ADF Data Container Structure

Introduction

When acquiring data from a target device, the ADF tools create a data container. This document describes the structure of that data container. A data container is created when you acquire, preview or scan a mobile device, capture a device screen, collect files, or image a computer through the remote agent (ADF Data Container format). Starting with version 6.4.0, the folder of an E01 or DD image also contains the metadata of a data container (see Files from a disk image below).

What is the Data Container?

Data containers are created to store the files and metadata found on target devices (a.k.a. data sources). Their goals are to make it easy to collect a variety of data, store it in a way that's easy to transport, and be searched and processed.

Structure

The data acquired from a data source is saved in a folder with the following files and folders. Which of them are present depends on the type of acquisition.

Acquisition metadata

- metadata.zip
    - This file contains information about the acquisition and the data source
        - info
            - data_container.json
            - acquisition_information.json
            - data_source.json
        - log (only when load files are created)
            - log files of the scan that ADF runs to create the load files
- forms (folder): contains the forms completed before an Acquire, Screen Capture or Collect Files acquisition, saved as PDF files (see the Managing Forms guide).
- meta_info: created by the ADF application when a tag is assigned to the acquisition on the Acquisitions page (see the Viewing Acquisitions guide). It is not part of the acquired data.

Files from a remote agent or Collect Files acquisition

- files.zip: contains the files acquired from the data source. The following file properties are preserved inside this archive: paths, file names and timestamps. In a Collect Files acquisition, each file is saved under its full path on the source; for a phone or camera connected over MTP, the path starts with the name of the device.
- files_meta.zip: contains json files called files_meta_00001.json, files_meta_00002.json and so on, which save the file system properties (path, name, size and dates) of the files that could not be read during the acquisition, 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.

example because they were blocked by the operating system. Up to 10,000 records are saved in each json file. This file is created only when such files are found.

Files from a disk image (E01 or DD)

- <Image Name>.E01, <Image Name>.E02 and so on (EWF format), or <Image Name>.001, <Image Name>.002 and so on (DD format): the image of the drive.
- <Image Name>.log: the imaging log, with the case and drive information, the start and end times, the image format and segments, and the MD5 and SHA1 hash values of the drive (see the Imaging a Target Computer guide). It is created only when the imaging completes.
- metadata.zip: the acquisition metadata described above, starting with version 6.4.0.

If the imaging is interrupted or fails, the segments written so far and metadata.zip stay in a folder whose name starts with incomplete_imaging_, in the destination.

Files from an iOS device acquisition

- afc_backup.zip: contains the files obtained from the Apple File Conduit protocol. It is not created by a device preview.
- iTunes_backup (folder): contains the files obtained from an iTunes backup that is not encrypted (usually a device with iOS 10 and no backup password).
- iTunes_encrypted_backup (folder): contains the files obtained from an encrypted iTunes backup. When no backup password is set on a device with iOS 11 or later, ADF sets the temporary password “adf” for the backup and removes it once the backup is complete, so the backup is saved in this folder.

For a device with iOS 9 or earlier, no iTunes backup is made: the acquisition contains only afc_backup.zip.

Files from an Android, ChromeOS or Wear OS device acquisition

- adb_backup.zip: contains the files obtained from an adb backup. It is not created for Wear OS devices.
- shared_backup.zip: contains the files obtained from the Android shared storage space and the SD card. It is not created by a device preview.

Acquisitions made with version 5.8 or earlier contain backup.zip instead of adb_backup.zip.

Files from a screen capture

- sc_files (folder): contains the screenshots and video recordings from the video stream or mirrored device.
    - screen_capture.json: contains the metadata of each screenshot and recording: path of the file, screen group, MIME type, size, capture date, screen orientation, length of the recording, and the comments and tags added during the capture.

When a single mobile device is scanned with a search profile that includes the Screen Recordings and Screenshots capture, the screenshots and recordings made during the scan are saved in the sc_files folder of the acquisition that the scan creates.

Digital artifacts

- artifacts_raw.zip: contains information obtained from API/system calls executed directly on the target device (for an Android device, also the data collected by the Backup Agent), and properties.json with the device properties and the acquisition status recorded by ADF. For a screen capture, it contains only properties.json.

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.

- artifacts.zip: contains json files with the digital artifacts extracted from the data source, and their JSON schemas in the schema folder. It is created only together with the load files (see Load Files section below).

Load Files

- load_files (folder): contains the .dat load files and the sub-folders with the message texts and attached files that they reference. It is created only when load files are requested (see Load Files section below).



Most of the zip files are multi-volume zip files: the data is saved in volumes named name.z01, name.z02 and so on, and the last volume, name.zip, holds the list of the files in the archive (for example files.z01 and files.zip). Except for files.zip of a remote agent acquisition, each volume is at most 4 GB minus 1 MB (4,293,918,720 bytes). For a remote agent acquisition, the volume size of files.zip is the Segment Size in GB entered on the Image screen (8 by default; 0 creates a single file). metadata.zip, files_meta.zip and artifacts_raw.zip are single files. The files are stored in the zip files without compression.

Forensic Integrity

The data container includes some built-in features that help with the forensic integrity of the data.

- The files that contain the acquired data are hashed with SHA-256: each volume of the zip files (for example adb_backup.z01 and adb_backup.zip) and, for a disk image, each E01 or DD segment. The hash values are saved, with the file names and sizes, in the acquisition_information.json file (see below), under the acquisition methods that the files belong to. This makes it possible to verify the integrity of these files over time. metadata.zip and files_meta.zip are not hashed.
- Folders are not hashed. For the sc_files, iTunes_backup or iTunes_encrypted_backup, and load_files folders, acquisition_information.json saves the number of files in the folder and its sub-folders and their total size in bytes (numberOfFiles and totalSize). For sc_files, these values do not include screen_capture.json.
- The unique identifier of the data container (defined in metadata.zip/info/data_container.json/id) is also saved in the comment of each zip file of the data container (metadata.zip, files.zip, files_meta.zip, afc_backup.zip, adb_backup.zip, shared_backup.zip, artifacts_raw.zip and artifacts.zip) as the UUID field. The comment also contains the version field: the version of the data container format (8 for data containers created with version 6.4.0). In a multi-volume zip file, the comment is in the last volume (the .zip file). This makes it possible to verify which files belong to the data container.

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.

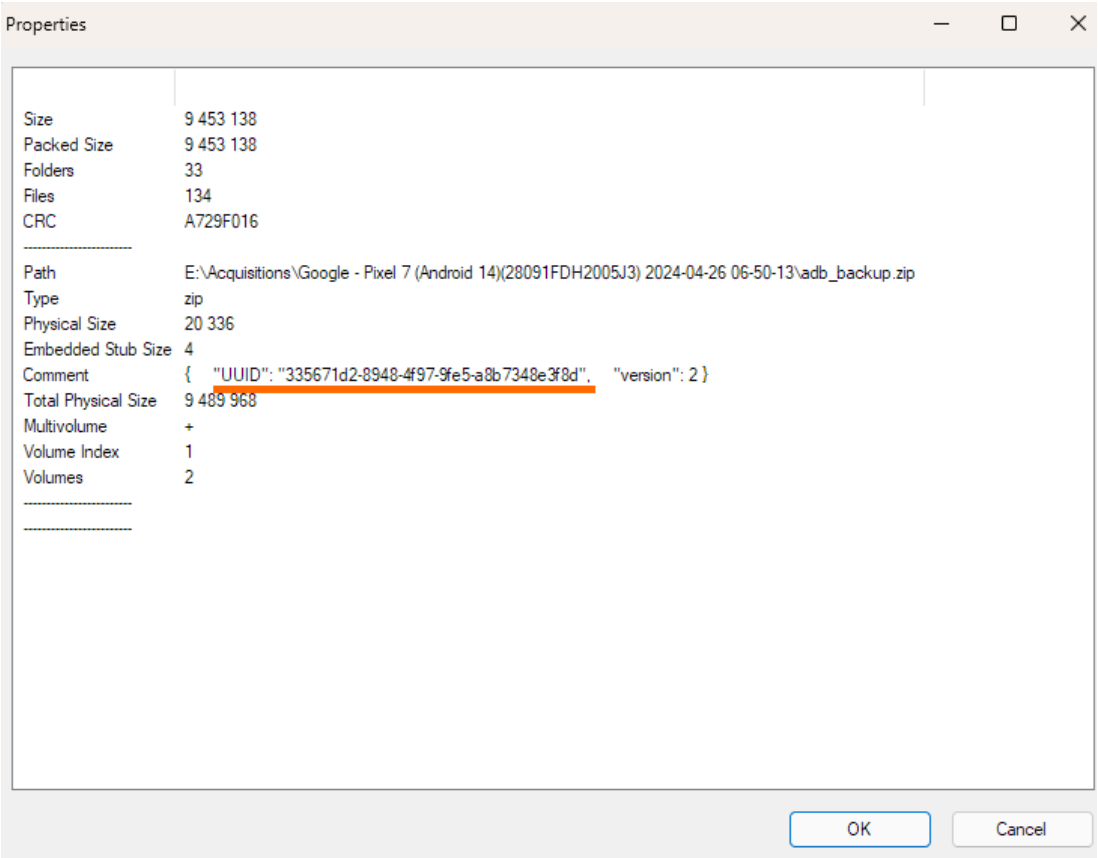


Figure: Zip file comment showing the UUID of the data container and the version of the data container format

metadata.zip

The metadata.zip file contains the following JSON files in its info folder. They are created for every acquisition and describe the data container, the acquisition and the data source. Starting with version 6.4.0, they use version 5 of the ADF data container schema, named in the $schema field of each file (for example /schema/cm/v5/data_container). The content is in the items array, or in the item object for data_source.json. Dates are in UTC.

data_container.json

This file contains information about the data container where the acquisition data is saved:

- id: the unique identifier of the data container, also saved in the comment of its zip files
- name: the name of the data container folder
- type: Acquisition, or Screen Capture when the data container holds only a screen capture
- size: the total size, in bytes, of the acquired files and folders (metadata.zip and files_meta.zip are not counted)
- startDate and endDate: when the acquisition started and ended. For a disk image, they show when its metadata was written at the end of the imaging; the imaging times are in the .log file.
- createdByApp: the name and 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.

- createdByUser and createdBySystem: the Windows user (name and security identifier) and the computer (SMBIOS UUID and MAC address) that made the acquisition
- caseNumber: the Case Number entered for the acquisition (starting with version 6.4.0)
- customFields: for a disk image or a remote agent acquisition, the Evidence Number, Unique Description, Examiner and Notes entered on the Image screen (evidenceNumber, uniqueDescription, examiner and notes); empty otherwise


```
{
    "$schema": "/schema/cm/v5/data_container",
    "items": [
        {
            "caseNumber": "2026-0147",
            "createdByApp": {
                "appName": "ADF PRO",
                "appVersion": "6.4.0.494"
            },
            "createdBySystem": {
                "macAddress": "00-00-5E-00-53-01",
                "startDateFromFirmware": "2026-10-02T14:26:18Z",
                "uuid": "A1B2C3D4-E5F6-4A7B-8C9D-0E1F2A3B4C5D"
            },
            "createdByUser": {
                "sid": "S-1-5-21-1111111111-2222222222-3333333333-1001",
                "username": "Examiner"
            },
            "customFields": {},
            "endDate": "2026-10-02T15:41:57Z",
            "id": "3f6c1d2a-8b4e-4c7f-9a15-2e8d0b7c4a61",
            "name": "Google - Pixel 8 (Android 15)(1A2B3C4D5E6F) 2026-10-02 10-26-16",
            "size": 6261000580,
            "startDate": "2026-10-02T14:26:18Z",
            "type": "Acquisition"
        }
    ]
}
```


acquisition_information.json

This file contains information about the acquisition process: when it started and ended, its status and, for each acquisition method used, its status, the format of the data and the files or folders it created (see Forensic Integrity). The status is Completed, Incomplete or Interrupted; when one method is Incomplete, the acquisition is Incomplete too, unless it was interrupted. The acquisition methods are:

- ADF agent: files.zip of a remote agent acquisition
- Disc File Copy and Media Transfer Protocol: files.zip of a Collect Files acquisition from a drive or from a device connected over MTP
- Disk Block Copy: the E01 or DD segments of a disk image (starting with version 6.4.0)
- Android Debug Bridge Backup, Android Debug Bridge File Transfer, Android Data Dump App and Android Debug Bridge Remote Shell: adb_backup.zip, shared_backup.zip and artifacts_raw.zip of an Android device
- iTunes Backup, Apple File Conduit and iTunes Protocol: the iTunes backup folder, afc_backup.zip and artifacts_raw.zip of an iOS device

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.

- Android Debug Bridge Casting, AirPlay and Screen Capture: the sc_files folder of a screen capture from an Android device, an iOS device or a video source
- ADF Load Files Processing Service and ADF Artifact Processing Service: the load_files folder and artifacts.zip

A file can be listed under several methods: artifacts_raw.zip is listed under every Android Data Dump App, Android Debug Bridge Remote Shell, iTunes Protocol and Apple File Conduit method of the acquisition.


```
{
    "$schema": "/schema/cm/v5/acquisition_information",
    "items": [
        {
            "acquisitionDetails": {
                "acquisitions": [
                    {
                        "files": [
                            {"filename": "adb_backup.z01", "sha256":
"34a591a41669339a5a51a504b18c87ac8e06243b3836cabace20fe48f2c82381", "size": 1974396},
                            {"filename": "adb_backup.zip", "sha256":
"4db08e1074b535ed1f1e56c16993897208075fd3b7605ee82ec5b5d55e87c142", "size": 3267}
                        ],
                        "formatDetails": {"compressionLevel": 0, "format": "zip", "segmentSize": 4293918720,
"type": "logical"},
                        "method": "Android Debug Bridge Backup",
                        "status": "Completed"
                    },
                    {
                        "files": [
                            {"filename": "artifacts_raw.zip", "sha256":
"aef8b9d5e4bbe4857c004cb0a63948313a6afe9ee50694612ad9d5f9fa722ff5", "size": 389362662}
                        ],
                        "formatDetails": {"compressionLevel": 0, "format": "zip", "segmentSize": 4293918720,
"type": "logical"},
                        "method": "Android Data Dump App",
                        "status": "Completed"
                    },
                    {
                        "files": [
                            {"filename": "shared_backup.z01", "sha256":
"777ff8ef4ec42aa5970939eb24cb9edd881b76cba723cc95c2f0a080ef5ca8a4", "size": 4293918720},
                            {"filename": "shared_backup.z02", "sha256":
"988d2037448fea524982a13cba612c821304946ad9abc57ee985a46cd971104b", "size": 1532871190},
                            {"filename": "shared_backup.zip", "sha256":
"29ac8d64d0be0020fa6ef2e2b75e54c0959b6e1d59a5145053ec0518cfb5eee7", "size": 2183477}
                        ],
                        "formatDetails": {"compressionLevel": 0, "format": "zip", "segmentSize": 4293918720,
"type": "logical"},
                        "method": "Android Debug Bridge File Transfer",
                        "status": "Completed"
                    },
                    {
                        "files": [
                            {"filename": "artifacts_raw.zip", "sha256":
"aef8b9d5e4bbe4857c004cb0a63948313a6afe9ee50694612ad9d5f9fa722ff5", "size": 389362662}
                        ],
                        "formatDetails": {"compressionLevel": 0, "format": "zip", "segmentSize": 4293918720,
"type": "logical"},
                        "method": "Android Debug Bridge Remote Shell",
```


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.

```
                        "status": "Completed"
                    },
                    {
                        "folders": [
                            {"folderName": "load_files", "numberOfFiles": 214, "totalSize": 31873522}
                        ],
                        "formatDetails": {"format": "flat file", "type": "logical"},
                        "method": "ADF Load Files Processing Service",
                        "status": "Completed"
                    },
                    {
                        "files": [
                            {"filename": "artifacts.z01", "sha256":
"9f4924df3caa2a6d5fa43b475114b07ac19c5c12bdf4f52044c76cfa20694d1b", "size": 8811040},
                            {"filename": "artifacts.zip", "sha256":
"906ffc7c87c8e749b36805684b71f98c532bb4d0351dd999fd01fa8bcdf8fade", "size": 2306}
                        ],
                        "formatDetails": {"compressionLevel": 0, "format": "zip", "segmentSize": 4293918720,
"type": "logical"},
                        "method": "ADF Artifact Processing Service",
                        "status": "Completed"
                    }
                ],
                "dataContainer": {"id": "3f6c1d2a-8b4e-4c7f-9a15-2e8d0b7c4a61", "name": "Google - Pixel 8
(Android 15)(1A2B3C4D5E6F) 2026-10-02 10-26-16"},
                "endDate": "2026-10-02T15:41:57Z",
                "id": "b7e2a9c4-1d3f-4e8a-a6b0-5c9d2f1e7a38",
                "startDate": "2026-10-02T14:26:18Z",
                "status": "Completed"
            }
        }
    ]
}
```


data_source.json

This file contains information about the target device (the data source):

- dsType: the type of data source: Mobile device, Smartwatch device (Wear OS), MTP device, Targeted files (Collect Files from a drive), Remote agent, Physical image (disk image) or Screen capture (video source)
- name: the name of the data source; for a mobile device, its manufacturer, model and operating system
- device: the name, model, manufacturer and serial number of the device and, for a mobile device, the IMEI, ICCID and phone number of its SIM cards
- drives, partitions and volumes: for a computer or a drive, its drives, partitions and volumes with their size, file system and encryption. For a mobile device, volumes holds the operating system, its version and the time zone of the device.
- encryptionPassword and encryptionPasswordKey: for an encrypted iTunes backup, the backup password and, except for a device preview, the key derived from it.


```
{
    "$schema": "/schema/cm/v5/data_source",
    "item": {
        "created": "2026-10-02T14:26:18Z",
```


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.

```
        "dataContainer": {
            "id": "3f6c1d2a-8b4e-4c7f-9a15-2e8d0b7c4a61",
            "name": "Google - Pixel 8 (Android 15)(1A2B3C4D5E6F) 2026-10-02 10-26-16"
        },
        "device": {
            "deviceName": "shiba",
            "manufacturer": "Google",
            "model": "Pixel 8",
            "serialNumber": "1A2B3C4D5E6F",
            "simCards": [
                {
                    "iccid": "8901260000000000006",
                    "imei": "350000000000006",
                    "phoneNumber": "+12025550123"
                }
            ]
        },
        "dsType": "Mobile device",
        "id": "5e0a3c7d-2f19-4b8e-9d64-a1c3e5f70b28",
        "name": "Google - Pixel 8 (Android 15)",
        "volumes": [
            {
                "os": "Android",
                "osVersion": "15",
                "timeZone": "America/New_York"
            }
        ]
    }
}
```


Load Files

Load Files can be created at the end of the acquisition of a mobile device, when Create Load Files for third-party eDiscovery platforms is selected on the Enter Information screen of Acquire or Screen Capture (see the Acquiring an iOS, Android, Wear OS or ChromeOS Device guide). In Screen Capture, they are created only if you click ACQUIRE after the capture. In ADF Mobile Device Collector, this option is selected by default. ADF scans the acquisition with the built-in Mobile Devices - Load Files search profile and creates the load files from the records found. Load files are created only if this scan ends with the status Complete. If it does not, or if the generation fails or you click CANCEL, the message “An error happened during Load Files generation” is displayed and the acquisition is marked Incomplete.

A load file is created for each one of these record types, when records of that type are found:

- Application
    - Installed Application (installed_application.dat)
- Communication
    - Call (call.dat)
    - Message (message.dat)
    - Saved Contact (saved_contact.dat)
    - Voicemail (voicemail.dat)

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.

- User Data
    - Calendar (calendar.dat)
    - Note (note.dat)

Emails are not exported to load files.

Load File Structure

The created load files use the following specifications:

- .dat file extension; the file name is the record type, for example message.dat
- UTF-8 encoding, with a byte order mark (BOM)
- Header row that defines the exact properties for each record, followed by one row per record and one row per attached file. Each row ends with a carriage return and a line feed (CR LF).
- Column definition
    - DOCID: mandatory column containing the unique identifier of the row within the load file (a number starting at 1)
    - ParentDocID: used to connect a child row to its parent record (for example an attachment to the message it comes from). It is empty for records.
    - DocType: the record type (for example message), or attached file for the row of an attachment
    - ExportFilePath (message.dat and note.dat only): references an external file (such as the text of a message, or an attachment). Note that this field contains a path that is relative to the location of the load file, for example message_txt_content_0/15.txt
    - The other columns contain the properties of the record type. When a property has several values, they are separated by a semicolon (;). Values that have several fields are written as JSON text.
- Reserved characters
    - Column delimiter: ASCII 20 (hexadecimal 0x14)
    - Quote: ASCII 254 (þ). Each value is enclosed in this character. In the UTF-8 file it takes two bytes (0xC3 0xBE).
- Date format: all date/time are in UTC and use this format YYYY-MM-DDTHH:MM:SS+00:00
- Sub-folders
    - RECORD_TYPE_NAME_txt_content_N: containing the textual content of the records, one DOCID.txt file per record. For example: message_txt_content_0, etc.
    - RECORD_TYPE_NAME_bin_content_N: containing the binary content of the files associated with the records, named after the DOCID of the record and the position of the file (for example 15_0.jpg). For example: message_bin_content_0, note_bin_content_0, etc.
    - N starts at 0. Each sub-folder will only contain up to 10000 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.