Introduction

This guide covers how to conduct a scan to collect information from a variety of targets.

This document applies to the following applications		
ADFPRO Mobile & Computer Triage	DEI Digital Evidence Investigator	MDI Mobile Device Investigator

What can be Scanned?

The ADF application can scan a variety of data sources in multiple environments:

- Target Windows computers live or booted using a USB Collection Key.
- Target macOS/Windows computers connected to the ADF desktop application over the network.
- Attached storage devices connected to a target computer or to the ADF desktop application.
- Forensic images of storage devices with the ADF desktop application.
- Mobile devices with the ADF Desktop application.
- Logical acquisition of mobile devices with the ADF desktop application.

The **Scan** screens on the Collection Key and the ADF desktop application are very similar and the few differences will be highlighted in the paragraphs below.

Boot Scan from the Collection Key

This document applies to the following applications		
ADFPRO Mobile & Computer Triage	DEI Digital Evidence Investigator	

A scan conducted from the Collection Key after rebooting the target computer is called a boot scan. See the Rebooting a Computer guide for details on how to get started. Once the target computer boots on the Collection Key, the ADF application starts on the **Home** screen and offers the following options:

- **Scan Computer**: to scan the target computer and any attached storage devices.
- **Image Computer**: to create a forensic image as described in the Imaging a Computer guide.

Copyright ©2016-2025 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.

- **Review Scan Results**: to review scan results present on the Collection Key. This menu is not displayed if no scan results are present. See the Reviewing Scan Results guide for details.

Two USB ports are required to complete a scan, one for the Collection Key and one for the Authentication Key (unless the Collection Key has been licensed), once the scan has started the Authentication Key can be removed. A USB hub may be used in cases where the target computer only has one USB port or in case the two flash drives do not fit side by side.

Live Windows Scan from the Collection Key

This document applies to the following applications		
ADFPRO Mobile & Computer Triage	DEI Digital Evidence Investigator	

A scan conducted from the Collection Key on a running Windows computer is called a live scan.

To run a live scan insert the Collection Key and Authentication Key into USB ports upon the target computer, open a File Explorer and execute the startWindowsLiveScanner.bat file stored on the Collection Key by double clicking on it. The Collection Key can be identified with its CKY label.



Administrator privileges are required to conduct a scan with the ADF application. If the account does not have these privileges, log into another account.



The Saved Credentials Capture may be blocked if an antivirus is running. Make sure to turn it off.

Once the ADF application starts, the **Home** screen is displayed and offers the following options:

- **Scan Computer**: to scan the target computer and any attached storage devices.
- **Image Computer**: to create a forensic image as described in the Imaging a Computer guide.
- **Create RAM Dump**: to create a copy of the RAM. See the Creating RAM Dump paragraph below.
- **Review Scan Results**: to review scan results present on the Collection Key. This menu is not displayed if no scan results are present. See the Reviewing Scan Results guide for details.

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

Copyright ©2016-2025 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.

Live scans alter the target system without compromising the investigation. See more details in the Technical Specifications guide.

Mac/Windows Scan from the Remote Agent

This document applies to the following applications		
ADFPRO Mobile & Computer Triage	DEI Digital Evidence Investigator	

To scan a Mac/Windows computer, the remote agent can be used in conjunction with the ADF desktop application.

Here is an overview of the process:

- Prepare a Collection Key so it contains the remote agent (see the Preparing Collection Keys guide for details). Note that it doesn't matter which Search Profile is selected on the Collection Key as it will be selected later in the ADF desktop application.
- The target computer and the ADF workstation have to be connected together to be part of the same local network. See below for details on how to connect them.
- On the target computer, run the remote agent. This can be done on a Mac /Windows target that is already running, or by placing the Mac in recovery mode. See below for details.
- On the ADF workstation, go to the Scan screen and select the remote agent as the target of your scan.
    - Note: if the "Remote agent is outdated, create a new Collection Key" message under the remote agent's name is shown, the new Collection Key should be created with the newer version of the remote agent.
- Once the scan is finished, unplug the Collection Key from the target computer, and disconnect the two computers.

Connecting a Mac/Windows Target Computer with the ADF Workstation

There are several ways to connect the target Mac/Windows computer and the ADF workstation. We recommend using the first method as it will provide the fastest and most reliable connection.

Method 1 - Direct Ethernet Connection

Use a regular Ethernet cable and connect it between the ADF workstation and the target computer. If no Ethernet port is present on the computer, use a USB-C to Ethernet adapter.
This will create a local network between the two computers and each will negotiate a network IP address (via the "link local addressing" process). It may take several minutes for the IP addresses to be assigned, especially if the computer already had an IP address.

Copyright ©2016-2025 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.

It is critical to provide proper power supply to the Mac/Windows computer to feed the adapter and any USB drives or you will experience disconnections.

Method 2 - Ethernet Connection to a Router

Use an Ethernet cable to connect the target computer and the ADF workstation to the same router. If no Ethernet port is present on the computer, use a USB-C to Ethernet adapter.
Once connected, the computer will join the local network and be assigned a network address (IP address).

It is possible for the IPv4 address assigned to the target computer to have a limited lease time which would make the remote agent unreachable after the lease expires. Please ensure that the DHCP service of the router has a long enough lease duration.

Method 3 - Wireless Connection

Find out if the local network offers a wireless access point or WAP. You will need the WAP identifier (SSID) as well as the login and password.

On the ADF workstation, click on the  icon in the bottom right corner to show the list of accessible WAP and select the appropriate one.
Do the same if the target computer is running Windows.

On a Mac target computer, click on the  icon in the upper right corner to show the list of accessible WAP and select the appropriate one.

Running the Remote Agent on a Mac

The remote agent is deployed on the Collection Key and can be executed on a Mac that is already running (a live Mac), or a Mac that is in Recovery mode. We recommend using the recovery mode that grants access to more files and is more stable. Note that the Recovery mode was only introduced in 2012 and older Macs do not offer it.
To prepare a Collection Key see the Preparing a Collection Key chapter in the Preparing Collection Keys guide.

Running in Recovery Mode

Follow these instructions to place the Mac in Recovery Mode and run the remote agent:

- Make sure the Mac is turned off.
- Turn the Mac on and be ready to press the key combinations to access the Recovery mode:
    - For older Macs, immediately press and hold down the Command (⌘) and R keys. You can release the keys when you see the Apple logo.
    - For newer Macs, with the Apple Silicon chip, press and hold the power button until “Loading startup options” appears. Select the Options menu to enter the Recovery mode.

Copyright ©2016-2025 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.

- You might be prompted to enter a password, such as a firmware password or the password of a user who is an administrator of this Mac. Enter the requested password to continue.
- Insert the USB Collection Key into the Mac.
- Run the Terminal application in Utilities > Terminal.
- For systems with FileVault encryption, especially on newer versions of macOS, the main user data volume may need to be unlocked manually. Follow these steps within the Terminal:
    - List all APFS (Apple File System) volumes by typing `diskutil apfs list` and pressing Enter.
    - Identify the correct user data volume. It is typically named 'Data' and will be the largest partition. It will also have the entry FileVault: Yes (Locked).
    - Note the identifier for this volume from the 'APFS Volume Disk (Role)' line (e.g., disk4s5).
    - Enter the command `diskutil apfs unlockVolume <disk-identifier>`, replacing <disk-identifier> with the one you noted (e.g., `diskutil apfs unlockVolume disk4s5`).
    - You will be prompted to enter the password for the device. Type it and press Enter.
    - Confirm the volume is unlocked by running `diskutil apfs list` again. The entry should now show FileVault: Yes, Unlocked and a mount point (e.g., /Volumes/Data).
- Type the command `/Volumes/CKY/startMacOSAgent` and press Enter.



Make sure to type the proper uppercase and lowercase letters as macOS is case sensitive.

You can press the “tab” key to autocomplete a file/folder name that you type. For example, type “/Vo” then press the “tab” key and it should autocomplete to “/Volumes”. Pressing the "tab" key twice will display the possible autocomplete values.

The agent should start and display the following information:

```
To connect to this device enter the following IP
address in the Scan screen of the ADF desktop application:
  192.168.0.131
  192.168.0.133
```

Running on a Live Mac

If the target Mac computer is already running you can start the remote agent without rebooting the target computer. To do so, follow these instructions:

- When connecting a USB device (the Collection Key or a USB to Ethernet adapter), you may be prompted to allow the accessory to connect. Make sure to allow.
- Grant full access privileges to the Terminal application (required for macOS Mojave 2018 and newer).
    - Go to > System Preferences > Security & Privacy > Privacy tab and select Full Disk Access in the left side list.
    - Click on the “Click the lock to make changes” to be able edit the settings and enter the admin password.

Copyright ©2016-2025 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.

    - Select the checkbox next to the Terminal option. If Terminal is not listed, click on the “+” button and select Applications > Utilities > Terminal.
    - Close the Security & Privacy window.
- For a wired connection (recommended), disconnect the WIFI by clicking on the WIFI icon in the top toolbar and using the toggle to turn it off.
- Insert the USB Collection Key into the Mac.
- Open a Finder window in File > New Finder Window.
- Navigate to the USB Collection Key called CKY under DEVICES and double click on startMacOSAgent

The agent should start and display the same information as described above.



If more than one IP address is listed it usually means that one network adapter is wired and the other one is wireless. Go to > System Preferences > Network and select the wired LAN adapter in the left side list. Its IP Address should be displayed in the detailed properties area.



When running live, some files might already be in use and locked by other applications. If that is the case, then the remote agent cannot read those files.
We recommend running in Recovery mode to avoid such situations, or closing running applications, such as web browsers.

Running the Remote Agent on Windows

The remote agent is deployed on the Collection Key and can be executed on a Windows computer that is already running.
To prepare a Collection Key see the Preparing a Collection Key chapter in the Preparing Collection Keys guide.

Once the Collection Key is ready, perform the following actions on the target computer:

- Insert the USB Collection Key into the target Windows computer.
- Open a File Explorer window in Start > File Explorer.
- Navigate to the USB Collection Key called CKY under This PC and double click on startWindowsAgent.bat
- The remote agent starts and is ready to communicate with the ADF Desktop application.

Starting the Remote Scan

Now that the remote agent is running, the rest of the process takes place on the workstation running the ADF desktop application:

- Navigate to the Scan screen (see details in the Desktop Scan section below).
- Click on the **Add Remote Agent** button.
- Select the agent in the list of agents discovered automatically by the ADF desktop application.
- Click on the **CONNECT** button.
- The remote agent should now be listed as a target device.

Copyright ©2016-2025 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.

If no agent is listed, make sure the agent and the ADF desktop application are on the same network. It is possible to enter the IP address of the target computer directly. Enter the IP address of the target computer that was provided by the remote agent earlier.
Note that the IP address should look similar to the one displayed by the ADF desktop application. For example if the remote agent has an IP address of 10.10.1.33 and the ADF desktop application has an IP address of 192.168.1.41, they are probably not on the same network and will not see each other.
Also, if a port number other than 80 is used by the remote agent, it needs to be entered after the IP address separated by a semicolon. For example “10.10.1.33:32772”.

Note that all available volumes will be scanned and only allocated files will be processed (no deleted files recovery and no unallocated file carving).

Terminating the Mac Remote Agent

Once the scan is finished, if the target computer was in recovery mode:

- Go to the Apple menu and select Shut Down.

If the target computer was running live:

- In the Terminal window, press Ctrl + c to stop the agent.
- Close the Terminal window.
- Go to the Finder and eject the Collection Key (CKY).

Terminating the Windows Remote Agent

Once the scan is finished:

- Close the Terminal window.
- Look for the Safely Remove Hardware icon on the taskbar.
- Press and hold (or right-click) the icon and select the USB Collection Key.

Troubleshooting Connection Issues

If after entering the IP address of the target computer, the connection cannot be established, try disabling the firewall on the ADF workstation and on the target computer.

Desktop Scan

A scan conducted from the ADF Desktop application is called a desktop scan. Desktop scans can process attached devices, drive images, folders, mobile devices and mobile acquisitions (the type of targets available differ based on the product).

Copyright ©2016-2025 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 conduct a desktop scan, navigate to **Home** > **Investigate Device** > **Scan**.

A valid license needs to be present for the duration of the scan. It can be a computer license, an ADF Authentication Key, or a licensed ADF Collection Key.

Targeted Scan

The targeted scans of mobile devices make it possible to search and collect only the data that matches the search criteria defined in the Search Profile thus better complying with the scope of a search warrant.

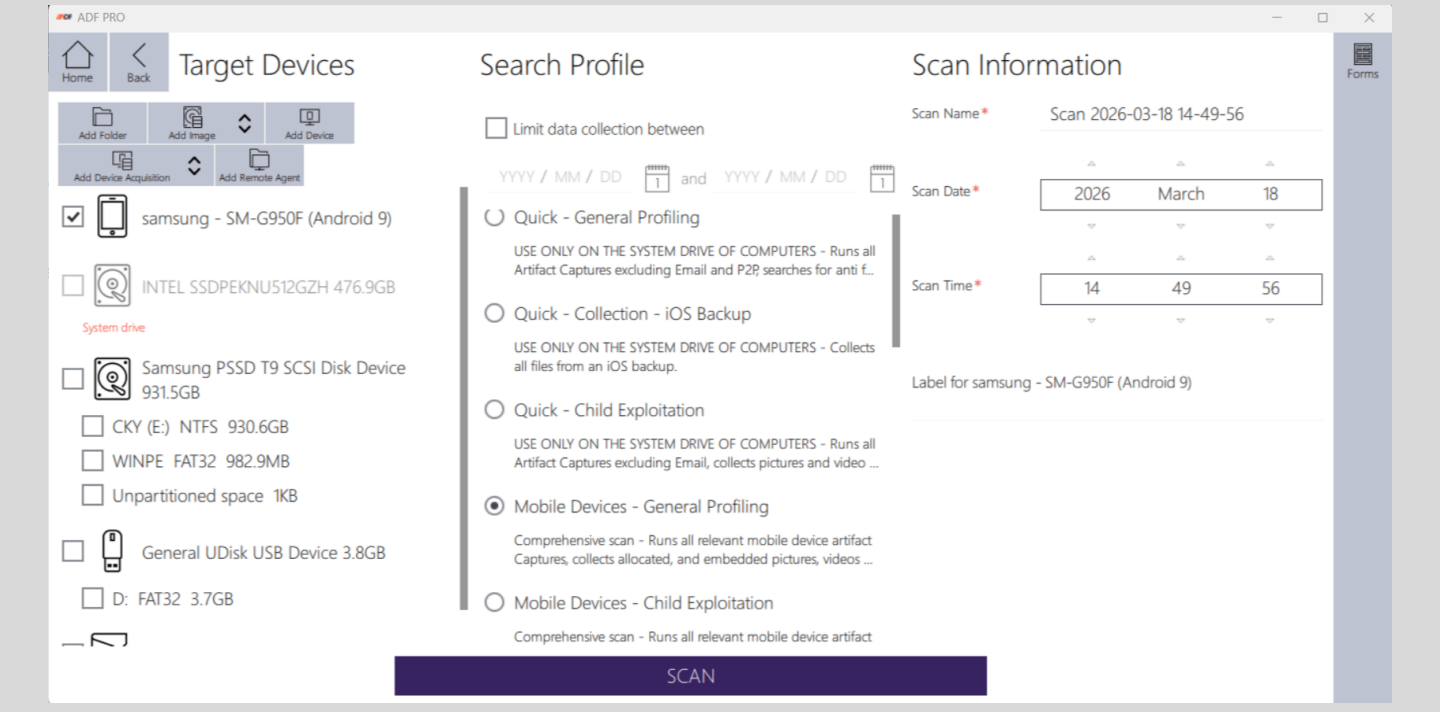
It is accessible from the following menus:

- MDI Mobile Device Investigator **Home** > **Investigate Device** > **Targeted Mobile Extraction Only**
- DEI Digital Evidence Investigator **Home** > **Investigate Device** > **Targeted ChromeOS Extraction Only**
- ADFPRO Mobile & Computer Triage **Home** > **Investigate Device** > **Targeted Mobile/ChromeOS Extraction Only**

In this mode, the mobile device advanced logical acquisition is safely discarded immediately following the scan.

Conducting a Scan

On the **Scan** screen, the left-hand side panel shows the scan targets, the central panel shows the Search Profiles or Captures that can be used for the scan, and the right-hand side panel shows the scan information that can be added to a scan.



Copyright ©2016-2025 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.

Copyright ©2016-2025 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.

Selecting Target Devices

This document applies to the following applications		
ADFPRO Mobile & Computer Triage	DEI Digital Evidence Investigator	MDI Mobile Device Investigator

The **Target Devices** panel shows the targets available to be scanned. On the ADF desktop application, connected storage devices are shown by default but the system partition cannot be selected. On the Collection Key, the target computer's drives and connected storage devices are shown by default.

It is possible to add targets:

 Add Folder	To add a folder accessible from this workstation (including network folders). This option is available from the ADF desktop application and when conducting a live scan with the Collection Key.
 Add Image	To scan a physical or logical drive image. The following image formats are supported: ● ADF Data Containers created by the ADF desktop application: ○ Mac Remote Agent (ADFPRO DEI) ○ Windows Remote Agent (ADFPRO DEI) ○ Collect Files - drives (ADFPRO DEI and with External Devices add-on MDI) ○ Collect Files - MTP (ADFPRO MDI) ○ EWF forensic image (with External Devices add-on MDI) ● Other forensic image formats ○ .dd, .001, .E01, L01, .aff4 (ADFPRO DEI) See the list of supported image formats in the "Supported Target Devices/Operating Systems" section of the "Technical Specifications" guide. This option is only available from the ADF desktop application and not the Collection Key.
 Add Remote Agent	To connect with an ADF remote agent running on a target computer. This option is only available from the ADF desktop application

Once the targets are listed, select the ones to be scanned. It is possible to select multiple targets and all the results will be saved in the same scan result.

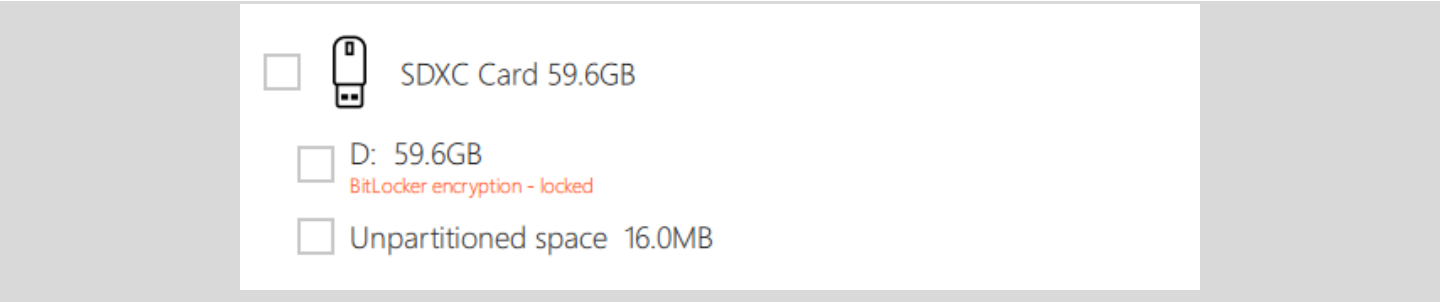
Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

Unlocking Encrypted Partitions

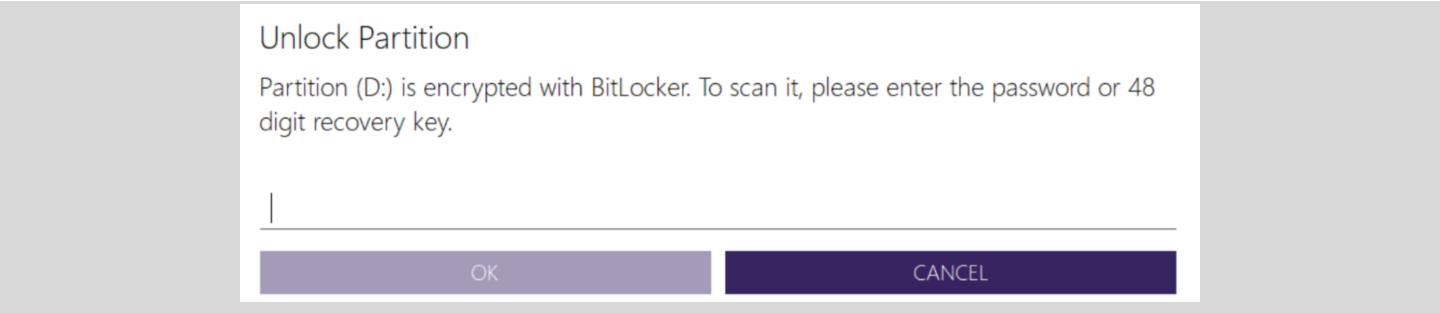
This document applies to the following applications		
ADFPRO Mobile & Computer Triage	DEI Digital Evidence Investigator	

When a drive partition is detected as encrypted (see the list of supported encryptions here), a warning caption is displayed.
To unlock the partition:

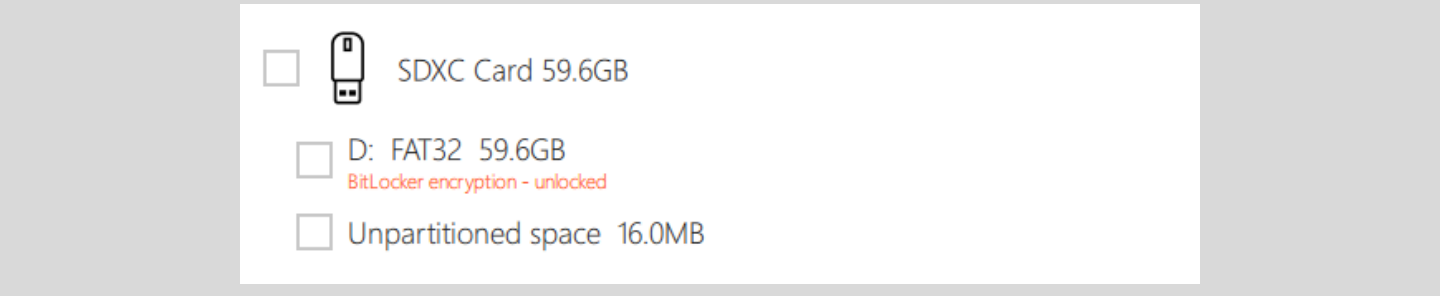
1. Check the partition's checkbox.



2. A dialog window is displayed to input the password, or recovery key, or wipekey file depending on the encryption used.



3. If successful, the caption indicates that the partition is now unlocked. If the entered unlocking information is not accepted it is possible to try again.



Copyright ©2016-2025 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.

BitLocker Encryption

Partitions protected by BitLocker are detected and can be unlocked by entering their passwords or recovery keys. Usually, system partitions are not protected by a password and require the recovery key. The recovery key can be obtained by contacting Microsoft and is often stored in the Microsoft account of the computer owner.

BitLocker Encryption with TPM Chip

Partitions protected by BitLocker and a TPM chip (which is the most common scenario for modern computers) are detected and can be unlocked by entering their recovery keys. The TPM chip is required to unlock the partition, so if such a partition is imaged while encrypted, it will not be possible to decrypt the image later even with its recovery key.

BitLocker Encrypted Image

Encrypted images are not supported by the ADF application. To scan an encrypted image, please mount the image with a third party application (such as OSFMount), open a Terminal window and use the manage-bde command line to decrypt the image, then select the decrypted volume as the scan target.

FileVault2 Encryption

Partitions protected by FileVault2 over HFS+ and APFS are detected and can be unlocked by entering their passwords. For FileVault2 over HFS+ a wipekey file is also required. When scanning or imaging the target computer, the ADF application will try to automatically locate the wipekey file on the other unencrypted partitions.

Selecting a Device

The **Target Devices** panel shows the mobile devices for which a connection has been established.

It is possible to add targets:

 Add Device	To add a device as a scan target. This opens the device connection wizard described in this document.
 Add Device Acquisition	To add a device acquisition. It is possible to select: • ADF Android (ADFPRO Mobile & Computer Triage, MDI Mobile Device Investigator) • ADF iOS (ADFPRO Mobile & Computer Triage, MDI Mobile Device Investigator) • ADF ChromeOS (ADFPRO Mobile & Computer Triage, DEI Digital Evidence Investigator) • ADF Wear OS (ADFPRO Mobile & Computer Triage, MDI Mobile Device Investigator) • ADF Screen Capture - iOS, Android, Wear OS (ADFPRO Mobile & Computer Triage, DEI Digital Evidence Investigator, MDI Mobile Device Investigator)

Copyright ©2016-2025 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.

	• ADF Screen Capture - ChromeOS (ADFPRO Mobile & Computer Triage DEI Digital Evidence Investigator)
	• ADF Screen Capture - Video Source (ADFPRO Mobile & Computer Triage (with Video Source add-on DEI Digital Evidence Investigator MDI Mobile Device Investigator)
	• iTunes Backup (ADFPRO Mobile & Computer Triage MDI Mobile Device Investigator)
	• GrayKey(ADFPRO Mobile & Computer Triage MDI Mobile Device Investigator)
	  ○ select the folder containing the zip file
	• UFD FFS (ADFPRO Mobile & Computer Triage MDI Mobile Device Investigator)
	  ○ select the ufd file

The added target should be automatically selected.

Copyright ©2016-2025 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.

Selecting an MTP Device

This document applies to the following applications		
ADFPRO Mobile & Computer Triage	MDI Mobile Device Investigator	

It is possible to scan devices that support the Media Transfer Protocol (MTP). Such devices include digital cameras, legacy phones, digital music players, and more.
Some devices are always MTP ready and when connected they will appear as a MTP device in the list of targets. Some other devices need to be configured to activate MTP. Please refer to the manufacturer's instructions to enable MTP.
MTP devices are scanned at the file level and no deleted files or file carving is performed.



Some legacy phones may require to activate file transfer for the USB connection before they are visible to the Desktop application.

Limiting the Collection of Data to a Predefined Time Range

It is possible to only collect artifact and file records that have their timestamps within a predefined time range. To do this, select the "Limit data collection between AFTER_DATE and BEFORE_DATE" option and set at least one date.
File records are processed if either one of their Last Written or File Created timestamp is within the time range. For files embedded within other files, the timestamps of the container are used.
Artifact records are included if at least one of their timestamps is within the time range.
The date comparison is inclusive of the predefined dates in the range.

Selecting Search Profiles

The **Search Profile** panel lists the Search Profiles available locally to conduct the scan. It is possible to expand the notes section if they are not entirely visible.

Select the Search Profile that matches your search goals by clicking on the appropriate radio button.



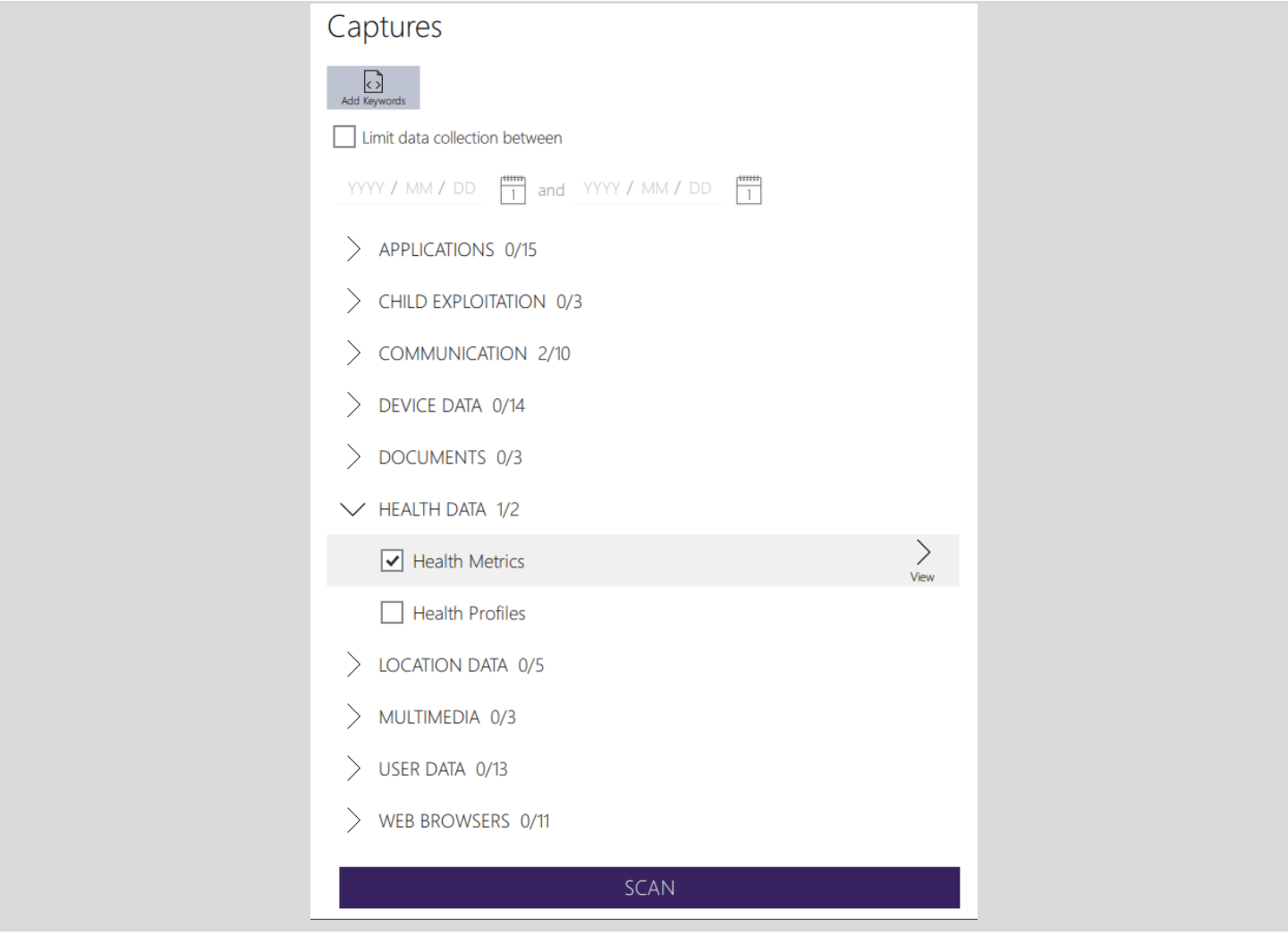
It is important to read the Search Profile description to make sure the search criteria apply to the selected targets.
For example, some of the Quick and Intermediate default Search Profiles are designed to process folders that are generally found on the Operating System drive and will not yield good results on data drives.

Copyright ©2016-2025 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.

Selecting Captures

This document applies to the following applications		
ADFPRO Mobile & Computer Triage	DEI Digital Evidence Investigator	MDI Mobile Device Investigator

When conducting a targeted extraction and scan or scanning from the Collection Key, and if no Search Profile was deployed (as described here), the **Captures** panel is displayed at the center and lists the Captures available to conduct the scan.



Captures are organized in their respective groups that can be expanded or collapsed to show how many Captures are available in that group and how many are selected. Select the desired Captures by clicking on the checkbox next to them.

Copyright ©2016-2025 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.

For Captures that collect app artifacts, it is possible to precisely select which apps should be processed by clicking the **View** button next to each Capture and reveal the individual apps.



Make sure to only select the minimum amount of Captures as each selected Capture adds time to the scan, and makes reviewing the scan results more time consuming.
A warning will be displayed in case the selected Captures overlap each other as described in the Creating a New Search Profile section of the Setting Up Scans guide.



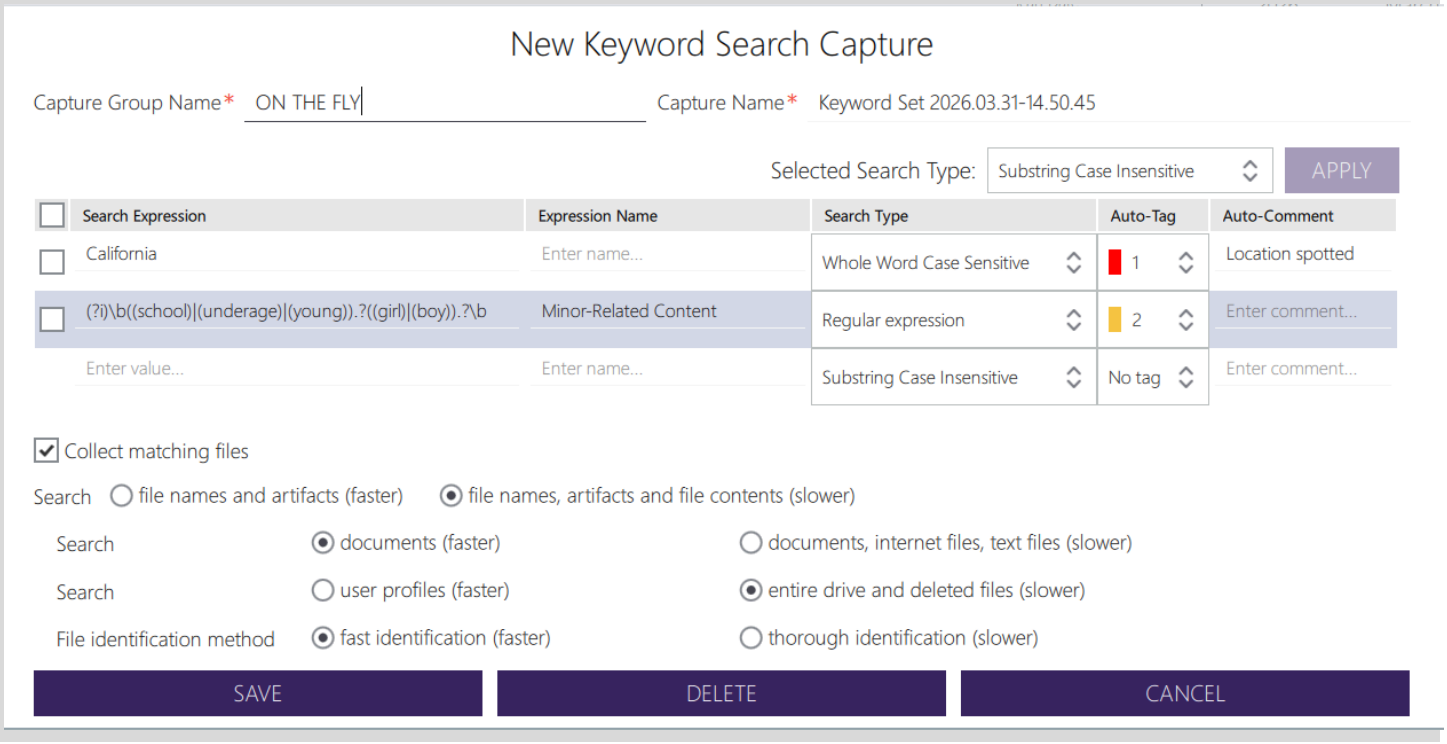
Default Captures that have been hidden in the configuration file are not presented.

Adding On-the-Fly Keywords

This document applies to the following applications		
ADFPRO Mobile & Computer Triage	DEI Digital Evidence Investigator	MDI Mobile Device Investigator

It is possible to add keywords just before starting a targeted extraction and scan or a scan from the Collection Key by pressing the **Add Keywords** button. The **New Keyword Search Capture** window appears to define the keywords and the search scope.

Copyright ©2016-2025 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.



- Capture Group Name: is the group name and defaults to “ON THE FLY”.
- Capture Name: is the Capture name and defaults to “Keyword Set YYYY.MM.DD-HH.MM.SS”
- Search Expression: enter the substring or regular expression to be searched. When a match is found, that record can also be automatically tagged or assigned a comment. To delete a search expression, select it and click on the **Delete** button.
    - Substring means that the text pattern can be found anywhere in a word. For example, when searching for “age”, the word “triage” will match.
    - Substrings are case-insensitive.
- Expression Name: use the 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.
- 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:
    - Substring - Case Insensitive (selected by default)
    - Substring - Case Sensitive
    - Whole Word - Case Insensitive
    - Whole Word - Case Sensitive
    - Regular Expression
- Search options: to define the scope of the search to make it faster or more thorough.
    - Searching file names and artifacts will not search within file contents.
    - Clicking the radio button to search file names, artifacts and file contents (slower) will provide further search options to choose between:
        - Search documents only or documents, internet files and text files.

Copyright ©2016-2025 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.

- Search user profiles only or entire drive and deleted files.
- Fast file identification (identifies files using the file extension) or thorough file identification (will check file signatures for all files).

Clicking the **SAVE** button will save the keyword Capture. Clicking the **DELETE** button will close the window and discard the keyword Capture. Clicking the **CANCEL** button will disregard any changes just made on the keyword Capture that had been previously created.

After saving the keyword Capture, the **Add Keywords** button changes to **Edit Keywords** if additional changes are needed.

A new Capture is created on the Collection Key and when the scan begins, that Capture is associated with the selected Search Profile. If a user-created Search Profile was used, it is modified to reference that Capture. If a default Search Profile was used it is copied and the copy is modified to reference that Capture.
The keyword search Capture and modified Search Profile stay on the Collection Key and are available until the Collection Key is prepared again.
In case of a targeted extraction and scan the Search Profile is not saved after the scan.

Entering Scan Information

Upon selecting a Search Profile, the corresponding scan information fields are displayed on the right-hand side panel:

- Scan Name: defaults to the word Scan followed by a real-time date and timestamp but is editable



Customize the scan name so the results are easily identifiable in Review Scan Results.

- Scan Date and Scan Time: these fields are populated by querying the system clock of the running computer and can be modified to reflect the actual time if the system clock is incorrect.
- Target label: It is possible to supply a label for each target within the label field below the scan time field. This will allow easier identification of targets within the scan results.

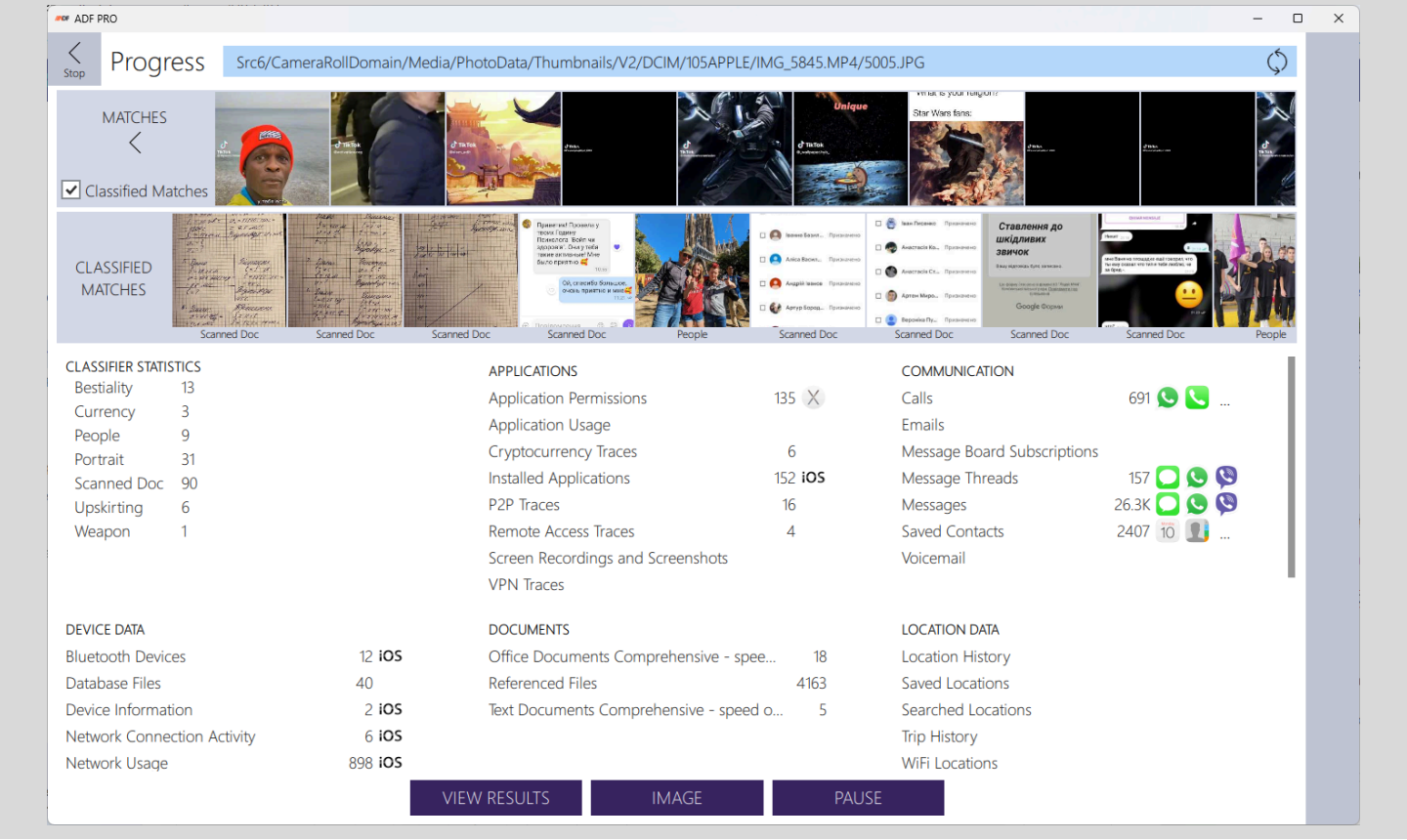
It is possible to add more scan information fields as described in the Scan Information Fields paragraph in the Configuring the ADF Application guide.

Starting the Scan

After all the required information has been entered, the **SCAN** button is available to start the scan. Make sure a license is available for the scan to start.

Copyright ©2016-2025 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.

Scan Progress



The **Progress** screen is displayed while the scan is running and it shows the following information:

- Progress bar: shows the name of the file being processed or the name of the task taking place.
- Matches log: shows a real time preview (thumbnail) of File Capture matches collected. Images and Video files are represented by thumbnail images, keyword matches will show the keyword found, all other matches will be represented by an associated icon. The Matches log can be collapsed to hide the matches by clicking on the **Collapse** ( ) button.
    - If Picture and Video Classification is enabled within the Search Profile, a "Classified Matches" checkbox appears below the Matches collapse/expand button.
    - When checked, a second ribbon, Classified Matches is displayed beneath the original Matches ribbon. This ribbon shows thumbnails of the pictures and frames that have been assigned a visual class (such as People, Weapon, CSAM, etc), with the class name displayed below each thumbnail.

Only a sample of the matches are displayed in the Matches log to avoid it scrolling too quickly across the screen.

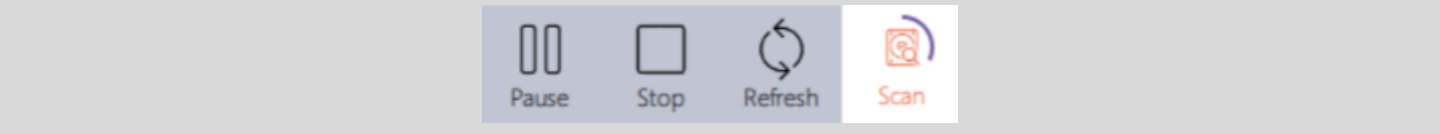
Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

- Tags Statistics: shows in real time how many records are being tagged.
- Classifier Statistics: Displays a list of picture and video classification categories in alphabetical order (excluding "Other"). Each category includes a real-time count of how many files have been classified into it.
- Capture results: indicates the cumulative count of records found by the Capture as well as the icon of the application from which the record was extracted.
- **VIEW RESULTS** button: to view the results currently collected by the scan. The scan will continue to run in the background.
- **IMAGE** button: to stop the scan and create an image of the target device or acquire the mobile device.
- **PAUSE** button: to pause the current scan. To resume a scan click on the **RESUME** button that has replaced the **PAUSE** button.

Once the scan completes, a message is displayed indicating the status of the scan (similar to the status displayed on the Summary view). From there it is possible to **VIEW RESULTS** and **IMAGE**.

Reviewing the Scan Result during the Scan

Clicking on the **VIEW RESULTS** button while a scan is running opens the Viewer on a snapshot of the scan result and the scan continues in the background.



A new **Scan** button is available in the function toolbar offering the following actions:

 Pause	To add pause the scan.
 Stop	To stop the scan.
 Refresh	To refresh the scan result and present a new snapshot.
	To open the scan control panel. The scan progress is shown by the yellow circle around the Scan icon.

Copyright ©2016-2025 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.

Scan	

It is possible to go back to the **Progress** screen by clicking the **Close** button in the **Navigation** toolbar.

Creating RAM Dump

This document applies to the following applications		
ADFPRO Mobile & Computer Triage	DEI Digital Evidence Investigator	

When running a live scan from a Collection Key it is possible to collect a RAM dump of the running computer.

Navigate to **Home** > **Create RAM Dump** to immediately start the process and see progress information.

The RAM dump is saved on the Collection Key in the ram_dump folder and named ram_dump-YYYY-MM-DD-HH-MM-SS.zip. The zip file contains a compressed raw dump file named ram_dump-YYYY-MM-DD-HH-MM-SS.bin.

The RAM dump can be analyzed with tools such as Volatility to extract information.



The RAM dump process may be blocked if an antivirus is running. Make sure to turn it off.

Copyright ©2016-2025 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.