Introduction

This guide covers how to establish a connection with an Android, iOS, Wear OS, or ChromeOS device and how to acquire its data.

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

The types of devices that can be acquired depend on the product license:

- ADFPRO Mobile & Computer Triage MDI Mobile Device Investigator : Android, iOS, Wear OS
- ADFPRO Mobile & Computer Triage DEI Digital Evidence Investigator : ChromeOS

What is a Logical Acquisition?

Acquiring logical data from an iOS, Android, Wear OS or ChromeOS device consists in establishing a connection with the device and using standard protocols such as file transfer and Application Level Interface (API) calls to request files and data that are then saved locally. By opposition, a physical acquisition usually consists in obtaining a copy of each block of a storage device.

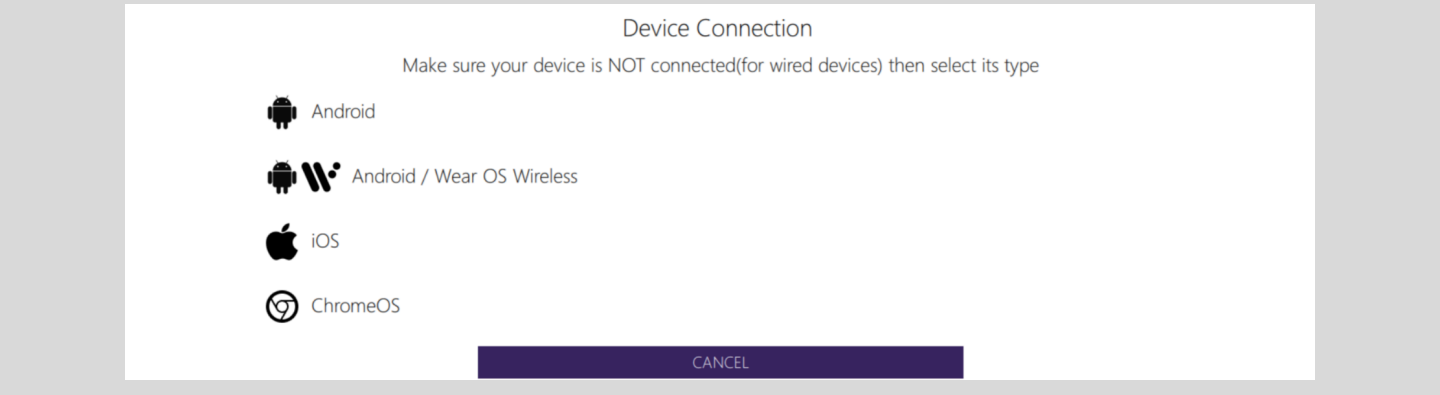
Establishing a Connection

From the acquisition screen, or preview screen, or scan screen, to establish a connection with a mobile device, the following steps have to be followed:

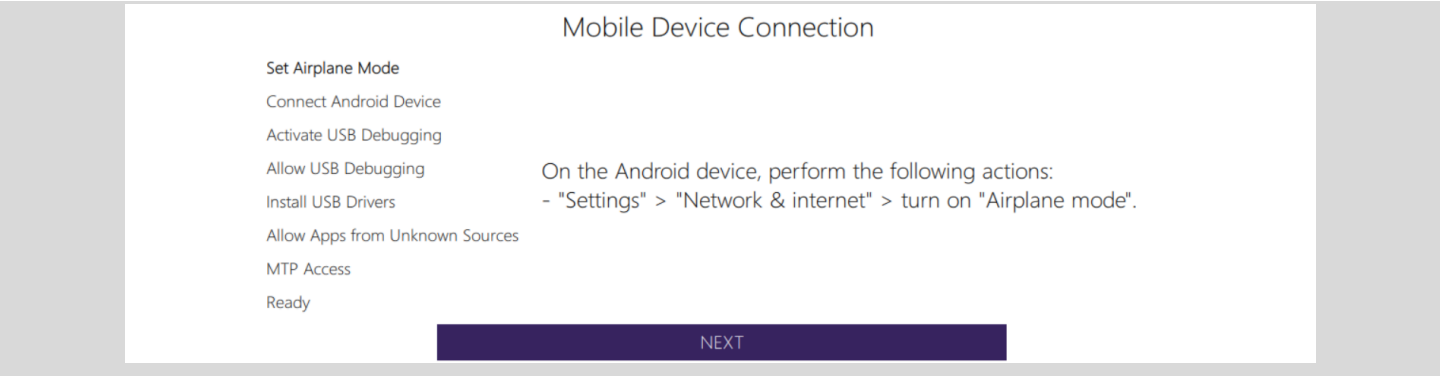
- Make sure the device is not connected.
- After clicking on the **Add Device** button, the device connection wizard is displayed.
- This wizard guides you through the steps required to properly establish a connection between the Android/iOS/Wear OS/ChromeOS device and your computer. Note that the instructions may not match exactly what you see on the Android/iOS/Wear OS/ChromeOS device screen and you may find further guidance in the appropriate table below.
- Make sure the device is unlocked as you start the data acquisition and it is recommended it stays unlocked for the duration of the acquisition.
- You shouldn't have to interact with the device once the acquisition starts.
- It is possible to unplug the device once the acquisition phase has completed.

The first screen of the wizard to select the type of 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.



Other wizard screens to help establish the connection with the device:



Connecting an Android Device

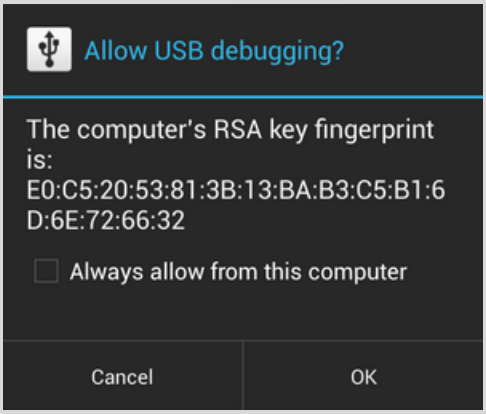
This section describes how to properly establish a wired connection with an Android device. It is also possible to connect wirelessly - see the "Connecting Android and Wear OS Devices Wirelessly" guide for full details.

Preparing the Android Device

To prepare the Android device, you usually have to:

- Know the passcode to unlock the device.
- Prevent auto-locking.
- Place the device in airplane mode.
- Activate the developer mode.
- Activate the USB debugging mode (and potentially another USB debugging Secure).
- In developer mode, find settings allowing you to install apps from USB and not verify apps over USB.
- Upon connecting the device, if it is not seen by Windows, make sure the device USB connection mode is set to transfer file (File Transfer, MTP, PTP).
- Allow USB debugging with the host when prompted on the device ("always allow from this computer").

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.

The table below describes the most common method to accomplish these actions.

Action	Android 12+	Android 10	Android 9	Android 8
Prevent auto-lock	“Settings” > “Security” > “Screen lock” > enter pin > select “None”	“Settings” > “Security & location” > “Screen lock” > enter pin > select “None”	“Settings” > “Security & location” > “Screen lock” > enter pin > select “None”	“Settings” > “Security & location” > “Screen lock” > unlock > select “None”
Prevent voice and data connections	“Settings” > “Network & internet” > turn on “Airplane mode”	“Settings” > “Network & internet” > turn on “Airplane mode”	“Settings” > “Network & internet” > turn on “Airplane mode”	“Settings” > “Network & internet” > turn on “Airplane mode”
Activate developer options	“Settings” > “About phone” > tap 7 times on “Build number”	“Settings” > “About phone” > tap 7 times on “Build number”	“Settings” > “About phone” > tap 7 times on “Build number”	“Settings” > “System” > “About phone” > tap 7 times on “Build number”
USB Debugging	“Settings” > “System” > “Developer options” > turn on “USB debugging”	“Settings” > “System” > “Developer options” > turn on “USB debugging”	“Settings” > “System” > “Developer options” > turn on “USB debugging”	“Settings” > “System” > “Developer options” > turn on “USB debugging”
USB connection mode	With the device connected to the computer > “Settings” > search for “USB Preferences” > set “Use USB for” to “File Transfer” or “MTP” or “PTP”	With the device connected to the computer > “Settings” > search for “USB Preferences” > set “Use USB for” to “File Transfer” or “MTP” or “PTP”	With the device connected to the computer > “Settings” > search for “USB Preferences” > set “Use USB for” to “File Transfer” or “MTP” or “PTP”	With the device connected to the computer > “Settings” > “System” > “Developer options” > “Select USB configuration” > set “Select USB configuration” to “MTP (Media Transfer Protocol)” or “PTP”
Install unknown apps	No longer needed	No longer needed	“Settings” > … > “Developer options” > turn on “Install via USB”	“Settings” > “Security” > turn on “Unknown sources”
Disable apps verification	“Settings” > … > “Developer options” > turn off “Verify apps over USB”	“Settings” > … > “Developer options” > turn off “Verify apps over USB”	“Settings” > … > “Developer options” > turn off “Verify apps over USB”	
Allow USB debugging once connected	“Allow USB debugging?” dialog > select “Always allow from this computer” and “OK”	“Allow USB debugging?” dialog > select “Always allow from this computer” and “OK”	“Allow USB debugging?” dialog > select “Always allow from this computer” and “OK”	“Allow USB debugging?” dialog > select “Always allow from this computer” and “OK”

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.

Action	Android 7	Android 6	Android 4
Prevent auto-lock	“Settings” > “Security” > “Screen lock” > unlock > select “None”	“Settings” > “Lock screen & password” > “Screen lock” > unlock > select “None”	“Settings” > “Lock settings” > “Screen lock” > unlock > select “None”
Prevent voice and data connections	“Settings” > turn on “Airplane mode”	“Settings” > “Network & internet” > turn on “Airplane mode”	“Settings” > “More” > turn on “Airplane mode”
Activate developer options	“Settings” > “About” > “Software information” > “More” > tap 7 times on “Build number”	“Settings” > “About phone” > tap 7 times on “Build number”	“Settings” > “About phone” > tap 7 times on “Build number”
USB Debugging	“Settings” > “Developer options” > turn on “USB debugging”	“Settings” > “Developer options” > turn on “USB debugging”	“Settings” > “Developer options” > turn on “USB debugging”
USB connection mode	With the device connected to the computer > “Settings” > “Developer options” > “Select USB configuration” > set “Select USB configuration” to “MTP (Media Transfer Protocol)” or “PTP”	With the device connected to the computer > “Settings” > “Developer options” > “Select USB configuration” > set “Select USB configuration” to “MTP (Media Transfer Protocol)” or “PTP”	With the device connected to the computer, bring the top drawer down > “USB options” > set “Connect as” to “MTP (Media Transfer Protocol)” or “PTP”
Install app from unknown sources	“Settings” > “Security” > turn on “Unknown sources”		“Settings” > “Security” > turn on “Unknown sources”
Disable apps verification		“Settings” > … > “Developer options” > turn off “Verify apps over USB”	“Settings” > … > “Developer options” > turn off “Verify apps over USB”
Allow USB debugging once connected	“Allow USB debugging?” dialog > select “Always allow from this computer” and “OK”	“Allow USB debugging?” dialog > select “Always allow from this computer” and “OK”	“Allow USB debugging?” dialog > select “Always allow from this computer” and “OK”

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.

Advanced Logical Acquisition for Android

The advanced logical acquisition uses the following standard transfer protocols that do not require rooting the device:

- Use adb backup to collect apps data. Note that only some apps register to use the Android Auto-Backup feature.
- Use a silently installed app to collect common artifacts via Android API calls. This app is uninstalled once the data has been transferred.
- Use the above mentioned app for direct file transfer from the shared storage space.

If one of these protocols fails, the acquisition process still tries to collect data via the other protocols.

Connection Troubleshooting

- Make sure the USB cable is properly connected to the Android device and the host computer. Try a different USB cable if possible.
- Try using a direct USB 3.0 port and avoid USB hubs.
- Do not use a direct USB C port as this is not yet supported.
- When the Android device is connected, verify what the option for the “USB Preferences” is set to. Most devices require using the “File Transfer” option. In some cases, using the “Charge only” option will work. See the table above to access this setting.
- On some computers the Android USB driver will not work for “File Transfer” in the above option. In this case select “PTP”.
- If the connection is lost during the data acquisition, try restarting the acquisition again as faulty contact can cause this type of issue.
- If the connection is lost during the “Application data” acquisition phase, the application will attempt to re-establish the connection. If successful, acquiring the current application package is likely to take much longer to complete (15 minutes or more).
- Some Android devices will trigger the Windows Device Manager to download and install their USB driver. Let this operation complete in order for Windows to properly interface with that device.
- Some Android devices require an SD card to be inserted for their driver to download.
- Some Android devices may require manually installing their driver. In this case, follow these instructions:
    - To install the Android USB driver on Windows 10 for the first time, do the following:
        - Connect your Android device to your computer's USB port.
        - From Windows Explorer, open Computer Management.
        - In the Computer Management left pane, select Device Manager.
        - In the Device Manager right pane, locate and expand Portable Devices or Other Devices, depending on which one you see.
        - Right-click the name of the device you connected, and then select Update Driver Software.
        - In the Hardware Update wizard, select Browse my computer for driver software and click Next.
        - Click Browse and then locate the USB driver folder. For example, the Google USB Driver is located in C:\Program Files\ADF Solutions Inc\ADF Mobile Device Investigator\drivers\Android.
        - Click Next to install the driver.
- Additional USB drivers for Android are listed here: https://developer.android.com/studio/run/oem-usb

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 even after installing the Google USB Driver, the device is not detected, you can try the Intel Android USB debug driver available here: https://software.intel.com/en-us/xdk/docs/installing-android-debug-bridge-adb-usb-driver-on-windows.
- It is possible that other applications that deal with Android devices could interfere with the ADF application and need to be uninstalled. Here is an example of such an application: Lenovo Phone Companion, SafeNet Authentication Client.
- In case there is not enough disk space on the Android device for the Backup Agent, some artifacts will not be collected (Calls, Calendar, etc), but the rest of the backup process will be executed.
- On Xiaomi phones, in addition to enabling USB debugging, make sure to enable “USB debugging (Security settings)”. This setting requires a SIM card to be present. Also, make sure to turn on Airplane mode after the other settings have been configured.

Connecting an iOS Device

This section describes how to properly establish a connection with an iOS device.

Preparing the iOS Device

To prepare the iOS device, you have to:

- Know the passcode to unlock the device.
- Know the iTunes backup password if one was ever set. Note that this is likely to be different from the handset passcode.
- Prevent auto-locking.
- Place the device in airplane mode, and ensure that both wifi and bluetooth are disabled.
- Trust the host computer when prompted on the device.
- Place the device in Developer Mode (iOS 16 or newer) for screenshots.

The table below describes the most common method to accomplish these actions.

Action	iOS 16+	iOS 12+	iOS 10
Prevent auto-lock	“Settings” > “Display & Brightness” > “Auto-Lock > “Never”	“Settings” > “Display & Brightness” > “Auto-Lock > “Never”	“Settings” > “Display & Brightness” > “Auto-Lock > “Never”
Turn off passcode	“Settings” > “Touch ID & Passcode” > enter passcode > “Turn Passcode Off”	“Settings” > “Touch ID & Passcode” > enter passcode > “Turn Passcode Off”	“Settings” > “Passcode” > enter passcode > “Turn Passcode Off” > “Turn Off”
Prevent voice and data	“Settings” > turn on “Airplane Mode”	“Settings” > turn on “Airplane Mode”	“Settings” > turn on “Airplane 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.

connections			
Trust the host computer	“Trust This Computer?” dialog > select “Trust”	“Trust This Computer?” dialog > select “Trust”	“Trust This Computer?” dialog > select “Trust”
Change iTunes password	In iTunes, “General tab” or “Summary tab” > select “Encrypt local backup” under the “Backups” section	In iTunes, “General tab” or “Summary tab” > select “Encrypt local backup” under the “Backups” section	In iTunes, “General tab” or “Summary tab” > select “Encrypt local backup” under the “Backups” section
Set Developer Mode	The ADF desktop application will set the Developer Mode flag which will require a reboot of the device		

Encrypted iOS Backup

An encrypted iTunes backup is used in order to collect as much data as possible from the iOS device. Encrypted backups are known to potentially recover more user data than unencrypted ones. If an encrypted backup was never set up for the target device, then the temporary password “adf” is used and removed once the backup is completed. If an encrypted backup was already set up, then the password has to be provided before the logical acquisition can begin.
Note that the mobile device has to be unlocked when the password is set or removed.

Advanced Logical Acquisition for iOS

The advanced logical acquisition uses the following standard transfer protocols that do not require jailbreaking the device:

- Use the password protected iTunes backup to collect apps data. The password is set to “adf” and removed or the original one is restored once the backup is complete.
- Use the Apple File Conduit (AFC) protocol for direct file transfer.

If one of these protocols fails, the acquisition process still tries to collect data via the other protocols.

Connection Troubleshooting

- Make sure the USB cable is properly connected to the iOS device and the host computer. Try a different USB cable if possible.
- Try using a direct USB 3.0 port and avoid USB hubs.

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 the connection cannot be established with an iOS device, make sure the Apple Mobile Device Service or the Apple Mobile Device Process is running. If it is not present you may need to re-install iTunes. See the "ADF Smartphone Driver Pack Installation" section of the "Installing the ADF Application" guide for details.

Connecting a ChromeOS Device

This section describes how to connect with a ChromeOS device. See the "Configuring Chromebooks for Acquisitions and Casting" guide for full details.

Preparing the ChromeOS Device

To prepare the Android device, you usually have to:

- Know the passcode to unlock the device.
- Prevent auto-locking.
- Place the device in airplane mode.
- Activate Linux.
- Activate Android Debug Bridge (ADB).
- Allow USB debugging when prompted on the device ("always allow from this computer").

Connecting a Wear OS Device

This section describes how to connect with a Wear OS device. See the "Connecting Android and Wear OS Devices Wirelessly" guide for full details.

Preparing the Wear OS Device

To prepare the Wear OS device, you usually have to:

- Ensure Screen Timeout is set to 1 minute.
- Enable:
    - Developer Options.
    - ADB Debugging.
    - Wireless Debugging.
- Pair the device with the computer running the ADF desktop application.

Acquiring a Device

It is possible to acquire a device by navigating to one of these menus:

- **Home** > **Investigate Device** > **Acquire**.
- **Scan Progress** > **IMAGE**.

Here are the instructions to acquire a mobile 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.

1. On the **Enter Information** screen, enter the following:
    a. **Source**: click on the **Add Device** button to connect the device as explained above.
    b. **Destination**: select the parent folder where the acquired data will be saved.
    c. **Acquisition** Name: the name of the folder where the acquired data will be saved.
    d. **Create Load Files for third-party eDiscovery platforms** checkbox**:** when checked, additional Load Files are created and accessible from C:\ProgramData\ADF Solutions Inc\v4\Acquisitions\[acquisition name]\load_files. See more details about the Load File format in the ADF Data Container Structure guide.
2. To add a form (as explained in the Managing Forms guide), click the **Forms** button located in the toolbar on the right-hand side.
3. When ready, click on the **PROCEED** button to start the acquisition.
4. A progress screen is displayed indicating the time elapsed and remaining.

Logical Acquisition File Structure

The acquired data is saved in the ADF Data Container. See more details about its structure in the ADF Data Container Structure guide.

Collected Data Interpretation

The table below provides some details on how to interpret some of the collected data.

OS	File	Note
iOS	Media/PhotoData/Thumbnails/V2/DCIM/100APPLE/IMG_0005.JPG/5003.JPG Media/PhotoData/Thumbnails/V2/DCIM/100APPLE/IMG_0006.JPG/5003.JPG	Different pictures have the same name and this could be confusing. These pictures are indeed saved with the same name on the iOS device, but notice the different path which includes a folder name resembling a file name.

Excluded Data

The table below describes data that is not processed.

OS	File	Note
Android	*/base.apk	No user data found in this container.

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.

Android	*/system.new.dat	No user data found in this container.

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.