FEX CLOUD Capture

User Guide

Published: 19-Jun-24 at 20:43:05

GetData

1.1 CONTENTS

1. FEX CLOUD CAPTURE OVERVIEW

Cloud servers are now commonly used to store every-day end user data, including emails, documents, photos, and communication logs. By acquiring data from cloud services, investigators can uncover critical evidence that may not be available on local devices.

FEX Cloud Capture™ is a software tool by GetData Forensics (www.getdataforensics.com) for the acquisition of data stored on remote cloud servers. FEX Cloud Capture aids in maintaining the integrity and authenticity of the evidence, by collecting data in a forensically sound manner.

Data captured by FEX Cloud Capture is done so locally by the investigator. No data, stored, or used by GetData Forensics.

1.1 CLOUD CAPTURE CONSIDERATIONS

When capturing data from the cloud, it is important that investigators consider critical factors to ensure the process is effective, legal, and secure:

- **Legal Compliance**: Investigators must adhere to legal requirements and obtain proper authorization, such as search warrants, to access cloud data. Different jurisdictions have varying laws regarding data privacy and access. Be aware of the legal jurisdictions and data sovereignty laws applicable to the data you are capturing.
- **Chain of Custody**: Maintaining a clear and documented chain of custody is essential to ensure the integrity and admissibility of the evidence in court.
- **Data Preservation**: It is crucial to preserve the original data without alteration. Where possible, investigators should use forensically sound methods and tools to capture and store data, ensuring it remains unchanged.
- **Service Provider Cooperation and Compliance**: Collaborate with cloud service providers to understand their data retrieval processes and ensure compliance with their terms and conditions.

It should be noted by the investigator that when a cloud account is accessed, it is likely that end user notifications will be generated, which can include email, text, and push notifications. The method and timing of notifying the account owner can vary based on the service provider's policies, legal requirements, and the nature of the access.

1.2 CLOUD API ACCESS

FEX Cloud Capture interacts with cloud storage services using APIs (Application Programming Interface) provided by cloud providers. These APIs enable comprehensive programmatic access to files and folders stored in the cloud. Through these APIs, FEX Cloud Capture can read files, including metadata, sharing, and permissions. Extensive documentation and resources are

published by cloud providers and should be referred to for detailed technical information. API references include:

- **Drop Box**: https://www.dropbox.com/developers/documentation
- **Google Drive:** https://developers.google.com/drive/api/reference/rest/v3
- **One Drive:** https://docs.microsoft.com/en-us/onedrive/developer/

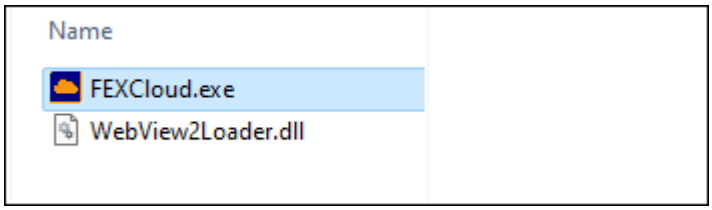
2. FEX CLOUD CAPTURE DOWNLOAD

FEX Cloud Capture is available for download from the GetData Forensic website:

- https://getdataforensics.com/product/FEX Cloud Capture-capture/

Unzip the download file. FEX Cloud Capture is a stand-alone executable. It does not require installation or activation.

Figure 1: FEX Cloud Capture installation.



3. FEX CLOUD CAPTURE SETUP

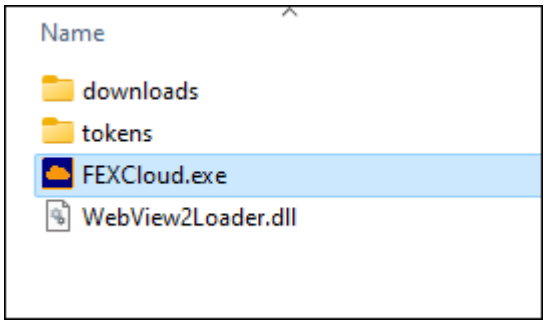
When an investigator captures cloud data, several considerations must be taken into account for the local forensic computer equipment and the network connection to ensure the process is secure and reliable:

- **Bandwidth and Speed**: A high-speed, reliable internet connection is crucial for efficiently capturing large amounts of data from the cloud. Consider having a redundant connection in place in case of network failures.
- **Workstation Capacity:** Ensure the forensic computer has sufficient CPU power and RAM to handle large volumes of data. Adequate storage capacity is essential, considering that cloud captures can involve significant data volumes.
- **Workstation and Network Security:** Third party data can expose a to security threats. Ensure consideration is given to protecting the local environment whilst maintaining the speed and stability of the capture.

3.1 FEX CLOUD CAPTURE – BASE FOLDERS

FEX Cloud Capture is launched by executing **FEXCloud.exe**. Additional folders will be created on first launch, including **downloads** and **tokens:**

Figure 2: FEX Cloud Capture folder after first launch.



3.1.1 DOWNLOADS FOLDER

The **downloads** folder is the default storage location for captured data. The structure of the data in the folder is discussed in more detail later in this document.

3.1.2 TOKENS FOLDER

An access token is a security credential issued by an authentication server that grants a user or application permission to access specific resources or services hosted in the cloud. These tokens are typically generated during the authentication process and contain encoded information about the user's identity and the permissions or scopes they have been granted.

Access tokens are essential for securing communications and ensuring that only authorized users or applications can access sensitive data or perform specific actions. They are usually short-lived to minimize security risks, and their usage is governed by various protocols such as OAuth 2.0, which is widely used for authorization in cloud services.

GetData Forensics

When a client application needs to access a protected resource, it includes the access token in its request to the resource server. The resource server then validates the token, ensuring it is still valid and that the requester has the necessary permissions. If the token is valid, the server grants access to the requested resource. This mechanism helps maintain robust security and control over cloud-based resources and services.

The default action of FEX Cloud Capture is to remove access tokens on disconnection or exit. This is set in **Options** as per section 5 below.

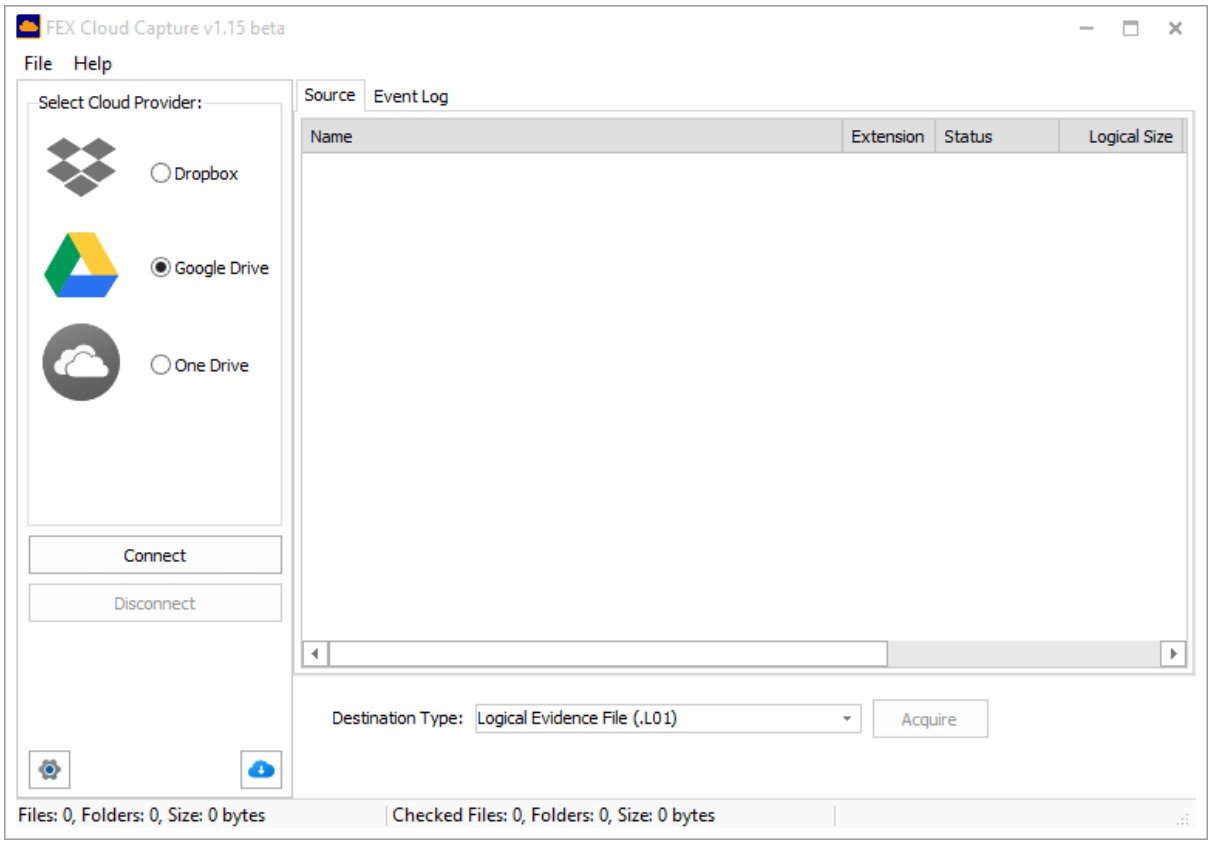
4. RUNNING FEX CLOUD CAPTURE

Launching **FEXCloud.exe** opens the program GUI.

4.1 SELECT THE CLOUD PROVIDER

Select the cloud provider from the left-hand column:

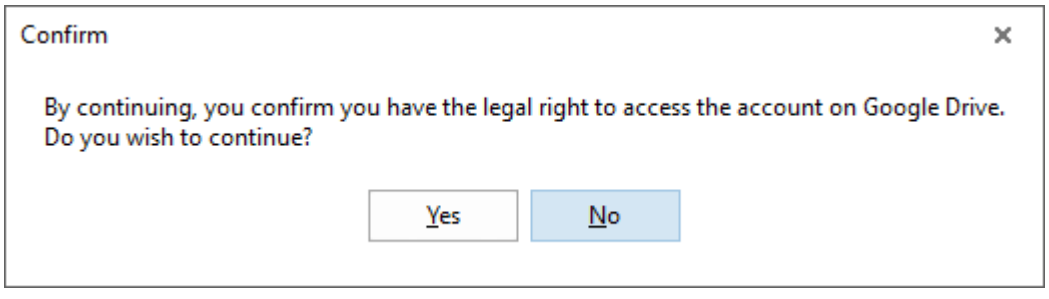
Figure 3: FEX Cloud Capture GUI



4.2 CONNECT

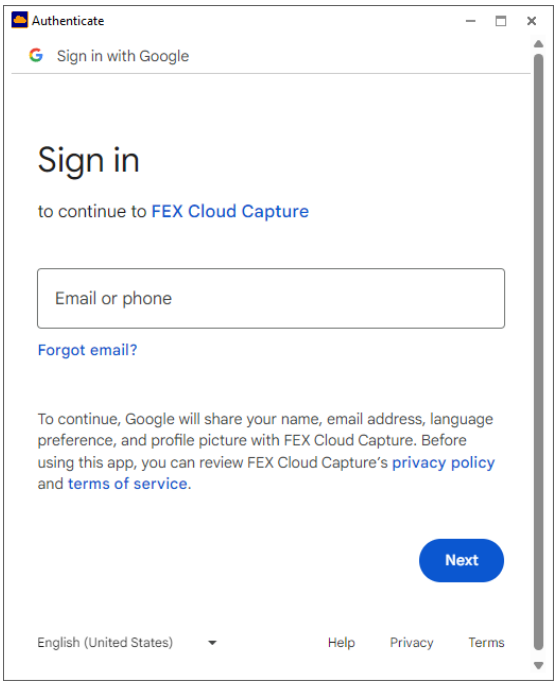
Press the Connect button. You will be prompted with the following confirmation message:

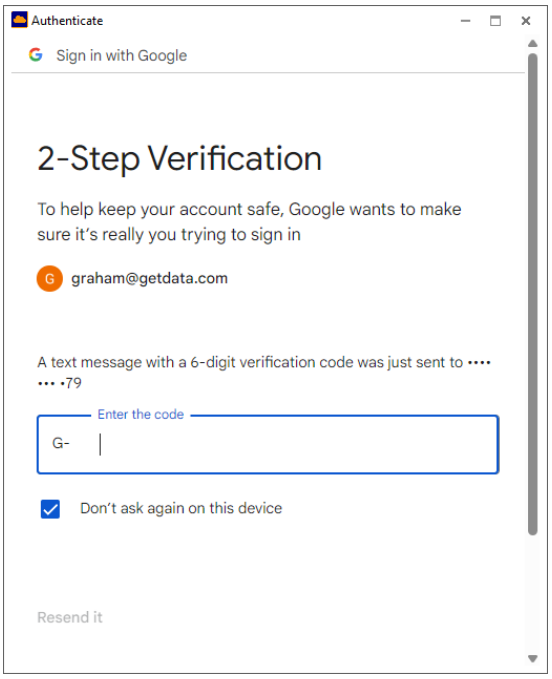
Figure 4: Legal right

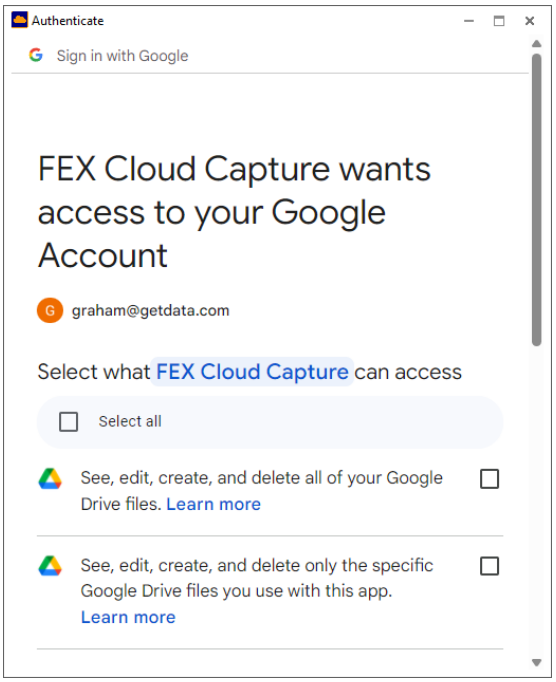


Depending on the cloud provider, you will be prompted with one or more account security questions. This can include a 2-Setp verification procedure:

Figure 5: Account access verification



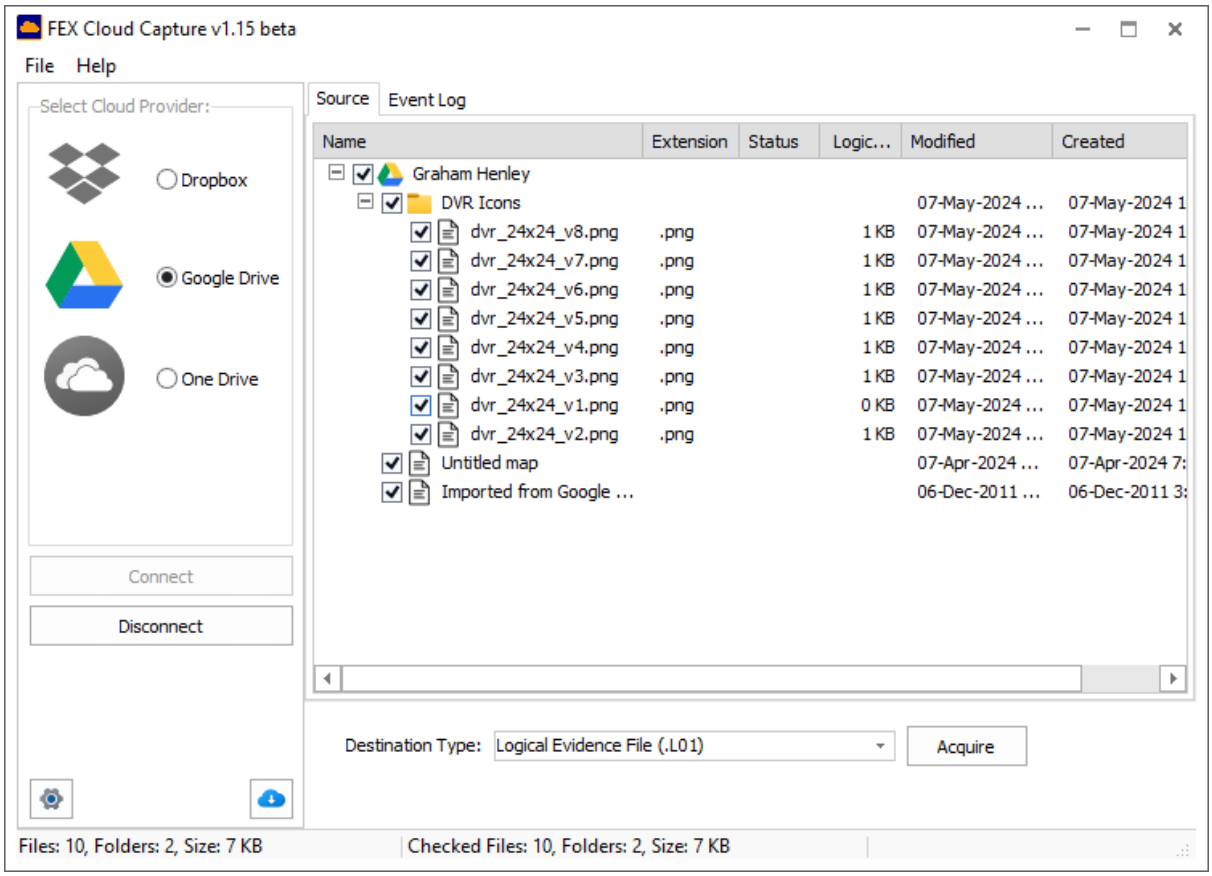




4.3 FILE LIST

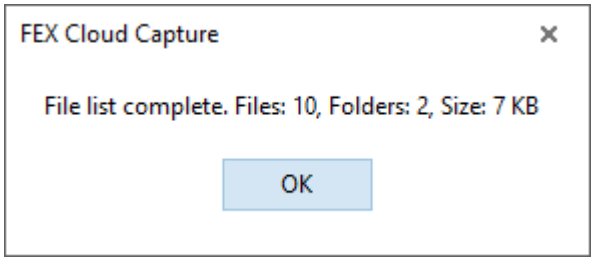
When the connection is made, the FEX Cloud Capture GUI will populate with a list of cloud files in the target account. Depending on the volume of content, this may take several minutes.

Figure 6: Checked Items



A message will display when the file list is complete.

Figure 7: File List.

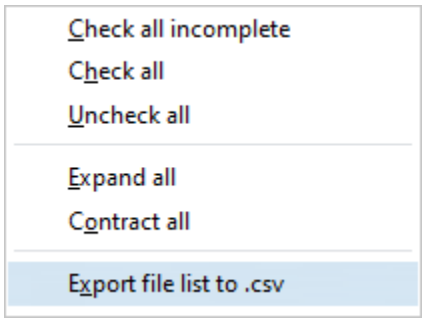


4.4 EXPORT A FILE LIST TO .CSV

To **export a list of files** in the target cloud account **to CSV**:

1. Right-click in the **Source** window.
2. Select **Export file list to .csv** from the drop-down menu:

Figure 8: Export a list of files to CSV.



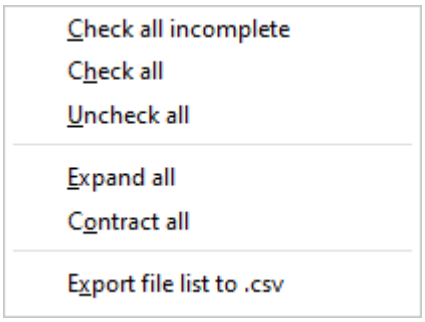
4.5 SELECT (CHECK) FILES TO CAPTURE

The user must select files to acquire by placing a check mark next to the file name, as shown in Figure 6: Checked Items above (the **Acquire** button will not become active until at least one file is selected).

To **select all files**:

- Place a check in the **root** folder and all sub-files and folders will be checked.
- Or right-click and select **Check all** from the menu.

Figure 9: Right-click checking options.



To select **groups of files**:

- Use the **SHIFT** key to select a folder and its entire contents.
- Use the **CTRL** key to select an individual file, or an individual folder and its contents.

4.6 DESTINATION TYPE (ACQUISITION FORMAT)

Each FEX Cloud Capture acquisition will be written to the **downloads** folder with a unique parent folder in the format:

yyyy-mm-hh-mm-ss [Account Name]-[Cloud Provider]

The following acquisition formats are available:

4.6.1 LOGICAL EVIDENCE FILE (L01)

A Logical Evidence File (L01) is a proprietary file format used in digital forensics to store the results of a logical acquisition from a digital device. The L01 format is an extension of the E01 format, used for physical disk images, but tailored for logical acquisitions.

- **Format and Structure**

  The L01 file format is designed to store selected files, folders, and metadata from a digital device or service. It includes a comprehensive metadata header containing information about the acquisition process, such as the date and time of acquisition, the name of the examiner, and the tool used for the acquisition. The structure allows for efficient storage and retrieval of individual files and directories, maintaining their original hierarchy.

- **Data Integrity and Verification**

  The L01 format supports hash values for each file included in the logical acquisition. Hash values are cryptographic fingerprints that ensure the integrity and authenticity of the files.

- **Compression and Encryption**

  The L01 file can be compressed to save storage space, making it easier to manage large volumes of data.

- **Flexibility and Compatibility**

  The L01 format is supported by various forensic analysis tools, making it widely compatible and versatile for investigators. It can be used to acquire data from different types of devices and cloud services.

- **Targeted Data Collection**

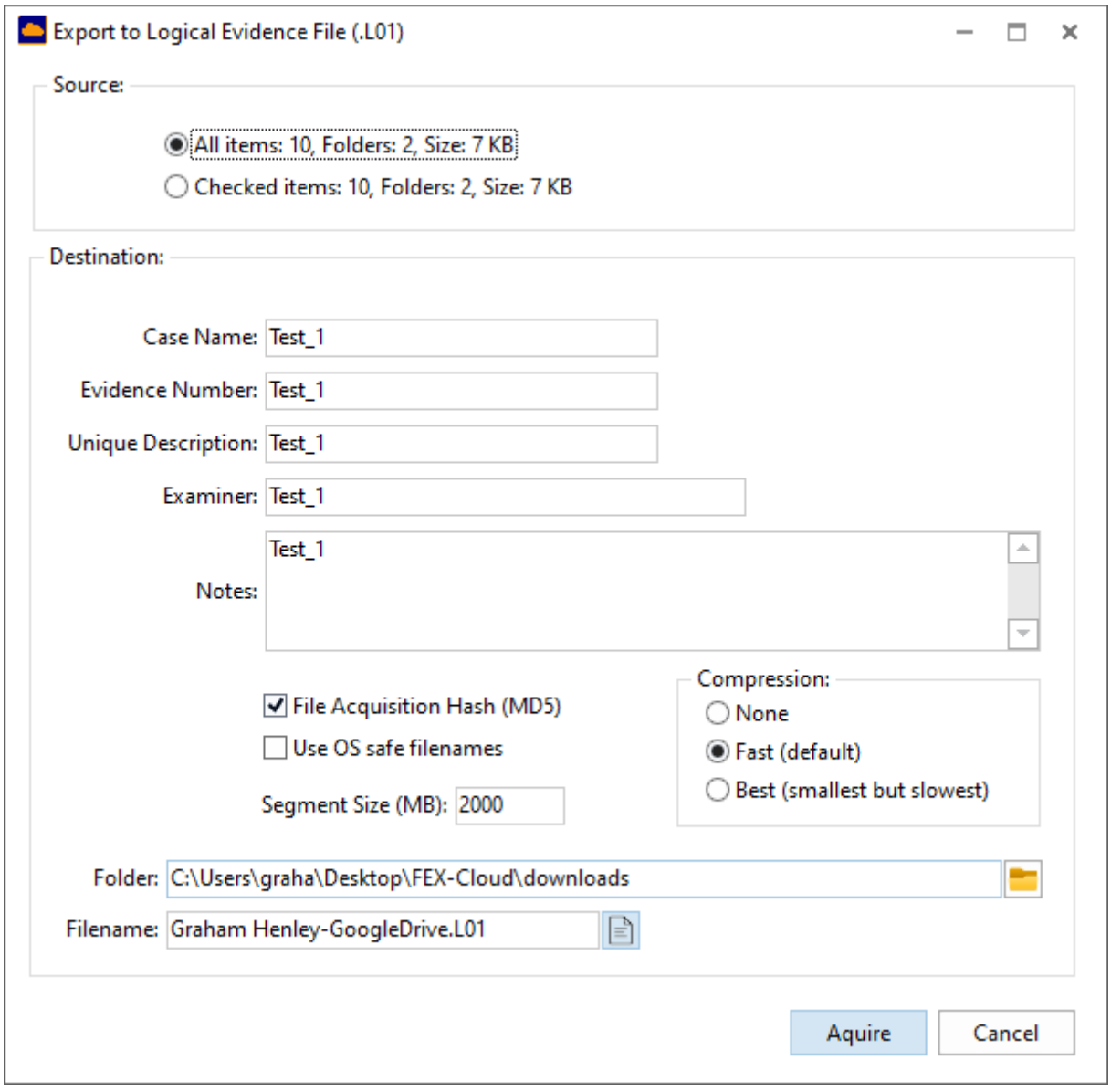
  Logical acquisitions focus on specific files, folders, or data structures rather than capturing an entire disk image. This is particularly useful in cloud environments where complete data sets may not be feasible or necessary. Investigators can select relevant data, reducing the volume of irrelevant information and speeding up the analysis process.

The L01 format allows for targeted data collection, has inbuilt data integrity checksums, and wide compatibility with forensic tools. These attributes make it a powerful format for securely and effectively managing digital evidence. The detailed metadata and hash values included in the L01

file provide robust evidence that can be presented in court, supporting the credibility and reliability of the forensic findings.

When **Logical Evidence File (.L01)** is selected as the **Destination Type** the following window will appear when the **Acquire** button is clicked.

Figure 10: L01 acquisition details.



File Acquisition Hash (MD5):

A MD5 acquisition hash is calculated for each individual file.

Use OS safe filenames:

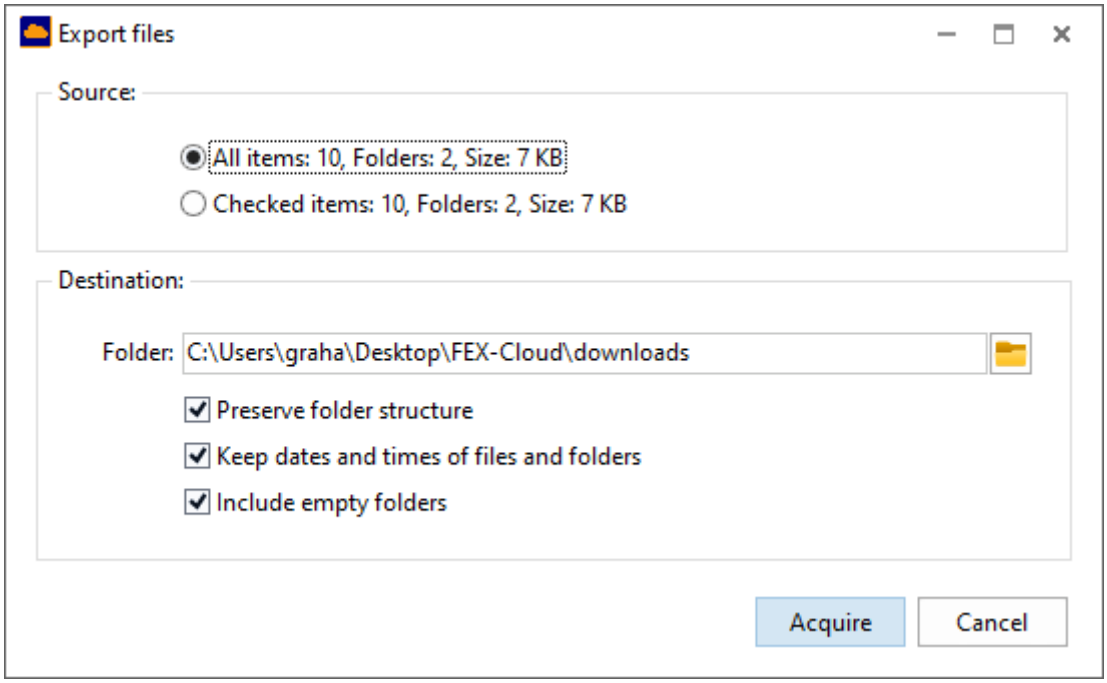
This option is used to ensure that filenames within the L01 are safe in cross-platform use (e.g., Linux to Windows). When this option is checked:

- Characters: #0 .. #31, ':', '\', '/', '?', '>', '<', '*', '|', '"' are replaced by space.
- Blank spaces at the end of filenames are trimmed.

4.6.2 LOCAL FOLDER

The **Destination Type Local Folder** writes acquired folders and files to disk.

Figure 11: Destination Type - Local Folder.



Preserver folder structure:

When checked GUI folder structure for acquired items is kept.

If not selected, the acquired files will be written into a single folder.

Keep dates and times of files and folders:

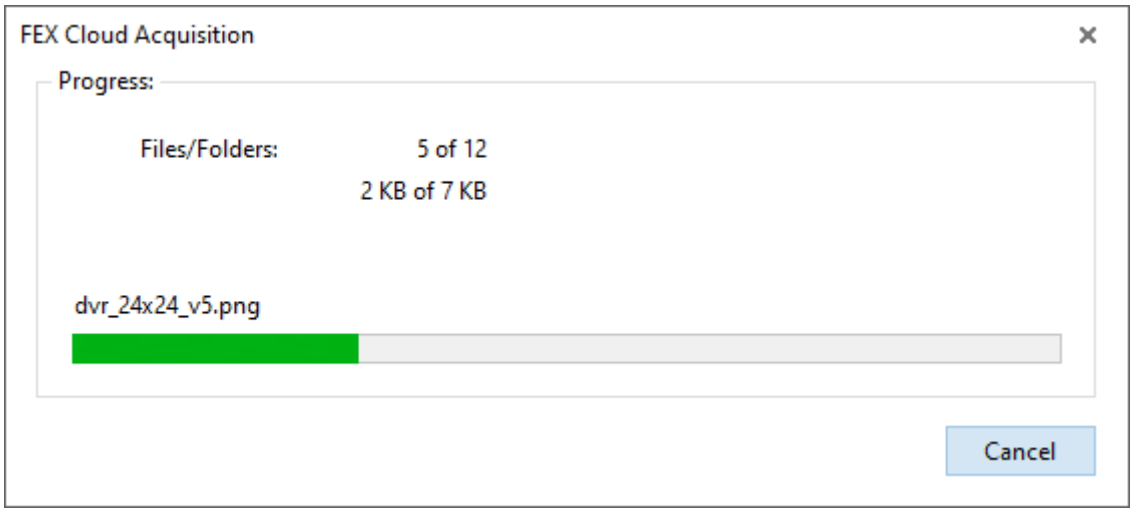
When selected the folder and file date and times shown in the GUI are kept.

If not selected, the date and times reflect acquisition date and time.

4.7 ACQUISITION PROGRESS

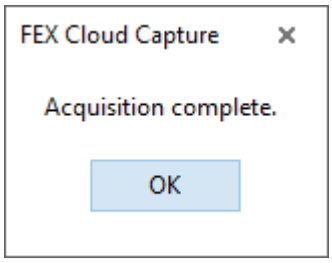
When the **Acquire** button is pressed the acquisition starts and is track with the following progress window:

Figure 12: Acquisition progress.



A message will display when the acquisition is complete:

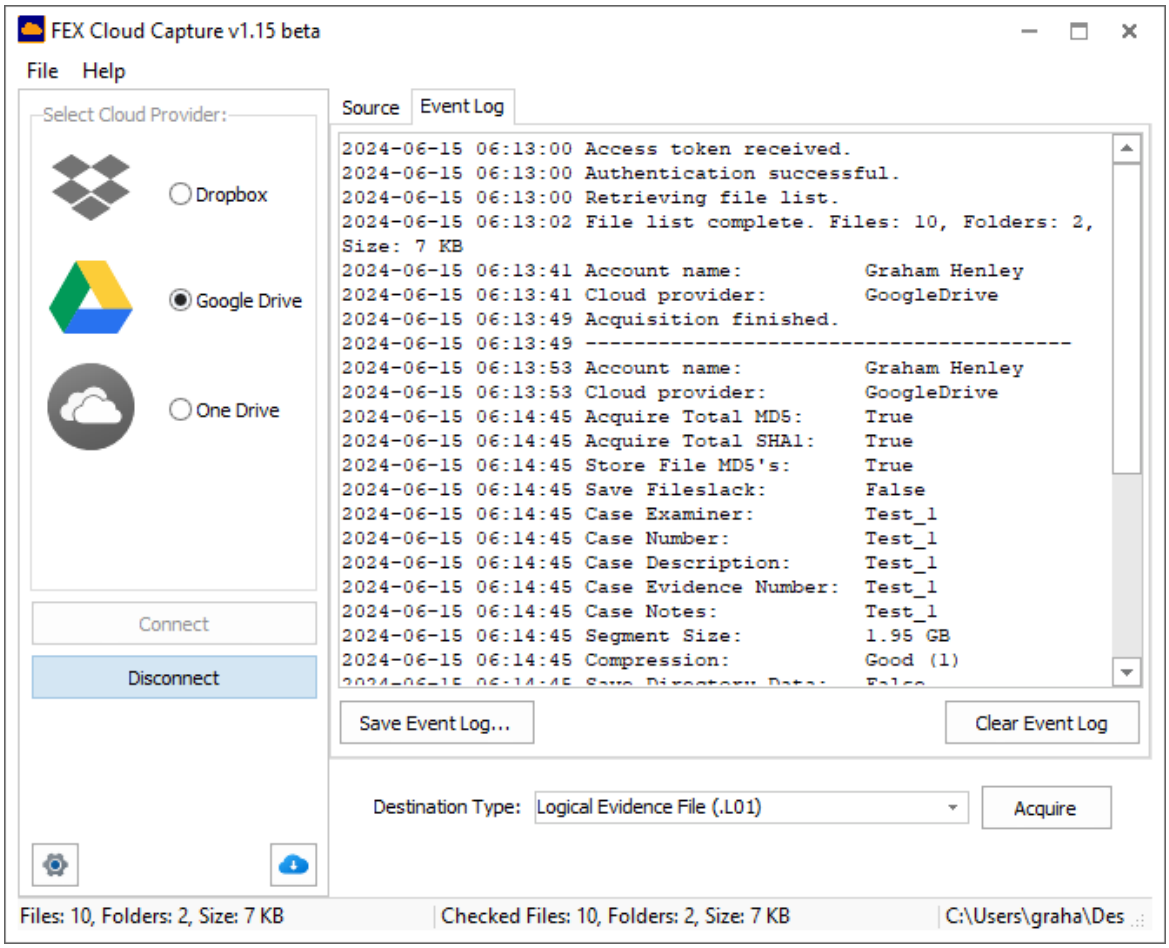
Figure 13: Acquisition complete.



4.8 EVENT LOGS

Acquisition logs are available in the **Event Log** tab. Logs can be exported using the **Save Event Log** button:

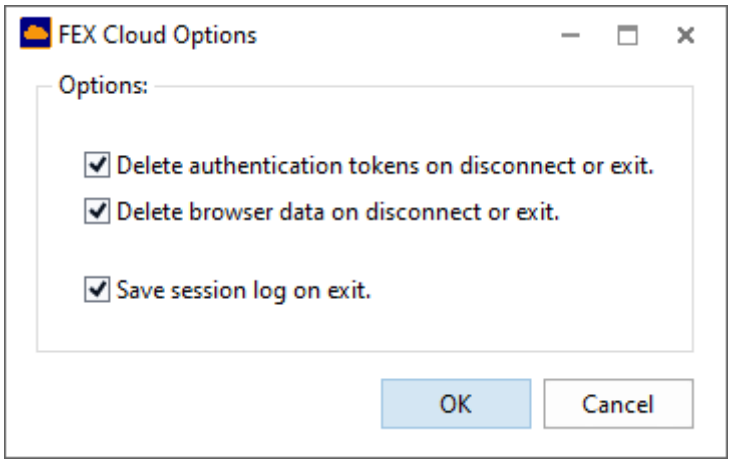
Figure 14: Event Log.



5. FEX CLOUD CAPTURE OPTIONS

 FEX Cloud Capture options are accessed using the options button:

Figure 15: FEX Cloud Capture Options.



 The downloads button gives fast access to the download folder.

6. LEGAL

6.1 LICENSE AGREEMENT

GetData® Forensics Pty Ltd ("GetData") – ACN: 143458039

IMPORTANT – END USER LICENSE AGREEMENT

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("AGREEMENT") CAREFULLY BEFORE USING FORENSIC EXPLORER ("the SOFTWARE"). BY USING THE SOFTWARE, YOU ARE AGREEING TO BE BOUND TO THE TERMS AND CONDITIONS OF THIS LICENSE SET OUT BELOW. IF YOU DO NOT AGREE TO BE BOUND BY THE TERMS AND CONDITIONS SET OUT BELOW, DO NOT INSTALL AND/OR USE THE SOFTWARE. PLEASE TERMINATE INSTALLATION IMMEDIATELY AND DO NOT USE THE SOFTWARE.

1. Software covered by This License

1.1. This License agreement applies to the GetData software package with which this agreement is included.

2. General

2.1. GetData is and remains the exclusive owner of the Software. You acknowledge that copyright in the Software remains at all times with GetData.

2.2. The Software and any other materials included under this License, are Licensed, not sold to you by GetData for use only under the terms of this Agreement.

2.3. GetData or its licensors own the Software, including all materials included with this package. GetData owns the names and marks of 'GetData,' 'GetData Forensics', 'Forensic Explorer', 'FEX-LAB ', 'FEX-CLI', 'FEX Cloud Capture', 'FEX Imager', 'FEX Triage' and 'Mount Image Pro' under copyright, trademark and intellectual property laws and all other applicable laws.

3. Permitted License Uses and Restrictions

3.1. Subject to the terms and conditions of this License, a single License of the Software permits you to run a single Licensed instance of the Software. Where multiple Licenses have been purchased, the License permits you to run concurrent instances of the Software equal to the number of Licenses purchased.

3.2. You are solely responsible for the protection of your data, your systems and your hardware used in connection with the Software. GetData will not be liable for any loss or damage suffered from the use of the Software.

3.3. You and others are not permitted to copy (except as expressly permitted by this Agreement), decompile, reverse engineer, disassemble, attempt to derive the source code of, decrypt, modify (except to the extent allowed in the documentation accompanying this Agreement) or remove or alter any proprietary legends contained in the Software.

3.4. You are not permitted to share the product activation information provided to you for this Software with other users.

3.5. You may not publicly display the Software or provide instruction or training for compensation in any form without the express written permission of GetData.

3.6. GetData reserves the right to check any and all License details at any time in any reasonable manner.

3.7. GetData may from time-to-time revise or update the Software and may make such revisions or updates available to you subject to payment of the applicable License fee.

3.8. The Software is protected under United States law and international law and international conventions and treaties. You may not rent, lease, lend, sell, redistribute, or sublicense the Software without the express written permission of GetData.

3.9. If you purchase a site License, there will be terms and conditions listed in the appendix of the site License.

4. Disclaimer of Warranty

4.1. To the extent not prohibited by applicable law, by using the Software, you expressly agree that all risks associated with performance and quality of the Software is solely held by you. GetData shall not be liable for any direct, indirect, special, or consequential damages arising out of the use or inability to use the software, even if GetData has been advised of the possibility of such damages.

4.2. To the extent not prohibited by applicable law, the Software is made available by GetData 'As Is' and 'With all Faults,' GetData or any GetData authorized representative does not make any representations or warranties of any kind, either expressly or implied concerning the quality, safety, accuracy, or suitability of the Software, including without limitation any implied warranties of merchantability, fitness for a particular purpose, non-infringement or that the Software is error free.

4.3. GetData or any GetData authorized representative makes no representations or warranties as to the truth, accuracy or completeness of any information, statements or materials concerning the Software.

4.4. No oral or written information or advice given by GetData or a GetData authorized representative shall create a warranty. Should the Software prove defective, you assume the entire cost of all necessary servicing, repair, or correction. Some jurisdictions do not allow the exclusion of implied warranties or limitations on applicable statutory rights of a consumer, the above exclusions and limitations may not apply to you.

5. Limitation of Liability

5.1. To the extent not prohibited by applicable law, in no event will GetData, its officers, employees, affiliates, subsidiaries or parent organisation be liable for any direct, indirect,

special, incidental, exemplary, consequential, or punitive damages whatsoever relating to the use of the Software.

5.2. Any and all data obtained from the use of the Software becomes the user's sole responsibility and liability.

5.3. Any and all data obtained from the use of the Software in any civil or criminal jurisdiction that results in wrongful conviction, erroneous charges, misrepresentation of data or death or any other civil or tortious wrong against a person, company, corporation, or any other entity, GetData shall bear no liability for any death, wrongful conviction or any other civil or tortious wrong against a person, company, corporation, or any other entity.

5.4. Any and all data obtained from the use of the Software is the sole responsibility of the user. In the event the user misconstrues, misinterprets, or misunderstands the data and causes it to be used in any and all civil or criminal jurisdictions, GetData shall bear no liability.

5.5. In no event will GetData's liability to you, whether in contract, tort (including negligence) or otherwise, exceed the amount paid by you for the License under this Agreement.

5.6. In the event that a company bearing the name of GetData operating as a separate legal entity, leases the Software to you, and you misconstrue, misinterpret or misunderstand the data that results in any wrongful conviction, erroneous charges, misrepresentation of data, death or any other civil or tortious wrong against a person, corporation or any other entity, GetData ACN: 143458039 shall bear no liability to you, the liability shall be borne by whatever company bearing the name of GetData operating as a separate legal entity.

6. Applicable Law

6.1. This Agreement and any dispute relating to the Software or to this Agreement shall be governed by the laws of the State of New South Wales and the Commonwealth of Australia, without regard to any other Country or State choice of law rules.

6.2. You agree and consent that jurisdiction and proper venue for all claims, actions and proceedings of any kind relating to GetData or the matters in this Agreement shall be exclusively in Courts located in NSW, Australia. If any part or provision of this Agreement is held to be unenforceable for any purpose, including but not limited to public policy grounds, then you agree that the remainder of the Agreement shall be fully enforceable as if the unenforced part or provision never existed. There are no third-party beneficiaries, or any promises, obligations or representations made by GetData therein.

7. Export

7.1. You acknowledge that the Software is subject to Australian export jurisdiction. You agree to comply with all applicable international and national laws that apply to the Software including destination restrictions issued by GetData.

8. Termination

8.1. This Agreement is effective on the date you receive the Software and remains effective until terminated. If you fail to comply with any and all terms set out above, your rights under this Agreement will terminate immediately without notice from GetData. GetData may terminate this Agreement immediately should any part of the Software become or in GetData's reasonable opinion likely to become the subject of a claim of intellectual property infringement or trade secret misappropriation. Upon termination, you will cease use of and destroy all copies of the Software under your control and confirm compliance in writing to GetData.

9. Entire Agreement

9.1. This Agreement constitutes the entire Agreement between you and GetData relating to the Software herein. This Agreement supersedes all prior or contemporaneous oral or written communications, proposals, representations, and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgement, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification, amendment or addendum to this Agreement will be binding, unless it is set out in writing and signed by an authorized representative of each party.

10. Translations

10.1. This agreement is translated into other languages. It is the English version which is the language that will be controlling in all respects. No version of this agreement other than English shall be binding or have any effect.

6.2 PRIVACY POLICY

Please see the GetData Forensics privacy policy at this page: https://getdataforensics.com/privacy/

7. INDEX

8. TABLE OF FIGURES