Previewing a Mobile Device

Introduction

This guide covers how to quickly preview an Android or iOS device without the need to run a logical acquisition first.

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

What is the Preview Mode?

The Preview mode makes it possible to review files and artifacts of mobile devices without waiting for a logical data acquisition to complete. In this mode, after the connection with the mobile device is established, the viewer is displayed and presents the files and artifacts on demand. Everything collected is kept: the data read from the device is saved as an acquisition, listed in View Acquisitions with the type Device Preview, and the preview itself is saved as a scan result in Review Scan Results.

Previewing a Mobile Device

To preview a mobile device, navigate to **Home** > **Investigate Device** > **Preview**.

Connecting the Mobile Device

Here are the instructions to preview a mobile device:

- On the **Enter Information** screen, enter the following:
    - **Source**: click on the **Add Phone** button to connect the mobile device as explained in this section of the Acquiring an iOS, Android, Wear OS or ChromeOS Device guide. Note that the mobile device connection wizard should appear automatically when no connected device is found. Only Android and iOS devices connected with a USB cable can be previewed: the wizard does not offer wireless Android, Wear OS or ChromeOS devices. An Android device must also allow file transfer (MTP), as the wizard asks in its MTP Access step; until then it is not listed.

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.



By default, multimedia files transferred from an iOS device are converted. Sometimes this conversion fails which in turn corrupts the MTP connection and prevents any further files from being transferred.
We highly recommend changing the transfer mode to “Keep Originals”. This option can be found on the iOS device in Settings > Photos > TRANSFER TO MAC OR PC. Change from “Automatic” to “Keep Originals”.
Photos and videos stored only in iCloud (iCloud Photos with Optimize iPhone Storage turned on) are not transferred, as Windows does not see them on the device. To preview them, turn on Download and Keep Originals in Settings > Photos and wait for the download to finish.

    - **Acquisition Path**: the folder where the acquired data will be saved. By default, a new folder in the Acquisitions folder is set in Settings, named after the device, its serial number, and the current date and time. If you select another folder, it must be empty and cannot be the root of a drive.
    - **Preview Name**: the name of the preview scan result, under which it is listed in Review Scan Results. By default, Preview followed by the current date and time; the name must be unique.
    - Case Number (optional): saved with the preview scan result and with the acquisition. Review Scan Results and View Acquisitions group them by case number.
- To add a form (as explained in the Managing Forms guide), click the **Forms** button located in the toolbar on the right-hand side.
- When ready, click on the **PROCEED** button to start the preview.
    - For an iOS device, the application first checks whether its backups are encrypted. If they are protected with a password, the Source shows Backup requires an existing password, and the password must be entered after **PROCEED**. If the device requires encrypted backups (for example, through a configuration profile), the message “Backup requires a new password” is shown and a new password must be set; it will be needed for later backups.
    - If the backups are not encrypted (iOS 11 and later), the application sets the backup password to ‘adf’ for the duration of the preview, because an encrypted backup contains more artifacts, and removes it at the end. When Enter Passcode on Device is displayed, enter the passcode on the iOS device. If the device is disconnected before the preview ends, the password may remain: in the Apple Devices app (or iTunes), turn off Encrypt local backup for the device, using the password ‘adf’.
- The application collects some basic information from the device and after a few seconds the viewer is displayed.

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

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.

Using the Viewer in Preview Mode

This section covers the specificities of the viewer in Preview mode. For a complete description of the viewer see the Reviewing Scan Results guide. While the preview is running, tags and comments cannot be added by click or with the number keys, and Search Tables and the Applications view are unavailable. They become available when the preview ends.

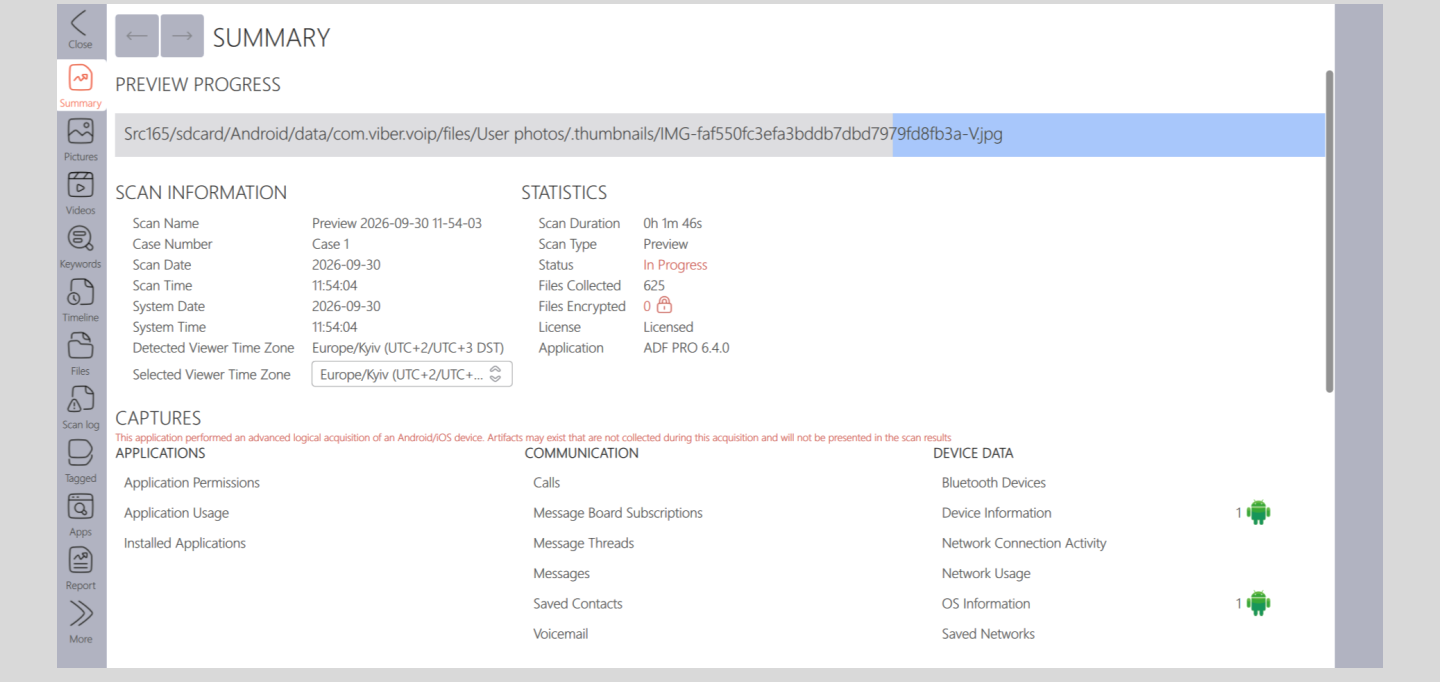
Navigation Toolbar

The Navigation toolbar is used to access the data views. The **Close** button terminates the Preview mode and goes back to the **Home** screen.

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.

Summary View

The first screen displayed is the **Summary** view.



It contains the **PREVIEW PROGRESS** section: while the preview runs, an animated bar shows the file being collected (or Artifact collection in progress…), and when the preview ends, the bar shows its final status, such as Completed or Interrupted. The number of files collected so far is shown in STATISTICS, under Files Collected.

The **CAPTURES** section shows which artifacts are collected, with the number found so far next to each capture; the numbers grow as the preview goes on. A capture name can be clicked at any time to open that view.

Capture Views

The Capture views display the artifacts that have been collected as soon as they become available.

For iOS devices, the artifacts can only be collected once the complete iTunes backup is finished. Only OS Information and Installed Applications are available earlier, as they come from the device properties read at the start.

Pictures, Videos, Files Views

It is possible to navigate to these views immediately even though files are still being collected. The files are displayed as they become available.

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.

Timeline View

This view is only updated when accessed and not in real-time. To see the latest activities, leave the view and go back to it.

Creating a Report

It is possible to create a report while in Preview mode. If some files, included in the report, have not been fully processed and collected, the report will only contain their basic properties. The Standalone viewer format is unavailable while the preview is running.

Information Collected and Sequence of Collection

On Android devices, the following data is collected in parallel:

1. Artifacts via the ADF backup agent, then the application data via an ADB backup. If the device is locked when the ADB backup starts, the application asks to unlock it; SKIP STEP continues without the application data.

2. The following files in this order:
    a. Pictures
    b. Videos
    c. Documents
    d. All the other files

On iOS devices, the following data is collected in parallel:

1. The iTunes backup of the device. On iOS 11 and later, a backup that is not encrypted is encrypted for the duration of the preview (see Connecting the Mobile Device), as an encrypted backup contains more artifacts.
2. The following files in this order:
    a. Pictures
    b. Videos
    c. Documents
    d. All the other files
3. When the iTunes backup process finishes, all the artifacts are processed.

The file collection sequence adapts based on the user interactions. For example, if the pictures are being collected, but the user navigates to the Videos view, then the video files get a higher collection priority.

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.