FEX DVR

User Guide

Published: 10-Jun-26 at 15:11:21

GetData

1.1 CONTENTS

1. INTRODUCTION

FEX DVR is a software program by GetData Forensics (getdataforensics.com). It is a forensic tool for extracting and viewing video from DVR (Digital Video Recorder) disk images. It supports multiple proprietary DVR filesystem formats and provides a browser-based interface for reviewing footage.

Key Features:

- Direct streaming from forensic images (E01, DD, RAW)
- No pre-extraction required — videos play on demand
- Multi-channel synchronized playback
- Forensic provenance tracking (disk offsets, hashes)
- Case management for organizing evidence

1.1 SUPPORTED VIDEO FORMATS

Format	Manufacturer	Video Codec
Hikvision (MPEG-PS)	Hikvision	H.264 / H.265
DHAV (DHFS)	Dahua / Amcrest	H.264 / H.265
RSFm	Swann	H.264
ZLAV	Pascal / Zhiling	H.264
ZENO 1.0 (DHAV variant)	Unifame / Zeno	H.264
HUAYI 1.1 (HYAV)	Avenir	H.264
WFS 0.5	Various	H.264
LVF	Various (Balitech)	H.264
PictMan FHDR	Various	H.264
KDB / Box	Samsung Box DVR	MPEG-4
StreamDB	Various	H.264
AVI, MP4, MKV, MOV	Stand alone video formats	

1.2 DOWNLOAD

FEX DVR is available for **download from:** https://getdataforensics.com/product/fex-dvr. It is downloaded as a setup executable.

1.3 SYSTEM REQUIREMENTS

FEX DVR is a RAM-intensive tool: video is transcoded on demand and held in a RAM cache (or user selected disk cache) for instant playback. The following minimum system specifications are recommended:

- Windows 11 or above.

- 64-bit.
- i7 processor.
- 32 GB RAM.

1.4 INSTALLATION

To **install FEX DVR**:

1. Launch the downloaded setup file and follow the on-screen instructions.
2. FEX DVR is a 64-bit application. By default, FEX DVR will be installed to:

   C:\Program Files\GetData\FEX-DVR\FEX-DVR.exe

1.5 OPENING THE APPLICATION

Launch FEX DVR from the Start menu or desktop shortcut. The application opens to the Case Manager.

Figure 1: FEX-DVR desktop icon

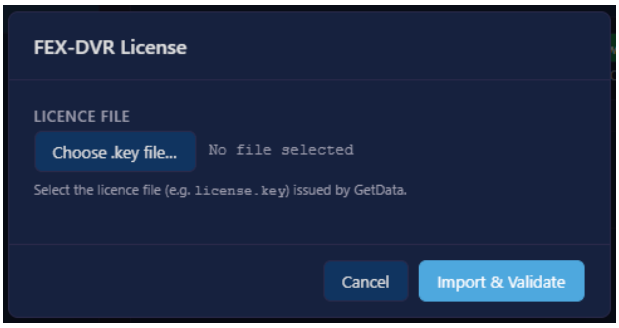
Important: In certain situations, an investigator may wish to examine video on a write protected **physical drive**. For physical drives to be visible, you must launch FEX-DVR as **local administrator**.

1.6 PRODUCT ACTIVATION

The activation status is written in the title bar of the program. You may be prompted to enter a product activation key, or open the following window from the top menu:

1. Help > Activate:

Figure 2: License activation



Import the .key file provided to you with your purchase.

1.7 TYPICAL WORKFLOW

A typical workflow to process a DVR is:

1. Create a Case	Click “New Case” and enter the case details.
2. Add Evidence	Browse to your forensic image file (.E01, .001, .dd, etc.).
3. View Videos	Click “View” to open the Evidence Viewer.
4. Review Footage	Select channels and play videos.
5. Filter Clips	Filter to locate relevant time periods.
6. Add Bookmarks	Bookmark specific events.
7. Create Reports	Create a report based on bookmarks.
8. Export Reports	Provide the report to a third party.

2. CREATING A CASE

2.1 CASE PREFERENCES

Processing DVR evidence is resource intensive. Complex cases can involve large video and the need to process the video into playable formats. For this reason, a minimum spec forensic workstation is recommended. FEX DVR examines the resources available and automatically adjust preference settings to maximise usability. Preferences and caching are described in more detail in section 0 below.

FEX DVR also manages video caching to maximise usability. Video is normally cached to RAM. When an item of interest is bookmarked, an existing RAM cache is converted to disk so that these videos are instantly available on next load. Caching is described in more detail in section 6 below.

2.2 CASE MANAGER

The **Case Manager** is the starting point of FEX DVR. It organises evidence images into cases and is the gateway to the Evidence Viewer and to report generation.

Each case is a self-contained folder, so it can be backed up, archived, or moved to another machine simply by copying that one directory.

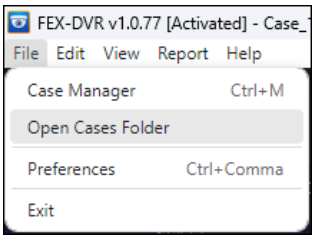
Cases live under FEX-DVR's data area **(%APPDATA%\FEX-DVR\cases** on an installed system), with each case in its own folder named from the case name plus the date and time it was created. Inside, case.json holds the case details (name, examiner, description, and the registry of evidence added to it), while bookmarks.json and excluded.json record the examiner's bookmarks and any set-aside clips.

Every item of evidence gets its own isolated sub-folder under **evidence** — keyed by a unique evidence ID — which keeps each source image's extracted recordings, working cache, and extraction manifest strictly separate so that data from one device can never bleed into another.

Generated reports and other outputs are written to the **exports** folder. This per-case, per-evidence isolation is a deliberate forensic design: everything relating to a case stays together, and everything relating to a single device stays clearly attributable to that device.

Access the current case folder at any time using the **File > Open Cases Folder** menu item:

Figure 3: Open Cases Folder

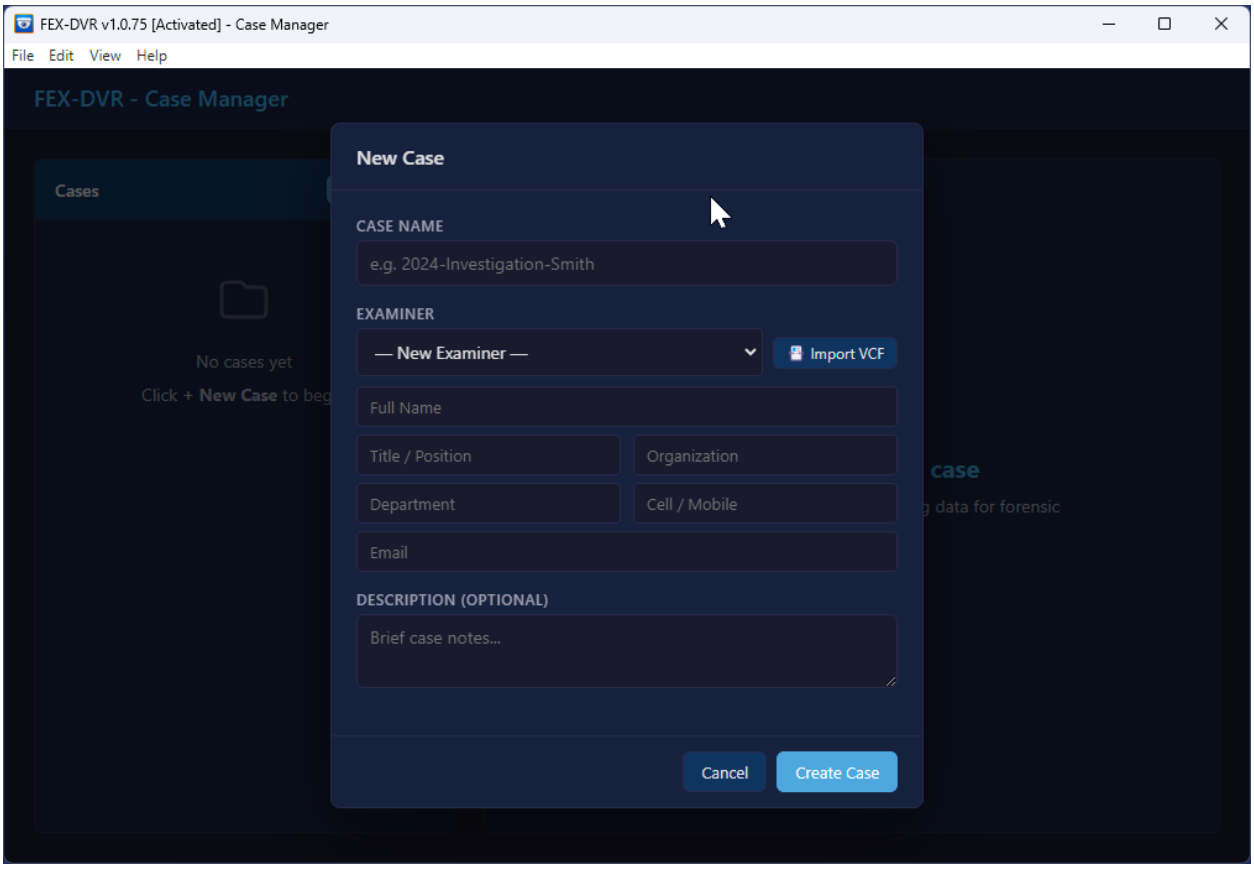


2.3 NEW CASE

To create a new case:

1. In the Case Manager, click the **New Case** button and fill in:
    a. **Case Name** — identifier for the case (required).
    b. **Examiner** — your name (optional).
    c. **Description** — notes about the case (optional).

Figure 4: Case Manager > New Case



2.4 ADDING EVIDENCE

Click Add Evidence to browse for forensic image files or physical disks. Supported forensic evidence containers include **.E01, Ex01, .001, .dd, .raw, .img**.

Figure 5: Case Manager > Add Evidence > Forensic Image

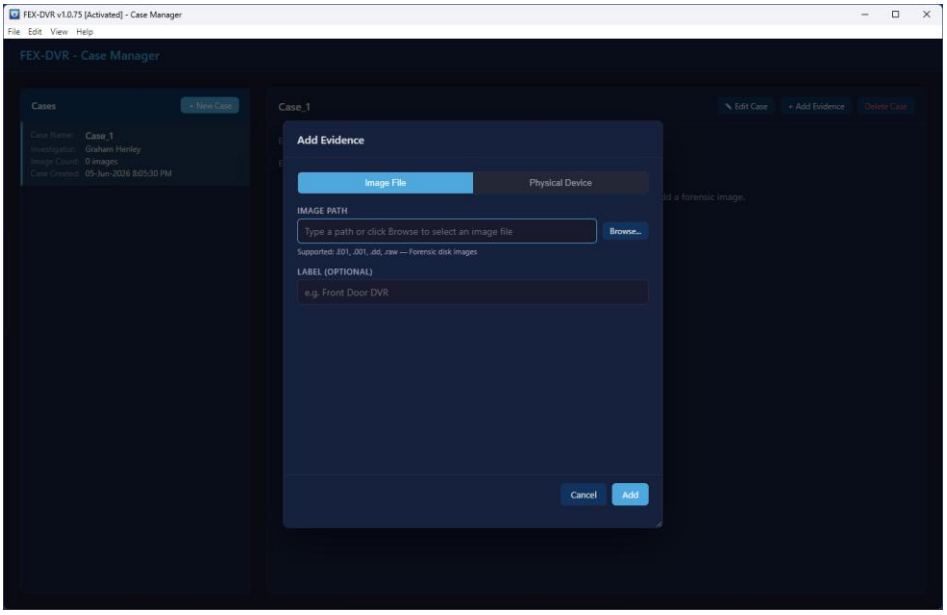
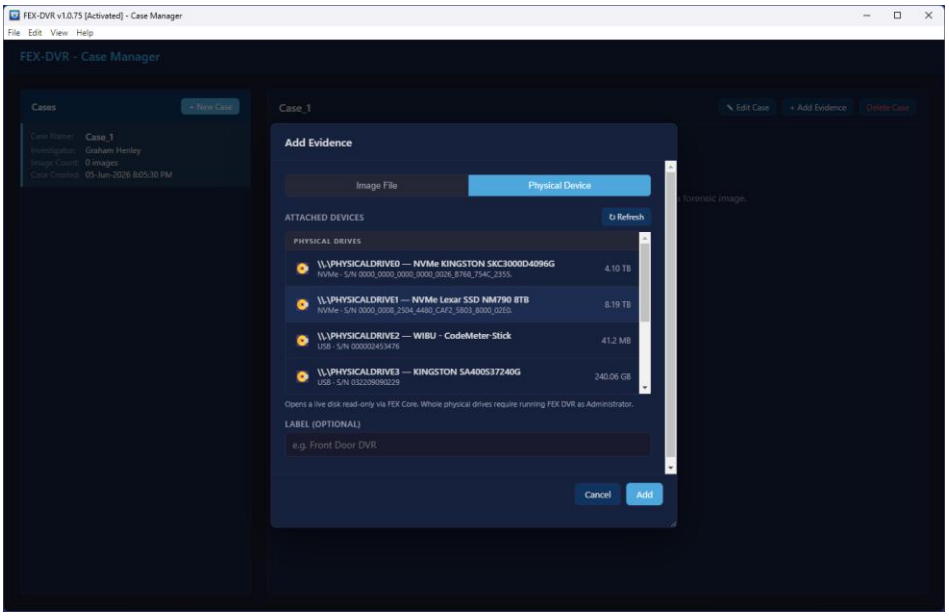


Figure 6: Case Manager > Add Evidence > Physical Disk (application must be launched as Administrator)



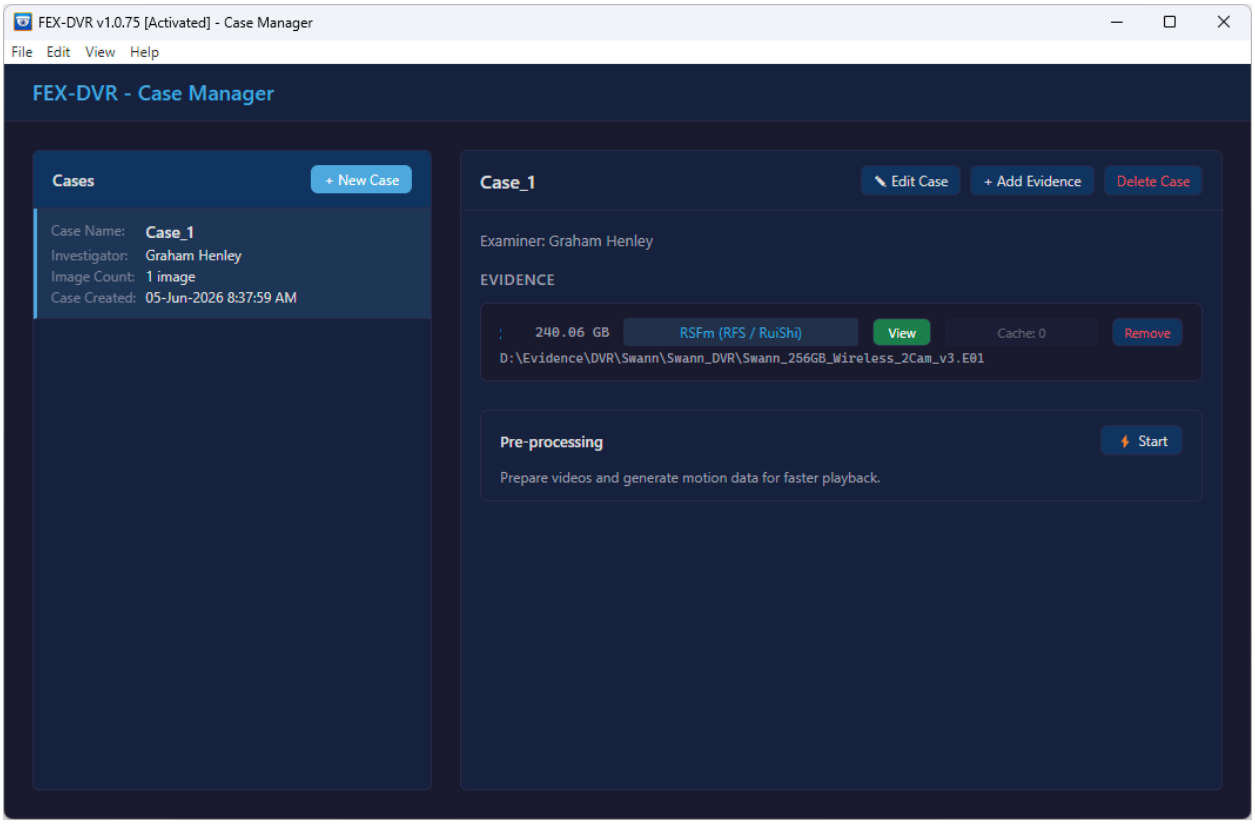
The DVR format is automatically detected when you add an image. Large images (100 GB+) may take several minutes to scan on first load; progress is shown in the interface, and results are cached for instant reload.

2.5 PRE-PROCESSING

In the Case Manager window, each case has a **pre-processing** option with a **start** button.

Pre-processing prepares a case's video ahead of time so that clips play back instantly and their motion timeline is ready the moment you open the Evidence Viewer. It is optional — you can always open the viewer directly — but it removes the short "Preparing" delay that otherwise occurs the first time each clip is played. The option appears for a case once at least one evidence image has been added.

Figure 7: Case Manager > Evidence



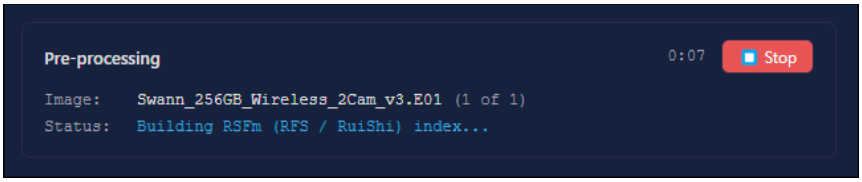
When you click **Start**, FEX DVR works through every evidence image in the case and:

- Scans the image and builds its video index — detecting the DVR format, enumerating every recording, and assigning Clip IDs.
- Reads any burnt-in date / time overlays (OCR) for the formats that support it.
- Prepares each video for playback and generates its motion-detection data, caching the result for instant replay.

While pre-processing runs, the **Start** button becomes a **Stop** button and an elapsed-time counter appears. The panel reports progress in two phases: first **scanning** (which image is being indexed), then **processing** (the current image, the current video and step, and an overall percentage). Click **Stop** at any

time to cancel; you are also prompted to stop if you open the Evidence Viewer while pre-processing is still running. When it finishes, the panel reports how many videos were processed.

Figure 8: Pre-processing



Pre-processing never modifies the forensic image. It only populates FEX DVR's cache, so clearing the cache simply means the work is repeated the next time it is needed.

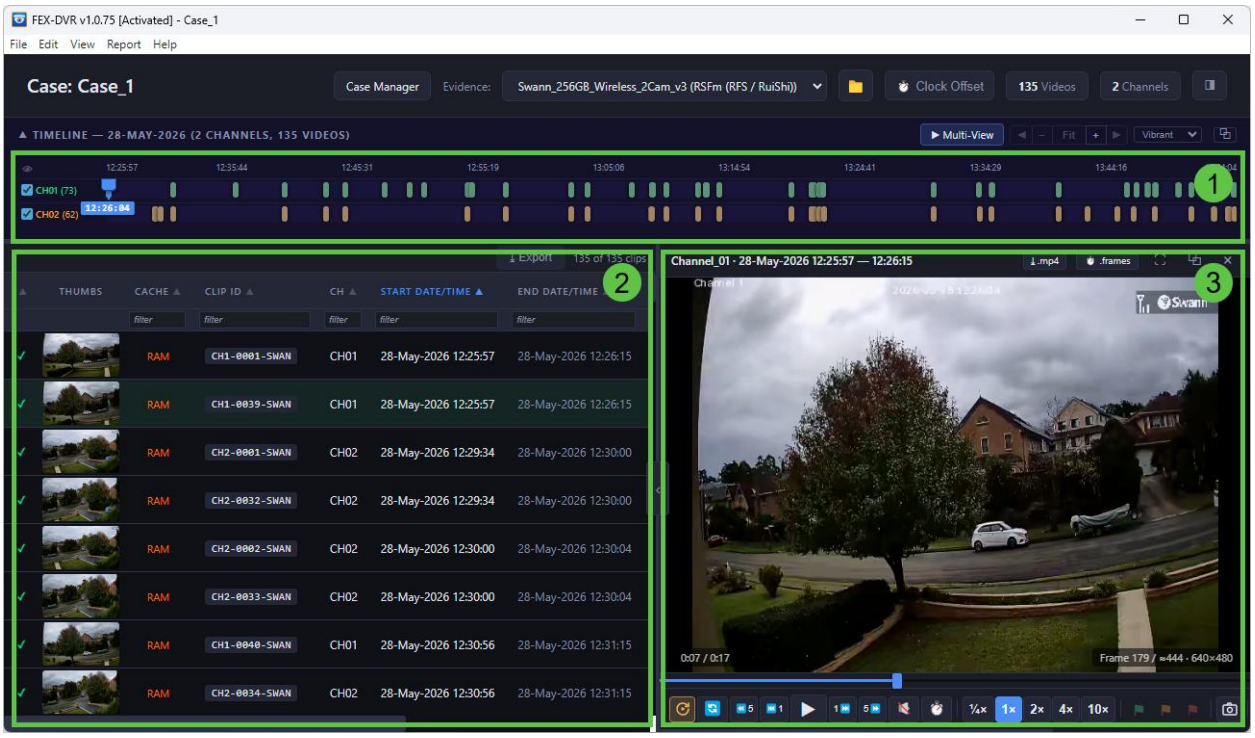
Click the **View** button next to any evidence item to open it in the Evidence Viewer.

3. INTERFACE LAYOUT

The interface is structured in four distinct windows:

1. Channel Timeline
2. Clip List
3. Viewer
4. Multi-View

Figure 9: Interface layout



3.1 CHANNEL TIMELINE

The timeline gives you a visual, time-based overview of all recorded footage in a case. Time runs left-to-right along the bottom axis, and each camera channel has its own row, with coloured blocks showing where that camera has recorded video. The timeline can be used to quickly isolate and play video:

- Use the channel checkboxes down the left to show or hide individual cameras.
- Use the zoom control (or your mouse wheel) to zoom on a period of interest.
- Dashed dividers mark each change of day.
- Bookmarks appear as markers on the relevant channel.
- A blue playhead runs through the selected channel: drag it to move forward and backward in time.

Figure 10: Timeline

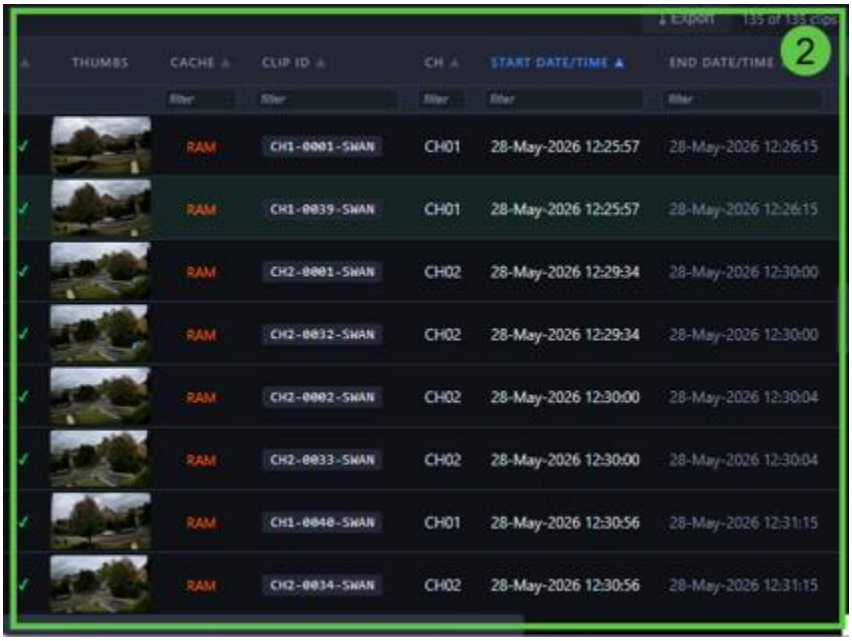
Timeline controls:

▲ TIMELINE	**Expand arrow** — collapse / expand the channel rows. The header stays visible when collapsed so the date and counts are always readable.
	Hide Unticked — suppresses rows for unticked channels so the timeline shows only what you are actively reviewing.
◀ − 5× + ▶	**Zoom group** — pan and zoom horizontally. The middle button shows the current zoom level (Fit when fully zoomed out) and goes amber when zoom is active. The mouse wheel over the timeline also zooms.
Vibrant	**Style picker** — choose the timeline color theme. Purely cosmetic; the choice persists per user.
	Undock — pop the timeline out into its own resizable window, useful on multi-monitor setups. Close the popout to re-dock.
	Auto-Next — when ON (amber), playback continues into the next clip on the same channel as soon as the current one ends.

3.2 CLIP LIST

The clip list is the central table of every recording found in the case, with one row per clip and a thumbnail preview alongside key details such as the Clip ID, start and end date/time, runtime, resolution, file size and camera channel. Right-click on the header bar to add and remove columns.

Figure 11: Clip list



Clip ID:

The clip ID is generated by FEX-DVR as a unique reference to that footage. It is constructed in the format: CH1-0002-SWAN, which is a construct of the channel number, a clip count, and an abbreviation of the evidence name.

Column Sorting:

Click any column heading to sort by that field. The sorting column will turn blue, and the arrow represents the direction of the sort.

Column Filtering:

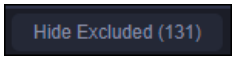
Type into the small filter box beneath a heading to quickly filter the list to matching rows — for example, narrowing to a particular channel, time or resolution.

graham

Exclude Clip(s):

Use the green tick in the first column to exclude video(s). Use the CTRL or SHIFT button to operate on multiple rows. A Hide/Show button will appear at the top of the clip list and controls whether these clips are visible or not. A hidden clip will also be marked in the timeline as hidden:

Figure 12: Hide/Show clips



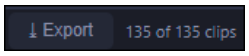
Playing a Clip:

Clicking a row plays that clip (if the auto-play button is selected, or if not, press the play button).

Export the Clip List:

The export button writes the currently visible rows — respecting any active filters — to a CSV file containing the curated forensic columns plus any format-specific metadata, so your working set can be carried straight into a report or spreadsheet:

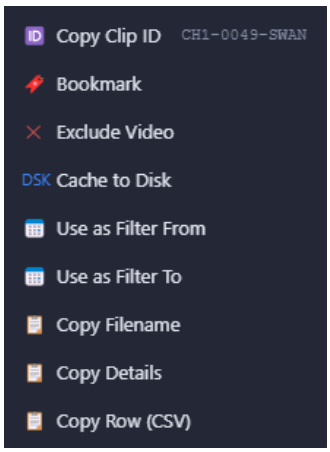
Figure 13: Export clip list



Clip List Options:

Right-click on a clip(s) to reveal additional options;

Figure 14: Right-click options



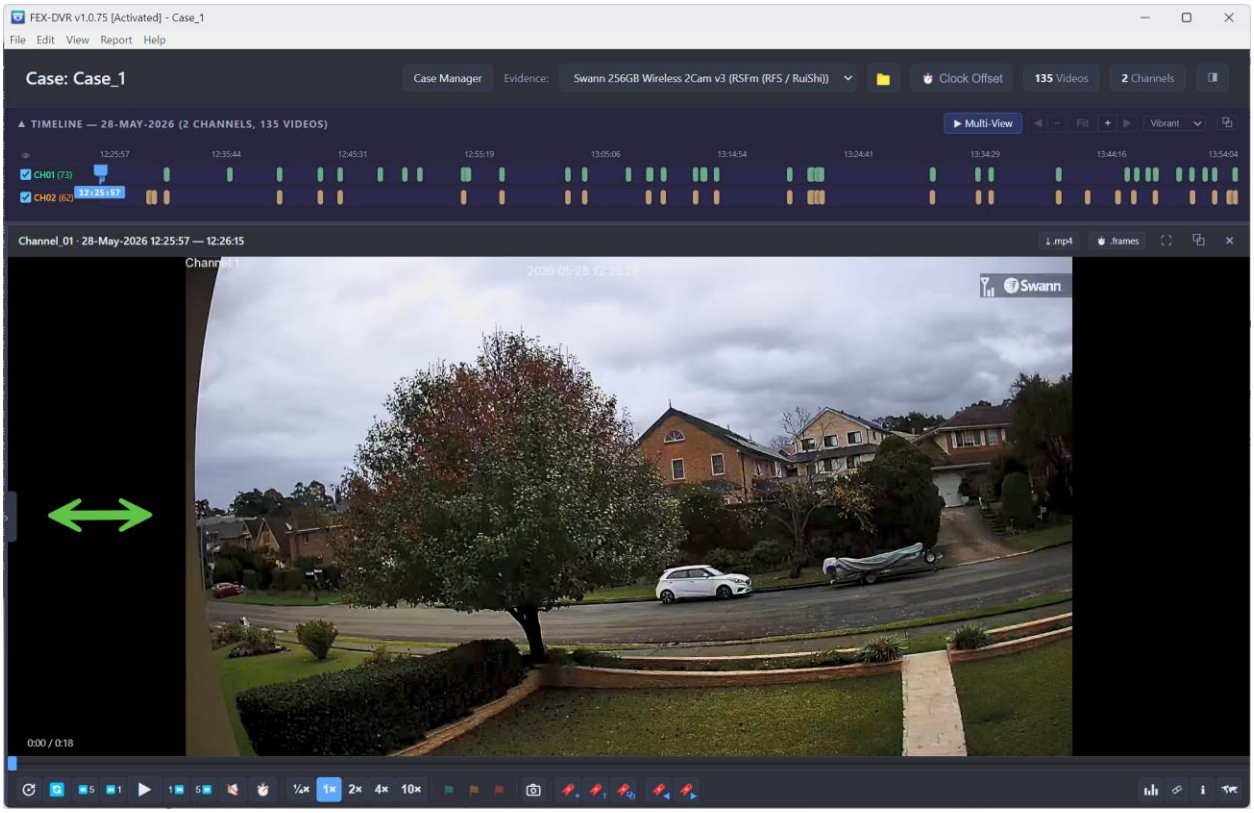
3.3 VIEWER

The player window is where the currently selected clip is decoded and played back. The clip is transcoded on demand the first time you open it — a brief Preparing indicator appears — and then plays in the viewport above a control bar and a scrub bar that shows the current time, total duration, and frame number, with amber diamonds marking any bookmarks on the clip.

The player can be made full screen by:

- Clicking the chevron in the middle of the splitter bar.
- Clicking the full screen icon.
- Detaching the viewer window.

Figure 15: Viewer (full screen mode)



3.3.1 VIEWER CONTROLS

The viewer has the following toolbar control icons:

Icon	Player Control Description
	Autoplay (clips autoplay in sequence).
	Restart playback from the beginning (R).
	Skip back 5 seconds (J).
	Step back one frame (,).
	Play / Pause (Space).
	Step forward one frame (.).
	Skip forward 5 seconds (L).
	Toggle sound (mute / unmute).
	Go to a specific frame (G).
	Set playback speed to one-quarter (¼×).
	Set playback speed to normal (1×). The active speed is highlighted.
	Set playback speed to 2×.
	Set playback speed to 4×.
	Set playback speed to 10×.
	Flags (adds a colored flag to the Clip List) as a visual marker.
	Screen capture. Captures are written to the case folder, e.g.: *"…\cases\Case_1_20260605_200530\evidence\Swann_256GB_Wireless_2Cam_v3\screenshots\Ch1_640x480_seg0039_321frames_F177_7.04s_20260609_000619.png"*

3.3.2 MOTION DETECTION

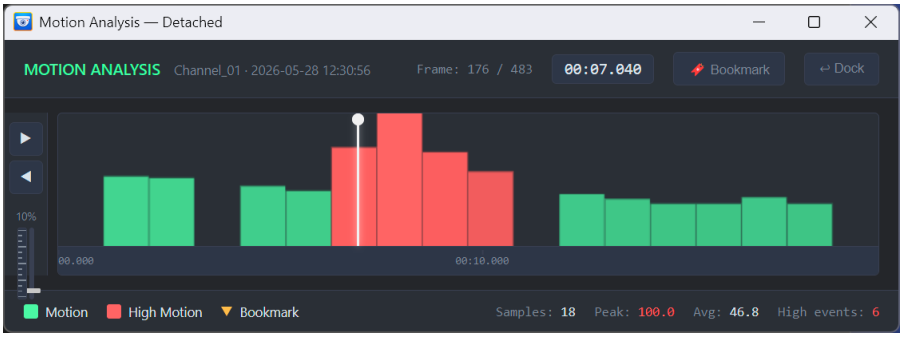
The **Motion Detection** graph analyses a clip for movement and plots the result as a coloured strip beneath the player, with one bar per second running the length of the clip. Clicking anywhere on the motion graph seeks straight to that moment, and the ◀ ▶ buttons jump between detected motion events so you can step through activity one event at a time.

A sensitivity slider sets how much movement counts as significant, letting you filter out minor noise like changing light or compression artefacts and isolate the events of interest. The analysis runs once per clip and is cached within the case, so the graph reappears instantly the next time you open it.

Undock the motion graph for a more detailed view.

Figure 16: Motion graph in the viewer

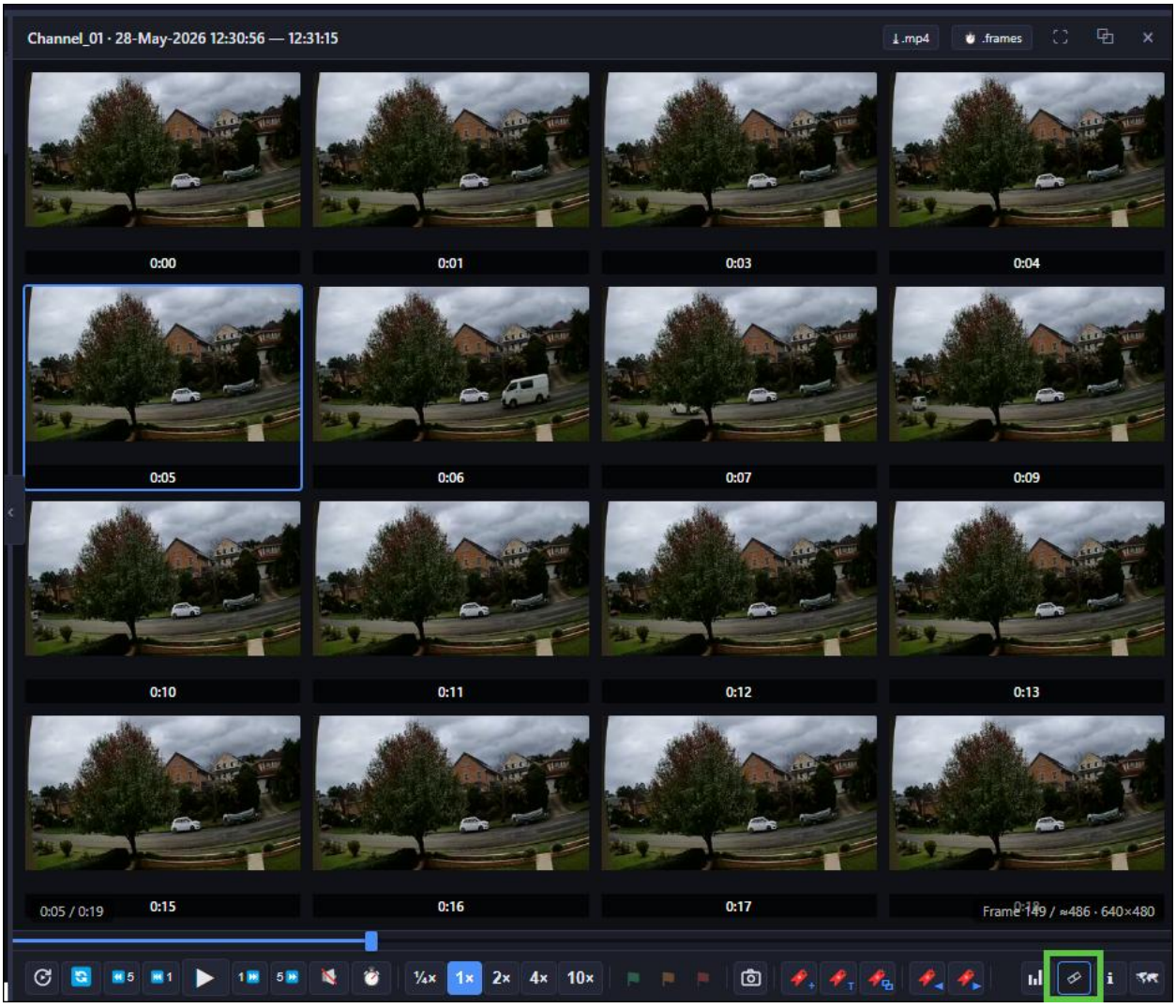
Figure 17: Motion graph undocked



3.3.3 SCENE INDEX

The Scene Index gives you a quick visual overview of a clip without watching it through. When opened, it samples frames at even intervals across the clip's full duration and lays them out as a grid of thumbnails, each stamped with its time offset. This lets you spot the moments of interest at a glance — when a scene changes, when someone enters frame, or where the recording is simply empty — and clicking any thumbnail jumps the player straight to that point and begins playback. The thumbnails are generated on first use and cached within the case, so reopening the Scene Index for the same clip is instant.

Figure 18: Scene index



3.3.4 CLIP METADATA

Click the **Metadata** button in the player controls to view forensic provenance data, including the source image path and hash, the disk sector ranges where the video data was read, and acquisition metadata (if available in the E01 header).

Figure 19: Metadata window

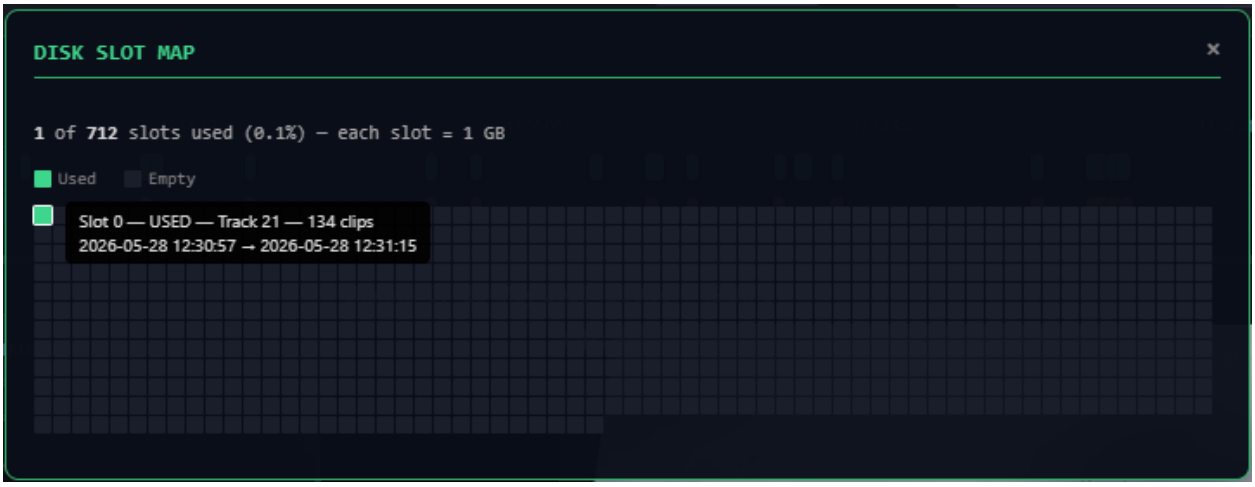
3.4 DISK SLOT MAP


The Disk Slot Map button appears only when the evidence is an RSFm-format image.

The Disk Slot Map gives a forensic view of how the recorder has used its hard drive. RSFm-family DVRs (such as Swann units) divide the disk into fixed one-gigabyte slots and write recordings into them in turn; the slot map renders these as a grid of small cells — green where a slot holds recorded video and dark where it is empty — above a summary showing the device model, firmware version, and how many of the total slots are in use.

Hovering over any cell reveals that slot's details, including the channel it belongs to, how many clips it contains, and the time span it covers, so you can see exactly where on the disk a given recording physically resides and judge at a glance how full the drive is and how its footage is distributed. Because it overlays the recovered video index onto the disk's own Part/File table, the map reflects the true on-disk layout even when the recorder has left its own metadata fields blank.

Figure 20: Disk slot map



3.5 MULTI-VIEW

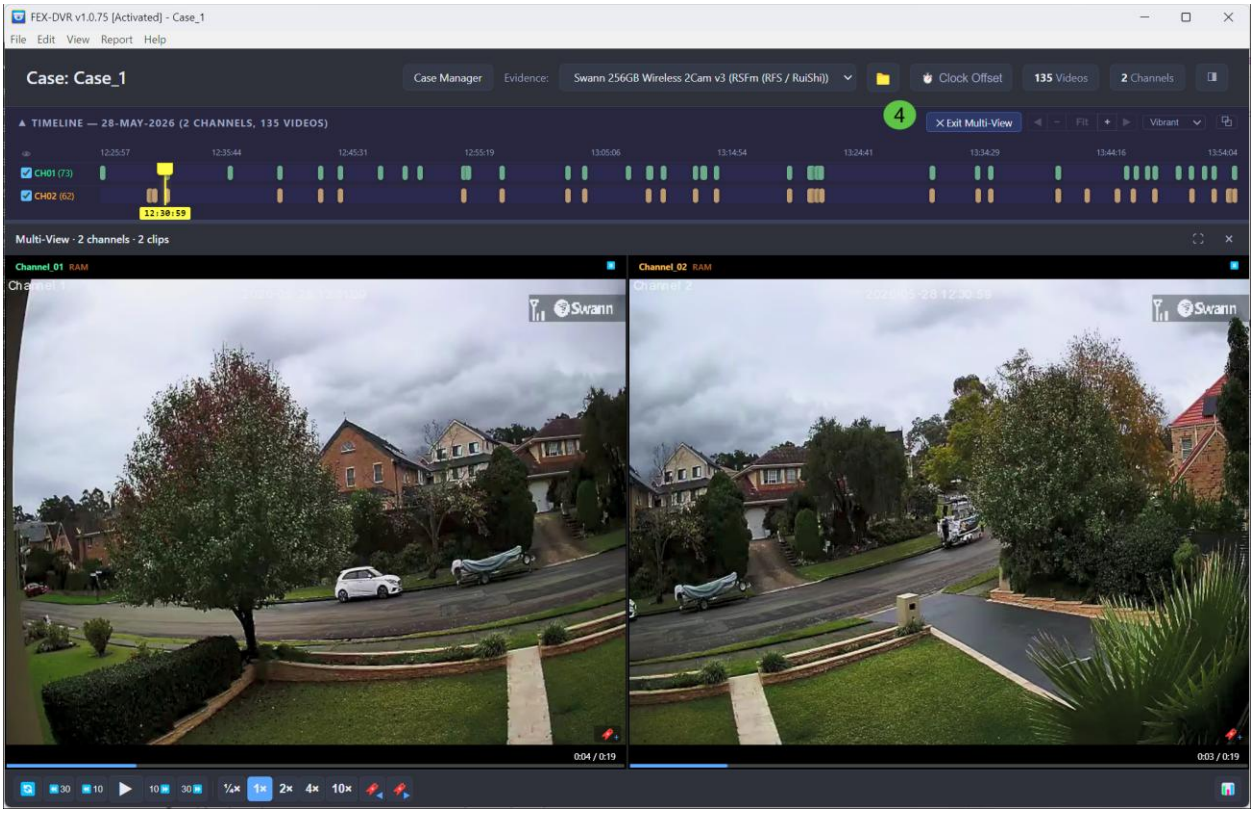
Enter and exit Multi View mode by pressing the Multi-View button above the timeline.

Multi-View plays two or more cameras side by side against a single shared clock, so you can watch what every channel was recording at the same moment.

The Multi View panes are laid out in a grid and are driven by one master playhead — the amber marker on the timeline.

Scrub or play and all panes move together in lock-step wall-clock time; as each camera's clip ends, Multi View automatically pages forward to that channel's next recording, so the views stay in sync. When a channel has no footage at the current moment, its pane shows a brief "no footage at HH:MM:SS — next at …" placeholder rather than a frozen frame, making coverage gaps obvious at a glance. This makes Multi View the right tool for cross-channel review — establishing what happened across the whole scene at a given time — while single-view remains best for studying one camera in detail.

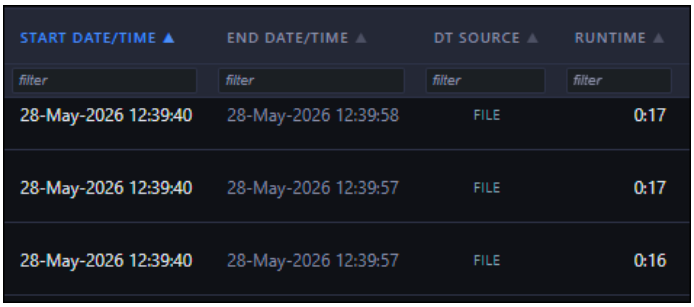
Figure 21: Viewer > Multi-View mode



Tip: If cameras are show out of sequence (e.g. Camera 01 should appear on the right), click on the camera pane and drag that camera into its correct location.

4. DATE AND TIME

The date and time of video events are of primary importance to an investigator. The FEX-DVR **Clip List** has the following relevant columns:



Start and End Date-Time show the wall-clock moments that bound a clip according to the metadata written by the DVR — typically the first and last frame timestamps in the file header.

Runtime (duration) is measured independently from the decoded video stream: the number of seconds of playable footage the clip contains. On a well-behaved recording, End minus Start equals Runtime.

- **Important:** On many forensic recoveries the Start/End and Runtime do not agree. A DVR may tag a clip with a header end-time several seconds (occasionally minutes) after the last frame it actually wrote because the unit was power-cycled, the write buffer was truncated, or the file was closed by a recovery sweep. In those cases, the footage ends at Start plus Runtime, and the interval from there to End Date-Time is a metadata-only tail with no viewable frames.
- **FEX DVR treats Runtime as the authoritative playable span** and draws the timeline, playhead and adjusted end accordingly, so every point the operator can click corresponds to a real frame. The original header End Date-Time is preserved verbatim in the clip metadata and in CSV exports for chain-of-custody purposes. It is never overwritten, only deferred to when the two values disagree.

4.1 OCR - READING BURNT-IN DVR OVERLAYS

Many DVRs imprint date/time/channel text directly into the video frame. If date/time information cannot be read from the DVR metadata, FEX DVR will attempt to read this overlay and use it as the source.

Important: OCR is not always successful due to factors such as poor video quality, non-existent stamping, and background noise behind the stamp. If OCR is used, the investigator should manually check each video to corroborate the available date/time information.

4.2 DT SOURCE COLUMN

The **DT SOURCE** column tells the investigator the source of the Start and End times for a clip. The column may contain the following values:

OCR-OK	OCR read both clock ends cleanly; times are sequential and plausible
OCR-Corrected	OCR read both ends; a small, bounded fix was applied (original kept in tooltip).
OCR-Warning	OCR-Warning — OCR read both ends, but the two times can't both be true for one clip.
OCR-Partial	OCR read only one end of the clip.
OCR-Failed	OCR ran but couldn't read either end.
OCR-Suspect	OCR parsed a time, but a value is implausible (e.g. bad year).
Inferred	Times calculated from a neighbouring clip plus this clip's duration.
File	Times read directly from the DVR's own header/index. Most authoritative.
None	No header time and OCR has not run (or isn't supported for this format).

4.3 CLOCK OFFSET — CORRECTING WRONG DVR TIMES

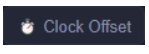
Even when date/time metadata is available from the DVR, the date/time information can be routinely wrong. Three failure modes recur:

- **Factory-default RTC** — the operator never set the clock, so the file metadata reads an epoch date while the burnt-in overlay tells a different date.
- **Incorrect DVR setting** – the DVR date/time has been set, but this setting is wrong.
- **Drift** — the clock was correct months ago and has since drifted by minutes or seconds, known by comparison against an external anchor.
- **Time-zone confusion** — the DVR stores and displays in one zone but the investigator is reasoning about another.
- **Daylight savings** – the DVR has not accounted for daylight savings shifts.

FEX DVR lets you record a known clock error against an evidence image and have every time it shows be the corrected one — without ever modifying the file on disk.

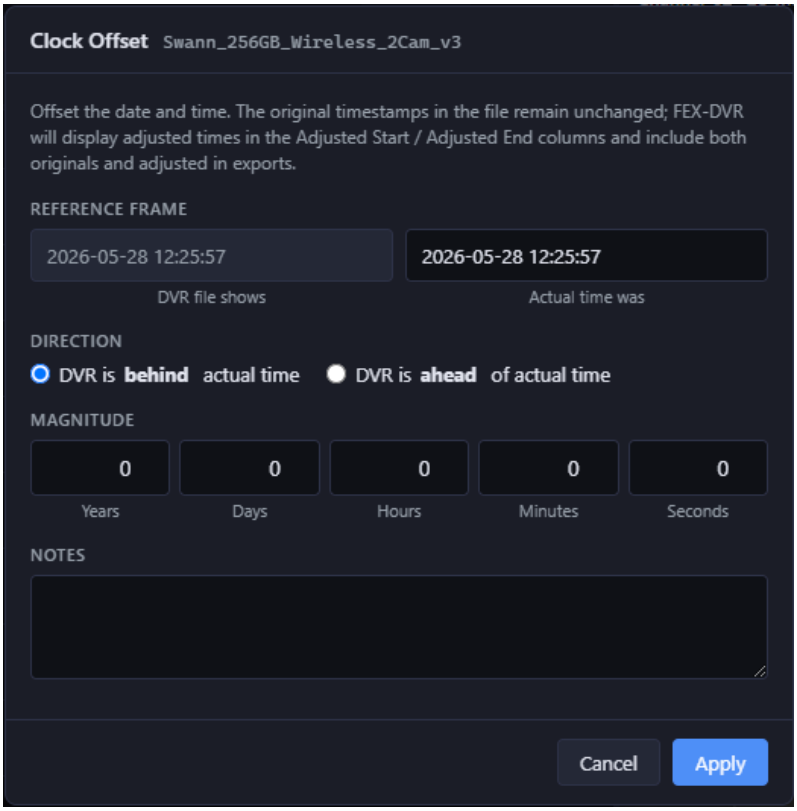
SETTING A DATE/TIME OFFSET

To add a date/time offset:

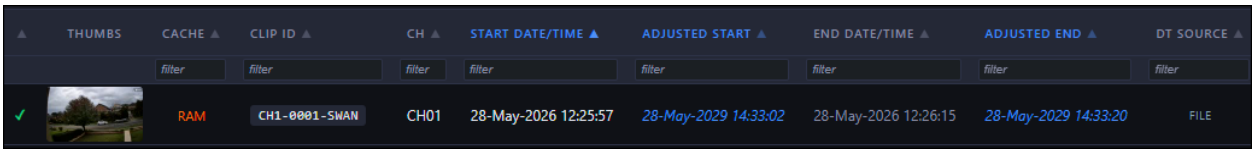
1. **Open the evidence** in the Evidence Viewer.
2. **Click the Clock Offset button** in the toolbar 

3. The following modal window opens:

Figure 22: Clock offset



4. Make and apply the date/time change. The result will be immediately visible in the **Clip List.** Both original and adjusted times are visible:



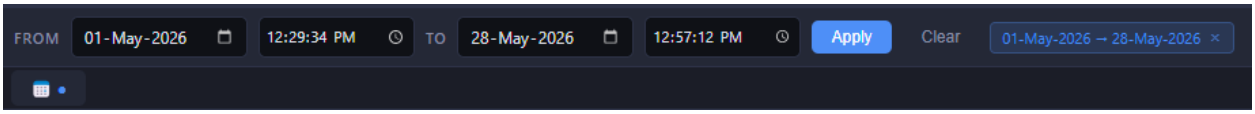
WHAT CHANGES WHEN AN OFFSET IS ACTIVE

- **A trailing asterisk** marks every adjusted time — on timeline ticks, the playhead pill, the active-clip title and the TMV range pill — so a corrected time is never confused with an original.
- **Hovering a corrected cell** shows the original time in a tooltip.
- **Filtering and Multi-View alignment use the adjusted time,** so two cameras with different clock drifts line up correctly when both have offsets configured.

4.4 DATE AND TIME FILTER

An investigator may with to filter videos between a specific start and end time. To apply this filter, click the calendar button at the top of the Clip List. This activates the filter bar:

Figure 23:

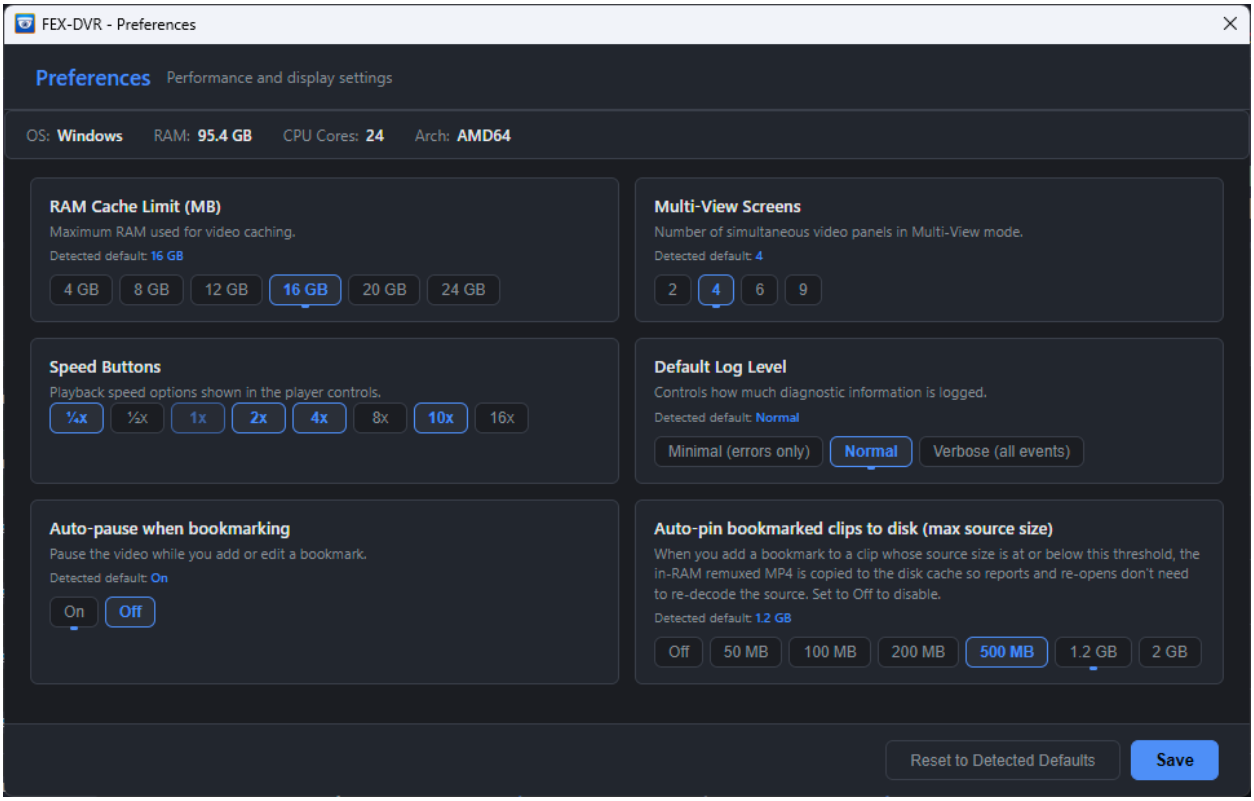


A fast way to populate the date range is to right click on a clip and select "**Use as Filter From**" and "**Use as Filter To**" menu options. This will copy the relevant dates into the date/time filter. Not that if an **Adjusted Start** and **Adjusted End** column are present, these are the date/time values that will be copied into the filter.

5. PREFERENCES

The Preferences window lets you tune how FEX-DVR uses your computer's resources and how the playback controls appear. When the window opens, FEX-DVR examines your hardware and tailors the available options to suit it, so the choices you see are matched to the machine you are running on.

Figure 24: Preferences



System summary

Along the top of the window is a read-only summary of the detected hardware: your operating system, total installed RAM, the number of CPU cores, and the processor architecture. FEX-DVR uses these figures to calculate sensible defaults and to set safe upper limits for the performance-related settings below. The information is shown purely for reference; it cannot be edited.

Detected defaults and recommended limits

Each setting displays its detected default, i.e. the value FEX-DVR has chosen for your system, directly beneath its description. Defaults scale with your hardware: a machine with more memory and more processor cores is offered higher cache limits and more simultaneous video panels than a modest one. Options that exceed what is advisable for your system are shown but greyed out and cannot be selected; hovering over a disabled option explains that it is not recommended for your system. You can change any

setting away from its default at any time, and you can return every setting to its detected default in a single step using the Reset to Detected Defaults button.

RAM Cache Limit (MB)

This setting controls the maximum amount of memory FEX-DVR will use to cache video while you work, expressed in gigabytes. A larger cache lets more footage stay in memory, which makes repeated playback and scrubbing more responsive, at the cost of higher memory use. The upper choices are capped according to your installed RAM, so you cannot set a cache so large that it would starve the rest of the system. Changes to this limit take effect immediately, without needing to restart the application.

Multi-View Screens

This determines how many video panels are shown at once when you are in Multi-View mode — for example 2, 4, 6, or 9 panels. More panels let you watch additional channels simultaneously but place greater demand on memory and the processor, so the highest options are only available on more capable systems. This value also sets the default page size used when stepping through channels in Multi-View.

Speed Buttons

This setting chooses which playback-speed buttons appear in the player controls, from a quarter speed (¼×) up to sixteen times speed (16×). Select the speeds you use regularly so the toolbar shows only the ones you need, keeping the control bar uncluttered. Normal speed (1×) is always included and cannot be removed, ensuring you can always return to real-time playback.

Default Log Level

This controls how much diagnostic information FEX-DVR records while it runs. Minimal (errors only) logs just faults, Normal records a balanced amount of activity, and Verbose (all events) captures the fullest detail. Verbose logging is most useful when investigating a problem or when asked to supply logs for support; for everyday use, Normal is recommended.

Auto-pause when bookmarking

When this is set to On, the video automatically pauses while you add or edit a bookmark, so the footage does not continue playing past the moment you are annotating. Set it to Off if you prefer playback to continue uninterrupted while you type.

Auto-pin bookmarked clips to disk (max source size)

When you bookmark a clip, FEX-DVR can copy the prepared, in-memory version of that clip to the on-disk cache so that reports and subsequent re-opens do not have to re-process the original footage again. This setting sets the maximum source-clip size for which that automatic copy happens: when you bookmark a clip at or below the chosen size (for example 500 MB or 1.2 GB), it is pinned to disk automatically. Choosing Off disables the behaviour entirely, and larger clips above the threshold are never pinned automatically.

This is a convenience-versus-disk-space trade-off — a higher threshold speeds up later work on bookmarked clips but uses more cache storage.

Saving your changes

Click Save to apply and store your preferences; a brief confirmation appears when they have been saved. Most settings, such as the RAM cache limit and the auto-pin threshold, take effect straight away. Your preferences are stored on a per-installation basis and are remembered the next time you open FEX-DVR, so you only need to set them once unless you wish to change them.

6. MEMORY MANAGEMENT AND CACHING

How FEX-DVR prepares footage for playback

FEX-DVR plays video directly from the forensic image — it does not extract or alter the original evidence on disk. Surveillance recorders, however, store footage in proprietary formats that a web browser cannot play, so the first time you open a clip FEX-DVR reads it out of the image and converts it into a standard, browser-playable MP4. This preparation step (a fast "**remux**", or a fuller "**transcode**" for formats the browser cannot decode natively) takes a moment the first time. To avoid repeating that work every time you revisit a clip, the prepared MP4 is kept in a cache, so scrubbing, replaying, and reopening the same clip afterwards is effectively instant.

The two-tier cache: RAM and disk

FEX-DVR uses two layers of cache that work together. The RAM cache holds recently prepared clips in memory for the fastest possible access; it is very quick but temporary, and its contents are lost when the application closes. The disk cache stores prepared clips as files inside the case folder; it is slower than memory but persists between sessions, so a clip that has been written to disk does not need to be re-prepared the next time you open the case. When you request a clip, FEX-DVR looks for it first in RAM, then on disk, and only re-prepares it from the source image if neither cache has it.

The RAM cache limit and how memory is reclaimed

The amount of memory the RAM cache may use is governed by the RAM Cache Limit setting on the Preferences page. FEX-DVR chooses a sensible default based on the memory it detects in your computer, and as a safeguard it will never let the cache exceed roughly half of the machine's physical RAM, regardless of the value chosen, so the rest of the system is not starved. When the cache fills up and a new clip needs room, FEX-DVR automatically discards the least recently used clips to make space. A clip that is currently being watched is protected from this clean-up, so active playback is never interrupted by the cache reclaiming the very clip you are viewing. A larger limit keeps more footage in memory at once — useful when comparing many channels in Multi-View — at the cost of higher memory use.

Pre-caching for smoother review

To make review feel responsive, FEX-DVR can quietly prepare upcoming clips in the background before you click on them, a process called pre-caching. This work runs at a lower priority so it always yields to whatever you are actively doing, and it pauses automatically once the RAM cache is around three-quarters full, leaving headroom for clips you open directly. The result is that clips are often ready to play the instant you select them, without you having to wait for preparation.

When clips are written to disk

Because the RAM cache is temporary and limited in size, FEX-DVR writes certain prepared clips to the disk cache so the effort is not wasted. This happens in two situations. First, if a clip is too large to keep in

memory, its prepared MP4 is spilled to disk rather than discarded, so it can still be served quickly later. Second, when you bookmark a clip, whose original size is at or below the Auto-pin bookmarked clips to disk threshold set in Preferences, FEX-DVR copies its prepared MP4 to the disk cache automatically. This "pinning" ensures that clips you have marked as significant — and which will appear in reports — can be reopened and exported without ever needing to re-process the source footage again. You can raise, lower, or switch off this threshold to balance convenience against the disk space the cache consumes.

Caches are per-case and the evidence is never changed

All cached data is stored separately for each case and evidence image, which keeps material from different investigations strictly isolated and preserves forensic integrity. No matter how much caching takes place, the original forensic image is only ever read, never modified. If you need to reclaim space, the cache for an evidence item can be cleared at any time; doing so simply means the affected clips will be prepared again from the source image the next time they are opened

7. BOOKMARKS

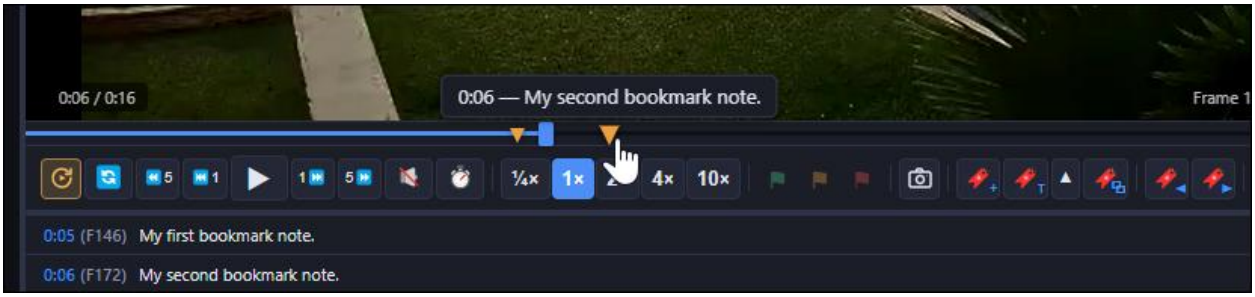
Bookmarks let the investigator identify specific clips and precise date/time points as areas of interest. They form the foundation of the reporting process, providing the evidential moments from which reports are generated.

Bookmarks are added using the following icons or shortcut keys:

Icon	Action	Shortcut
+	Quick bookmark. Instantly saves a bookmark at the current playback position.	CTRL B
T	Add bookmark with note. Saves a bookmark at the current position and prompts for a short text note describing it.	CTRL M
◀	Previous bookmark. Jumps play back to the preceding bookmark.	
▶	Next bookmark. Jumps playback forward to the following bookmark.	
	Undock bookmarks. Opens the bookmark list in a separate, detachable window.	
	Bookmarks are represented on the scrub bar and the timeline by a yellow down arrow.	

Bookmarks can be managed using the icons in viewer toolbar. Mousing over a bookmark on the progress bar will show the bookmark note:

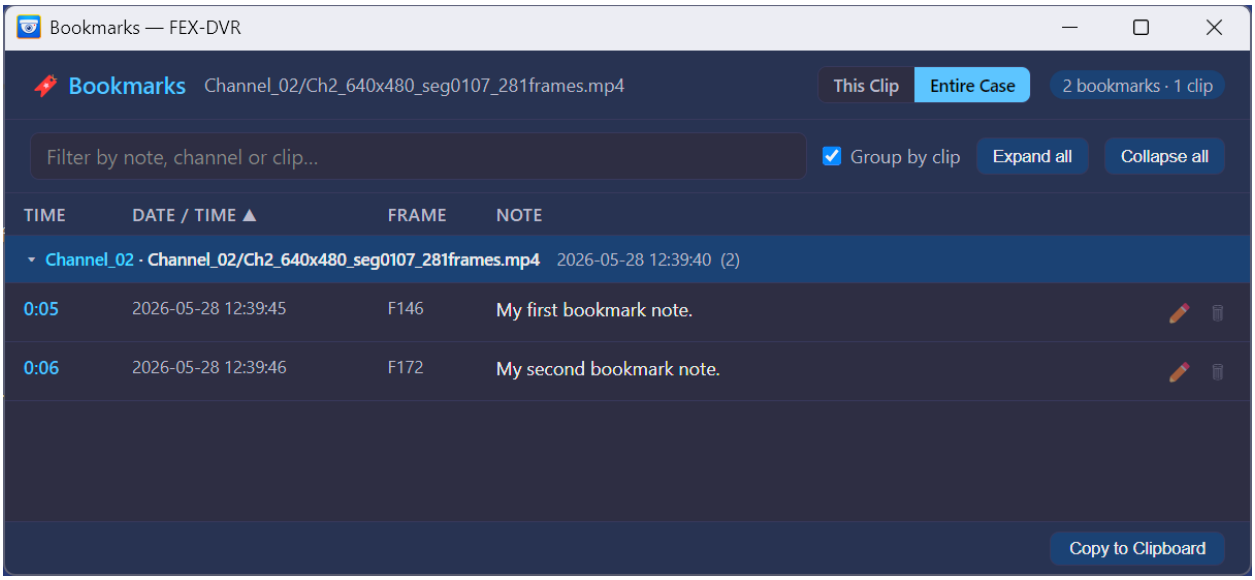
Figure 25: Bookmark in the Viewer toolbar



7.1 BOOKMARKS WINDOW

For more detailed bookmark control, open the undocked bookmark control window:

Figure 26: Bookmarks window



The Bookmarks window lists the time-stamped notes you have added to your footage. Use it to review, edit, navigate to, and export bookmarks. It stays in sync with the player, so changes appear immediately in both places.

Choosing what to view

A scope toggle in the top bar controls which bookmarks are shown:

- **This Clip** — shows only the bookmarks on the clip currently loaded in the player. The clip's name is displayed next to the title.
- **Entire Case** — shows every bookmark in the case, drawn from all clips. The counter (e.g. *3 bookmarks · 2 clips*) summarizes the totals.

Reading the list

Each bookmark row shows:

- **Time** — the position within the clip (e.g. 0:05).
- **Date / Time** — the absolute date and time of the bookmark. A trailing * indicates the time has been adjusted by the clip's clock offset; hover to see the original.
- **Frame** — the frame number (e.g. F146).

- **Note** — your text. Rows showing *Click to add note…* have no note yet.

In **Entire Case** view, bookmarks are organized under a header for each clip, showing the channel, clip name, and start time. A clip marked *(filtered out)* is hidden by the filters in the main window; clear those filters to open it.

Navigating and organizing

- **Go to a bookmark** — click a row to seek the player to that point. In Entire Case view, the relevant clip is loaded automatically if it is available.
- **Filter** — type in the *Filter by note, channel or clip* box to narrow the list (Entire Case view).
- **Group by clip** — tick to group bookmarks under their clip; untick for a single flat list.
- **Expand all / Collapse all** — open or close every clip group at once.
- **Sort** — click the **Date / Time** column heading to sort; click again to reverse the order.

Editing bookmarks

- **Add a note** — click an empty *Click to add note…* cell, type, and press **Enter**. In This Clip view you can also add a bookmark at the current position using the input field, or press **M** in the player.
- **Edit a note** — click the note (or the pencil icon), edit the text, and press **Enter** to save or **Escape** to cancel.
- **Delete** — click the trash icon on the row.

Exporting

Click **Copy to Clipboard** to copy the visible bookmarks as plain text for pasting into a report or notes. If the clipboard is unavailable, the text is offered as a file download instead.

8. REPORTS

Reports are created with the **Build Report** wizard, opened from **Report > Case Report** (or by pressing **F7**). The wizard guides you through three steps:

1. **Devices**
2. **Sections**
3. **Output**

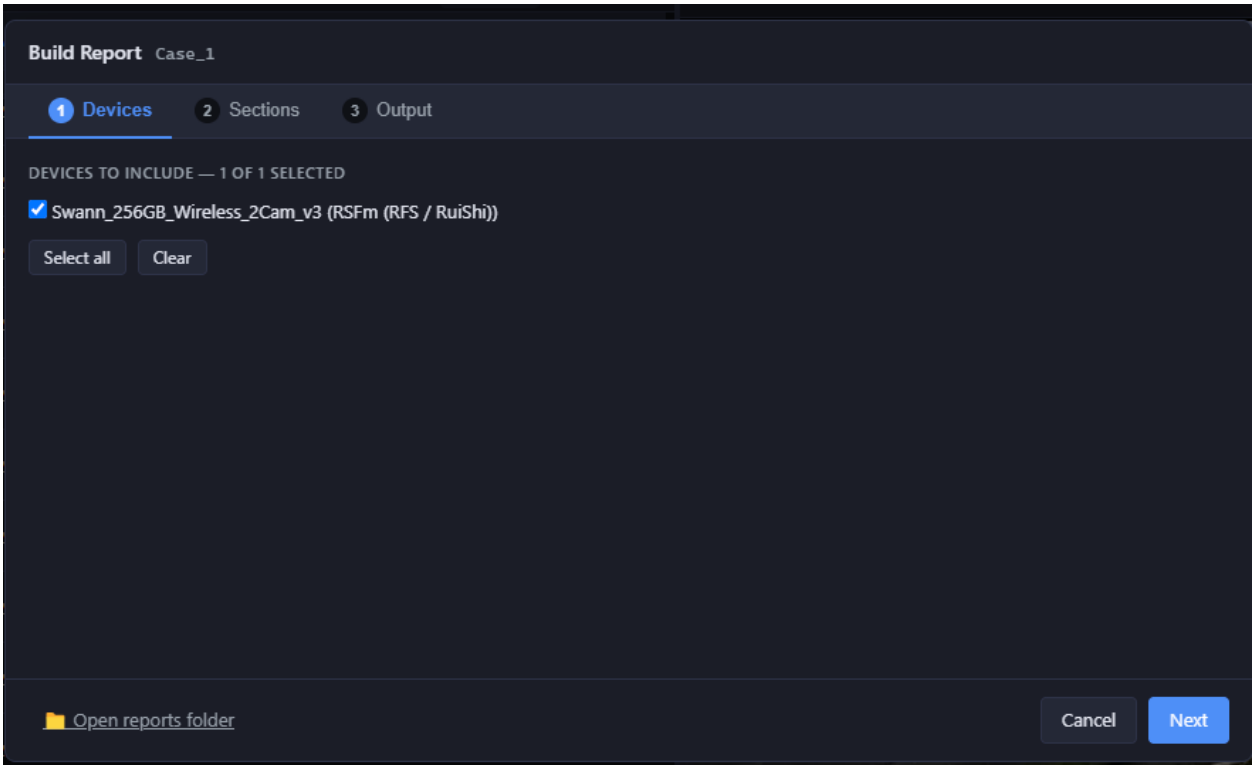
Use **Next** and **Back** to move between them, **Cancel** to discard, and **Open reports folder** (bottom left) to view previously generated reports.

STEP 1 — DEVICES

Choose which evidence devices to include in the report.

- Tick the devices you want to cover. The header shows how many are selected (e.g. *1 of 1 selected*).
- Use **Select all** to include every device, or **Clear** to deselect all.
- Click **Next** to continue.

Figure 27: Report wizard > Devices



STEP 2 — SECTIONS

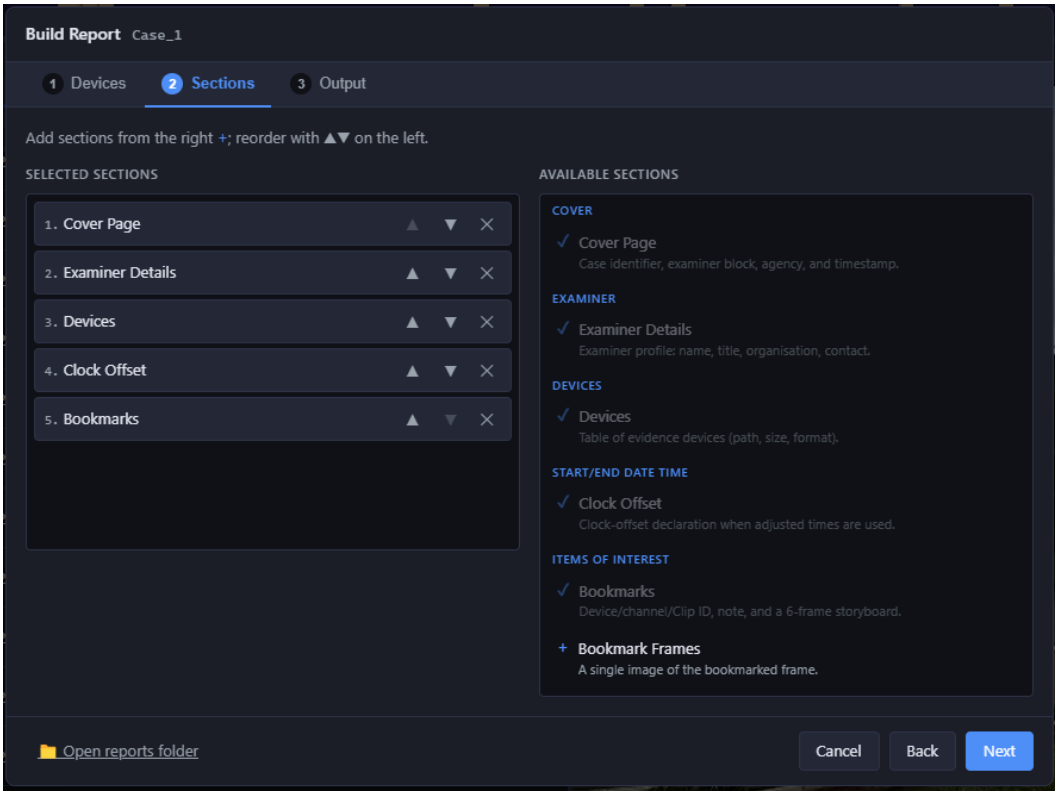
Choose which sections appear in the report and the order in which they appear.

- **Add a section** — click the **+** beside an entry under *Available Sections* on the right. A tick (✓) indicates a section is already included.
- **Reorder** — use the ▲ and ▼ buttons on a row under *Selected Sections* on the left to move it up or down.
- **Remove** — click the ✕ on a row to take it out of the report.

Available sections include:

- **Cover Page** — case identifier, examiner block, agency, and timestamp.
- **Examiner Details** — examiner profile: name, title, organization, and contact.
- **Devices** — a table of evidence devices (path, size, format).
- **Clock Offset** — a clock-offset declaration, included when adjusted times are used.
- **Bookmarks** — device/channel, Clip ID, note, and a six-frame storyboard for each bookmark.
- **Bookmark Frames** — a single image of each bookmarked frame.

Figure 28: Report sections



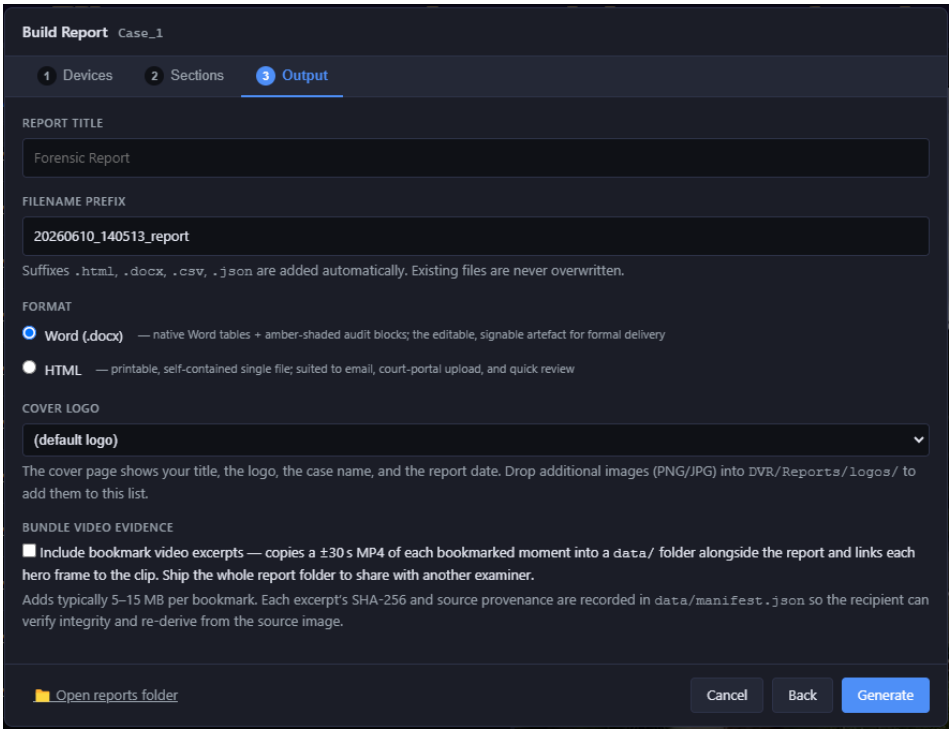
STEP 3 — OUTPUT

Set the report's title, file name, format, and packaging options, then generate it.

- **Report Title** — the title shown on the cover page (e.g. *Forensic Report*).
- **Filename Prefix** — the base name for the output files. Suffixes (.html, .docx, .csv, .json) are added automatically, and existing files are never overwritten.
- **Format** — choose the output:
    - **Word (.docx)** — native Word tables with amber-shaded audit blocks; the editable, signable artefact for formal delivery.
    - **HTML** — a printable, self-contained single file; suited to email, court-portal upload, and quick review.
- **Cover Logo** — select the logo shown on the cover page. To add more options, drop PNG or JPG images into the DVR/Reports/logos/ folder.
- **Bundle video evidence** — tick **Include bookmark video excerpts** to copy a ±30-second MP4 of each bookmarked moment into a data/ folder beside the report, with each frame linked to its clip. This adds roughly 5–15 MB per bookmark. Each excerpt's SHA-256 and source provenance are recorded in data/manifest.json so a recipient can verify integrity and re-derive the excerpt from the source image. Ship the whole report folder when sharing with another examiner.

Click **Generate** to produce the report. Use **Open reports folder** to locate the output files.

Figure 29: Report output



9. KEYBOARD SHORTCUTS

Shortcuts only fire when the focus is outside an input field. Most player keys require a clip to be loaded.

9.1 PLAYBACK

Key	Action
Space or K	Play / Pause
Comma or Left Arrow	Previous frame
Period or Right Arrow	Next frame
J	Skip back — 5 s in single-view, 10 s in Multi-View (all panes)
L	Skip forward — 5 s in single-view, 10 s in Multi-View (all panes)
1–9	Select the Nth playback-speed button (set in Preferences → Speed Buttons)
R	Restart playback — current clip in single-view, every pane in Multi-View
G	Go to frame... (numeric prompt)
F	Toggle full screen

9.2 ANNOTATION & CAPTURE

Key	Action
M	Add a scrub-bar marker at the current time (in-clip colored dot with optional note). Local to the clip.
B	Add a bookmark at the current frame. Bookmarks appear as amber diamonds across the timeline and survive between sessions.
C	Copy current frame to the clipboard as a PNG snapshot

9.3 VIEWS & NAVIGATION

Key	Action
S	Toggle scene index (storyboard)
Y	Toggle Multi-View mode for the currently ticked channels
D	Toggle the sync-debug overlay (Multi-View only)
Up / Down Arrow	Move to the previous / next visible row in the video list and load it
Esc	Exit Multi-View → close the scene index → close the active player (priority order)

10. DEFINITIONS

Clip ID	The Clip ID is generated by FEX-DVR as a unique reference to that footage. It is constructed in the format: CH1-0002-SWAN, which is a construct of the channel number, a clip count, and an abbreviation of the evidence name
Codec	Short for coder/decoder. A method for compressing video (or audio) so it takes up less storage space, and then decompressing it again for playback. CCTV and DVR systems record footage using a codec — most commonly H.264 or H.265 — to fit long hours of video onto the device's drive. To view that footage, software must support the same codec to decode it. FEX-DVR includes the decoders needed to read the codecs used by the DVR formats it supports, so recordings can be played back and exported to standard video files.
.E01	A forensic file format used to create forensic image files of physical devices or partitions (see also .L01). Developed by Guidance Software (http://www.guidancesoftware.com/).
DD	DD (also referred to as RAW) is a disk image format that stems from the DD command on UNIX and Linux operating systems. DD images are considered a forensic format as they are a bit by bit copy of a device.
Forensic Image	A "forensic image is a file (or set of files), is used to preserve an exact "bit-for-bit" copy of data residing on digital media. The most commonly used format is .E01 by Guidance Software (www.guidancesoftware.com). The image contains all data, including deleted and system files, and is an exact copy of the original. Most forensic imaging software integrates additional information into the image file at the time of acquisition. This can include descriptive details entered by the examiner, as well as the output of mathematical calculations, an "acquisition hash", which can be later used to validate the integrity of the image. The forensic image file acts as a digital evidence container that can be verified and accepted by courts.
Forensically Sound	Digital evidence by its very nature is volatile. The term forensically sound refers to the accepted industry principle that maintaining the integrity of digital evidence is paramount, and that no action by the investigator should change data that is to be relied upon. FEX Imager collects evidence in a manner that preserves the integrity of evidence and provides an audit trail so that an independent third party can examine the actions undertaken. An investigator should also apply standard principles of crime-scene preservation (photographs, documentation, etc.) to any matter involving digital evidence.
H.264/H.265	H.264 / H.265 — The two video compression standards (codecs) most commonly used by CCTV and DVR systems to shrink recorded footage so it fits on the drive. H.264 (also called AVC) is the long-established, widely supported standard. H.265 (also called HEVC) is its successor, achieving roughly the same picture quality at about half the file size, at the cost of needing more processing power to decode. DVR recordings are stored in one of these formats inside the device's proprietary container; FEX-DVR decodes both so the footage can be viewed and exported to standard playable video.
Hikvision	One of the world's largest manufacturers of CCTV cameras and digital/network video recorders (DVRs/NVRs). Hikvision recorders store footage using a proprietary on-disk format (identified by the HIK.2011 filesystem signature) rather than ordinary video files, so the raw drive cannot simply be opened in a media player. FEX-DVR recognises this format automatically and reconstructs the individual recordings, channels, and timestamps from a Hikvision drive or disk image so they can be reviewed and exported.
.L01 File	A .L01 file (also commonly referred to as a logical evidence file or LEF) is a forensic file format created by Guidance Software (www.guidancesoftware.com). FEX Imager can export files from a target computer system into a L01 file whilst preserving the integrity of the original file information (dates,

	times, size, etc.). A .L01 is usually used to store a selection of files, rather than a copy of an entire drive, for which the Guidance Software .E01 format is most frequently used.
MD5	MD5 is a widely used cryptographic algorithm designed in 1991 by RSA (Ron Rivest, Adi Shamir and Len Alderman). It is a 128-bit hash value that uniquely identifies a file or stream of data. It has been extensively used in computer forensics since the late 1990's. MD5 has been identified to have a theoretical collision weakness (when two files have the same hash). For more information see: - MD5 Collisions, The Effect on Computer Forensics, April 2006, Access. - The Hash Algorithm Dilemma–Hash Value Collisions, Lewis, 2009, Forensic Magazine.
Remux	Remux (short for re-multiplex) is the process of repackaging existing audio and video streams into a different container format without re-encoding the actual picture or sound. The original video data is copied across unchanged and simply placed inside a new "wrapper" that the playback software can read. In FEX-DVR, remuxing is used to make footage from a DVR's proprietary format playable in the viewer: the recorded video stream is lifted out of the forensic image and rewrapped as a standard MP4 file. Because the video itself is copied rather than re-compressed, remuxing is fast and preserves the original image quality — no pixels are altered or degraded.
Runtime (Clip List)	In the Clip List, the Runtime column shows the actual playback length of a clip — how long the footage runs when played — calculated from the clip's frame count divided by its frame rate. This can differ from the wall-clock span (End Date/Time minus Start Date/Time): on time-lapse, motion-triggered, or variable-frame-rate recordings the camera may cover a long period of real time while containing only a short amount of actual video, so a clip's Runtime is often shorter than the elapsed time between its start and end. Where a value is shown with a "(span)" suffix, the true runtime isn't yet known and the figure is the wall-clock span until the clip has been probed.
Scrub	Scrub is to drag the playhead along the timeline (or the player's progress bar) to move quickly to a different point in the footage, rather than waiting for it to play there. Scrubbing lets you jump forwards or backwards to a specific moment; in Multi-View, scrubbing moves the shared amber playhead so every channel jumps to that same wall-clock instant together.
SHA1	SHA1 is a widely used cryptographic algorithm that uniquely identifies a file or stream of data. SHA1 is considered a stronger hash than MD5, but as a result takes longer to calculate. SHA1 has been identified to have a theoretical collision weakness (when two files have the same hash). For more information see: - MD5 Collisions, The Effect on Computer Forensics, April 2006, Access. - The Hash Algorithm Dilemma–Hash Value Collisions, Lewis, 2009, Forensic Magazine.
SHA256	SHA256 is a widely used cryptographic algorithm that uniquely identifies a file or stream of data. It is designed by the United States National Security Agency (NSA) and first published in 2001. SHA256 is a stronger hash than MD5 and SHA1, but as a result takes longer to calculate.
Transcode (transcodiing)	Transcoding is the process of a full decode and re-compresses of the video (changing the underlying data). FEX-DVR only transcodes when a recording uses a codec the browser cannot play directly; whenever possible it remuxes instead, to keep playback faithful to the source.
Unknown format error	The DVR filesystem format was not recognised. The image type is not yet. Contact support@getdata.com for assistance.
Write Blocker	A write blocker is a tool which sits between the target media and the investigators workstation. It ensures that it is not possible for the investigator to inadvertently change the content of the examined media. It permits read-only access target data without compromising its integrity. Write blockers exist as both software and as hardware. In computer forensics it is write blocking hardware that is more commonly used as its hardwired configuration provides more certainty as to its use.

11. CONTROL ICONS

Icon	Description
	Autoplay toggle. When active, clicking a clip (or a timeline / list row) starts playback immediately; when off, clips load paused and you press Play or Space.
	Restart playback from the beginning (R).
	Skip back 5 seconds (J).
	Step back one frame (,).
	Play / Pause (Space).
	Step forward one frame (.).
	Skip forward 5 seconds (L).
	Toggle sound (mute / unmute).
	Go to a specific frame (G).
	Set playback speed to one-quarter (¼×).
	Set playback speed to normal (1×). The active speed is highlighted.
	Set playback speed to 2×.
	Set playback speed to 4×.
	Set playback speed to 10×.
	Flag the current clip as Reviewed (green).
	Flag the current clip as Evidence (orange).
	Flag the current clip as Flagged (red).
	Snapshot the current frame: copy it to the clipboard and save it to the case (C).
	Add a quick bookmark at the current time (B).
	Add a bookmark with a typed note (M).
	Open the bookmarks list in its own window.
	Jump to the previous bookmark ([).
	Jump to the next bookmark (]).
	Show or hide the motion-detection graph.
	Show or hide the scene index / storyboard (S).
	Show or hide forensic metadata and provenance for the clip (I).
	Detach as a stand alone window
	Date/Time filter.

12. ACKNOWLEDGEMENTS

FEX-DVR is built with the help of open-source software, and we gratefully acknowledge the projects that make it possible, including FFmpeg (video decoding and transcoding), OpenCV, RapidOCR and the PaddleOCR models (on-screen timestamp and channel recognition), ONNX Runtime, NumPy, psutil, Pillow, and Python.

Each component remains the property of its respective authors and is used under its own licence. The full licence texts, copyright notices, and for the GPL-licensed FFmpeg components a written offer of source code are provided in the accompanying THIRD_PARTY_LICENSES.md file distributed with the application. The bundled Chromium component licences are listed in LICENSES.chromium.html.

13. LICENSE AGREEMENT

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

IMPORTANT – END USER LICENSE AGREEMENT

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("AGREEMENT") CAREFULLY BEFORE USING GETDATA SOFTWARE ("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 only to the version of the Software package with which this agreement is included. Different license terms may apply to other software packages from GetData and license terms for later versions of Forensic Explorer may also be changed.

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,' and 'Forensic Explorer' 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 authorised 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 authorised 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 authorised 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 Forensic Explorer 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 authorised 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.