Forensafe Software Solutions

ArtiFast Suite

User Guide

Investigator Workflow Handbook

Operational reference for digital forensics practitioners.

ArtiFast Suite is a digital forensics Software for evidence processing, artifact analysis, timeline review, and defensible reporting.

Notice

This document is an operational user guide for ArtiFast Suite. It is intended to support repeatable workflows in digital forensics investigations.

ArtiFast Suite outputs (reports, exports, extracted files, hash lists) should be handled according to your organization's evidence-handling policy.

Quick Start: Run Your First Case (3 Minutes)

Follow this checklist to create a case, process evidence, and review your first results without reading the full guide.

1. Launch ArtiFast Suite.
2. Confirm licensing (**License → License Information**).
3. Set default paths and Evidence Time Zone (**Settings → Configurations**).
4. Start a case (**Case → New**) or run a fast triage (**Case → Quick Run**).
5. Add evidence (image, drive, folder, memory, or mobile extraction).
6. Choose processing options (hashing, hash lists, encryption detection, file exports, rule scanning).
7. Select artifact scope (all artifacts, or targeted categories).
8. Run processing.
9. In the workspace, narrow scope using the left hierarchy + filters.
10. Export results using Reporting, and record your scope (filters + time zone).

> **Caution**
> Set the **Evidence Time Zone** *before* processing. Time zone changes later can affect how timestamps are interpreted in the Timeline and reports.

Contents

Part I

Foundations

About this guide

Purpose: Operational reference for digital forensics workflows—create cases, process evidence, investigate artifacts and timelines, and generate defensible exports.

Audience: Digital forensics examiners and investigators, technical reviewers, and incident response analysts.

How to use this guide:

- Follow **Part I** and **Part II** for first-time setup and your first case.
- Use **Part III** and **Part IV** during investigations, filtering, and reporting.
- When reporting findings, always record:
  - evidence time zone used for display
  - artifact scope selected during processing
  - filters applied during analysis
  - export type and scope (Timeline vs Artifact)

Conventions used in this guide:

- Menu paths are written as **Menu** → **Item**.
- "Scope" means your current selection + active filters that control what you see and what you export.
- "Processing / parsing" refers to the automated stage that extracts artifacts and builds indexed results.

1.1 ArtiFast Suite structure at a glance

ArtiFast Suite is organized into four operational zones. Thinking in these zones makes the rest of the guide easier to follow:

1. **Welcome Page (before processing):** licensing, environment defaults, and entry points to start work.
2. **Case setup (wizard or Quick Run):** choose evidence, time zone, and processing scope (options + artifacts).
3. **Processing (parsing stage):** ArtiFast Suite reads evidence, parses selected artifacts, and prepares searchable results.
4. **Workspace + Reporting (after processing):** review artifacts/timeline/files, apply filters, then export defensible outputs.

Why this matters: what you select during case setup (time zone, artifacts, options) directly affects what you can see, filter, and export later.

1.2 "Scope" means what you will export

In ArtiFast Suite, *scope* is not one thing—it is the combination of:

- the evidence source(s) you loaded
- the artifact scope you processed

- your current workspace mode (Artifacts / Files / File Categories / Incident Response)
- the selected hierarchy node
- active filters (Quick Search, Timeline Filtering Panel, or DQL)

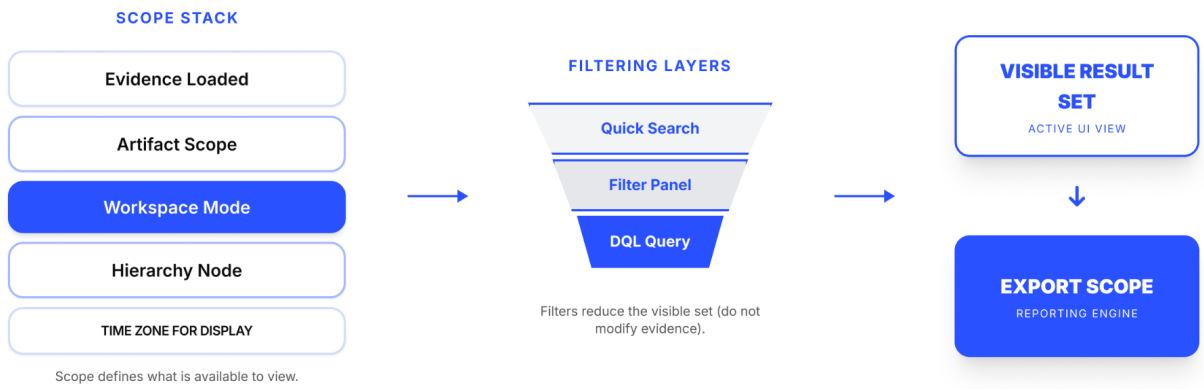

Figure 1.1: ArtiFast Suite scope and filtering model (visible results and export scope).

If your scope changed during analysis, record it. Scope is what makes results repeatable.

Evidence handling and forensic integrity

This section is tool-agnostic and exists to prevent common operational mistakes.

2.1 Work from forensic copies

Recommendation: Process forensic images or verified copies whenever possible. Avoid working on original media unless your lab policy explicitly allows it.

2.2 Keep a clear chain-of-custody

Maintain:

- evidence source identifiers (serials, image names, paths)
- acquisition method (how the image was created)
- hash values (if available)
- who handled evidence and when

2.3 Record investigative scope

ArtiFast Suite supports scoping through:

- evidence selection (what you loaded)
- artifact selection (what you parsed)
- analysis-time filters (what you viewed and exported)

> **Note**
> If you filtered to find evidence, include the filter logic and time zone in your reporting notes.

2.4 Hashing as integrity support

If enabled during case setup, hashing helps validate evidence integrity and supports correlation with external tools and hash sets. Hashing increases processing time.

Part II

Setup and First Launch

Install and Launch ArtiFast Suite

3.1 System Requirements

Category	Minimum	Recommended	Notes
Operating system	64-bit Windows, macOS, or Linux	Latest stable release	Packaging and support can vary by deployment.
Memory (RAM)	4 GB	16 GB+	Large evidence sets scale memory usage.
Storage (free space)	Enough for Case + Temp + Exports	SSD + high free space	Temp data and detailed exports can grow quickly.
Permissions	User-level access	Admin when required	Installation and some system paths may require admin rights.

> **Note**
> Storage speed and free space strongly affect performance and stability on large evidence.

3.2 Installation

Windows:

1. Run the installer.
2. Follow the setup wizard.
3. Launch ArtiFast Suite.

macOS/Linux:

- Some deployments ship a packaged application.
- Some deployments ship a Java archive (JAR).

If you received a JAR distribution, launch it using your organization's provided command (commonly `java -jar <jarfile>.jar`). If your deployment provides a "UI" flag, append it as instructed by your build/package notes.

ArtiFast Suite Licensing

Licensing is managed from the top menu bar → **License**.

4.1 Open License Information

Path	License → License Information
Output	Opens license status, activation state, expiration, and licensee identity.

4.2 What License Information shows

Field	Meaning
License identifier/value	The license key or internal identifier used to validate the installation.
License Status	Whether the license is valid for use on this machine.
Activation Status	Whether the license is activated and ready for use.
Expiration Date	The date after which the license is no longer valid (if applicable).
Licensee identity	The registered Name, E-mail, and Company tied to the license.

4.3 Update License

Path: License → Update License Use this to apply a new license key or renew/replace a license.

4.4 Deactivate License: Transfer

Deactivation releases the license from the current machine so it can be used elsewhere.
Do this before:

- uninstalling
- formatting the workstation
- moving to a new device

4.5 Export Deactivation Request

Use this for offline/support-assisted transfer workflows.

4.6 License actions summary

Action	Path	Use when
Update License	License → Update License	Renewal, replacement, or applying a new license key.
Deactivate License	License → Deactivate	Moving the license to another workstation (transfer).
Export Deactivation Request	License → Export Deactivation Request	Offline or support-assisted transfer workflows.

ArtiFast Suite Welcome Page and Menus

After launch, ArtiFast Suite opens to the **Welcome Page**, which is the control center before processing begins.

5.1 Main menus at a glance

Menu	Purpose
Case	Create, open, run, export, and close cases.
Settings	Language, directories, evidence time zone, and rule managers.
Help	About, features, supported artifacts references, and Log Viewer.
License	License status and license actions.
Feedback	Send feedback to Forensafe (deployment-dependent).

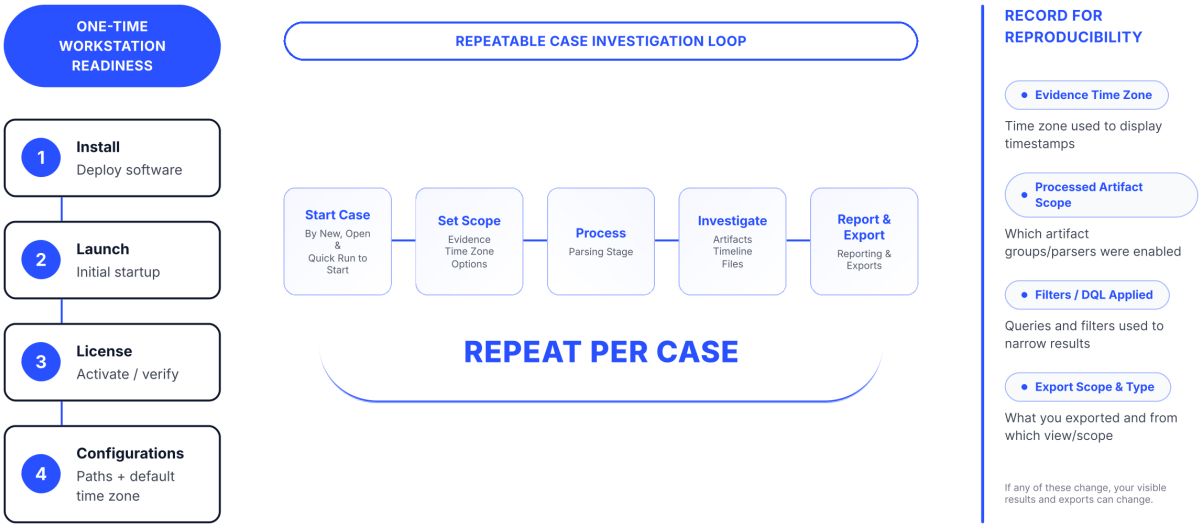

Figure 5.1: ArtiFast Suite operational model (one-time readiness → case loop → outputs).

> **Note**
> This diagram is the mental model for the guide: workstation readiness is completed once, each investigation repeats the case loop, and outputs depend on the current scope (time zone, artifact scope, filters/DQL, and export scope).

5.2 Case Menu

Path	**Case → ...**
Output	Access case lifecycle actions (create, open, triage, export, close).

Figure 5.2: ArtiFast Suite entry paths (New Case, Quick Run, or Open Case).

Item	Shortcut	What it does
New	Ctrl+N	Opens the Create New Case wizard (recommended for full investigations).
Open	Ctrl+O	Opens an existing case from disk.
Open Recent	—	Opens a recently used case.
Quick Run	Ctrl+Q	Starts a fast triage workflow with minimal metadata.
Case Information	Ctrl+I	Shows case metadata and processing statistics (when a case is loaded).
Export Case	Ctrl+E	Creates an exported case package (content depends on the export dialog).
Close	Ctrl+W	Closes the current case.

5.3 Settings Menu

5.3.1 Language

Path: Settings → Language Select the UI language (available options depend on your deployment).

5.3.2 Configurations

Path	Settings → Configurations
Output	Sets default directories and interpretation settings used during case setup and processing.

Configuration	Purpose / Recommendation
Evidence Temp Directory	Processing working directory. Put it on fast storage (SSD) with sufficient free space.
Reports Directory	Default location for exports and reports. Store outputs according to lab policy.
Cases Directory	Default case storage directory. Use backed-up storage if required.
Evidence Time Zone	Determines how timestamps are displayed in Artifact View, Timeline View, and exports. Record it in reports.
Hashsets Directory	Location of hash sets (white/black lists) used for correlation (when enabled).

> **Note**
> Cases and Temp should be on fast storage with sufficient free space. Evidence Time Zone is a forensic interpretation choice—document it in reports.

5.4 Rule Managers: YARA and Sigma

Some deployments include rule managers to maintain rule libraries used during processing and Incident Response analysis.

Capability (when available)	What it enables
Create / edit / delete rules	Maintain organization-specific detection rules.
Activate all / deactivate all rules	Quickly enable or disable entire libraries.
Import / export rules	Move rule sets between environments or analysts.
Download rules from GitHub	Pull rule sets from a repository (optionally using branch/tag/subfolder).
Enable/disable scanning toggles	Controls whether YARA/Sigma scanning runs during processing.

> **Note**
> Large rule sets increase processing time and resource usage. Treat rule hits as investigative leads—validate against source context before reporting conclusions.

5.5 Help menu and Log Viewer

Item	Shortcut	Purpose
About	F1	Shows product version/build information.
Features	F2	Summary of major capabilities (deployment-dependent).
Supported Artifacts	F3	Lists structured artifacts supported in your deployment.
Supported File Artifacts	F4	Lists supported file types and file artifact handling.
Log Viewer	F5	Troubleshooting and processing progress logs.

Use Log Viewer to confirm processing progress, rule loading, and to troubleshoot errors.

5.6 Feedback

Path: Feedback Behavior depends on deployment configuration. Use it to report issues and suggestions to the Forensafe team.

Part III

Case Workflow

Create a Case in ArtiFast Suite

Path	Case → New
Shortcut	Ctrl+N
Output	Creates a case with defined evidence, processing options, artifact scope, and defensible exports.

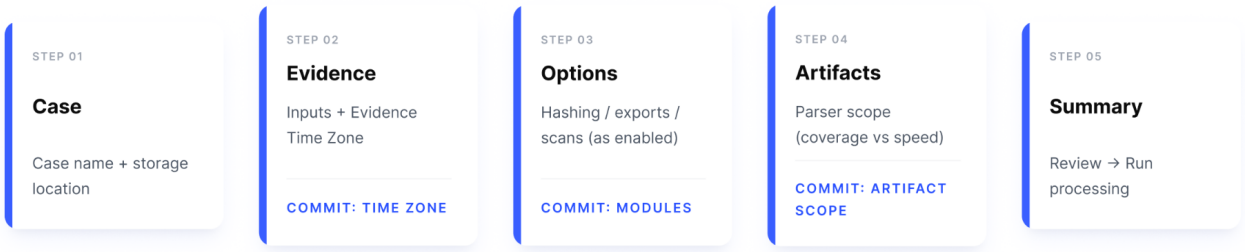

Figure 6.1: ArtiFast Suite Create New Case wizard (commit points).

This wizard defines what ArtiFast Suite will process and how results will be interpreted. It is a five-step workflow:

Step	Outcome
Step 1 – Case	Capture case identity, storage locations, and examiner metadata.
Step 2 – Evidence	Select evidence inputs and set the evidence time zone for timestamp interpretation.
Step 3 – Options	Choose processing depth (hashing, exports, scans) and output behaviors.
Step 4 – Artifacts	Select which artifact parsers will run (coverage vs speed).
Step 5 – Summary	Review scope and start processing.

6.1 Step 1 – Case: Identity and Storage

Goal: Define where the case is stored and capture case metadata.
Typical fields:

Field	Meaning / recommended practice
Case Directory	Where the case is stored. Use fast storage with sufficient free space.
Case Name	Human-readable case label used in the workspace and reporting.
Case Number (optional)	Traceability identifier (use lab standard if required).
Case Description (optional)	Short narrative used for internal documentation.
Examiner (optional)	Investigator name/ID for accountability and handoff.
Temp Directory	Working folder used during processing; place on SSD when possible.
Notes (optional)	Free-form notes captured at case creation.

> **Note**
> - Store Case Directory and Temp Directory on fast storage with sufficient free space.
> - Use Case Number and Examiner consistently if your lab requires traceability.

6.2 Step 2 – Evidence: Inputs and Time Zone

Goal: Select evidence input and the time zone used to display timestamps.
Common evidence inputs:

Input type	Example	Best for / notes
Image	E01, RAW (DD/IMG)	Preferred for repeatable forensic workflows and integrity handling.
Drive	Physical or logical disk access	Live acquisition scenarios (policy-dependent). Ensure you have the required permissions.
Folder	Collected evidence folder	Targeted collections and triage. Record provenance and acquisition context.
Memory dump	.raw / .mem	Volatile artifacts and live response workflows (tool dependent).
Mobile extraction	Vendor export/container formats	Mobile datasets when supported by your environment and parsers.

Common supported image/container types (typical):

Type	Typical extensions	Notes
Raw images	.dd, .raw, .001, .img, .bin	Common forensic formats; multi-segment support is deployment-dependent.
E01 images	.e01	Widely used forensic container format.
L01 images	.l01	Logical image/container (deployment-dependent).
Archive containers	.zip, .tar, .tgz, .7z	Support and password handling depend on build and configuration.
Virtual disks	.vmdk, .vhd, .vhdx	Support is deployment-dependent; validate mounts and access.

Evidence fields (typical):

Field	Meaning
Evidence Path	The selected evidence item (file, device, or folder) to be processed.
Name	Investigator label used in reporting and scope notes.
Time Zone	Timestamp display/normalization used in Artifact View, Timeline View, and exports.
Description / Notes (optional)	Optional context (acquisition notes, handling notes, or hypotheses).

> **Note**
> Evidence Time Zone affects how timestamps are shown in Artifact View, Timeline View, and exports. Set it before processing, and record the selected time zone in your report notes (especially if results appear shifted).

6.3 Step 3 – Options: Processing Depth and Outputs

Goal: Choose processing behaviors that affect depth, speed, and outputs.

These options do not change the evidence itself; they change how deeply ArtiFast Suite processes, correlates, flags, and exports what it finds. For defensible work, record any options that materially affect calculations, rule hits, or generated output sets.

Common options may include:

Option	What it does	Tradeoff	Outputs
Hash calculation	Computes hashes (e.g., MD5/SHA) for integrity and correlation.	Slower processing	Hash values in results/exports.
Hash set usage	Uses allow/deny hash lists to flag known-good or known-bad items.	Requires curated sets	Flagged hits and correlation context.
Encrypted-file detection	Detects likely encrypted files (entropy-based, when available).	Extra compute	Encrypted candidates list/flags.
Export files by extension	Creates file outputs for selected extensions during/after processing.	Disk usage grows	Exported files directory.
Incident Response scanning	Runs YARA/Sigma scans when enabled in your environment.	Compute-heavy	Rule hits, match lists, optional hash lists.

Note

- More options increase processing time and disk usage.
- If you export files, treat outputs as case artifacts and track them in your notes.

6.4 Step 4 – Artifacts: Parser Scope

Goal: Select which artifact parsers run.

Common selection methods:

Approach	When to use	Risk / recommendation
Parse all artifacts	Unknown scope or broad investigations	Highest coverage but slower. Use when you cannot narrow upfront.
Search artifacts by name	You know what you need	Fast targeting, but can miss related artifacts. Record your selection logic.
Filter by category	You have a domain focus (e.g., browser, system)	Balanced approach. Ensure categories cover your hypothesis.
Select by platform grouping	Platform-specific cases	Reduces noise. Verify platform filters before reporting.

If you are prompted for passwords (deployment-dependent): Some workflows may request passwords for encrypted containers or application datasets. Provide them to enable decryption for supported sources.

> **Caution**
> Artifact selection directly determines what you can find later. If something is missing, confirm it was included in the selected artifact scope.

6.5 Step 5 – Summary: Review and Run

Goal: Confirm scope and start processing.

Before you run:

- Verify evidence path and time zone.
- Verify options that affect performance (hashing, exports, rule scanning).
- Verify artifact selection.

Click **Run** to begin processing.

Quick Run: Fast Triage

Path	Case → Quick Run
Shortcut	Ctrl+Q
Use when	Fast triage when you do not need full case metadata and repeatable reporting.

Quick Run is designed for temporary triage workflows. Use Case → New for investigations that require preservation, repeatability, and reporting.

Typical behavior:

- You select evidence and artifact scope.
- You run processing.
- Results are treated as temporary unless you explicitly save/export per your workflow.

Quick Run vs New Case

Aspect	Quick Run	New Case wizard
Goal	Fast triage	Defensible investigation workflow
Metadata	Minimal	Full case fields (directory, examiner, notes)
Repeatability	Lower unless saved/exported	Higher (case structure is explicit)
Recommendation	Use for early signal-finding	Use for reporting and handoff

Caution

Use a standard case (Case → New) for investigations where preservation, repeatability, and reporting are required.

Open and manage cases

Use the Case menu to open, inspect, export, and close cases.

Note: Export Case creates a portable case package for transfer/handoff; Reporting and Exports outputs investigation results based on your current scope and filters.

Action	Path	Shortcut	Result
Open a case	Case → Open	Ctrl+O	Loads an existing case from disk.
Open Recent	Case → Open Recent	—	Opens a recently used case.
Case Information	Case → Case Information	Ctrl+I	Shows case metadata and processing statistics.
Export Case	Case → Export Case	Ctrl+E	Generates an exported case package (content depends on the export dialog).
Close	Case → Close	Ctrl+W	Closes the current case.

Note

Treat exported cases as controlled outputs and store them according to lab policy. Distinguish clearly between:

- **Export Case**: handoff or archive of the case package itself
- **Reporting and Exports**: scoped investigative outputs based on what you filtered and reviewed

Part IV

Processing and Analysis

ArtiFast Suite Processing: Parsing Stage

Processing is the stage where ArtiFast Suite reads evidence and produces the structured results you later review in the workspace.

9.1 What Happens During Processing

Depending on the evidence type and the options you enabled, processing commonly includes:

- evidence intake and validation (opening containers / reading file systems)
- file discovery and targeted extraction for selected artifacts
- artifact parsing (turning raw sources into structured records)
- normalization (standardizing timestamps/fields so results are consistent across sources)
- optional integrity and analysis tasks (hashing, encrypted-file detection, file export, rule scanning)
- building searchable storage (database tables and indexes used by the workspace)

9.2 Processing Pipeline Stages

The UI may show task timings while processing. The exact task labels can vary by build or evidence type, but the underlying pipeline is consistent. In this guide, we describe the pipeline using the following stable stage names:

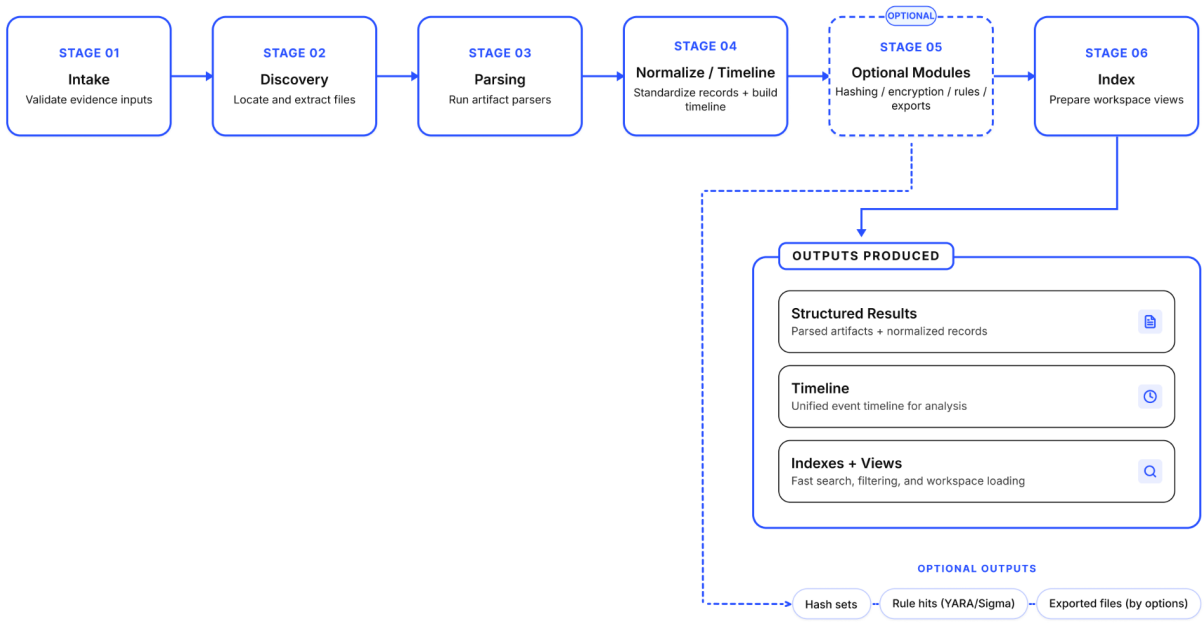

Figure 9.1: ArtiFast Suite processing pipeline (stages and outputs).

1. **Intake & Validation** Open the evidence source, verify it is readable, and prepare the case storage structure.

2. **File Discovery & Collection** Enumerate relevant file paths and collect sources required by the selected artifact scope.

3. **Artifact Parsing** Run parsers for the selected artifacts (for example: browser, registry, event logs, application databases).

4. **Normalization & Timeline Build** Standardize field names and timestamp interpretation so results can be compared and sorted reliably.

5. **Optional Integrity & Threat Scans (if enabled)**
   - Hash calculation (integrity/correlation)
   - Encrypted-file detection (entropy-based, when enabled)
   - YARA/Sigma scanning (incident response leads)
   - Export-by-extension (case outputs)
6. **Indexing & Workspace Preparation** Write final tables/indexes and prepare the case for fast searching and filtering in the workspace.

9.3 Performance and Stability

For faster, more stable processing:

- Keep **Temp Directory** on fast local storage with enough free space (processing can generate large temp data).
- Avoid exporting all file types unless it is explicitly required for your workflow.
- For targeted investigations, reduce artifact scope instead of parsing everything.
- Enable large YARA/Sigma rule sets only when needed (rule scanning is compute-heavy).

Use **Help** → **Log Viewer** to confirm progress, warnings, and any errors that affect completeness.

ArtiFast Suite Workspace Basics

After processing completes, ArtiFast Suite opens the workspace.

Primary tabs	Artifacts, Timeline, and Reporting (plus other views depending on mode and deployment).
Investigation method	Select a scope on the left, review structured results in the center, and validate full details on the right.
Reporting impact	Whatever is visible after scope + filters is the basis for what you can export and explain.

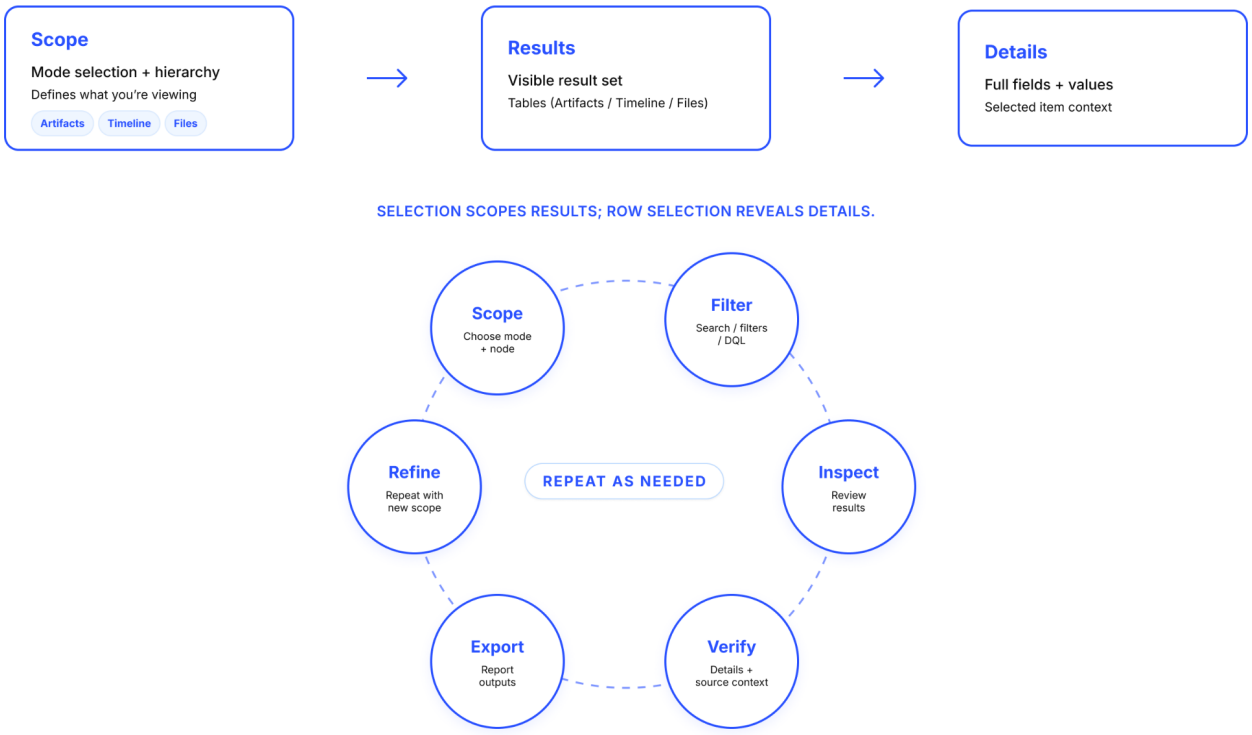

Figure 10.1: ArtiFast Suite workspace method (layout and investigation loop).

10.1 Workspace Layout

- Left: mode selection and hierarchy scoping
- Center: tabbed views (Artifact View / Timeline View / Reporting; and additional tabs depending on mode)
- Right: details panels for selected entries (fields + full values)

10.2 Workspace modes

- Artifacts
- Files
- File Categories
- Incident Response

10.3 Selection Model

Across the workspace:

- selecting a group/node scopes results
- selecting a row shows details on the right
- filters change visibility (not evidence)

Artifacts Mode: Artifact-Centric Analysis

Path: Left sidebar → Artifacts

11.1 Scope using the hierarchy tree

Goal: Narrow results by category and artifact grouping. **Outcome:** Selecting a node scopes the center results table.

11.2 Platform Scoping

Some deployments display platform filter icons (Windows/macOS/Linux/Android/iOS). Use them as analysis-time scoping filters and record them when exporting.

11.3 Artifact View

Path: Center pane → Artifact View

Steps:

1. Select a node in the hierarchy tree.
2. Review the results table.
3. Click a row to open details on the right.
4. Adjust visible columns (when available) to expose bookmarks, notes, and additional fields.

What to check on the right:

- context/breadcrumb (what group you are in)
- Artifact Fields (field list)
- Field Contents (full value display)

11.4 Timeline View

Path: Center pane → Timeline View

Use when: You want a time-ordered reconstruction across scoped results.

Outcome: Selecting an entry shows detailed fields on the right (same selection model as Artifact View).

11.5 Context Actions

Right-click inside result tables to access actions (availability depends on mode and context), such as:

- coloring entries / clearing colors / loading and saving coloring profiles
- time-window filters (same minute/hour/day/week/month/year)
- bookmark-only filtering
- hiding entries without timestamps (“timeless”)
- showing items related to deleted files
- extracting source / viewing source location

> **Note**
> These actions change visibility or generate outputs. Record them when they define your reported scope.

11.6 Multiple Workspaces

Some deployments allow creating additional workspaces from a selection or keyword. Use this to separate investigation tracks without losing your original view.

Files Mode: File Review and Triage

Path: Left sidebar → Files

12.1 Files View

Use Files mode to:

- browse evidence folder structures
- inspect file metadata
- preview supported file types
- export selected files

12.2 Typical actions

1. Navigate folders to reach the file of interest.
2. Open/preview using available viewers (depends on file type and build).
3. Export selected files when needed.

12.3 Viewing Raw Data

Some builds provide a Hex Viewer for raw inspection of file contents. Use it to confirm signatures, offsets, and raw values when needed.

> **Note**
> Raw viewing supports verification; it does not modify evidence.

12.4 File Categories View

Path: Left sidebar → File Categories

Use File Categories to quickly group and review files by type (documents, media, archives, etc.). Actions are typically similar to Files mode, but grouped by category for faster triage.

Incident Response Mode: YARA/Sigma Triage

Path: Left sidebar → Incident Response
Incident Response is designed for security-focused triage using processed evidence and enabled rule sets.

13.1 Core workflow

1. Select Incident Response mode.
2. Choose a relevant group from the incident response hierarchy (for example, YARA rule matches).
3. Review results in:
   - Artifact View
   - Timeline View
   - Threat Intelligence (when available)
   - Reporting

13.2 Threat Intelligence

Threat Intelligence provides specialized views for rule-related analysis.

13.2.1 YARA View

Common capabilities:

- filter by rule
- review match list and source file context
- preview rule content and source content (deployment-dependent)
- export to CSV/JSON and export MD5 hash lists (deployment-dependent)

13.2.2 Sigma View

Common capabilities:

- filter by rule title and severity/level
- review event-oriented results (timestamp, rule title, event identifiers, etc.)
- inspect event details and rule preview panels (deployment-dependent)

13.2.3 VirusTotal View

Some deployments may show a placeholder or may require additional configuration. Do not assume enrichment is available unless it is enabled and verified in your environment.

> **Caution**
> Treat rule hits as investigative leads. Validate hits against underlying source artifacts before reporting conclusions.

Search and Filtering

Searching and filtering control what you see and what you export.

14.1 Quick Search (Keywords)

Path: Top bar → Quick Search
Use Quick Search to narrow the current scoped result set (current mode + selected hierarchy node + current filters).

14.2 Filters

Path: Top bar → Timeline Filtering Panel
Use this panel to build structured filters such as:

- OS
- Category
- Artifact Name
- Timeline Date
- Fields and Field Values (text/date/number)
- Custom filters (when available)

Some deployments provide filter management actions (for example, Clear current filters or Load filters from a saved file). Use these to support repeatable workflows across analysts/cases.

14.3 DQL / Advanced Search

DQL (Digital Query Language) is used to express advanced filtering logic when your deployment exposes a query input or when filters are shown as a generated expression.

Use DQL for	Operational value
Repeatable, explicit filtering	Easy to copy into notes, reports, and peer review records.
Complex combinations	Supports `AND`/`OR` logic that can be harder to build manually from nested UI filters.
Field-level precision	Useful when you need targeted filtering against specific fields or values.
Common value types	Text, date/time, and numeric fields.
Common operators	`AND`, `OR`, and `IN` (operator support depends on field type/build).
Example	`"Os Name" IN ('Neutral', 'Windows')`

Note

If DQL defines your investigative scope, include the exact expression in your report notes together with the evidence time zone and the active workspace context.

Reporting and Exports

15.1 Reporting Tab

Path	Center pane → Reporting
Output	Generates exports (PDF/CSV/TSV/HTML/JSON) based on the current scope and filters.

Typical workflow:

1. Choose scope (Timeline or Artifact).
2. Choose language and template if applicable.
3. Choose output type.
4. Choose output location.
5. Generate the export.

15.2 Export Types

Standard export formats

Format	Best for	Notes
PDF	Human-readable review and case files	Good for narrative reporting; can be large on big scopes.
Detailed PDF (Entry Per Page)	Deep review and recordkeeping	Output size grows quickly with large datasets.
Detailed PDF with Thumbnails	Multimedia and visual review	Best for targeted scopes; typically larger output.
CSV	Analysis in spreadsheets/tools	Better for large datasets and downstream filtering.
Text (TSV)	Lightweight data exchange	Easy to parse; preserves column structure.
HTML	Browser-based review	Useful for sharing internally; depends on template.
JSON	Automation and scripting	Structured output for pipelines and tooling.

Pre-built summary reports (deployment-dependent)

Report	Typical use
Most Visited Websites	High-level browser activity overview for fast triage.
Browser Favorites	Saved links/bookmarks review.
Installed Applications	Application inventory and presence validation.
Recent Applications	Recently used apps and user activity signals.
Recent Documents	Recently accessed documents (user activity reconstruction).
Facebook Friends	Social connections overview (when supported).
Twitter Followed Users	Account follow relationships overview (when supported).

Note

- Detailed PDF options can create large outputs.
- CSV/TSV/JSON are better for large datasets and scripting.
- Always record your scope (filters + time zone) alongside exports.

Part V

Support and References

Troubleshooting and Support

16.1 Use Log Viewer first

Path: Help → Log Viewer (F5)

When something fails or behaves unexpectedly:

1. Reproduce the issue (if safe to do so).
2. Open Log Viewer and locate the time window of the action.
3. Record the relevant messages and errors.

16.2 Common issues

License problems

- Confirm License Status is valid and Activation Status is completed.
- If transferring to a new machine, deactivate on the old machine when possible.

Slow processing or failures

- Verify free disk space for Case + Temp + Reports locations.
- Move Temp/Case directories to faster storage.
- Reduce artifact scope for targeted runs.
- Disable heavy outputs (export-by-extension, large rule sets) unless required.

Timestamp confusion

- Confirm the Evidence Time Zone used for the evidence.
- If results look shifted, re-check the case evidence time zone and document it in reports.

Rule scanning issues (YARA/Sigma)

- Confirm the rule sets are enabled in rule managers.
- Use Log Viewer to confirm rule loading and progress messages.

Missing expected results

- Confirm the artifact was included in the selected artifact scope.
- Clear filters to confirm whether results are hidden by scoping.

16.3 Support Escalation and Close-Out

16.3.1 What to include

When escalating an issue, include:

- ArtiFast Suite version/build (Help → About)
- a short description of the action that failed and exact wording of any error
- relevant Log Viewer lines covering the time window of the issue

- whether YARA/Sigma or other heavy options were enabled
- the type of evidence source (image/drive/folder/memory/mobile) and approximate size

If your deployment provides a Feedback workflow, you can submit the same information through **Feedback**.

16.3.2 Close-out steps

Before you close a case or hand it off:

- Save the case (and confirm the case directory is on backed-up storage if your lab requires it).
- Record your scope: evidence time zone, processed artifact scope, and any active filters/DQL.
- If you exported results, record: export type, export location, and the exact scope used for the export.
- If rule hits (YARA/Sigma) influenced conclusions, validate them against the underlying source context and capture supporting details.

These steps make ArtiFast Suite results defensible and repeatable when another examiner reviews the same case.

> **Note**
>
> **Minimum handoff record:**
>
> - evidence time zone used for interpretation
> - processed artifact scope and any active filters/DQL
> - export type, location, and the exact scoped output that was generated

If you need further assistance, contact Forensafe Support through the channel provided with your license and include relevant Log Viewer output.

Appendix

A.1 Keyboard shortcuts

Shortcuts can vary by platform/deployment. Common shortcuts:

- Case → New: Ctrl+N
- Case → Open: Ctrl+O
- Case → Quick Run: Ctrl+Q
- Case → Case Information: Ctrl+I
- Case → Export Case: Ctrl+E
- Case → Close: Ctrl+W
- Help → About: F1
- Help → Features: F2
- Help → Supported Artifacts: F3
- Help → Supported File Artifacts: F4
- Help → Log Viewer: F5

A.2 Supported Artifacts

ArtiFast Suite's supported artifact coverage and file artifact support can be reviewed inside the product.

- **Help** → **Supported Artifacts** provides the artifact list as shipped in your deployment.
- **Help** → **Supported File Artifacts** provides file-type artifact support references.

Use these screens when:

- confirming whether a data type is supported
- documenting tool capability for internal validation
- aligning expectations before running processing