

Special Characters

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

Groups and Ranges

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

Ranges are inclusive.

Pattern Modifiers

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

* PCRE modifier

String Replacement

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

Some regex implementations use \ instead of $.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.