Bulk Forensic Image Processor- V5.3

Release Notes & Guide

Release Notes V5.3

Major Updates:

- Added support Griffeye Collaboration Server(CS) Operation/Enterprise.
  - Numerous UI and API Additions for connecting and authenticating to Griffeye CS.
  - Ability to Conduct File Carving/Processing of forensic images with Breakpoint Processing Engine, then automatically push to an Existing CS Case on server, or to create and push to a new case.

General Improvements:

- Minor Messaging bug fixes and cleanup
- Added progress indicators to Status bar reporting total BPE carving process completed out of Total Queued.
- Changes to BFIP settings file naming convention and improved logic for handling of legacy settings file following BFIP updates.

Breakpoint Processing Engine:

- Changes to Hypercarve thread slider logic default with new initial default of 4 concurrent carving threads.
- Updated logic for determining default/initial Hypercarve Pool size based on analysis of available CPU cores on workstation.
- Numerous updates to multithreading code and logic for improved speed, exception handling and stability.
- Updated allocated file carving threads to equal total cores - 2, from only half the total cores. But no less than 5 threads.

Release Notes V5.2

General Improvements:

- Improvements to function that checks for active instance of main Griffeye GUI application running. Now checks once at very beginning of process, and then conducts a second check following any carving, but prior to importing carved data into Griffeye and calling the Griffeye CLI. If active instance is running, program will now automatically pause the import process at this point and wait until it detects Griffeye has closed (polling every 10 seconds), then will automatically resume.

Griffeye Import Options:

- Updated Griffeye CLI paths to reflect Magnet Forensics path changes and renames of CLI binaries following rebranding starting at 24.3.x

Release Notes V5.1

Breakpoint Processing Engine:

- Disabled logging of deleted file entry renames during normal parsing of file-systems, and will now only be written to log if *verbose messaging* is *enabled*. This will significantly reduce file-size of baseline BFIP log file, and improve processing speed.

General Improvements:

- Added explicit fields for either *Create New Case* or *Add to Existing Case* to limit confusion or error when using prior unified section.
- Added dyonically updating *'Current Working Case File'* indicator.
- Various Minor UI Adjustments
- Added check at beginning of full carve and import process to see if an additional instance of Griffeye is already running with warning to close before proceeding.

Griffeye Import Options:

- Added support for new Griffeye EXIF AI Detector Plugin
- Added support for new Thorn CSAM Classifier

Lace Carving Options:

- Added controls for Lace 'Shadow Copy Limit'
- Added controls for Lace 'CPU Count'

BFIP API-Mode:

- Updates to API-Mode UI to unify with recent changes to normal BFIP UI.
- Resolved bug verbose messaging defaulting to True when not specified in API call.
- Documentation Updated

Release Notes V5

Breakpoint Processing Engine:

- Enhancements:
  - **New Feature**! APFS Snapshots now supported for recovery of additional historic/deleted files not present in current APFS file-system.
  - Updates to JSON libraries for improvements in JSON write speeds.
  - Updated TSK libraries to 4.12.1
- Fixes:
  - Resolved issue where MD5 value incorrectly written to JSON for allocated files showing '0' value.
- JSON Updates:
  - Unused MD5 field completely stripped from Unallocated JSON for cleaner output.
  - Update to path displayed for Single Volume disks containing no partition tables so root folder structure now shows as beginning following sourceID in folder path view in Griffeye.
  - Update to 'FilePath' field stripping 'FileName' from end of this string. Eliminates each individual file showing in 'Folders' view in Griffeye and ensures display of filenames and file paths are formatted consistent with native Griffeye import engines.

General Improvements:

- Big visual refresh
- Large rework of UI and Case Processing setup flow.
- Legacy 'Basic Mode' radials for processing modes deprecated
- Advanced Source Setup renamed and now default workflow for adding sources and designating processing mode selection.
- Improvements to Case File/Path Selection process and logic to address issues caused when users created multiple levels of folders with identical names.
- New auto-update check API added. BFIP will now query breakpointforensics.com to see if new version is available and offer to download update if available. (Can also be triggered from 'right-click' menu.
- Improved support for multi-monitor environments. Secondary settings windows now check for current location of main program window and will open to same position as main window.

Requirements:

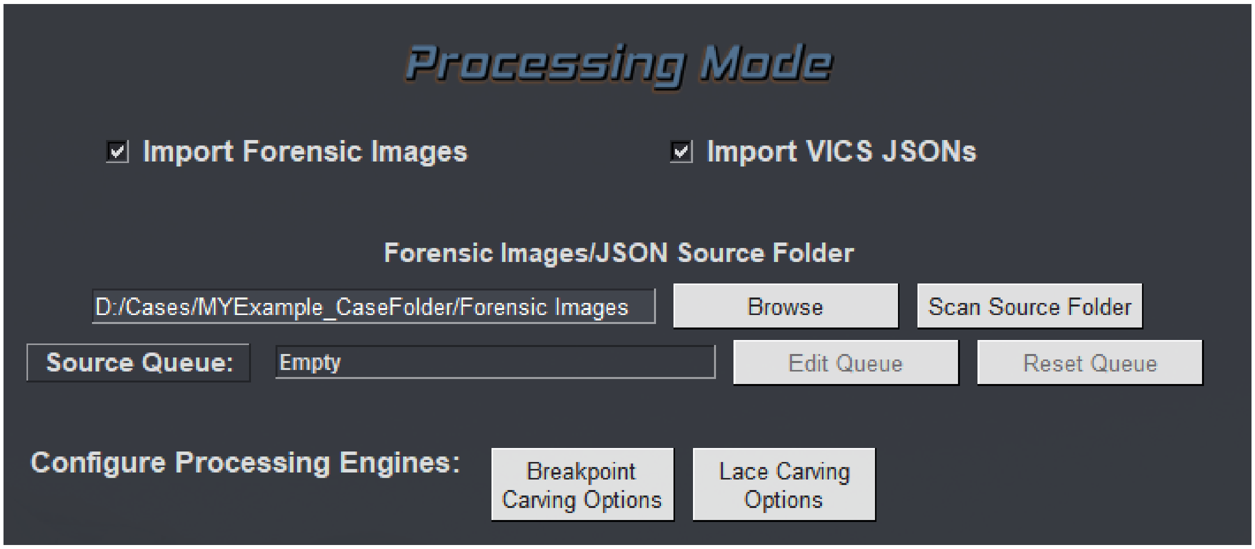
- Windows 7, 10, 11
- Griffeye DI or Processing Engine 24.3 or Newer
  - Pro License *required* from Lace and Auto Case Creation and Import Functions.
  - Griffeye Plugins such as EXIF AI, Thorn, Brain, etc. must be installed and configured per instructions in Griffeye Analyze Forensic Market prior to use.
  - Pro *not required* for *Break Point Processing Engine* Carving
- ***Griffeye Collaboration Server Integration requires:***

  Magnet Griffeye Connect CLI
  Version:24.4.1.0 or newer
  Newest Download available on Magnetforensics.com support page on Griffeye Operations/Enterprise Downloads section or here:

Contents

Processing Mode

BFIP offers 3 different Processing Engines that offer different features and availability depending on Griffeye License, in addition to the ability to import Forensic Images and/or JSON Packages.   As of Version 5.0, the legacy single mode selection interface has been deprecated and the previously name 'Advanced Source Queue Setup', is now used for configuration of processing modes. This allows the ability to apply different and unique process modes to various forensic images, and also to add forensic images from a variety of different paths and drives all in a single import. Please see the 'Advanced Source Queue Setup' section for details on how to add and configure sources.



Processing Mode

☑ Import Forensic Images   ☑ Import VICS JSONs

Forensic Images/JSON Source Folder: D:/Cases/MYExample_CaseFolder/Forensic Images

Source Queue: Empty

Source Type

Import Forensic Images

- Select this Checkbox to have BFIP search for forensic images to add to import queue and process them based on configured Processing Engine Selection.

Import VICS JSON

- Select this Checkbox to have BFIP search for JSON Packages to add to import queue. Can be run alongside Forensic Image Import and/or independently.

Forensic Images/JSON Source Folder:

Select the parent folder for where your specific cases forensic images and/or JSON packages are stored. BFIP will intelligently search the specified folder and *all subfolders* for supported forensic images, as well as JSON packages and add them to processing queue. Source ID's for each forensic image will be auto-generated based on the forensic image's filename with the extension stripped, but may be further customized in the advanced source queue window.

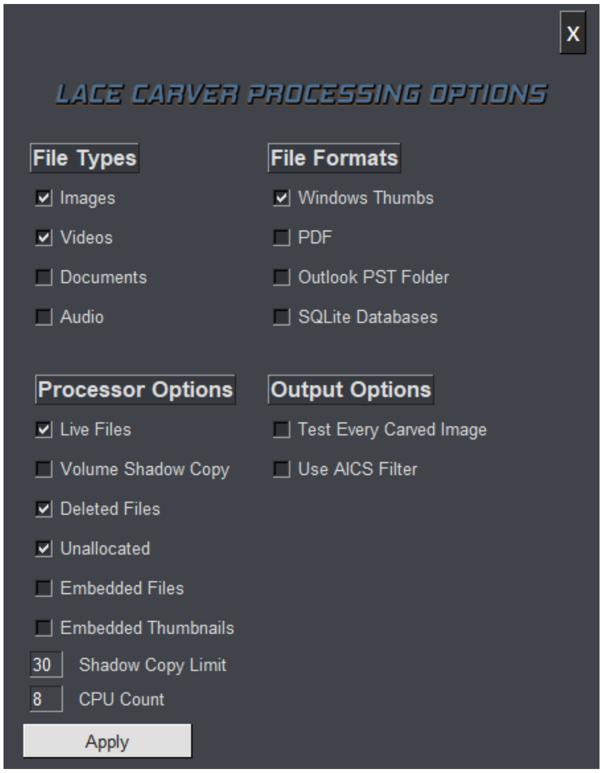
Processing Mode Engines

Standard

- Standard calls the standard/default import engine included with Griffeye.
- Includes Active Files and ‘Flagged Deleted’ Files.
- *Does not* recover data from unallocated space.
- *Supported Image Types: ['.001', '.bin', '.dd', '.dmg', '.e01', '.ewf', '.iso', '.raw', 'vhd']*

Lace

- Requires Lace Addon with your Griffeye DI or Griffeye Processing Engine License.
- Completely replaces the Standard Griffeye Import Engine.
- Many Selectable Options to includes Active, Deleted, Unallocated, VSS, and Embedded Files
- Options Configurable via ‘Lace Carver Options’ menu.
- *Supported Image Types: ['.001', ‘.aa’, ‘.aff’, '.ad1', '.bin', '.dd', '.dmg', '.e01', '.ex01', '.ewf', '.iso', '.l01', '.raw', '.s01', ‘.smart’, '.vhd', ‘.vmdk’]*



LACE CARVER PROCESSING OPTIONS

File Types

☑ Images
☑ Videos
□ Documents
□ Audio

File Formats

☑ Windows Thumbs
□ PDF
□ Outlook PST Folder
□ SQLite Databases

Processor Options

☑ Live Files
□ Volume Shadow Copy
☑ Deleted Files
☑ Unallocated
□ Embedded Files
□ Embedded Thumbnails
30 Shadow Copy Limit
8 CPU Count

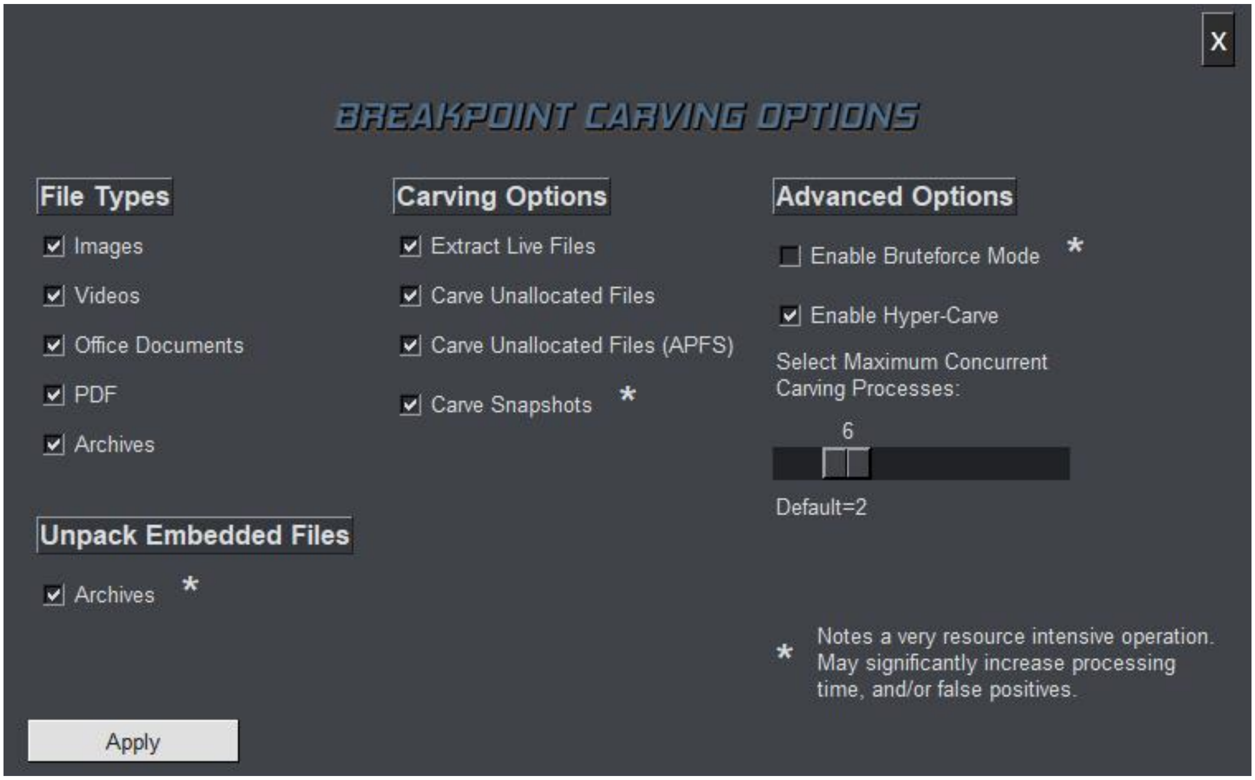
Output Options

□ Test Every Carved Image
□ Use AICS Filter

Breakpoint Processing Engine

- Custom Processing Engine that provides a Hybridized import process leveraging several custom modules in combination with a fully automated implementation of PhotoRec.
- Includes additional support for parsing forensic images containing common file systems including APFS(Apple File System), with automated extraction of media files and import into Griffeye with *no additional addon plugins required.*
- Includes Active Files, Deleted Files, and Carving of Unallocated Files, Carving Files from APFS Snapshots, and Carved Archive Extraction.
- No additional licensing addons required.
- Ability to conduct several parallel carve processes using 'Hyper-Carve' option for significant reduction in typical carving time.
- Passes recovered data to custom VICS JSON generator to build out JSON containing notable metadata and fields (i.e. Physical Location, Files Paths, Deleted Status, Unallocated Status, etc.)
- *Supported Image Types: ['.001', '.bin', '.dd', '.dmg', '.e01', '.ewf', '.iso', '.raw', 'vhd']*

Breakpoint Processing Engine Options



BREAKPOINT CARVING OPTIONS

File Types

☑ Images

☑ Videos

☑ Office Documents

☑ PDF

☑ Archives

Carving Options

☑ Extract Live Files

☑ Carve Unallocated Files

☑ Carve Unallocated Files (APFS)

☑ Carve Snapshots *

Advanced Options

□ Enable Bruteforce Mode *

☑ Enable Hyper-Carve

Select Maximum Concurrent Carving Processes:

6

Default=2

Unpack Embedded Files

☑ Archives *

* Notes a very resource intensive operation. May significantly increase processing time, and/or false positives.

File Types:

Images: Carve for Common Image Formats:

[bmp,crw,dsc,gif,heic,jpg,mrw,orf,pct,png,psb,psd,psp,raf,raw,rw2,tif,wdp,x3f,xcf]

Videos: Carve for Common Video Formats:

[asf,cam,dv,m2ts,mkv,mov,mpg,riff,ts]

Office Documents: Carve for Common MS Office Style Docs:

[doc,xls,ppt]

PDF: Carve for standard PDF files.

Archives: Carve for Common Compressed Archive and MS Office 2007+ Files:

[RAR, 7Zip, Zip, MSOffice07+]

Unpack Embedded Files:

Archives: Processes Rar, 7Zip, Zip, and DMG files that were recovered from unallocated carve and auto extracts the embedded files and adds to Griffeye Import Queue.

> ***Can significantly increase processing time and case size depending on number and size of archives found.***

Carving Options:

Extract Live Files: Have Breakpoint Processing Engine extract Live and Flagged Deleted files from common file systems.

Carve Unallocated Files: Have Breakpoint Processing Engine carve and extract selected file types from unallocated space.

Carve Unallocated Files (APFS): Force Breakpoint Processing Engine to conduct deep carve and extraction of selected file types from APFS volumes.

Carve Snapshots): Have Breakpoint Processing Engine check for APFS snapshots and recover deltas of files not located in the current ‘Live File-System’.

Advanced Options:

Bruteforce Mode: Enables PhotoRec brute force mode that can increase the number of fragmented files recovered.

> **Can significantly increase processing time, false positives, and has increased CPU demand.*

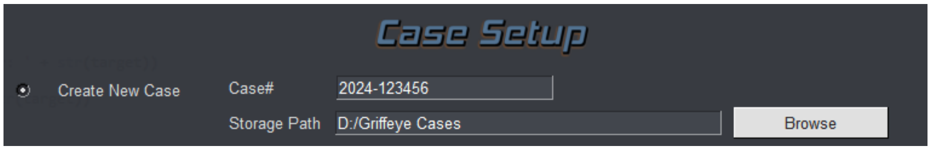
Hyper-Carve: When enabled the Breakpoint Processing Engine will initialize the carving, archive extraction, and JSON creation for each Forensic Image into separate concurrent threads. The maximum number of concurrent threads available is specified by the adjoining slider. If the number of forensic images in your queue exceeds the number of carving threads available, Hyper-Carve will intelligently hold, queue, and dispatch the next forensic image as soon as a prior processing thread becomes available. This has the potential to reduce typical carving times by several-fold.

> **Feature is experimental and exact results highly dependent on several factors such as CPU capacity, IO capacity, etc.*

Case Setup

Case Name and Location:

Create New Case



● Create New Case

Case# 2024-123456

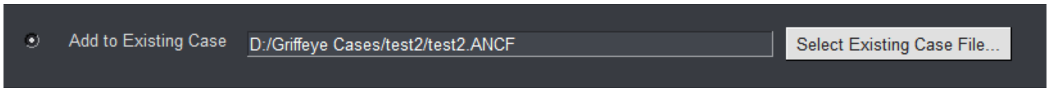
Storage Path D:/Griffeye Cases

Enter the case name/# and storage location where you want your Griffeye Case Folder to be created. BFIP will automatically generate all needed additional case-folders and files based on the information you enter.

If you choose to use the 'Carve Only' option, the carved data will be output to the same path specified here.

> ***Example: [Storage Path] + [Case#] = D:/Griffeye Cases/2024-123456/***

Add Additional Sources to Existing Case



● Add to Existing Case D:/Griffeye Cases/test2/test2.ANCF

BFIP can also be used to add additional sources/data to an existing Griffeye Case. Select the radial for 'Add to Existing Case, and the locate the existing Griffeye ANCF case file using the selection button. BFIP will automatically *add* any new sources/data to the existing case. Your existing case *WILL NOT* be overwritten.

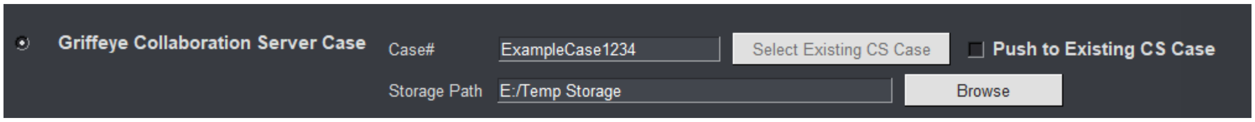
Griffeye Collaboration Server Case Setup

In order to utilize Griffeye CS Integration, please ensure latest Griffeye Connect CLI is installed, and a connection to your Collaboration Server has been successfully completed in the BFIP 'Advanced Settings' menu.

Initial Configuration Settings Covered in Advanced Settings Menu Discussed Here.

Once Griffeye CS integration has been successfully enabled, users may conduct processing of forensic images using the Breakpoint Processing Engine, and recovered files can then be automatically pushed to cases on the configured Collaboration Server.

Case Name and Storage Path:



● Griffeye Collaboration Server Case

Case# ExampleCase1234

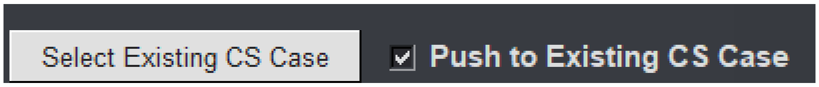
Storage Path E:/Temp Storage

New CS Case

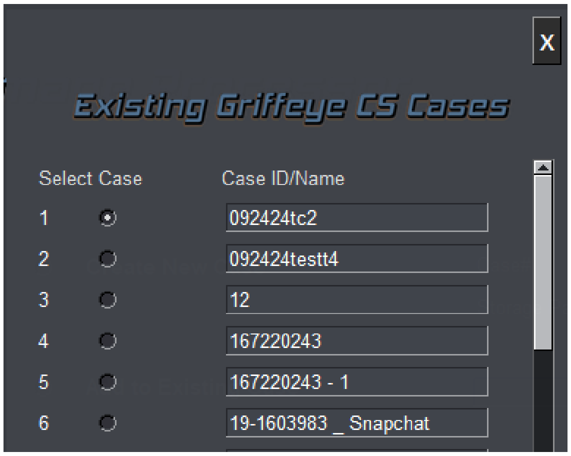
For new cases, with an existing matching Case # not already on the server, enter a Case# or identifier.

Select Existing CS Case

If a case already exists on the collaboration server that you would like to push new data to, check the box for 'Push to Existing CS Case'.



Press the 'Select Existing CS Case' button. BFIP will query the configured collaboration server for a list of existing Case IDs and return a selection window for the user to confirm which existing case they would like to push new data to.



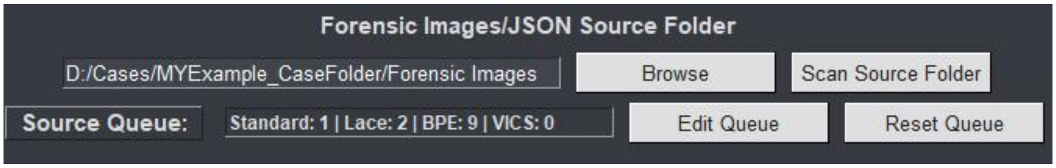
Existing Griffeye CS Cases

Select Case		Case ID/Name
1	●	092424tc2
2	○	092424testt4
3	○	12
4	○	167220243
5	○	167220243 - 1
6	○	19-1603983 _ Snapchat

Griffeye CS Storage Path

Under 'Storage Path', designate an available folder or mapped drive where carved data and JSONs generated from your cases forensic images can be temporarily saved to.

Advanced Source Queue Setup



D:/Cases/MYExample_CaseFolder/Forensic Images

Source Queue: Standard: 1 | Lace: 2 | BPE: 9 | VICS: 0

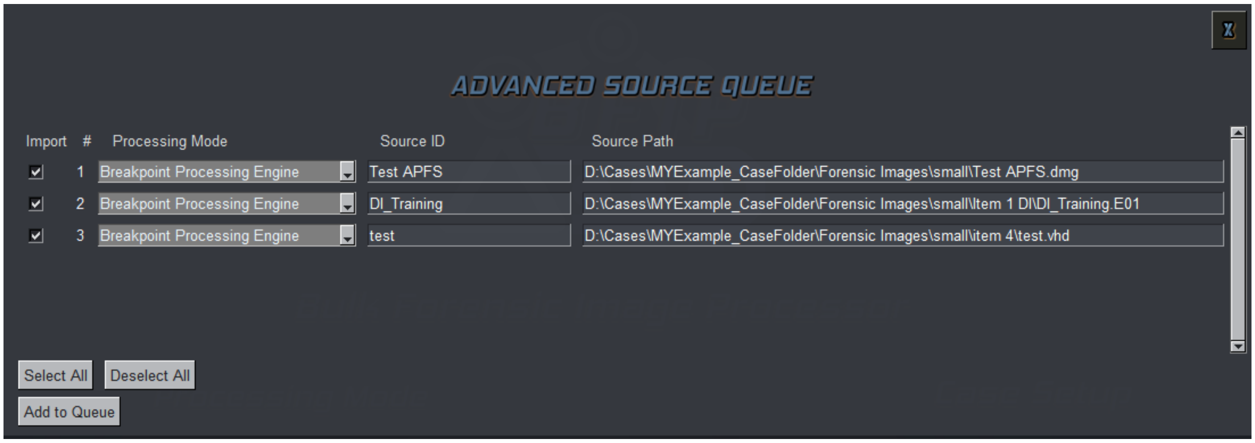
Advanced Source Setup offers the ability to maintain the quick automated case creation process as before, while also providing highly granular control over several automatically generated values, adding the ability to combine multiple Processing Modes in a single run of BFIP, and enables the ability to stack forensic image and JSON sources from multiple locations in a single queue.

Instructions:

1. Forensic Images/JSON Source Folder:
   Select the parent folder for where your specific cases forensic images and/or JSON packages are stored.

2. Scan Source Folder
   BFIP will intelligently search the specified folder and *all subfolders* for supported forensic images, as well as JSON packages. Any located forensic images/JSONs will then be displayed in a new window that will be automatically generated and filled with the located, supported sources.

3. Advanced Source Queue Configuration Window

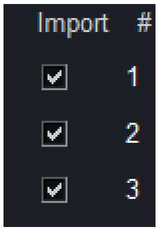


ADVANCED SOURCE QUEUE

Import	#	Processing Mode	Source ID	Source Path
☑	1	Breakpoint Processing Engine	Test APFS	D:\Cases\MYExample_CaseFolder\Forensic Images\small\Test APFS.dmg
☑	2	Breakpoint Processing Engine	DI_Training	D:\Cases\MYExample_CaseFolder\Forensic Images\small\Item 1 DI\DI_Training.E01
☑	3	Breakpoint Processing Engine	test	D:\Cases\MYExample_CaseFolder\Forensic Images\small\item 4\test.vhd

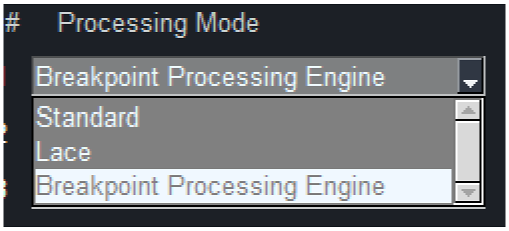
This new window will have 4 primary fields available to customize for each located source:

Import Checkbox: Place a checkbox next to any source you want to be included in the carving/import process. Any item that is unchecked will be completely removed from the current queue and no further processes will be conducted on it.

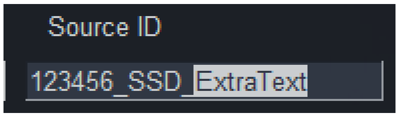


Import	#
☑	1
☑	2
☑	3

Processing Mode: Select the preferred processing mode/engine you'd like to use for the specific forensic image. A mix of Processing modes/engines can be utilized and different sources can use different/unique processing engines depending on the needs of the examiner level of processing required.



Source ID: Source ID's for each forensic image will be initially auto-generated based on the forensic image's filename with the extension stripped, however they can now be individually edited and customized.



Source ID

123456_SSD_ExtraText

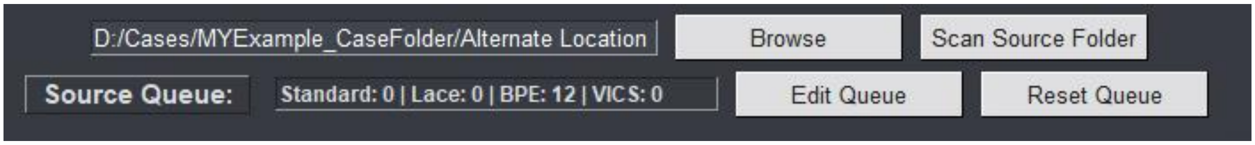
Source Path: The unique source path for each file will be shown in this field automatically.
**While this field can be manually adjusted by the user, it is highly recommended you use the automatically generated value.*

4. Add to Queue

After customizing processing mode selections, Source ID selection, etc., select 'Add to Queue', and the Advanced Source Queue Status bar will update to reflect the added sources.

5. Adding additional files to queue (Optional):

The examiner may repeat this workflow adding a different 'Source Folder' to scan, pressing 'Scan Source Folder', and adding files to the queue multiple times. This allows for stacking multiple sources scattered amongst several different folder locations to a single queue.

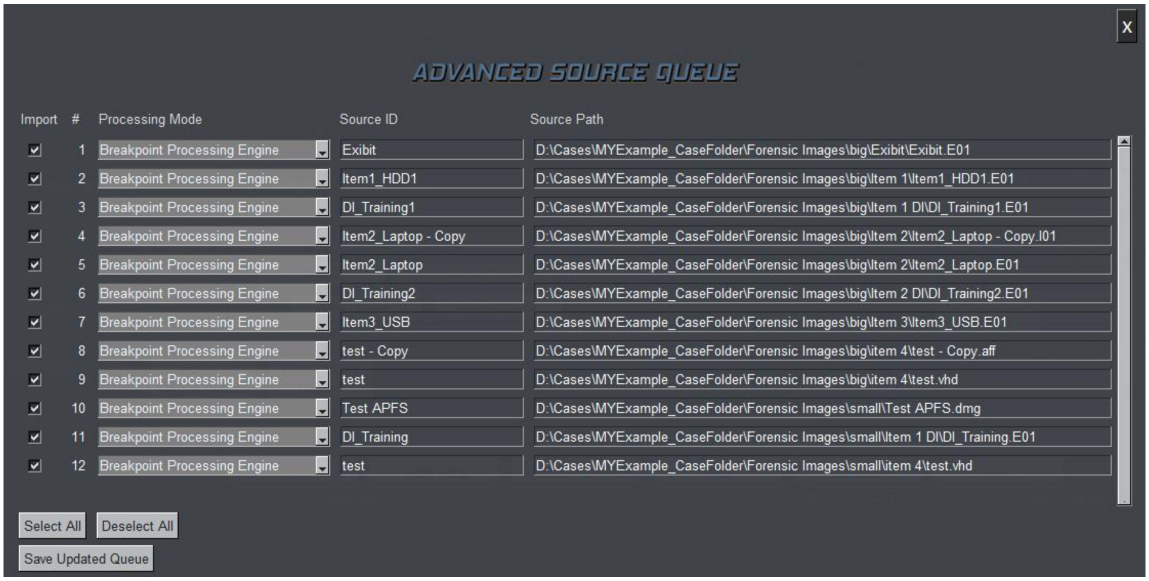


D:/Cases/MYExample_CaseFolder/Alternate Location

Source Queue: Standard: 0 | Lace: 0 | BPE: 12 | VICS: 0

6. Edit Queue

This opens a menu containing all sources and their current settings that have already been added to the queue using the 'Scan Source Folder' button. Existing Source IDs, Processing Modes, etc., can all be further edited or changed from here.



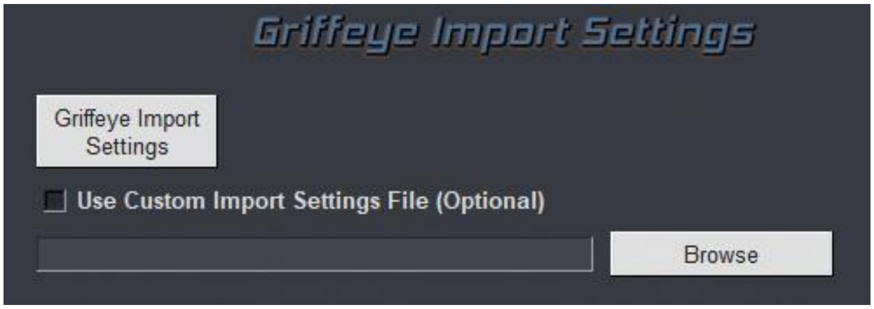
ADVANCED SOURCE QUEUE

Import	#	Processing Mode	Source ID	Source Path
☑	1	Breakpoint Processing Engine	Exibit	D:\Cases\MYExample_CaseFolder\Forensic Images\big\Exibit\Exibit.E01
☑	2	Breakpoint Processing Engine	Item1_HDD1	D:\Cases\MYExample_CaseFolder\Forensic Images\big\Item 1\Item1_HDD1.E01
☑	3	Breakpoint Processing Engine	DI_Training1	D:\Cases\MYExample_CaseFolder\Forensic Images\big\Item 1 DI\DI_Training1.E01
☑	4	Breakpoint Processing Engine	Item2_Laptop - Copy	D:\Cases\MYExample_CaseFolder\Forensic Images\big\Item 2\Item2_Laptop - Copy.I01
☑	5	Breakpoint Processing Engine	Item2_Laptop	D:\Cases\MYExample_CaseFolder\Forensic Images\big\Item 2\Item2_Laptop.E01
☑	6	Breakpoint Processing Engine	DI_Training2	D:\Cases\MYExample_CaseFolder\Forensic Images\big\Item 2 DI\DI_Training2.E01
☑	7	Breakpoint Processing Engine	Item3_USB	D:\Cases\MYExample_CaseFolder\Forensic Images\big\Item 3\Item3_USB.E01
☑	8	Breakpoint Processing Engine	test - Copy	D:\Cases\MYExample_CaseFolder\Forensic Images\big\item 4\test - Copy.aff
☑	9	Breakpoint Processing Engine	test	D:\Cases\MYExample_CaseFolder\Forensic Images\big\item 4\test.vhd
☑	10	Breakpoint Processing Engine	Test APFS	D:\Cases\MYExample_CaseFolder\Forensic Images\small\Test APFS.dmg
☑	11	Breakpoint Processing Engine	DI_Training	D:\Cases\MYExample_CaseFolder\Forensic Images\small\Item 1 DI\DI_Training.E01
☑	12	Breakpoint Processing Engine	test	D:\Cases\MYExample_CaseFolder\Forensic Images\small\item 4\test.vhd

7. Reset Queue:

This function completely clears the Advance Source Queue.

Griffeye Import Settings

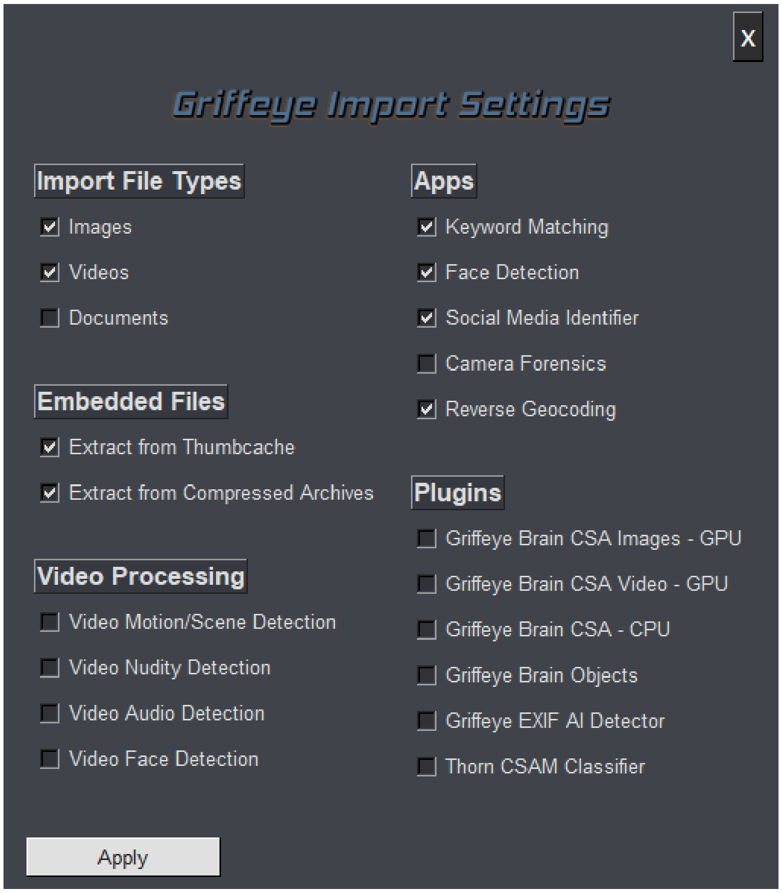


☐ Use Custom Import Settings File (Optional)

Griffeye Import Settings Menu

The ‘Griffeye Import Settings’ Menu allows for direct UI control over several of the most common settings, apps, and plugins that you may want to enable/disable. Associated plugins must be preactivated manually within Griffeye prior to using this interface however. Most apps are now preactivated by default, however Brain plugins will require associated installers and Forensic Market activation.

> **Note in order to ensure these settings are committed to Griffeye you must explicitly open this menu and click ‘Apply’ with your preferred options set. Otherwise, Griffeye will default to using the configuration settings from your last import job.*



Import File Types

☑ Images

☑ Videos

☐ Documents

Embedded Files

☑ Extract from Thumbcache

☑ Extract from Compressed Archives

Video Processing

☐ Video Motion/Scene Detection

☐ Video Nudity Detection

☐ Video Audio Detection

☐ Video Face Detection

Apps

☑ Keyword Matching

☑ Face Detection

☑ Social Media Identifier

☐ Camera Forensics

☑ Reverse Geocoding

Plugins

☐ Griffeye Brain CSA Images - GPU

☐ Griffeye Brain CSA Video - GPU

☐ Griffeye Brain CSA - CPU

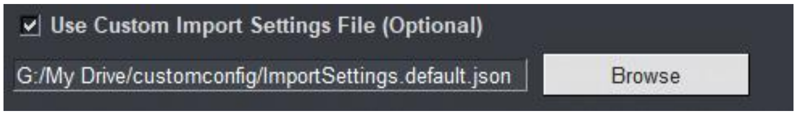
☐ Griffeye Brain Objects

☐ Griffeye EXIF AI Detector

☐ Thorn CSAM Classifier

Custom Import Settings JSON

If you prefer to configure specific import settings beyond those available in the BFIP menu options, you can optionally specify a custom Griffeye Import Settings JSON file. This will override any Griffeye Import Settings specified in the menu.



☑ Use Custom Import Settings File (Optional)

G:/My Drive/customconfig/ImportSettings.default.json

Starting Functions

Start

Run Selected Processing Engine/File Carving. Conduct Griffeye Case Creation. Import Forensic Images and/or JSON Files into Griffeye.

**Griffeye DI Pro or Griffeye Processing Engine License Required or Griffeye CS(Ops/Enterprise).*

Carve Only

Conducts carve using Breakpoint Processing Engine based on settings specified in 'Breakpoint Carving Options' menu.

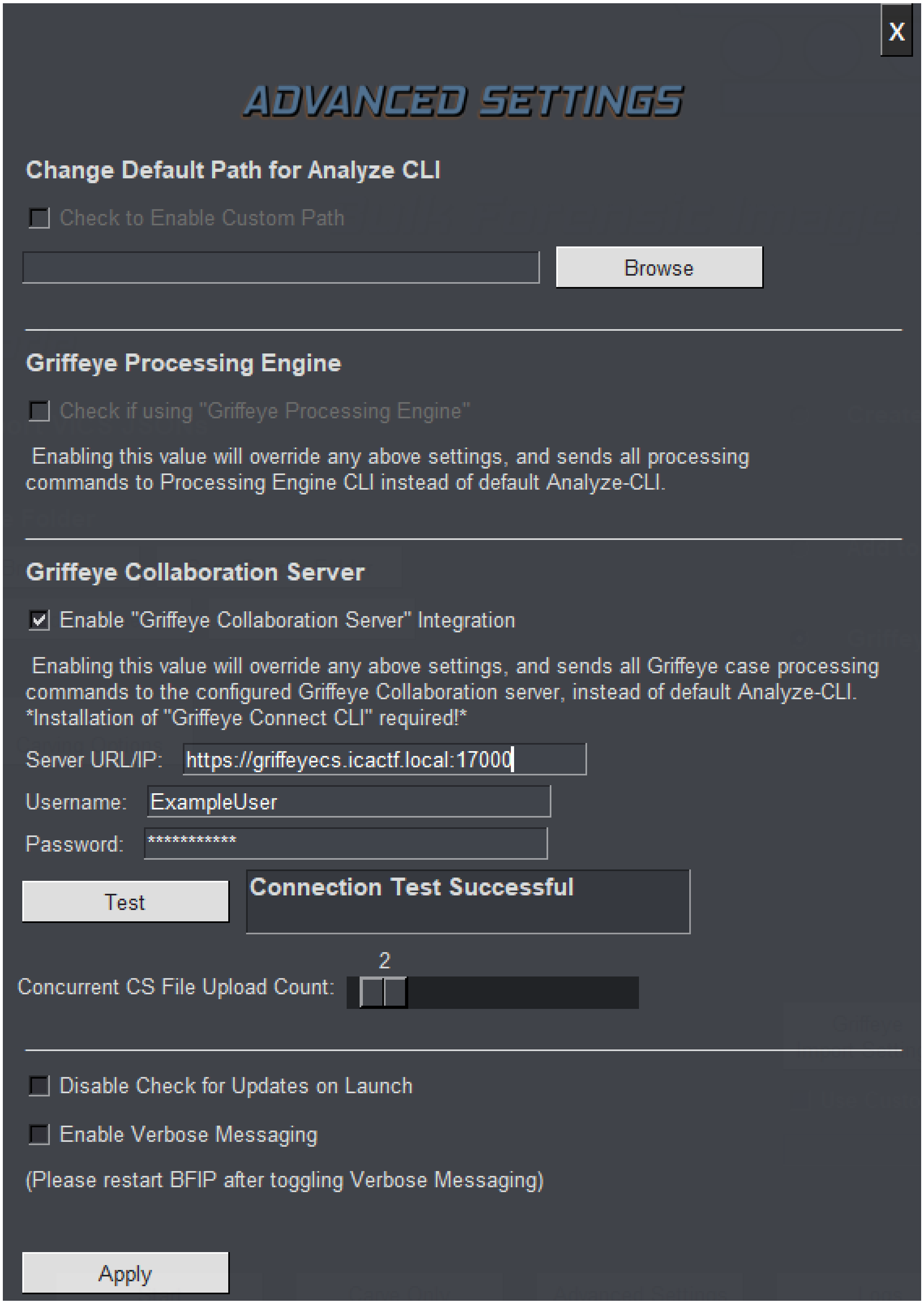
Generates JSON Packages of Carved Content.

Conducts automated file extraction from any support file-systems on forensic images by extracting media and archive files, and generating a VICS JSON package from the extracted files.

Does not automatically pass recovered files/JSON to Griffeye.

No Griffeye License Required.

Advanced Settings



ADVANCED SETTINGS

Change Default Path for Analyze CLI

□ Check to Enable Custom Path

Griffeye Processing Engine

□ Check if using "Griffeye Processing Engine"

Enabling this value will override any above settings, and sends all processing commands to Processing Engine CLI instead of default Analyze-CLI.

Griffeye Collaboration Server

☑ Enable "Griffeye Collaboration Server" Integration

Enabling this value will override any above settings, and sends all Griffeye case processing commands to the configured Griffeye Collaboration server, instead of default Analyze-CLI. *Installation of "Griffeye Connect CLI" required!*

Server URL/IP: https://griffeyecs.icactf.local:17000

Username: ExampleUser

Password: ************

Connection Test Successful

Concurrent CS File Upload Count: 2

□ Disable Check for Updates on Launch

□ Enable Verbose Messaging

(Please restart BFIP after toggling Verbose Messaging)

Change Analyze CLI Path:

BFIP looks for the file ‘analyze-cli.exe’ in the default install location of:

C:\Program Files\Griffeye Technologies\Griffeye Analyze

If you have changed the default install location, this value can be overridden with a new folder location for ‘analyze-cli.exe’. Both the ‘Check to Enable Custom Path’, and new folder location must be specified.

Griffeye Processing Engine:

BFIP Supports interfacing with the CLI-only ‘Griffeye Processing Engine’. In order to use the Griffeye Processing Engine you must check the associated box under Griffeye Processing Engine. This will direct all Griffeye commands, settings updates, etc. to the Griffeye Processing Engine instead of Analyze-CLI.

Griffeye Collaboration Server Configuration:

To Enable Griffeye Collaboration Server Integration, located and check the activation box under the ‘Advanced Settings’ menu.

URL

Enter the full URL including the port # for Griffeye CS. (Default typically 17000)

Example: ***https://griffeyecs.ICACSERVER.local:17000***

User Credentials

Enter a username and the associated password for a user account configured on the collaboration server that will be used for authenticating all case creation commands. Ensure the configured user account is properly configured on the collaboration server with the necessary permissions/claims for creating and editing cases.

Test

After entering the credentials, click ‘Test’ to validate BFIP is able to establish a connection with the configured server, and that the credentials are excepted.

Concurrent CS File Upload Count

The CS Connect CLI’s file pushing function can be configured for multiple parallel file uploads depending on desired performance and network conditions. This value can be increased or decreased as desired by the user.

Apply

If the Connection Test is Successful, click ‘Apply’ to save the configured settings. The credentials will be encrypted, and securely stored on the local workstation for later recall the next time BFIP is launched.

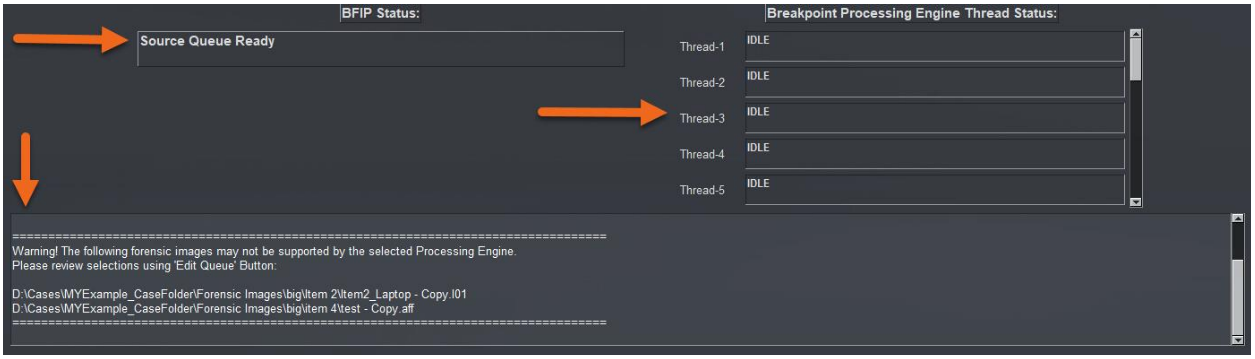
Verbose Messaging:

Enabling verbose messaging increases status messages in console and enables additional debug logging.

Output Window and Status Bar

Griffeye utilizes an integrated output window. Various confirmation messages, processing status, errors, etc. will be printed here for reference.

Directly above the window is a dynamic status bar that will occasionally update with carving status, progress indicators and completion percentages.



BFIP Status: Source Queue Ready

Breakpoint Processing Engine Thread Status:

Thread-1 IDLE
Thread-2 IDLE
Thread-3 IDLE
Thread-4 IDLE
Thread-5 IDLE

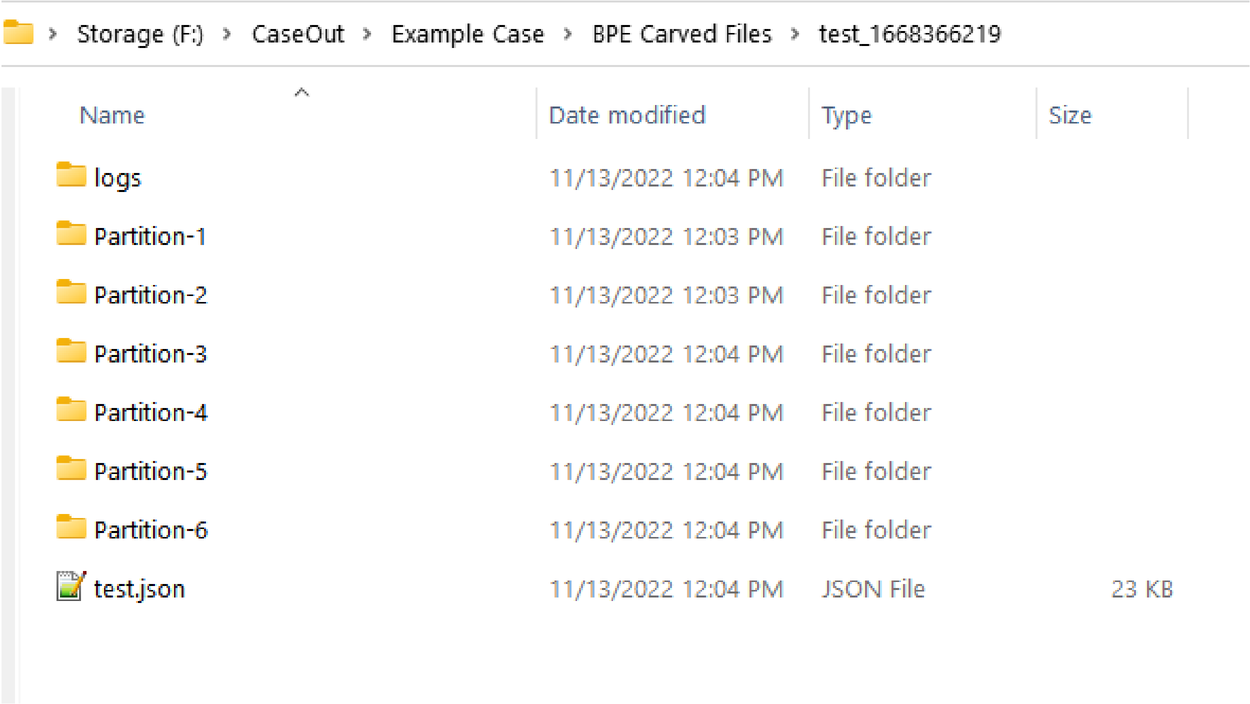
```
=========================================================================================
Warning! The following forensic images may not be supported by the selected Processing Engine.
Please review selections using 'Edit Queue' Button:

D:\Cases\MYExample_CaseFolder\Forensic Images\big\Item 2\Item2_Laptop - Copy.I01
D:\Cases\MYExample_CaseFolder\Forensic Images\big\item 4\test - Copy.aff
=========================================================================================
```

Post Import

Breakpoint Processing Engine

Data Output Locations:

Following a carve or complete carve and import process using the Breakpoint Processing Engine you will find the recovered data, logs, and generated JSON's for each sourceID stored inside the Griffeye Case folder. Specifically, they will be located inside a subfolder titled, 'BPE Carved Files'. Inside that will be an additional subfolder for each individual Source processed. Each Source will further have a number of files and subfolders that will vary based on the number of partitions identified on the source image. The recovered files will be seeded inside their respective partition's subfolder. At the root of the sources folder will also be a VICS JSON files which stores any available metadata about the recovered files.

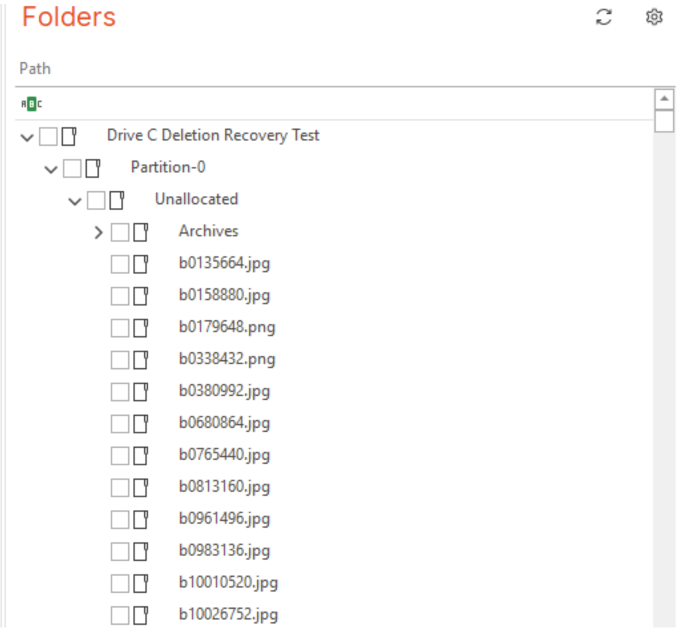


Storage (F:) › CaseOut › Example Case › BPE Carved Files › test_1668366219

Name	Date modified	Type	Size
logs	11/13/2022 12:04 PM	File folder	
Partition-1	11/13/2022 12:03 PM	File folder	
Partition-2	11/13/2022 12:03 PM	File folder	
Partition-3	11/13/2022 12:04 PM	File folder	
Partition-4	11/13/2022 12:04 PM	File folder	
Partition-5	11/13/2022 12:04 PM	File folder	
Partition-6	11/13/2022 12:04 PM	File folder	
test.json	11/13/2022 12:04 PM	JSON File	23 KB

BPE Post Griffeye Import

If you elected to use the standard '*Start'* option, the data generated with the Breakpoint Processing Engine will automatically be imported into a Griffeye case. For data that was recovered, it will appear under the folder path nomenclature of '**[sourceID]/[Partition-#]/[folderpath]'**

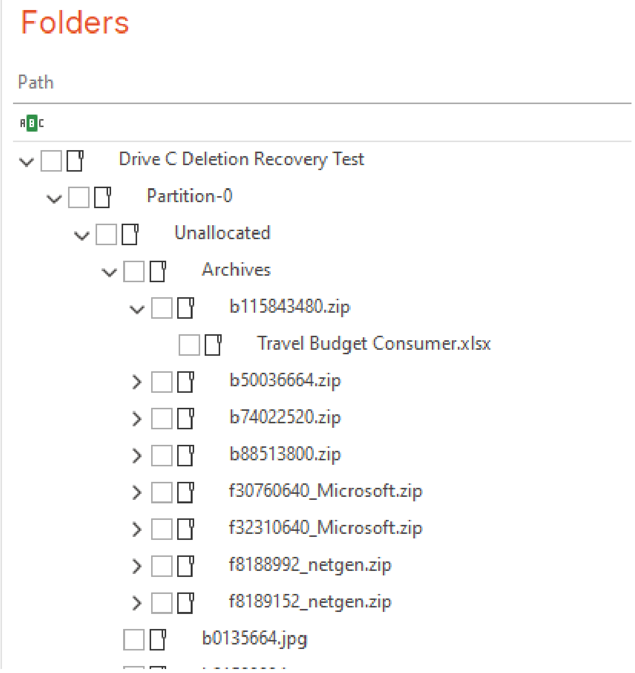


Folders

Path

Drive C Deletion Recovery Test
Partition-0
Unallocated
Archives
b0135664.jpg
b0158880.jpg
b0179648.png
b0338432.png
b0380992.jpg
b0680864.jpg
b0765440.jpg
b0813160.jpg
b0961496.jpg
b0983136.jpg
b10010520.jpg
b10026752.jpg

If you elected to both carve and expand archive files, the expanded archives and their respective files will be seeded under an additional subfolder named '**Archives'**, followed by the path to the original parent Archive file.



Folders

Path

Drive C Deletion Recovery Test
Partition-0
Unallocated
Archives
b115843480.zip
Travel Budget Consumer.xlsx
b50036664.zip
b74022520.zip
b88513800.zip
f30760640_Microsoft.zip
f32310640_Microsoft.zip
f8188992_netgen.zip
f8189152_netgen.zip
b0135664.jpg

File MetaData Unallocated

Data recovered and imported using the Breakpoint Processing Engine will fill several metadata fields based on the limited data that can be recovered from unallocated content.

These will include at least:

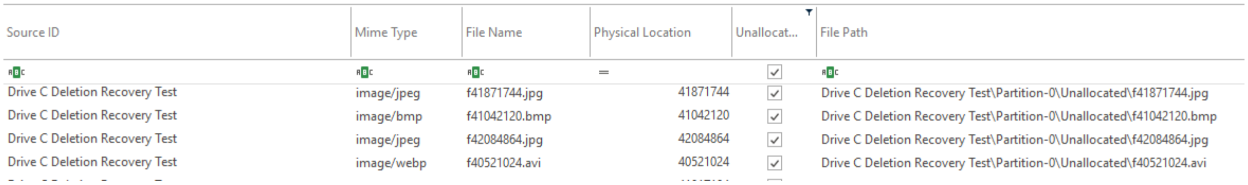
SourceID: Based on name derived from original forensic image.

Mime Type: Identified File Type Based on File Recovery Process

File Name: Does not reflect original file name prior to deletion. This is named based off the physical location recovered on disk.

Physical Location: The first physical sector where the file was located.

If the file was extracted from a recovered archive, this value will reflect the physical sector of the parent archive file



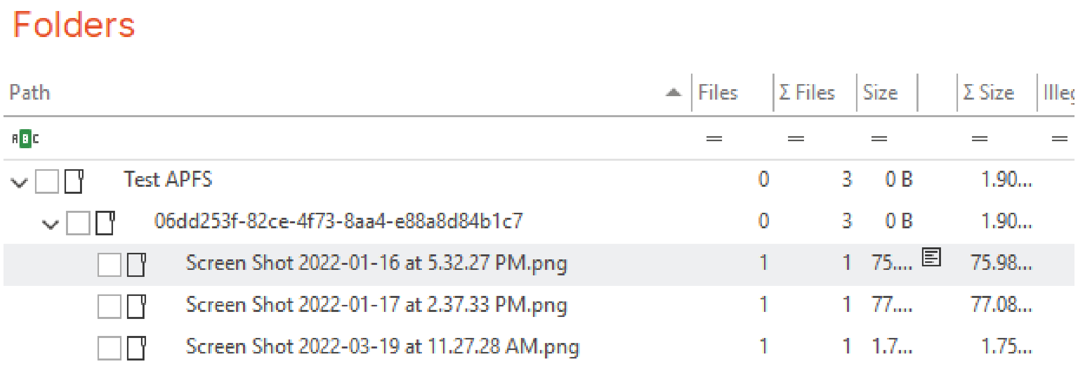
Source ID	Mime Type	File Name	Physical Location	Unallocat...	File Path
Drive C Deletion Recovery Test	image/jpeg	f41871744.jpg	41871744	☑	Drive C Deletion Recovery Test\Partition-0\Unallocated\f41871744.jpg
Drive C Deletion Recovery Test	image/bmp	f41042120.bmp	41042120	☑	Drive C Deletion Recovery Test\Partition-0\Unallocated\f41042120.bmp
Drive C Deletion Recovery Test	image/jpeg	f42084864.jpg	42084864	☑	Drive C Deletion Recovery Test\Partition-0\Unallocated\f42084864.jpg
Drive C Deletion Recovery Test	image/webp	f40521024.avi	40521024	☑	Drive C Deletion Recovery Test\Partition-0\Unallocated\f40521024.avi

BPE Post Griffeye Import – Live Files

If you process live/allocated files using Breakpoint Processing Engine, any active/allocated files located in the file-system will be extracted and imported into Griffeye with their original associated metadata. They will appear under the folder path nomenclature of '**[SOURCEID]/[Partition#]/FOLDERS]**

For APFS Data it will include APFS Container information as part of the path:

'**[SOURCEID]/[APFS Container-GUID]/[CONTAINER-FILES/FOLDERS]**



Folders

Path	Files	Σ Files	Size	Σ Size	Illeg
Test APFS	0	3	0 B	1.90...	
06dd253f-82ce-4f73-8aa4-e88a8d84b1c7	0	3	0 B	1.90...	
Screen Shot 2022-01-16 at 5.32.27 PM.png	1	1	75....	75.98...	
Screen Shot 2022-01-17 at 2.37.33 PM.png	1	1	77....	77.08...	
Screen Shot 2022-03-19 at 11.27.28 AM.png	1	1	1.7...	1.75...	

File MetaData Live Files

Data recovered and imported using the Breakpoint Processing Engine will recover and fille common metadata fields as located in the file-system.

These will include at least:

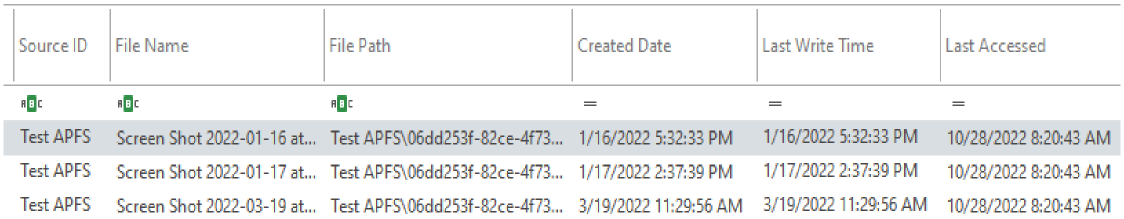
SourceID: Based on name derived from original forensic image.

Mime Type: Identified File Type Based on File Recovery Process

File Name: Original File Name as located in APFS file-system.

File Path: Original File Path as located in APFS file-system.

MAC Timestamps: Original modified, created, and accessed timestamps as located in APFS file-system.



Source ID	File Name	File Path	Created Date	Last Write Time	Last Accessed
ABC	ABC	ABC	=	=	=
Test APFS	Screen Shot 2022-01-16 at...	Test APFS\06dd253f-82ce-4f73...	1/16/2022 5:32:33 PM	1/16/2022 5:32:33 PM	10/28/2022 8:20:43 AM
Test APFS	Screen Shot 2022-01-17 at...	Test APFS\06dd253f-82ce-4f73...	1/17/2022 2:37:39 PM	1/17/2022 2:37:39 PM	10/28/2022 8:20:43 AM
Test APFS	Screen Shot 2022-03-19 at...	Test APFS\06dd253f-82ce-4f73...	3/19/2022 11:29:56 AM	3/19/2022 11:29:56 AM	10/28/2022 8:20:43 AM

Breakpoint Processing Engine API-Mode

BFIP’s Breakpoint Processing Engine can be controlled and executed via CLI and a structured JSON API. This allows for use and integration of the full Breakpoint Processing Engine in other tools or your own custom scripts/automations. The API functions by calling the same BFIP executable, followed by a string of supported arguments and designating the path for a supported JSON File.

Example: **BFIP.exe -JF “d:\myBPESources.json”**

Further details and the most up to date example of the recommended JSON API spec is available here:

https://github.com/breakpointforensics/BPE_API_DATAMODEL

Logs and Troubleshooting

Logging for operations initiated with BFIP are maintained in 3 primary locations.

BFIP Logs

BFIP specific logs, such as Breakpoint Processing Engine, import status, etc. are logged in a BFIP’s AppData folder along with saved user preferences. These can be directly accessed by clicking on the ‘Logs’ button at the bottom of the main BFIP interface. A new log is generated for each calendar day.

Default:

C:\Users\[USERNAME]\AppData\Local\BreakpointForensics\BFIP\Logs

Breakpoint Processing Engine - Source Specific Logs

BFIP Source specific logs generated by the Breakpoint Processing Engine are logged in the case output folder under:

[CaseFolder]\BPE Carved Files\[SOURCEID]\Logs

Griffeye Logs

Once BFIP passes the import parameters to the Griffeye CLI during the Griffeye Processing phase, all Griffeye related messages, errors, and status will be reflected in the normal Griffeye log folder/file.

Default:

C:\ProgramData\Griffeye Technologies\Griffeye Analyze\Error