MalChela Documentation

None

None

None

Table of contents

1. Welcome to MalChela

This site hosts the MalChela user guide, tool documentation, and integration instructions.

- Use the tabs above to navigate.
- The full PDF version of the user guide is available here.

2. About

🦀 **MalChela** is a modular toolkit for digital forensic analysts, malware researchers, and threat intelligence teams. It provides both a Command Line Interface (CLI) and a Graphical User Interface (GUI) for running analysis tools in a unified environment.

mal — malware

chela — “crab hand”

A chela on a crab is the scientific term for a claw or pincer. It’s a specialized appendage, typically found on the first pair of legs, used for grasping, defense, and manipulating things; just like these programs.

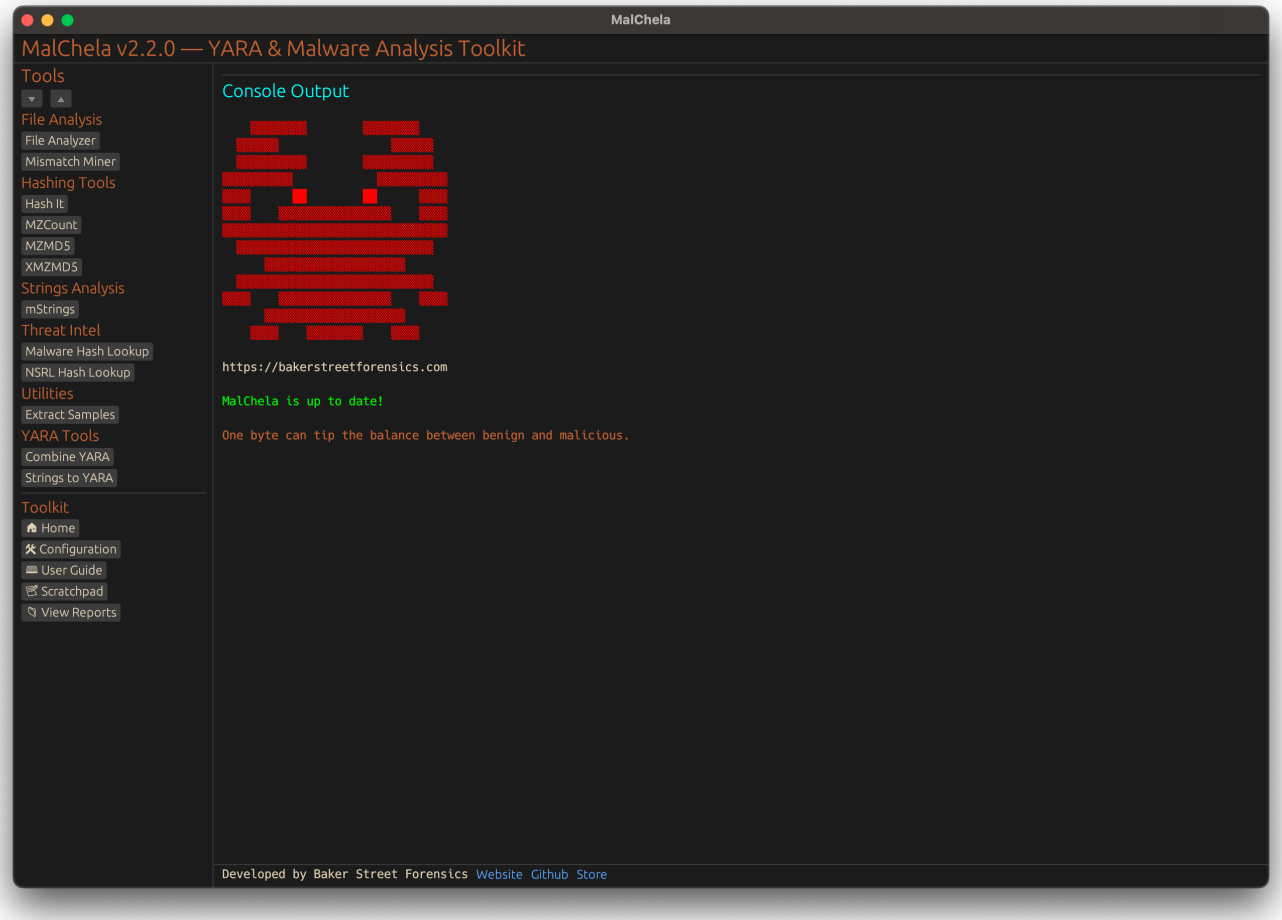

Figure 1: MalChela GUI

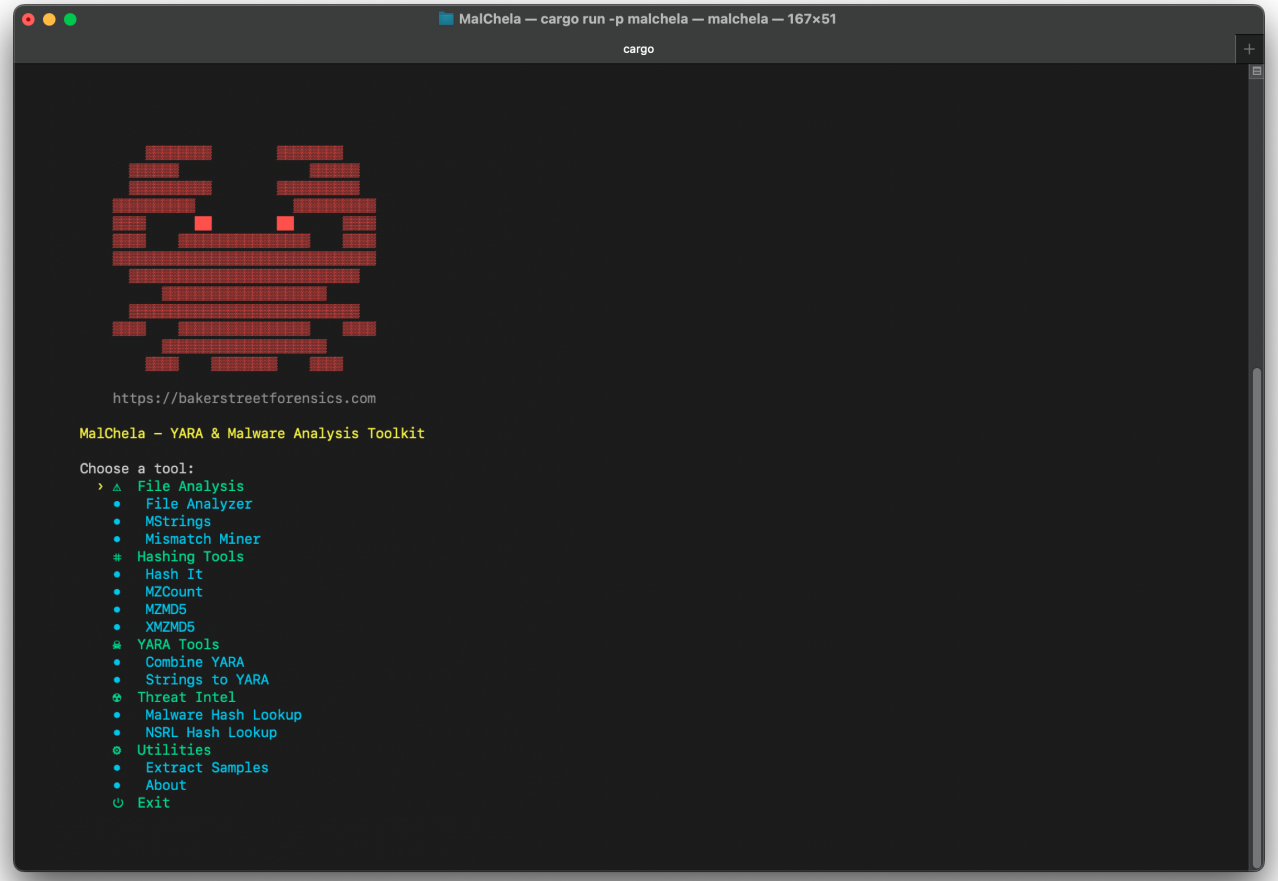

Figure 2: MalChela CLI

3. Installation

3.0.1 Prerequisites

- Rust and Cargo
- Git
- Unix-like environment (Linux, macOS, or Windows with WSL)

3.0.2 System Dependencies (Recommended)

To ensure all tools build and run correctly, install the following packages (especially for Linux/REMnux):

```
sudo apt install openssl libssl-dev clang yara libyara-dev pkg-config build-essential libglib2.0-dev libgtk-3-dev ssdeep
```

These are required for: - YARA and YARA-X support - Building Rust crates that link to native libraries (e.g., GUI dependencies) - TShark integration (via GTK/glib) - `ssdeep` is used for fuzzy hashing in tools like `fileanalyzer`. If not installed, fuzzy hash results may be unavailable.

3.0.3 Clone the Repository

```
git clone https://github.com/dwmetz/MalChela.git

cd MalChela
```

3.0.4 Build Tools

```
cargo build                # Build all tools
cargo build -p fileanalyzer # Build individual tool
```

3.0.5 Windows Notes

- Best experience via WSL2
- GUI is not supported natively on Windows

4. Configuration

4.1 tools.yaml

4.1.1 Tool Configuration

MalChela uses a central `tools.yaml` file to define which tools appear in the GUI, along with their launch method, input types, categories, and optional arguments. This YAML-driven approach allows full control without editing source code.

Key Fields in Each Tool Entry

Field	Purpose
name	Internal and display name of the tool
description	Shown in GUI for clarity
command	How the tool is launched (binary path or interpreter)
exec_type	One of `cargo`, `binary`, or `script`
input_type	One of `file`, `folder`, or `hash`
file_position	Controls argument ordering
optional_args	Additional CLI arguments passed to the tool
category	Grouping used in the GUI left panel

⚠️ All fields except `optional_args` are required.

4.1.2 Swapping Configs: REMnux Mode and Beyond

MalChela supports easy switching between tool configurations via the GUI.

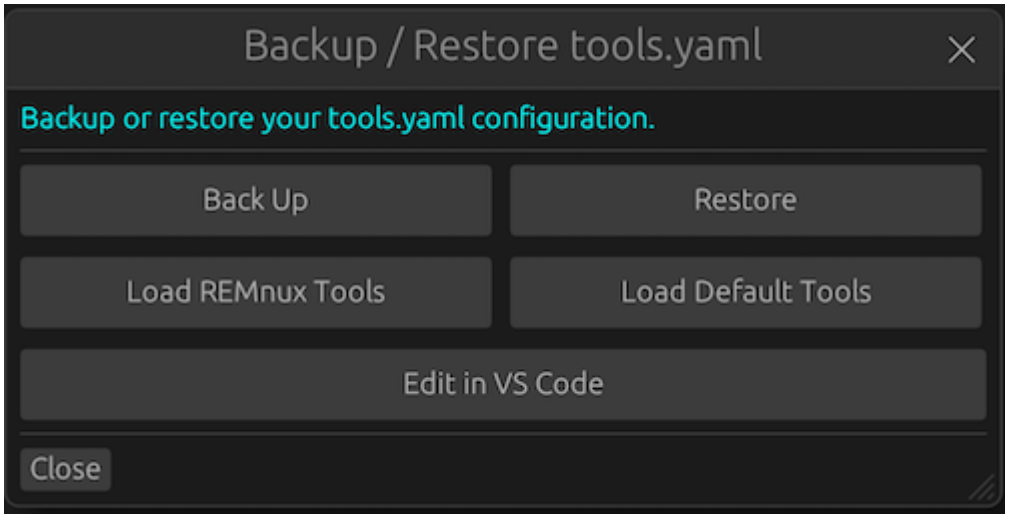

Figure 3: YAML Config Tool – Tool entry shown in table and form

To switch:

- Open the **Configuration Panel**
- Use **“Select tools.yaml”** to point to a different config
- Restart the GUI or reload tools

This allows forensic VMs like REMnux to use a tailored toolset while keeping your default config untouched.

A bundled `tools_remnux.yaml` is included in the repo for convenience.

KEY TIPS

- Always use `file_position: "last"` unless the tool expects input before the script
- For scripts requiring Python, keep the script path in `optional_args[0]`
- For tools installed via `pipx`, reference the binary path directly in `command`

4.1.3 Backing Up and Restoring tool.yaml

The MalChela GUI provides built-in functionality to back up and restore your `tools.yaml` configuration file.

Backup

To create a backup of your current `tools.yaml`:

- Open the **Configuration Panel**
- Click the **“Back Up Config”** button
- A timestamped copy of `tools.yaml` will be saved to the default location

You’ll see a confirmation message when the operation completes successfully.

Restore

To restore from a previous backup:

- Click the **“Restore Config”** button in the Configuration Panel
- Select a previously saved backup file
- The selected file will overwrite the current configuration

This feature makes it easy to experiment with custom tool setups while retaining a safety net for recovery.

4.2 API Configuration

Some tools within MalChela rely on external services. In order to use these integrations, you must configure your API credentials.

4.2.1 Tools That Use API Keys

Tool	Service	Purpose
`malhash`	VirusTotal	Hash lookup and enrichment
`malhash`	MalwareBazaar	Hash lookup and sample classification
`fileanalyzer`	VirusTotal	Hash lookup

4.2.2 Where to Configure

MalChela uses two plain text files to store API keys for its third-party integrations:

```
vt-api.txt
mb-api.txt
```

These files should be placed in the **root of your MalChela workspace**, alongside `tools.yaml`. Each file should contain a single line with your API key.

These keys will be read at runtime by tools such as `malhash` to enable external lookups.

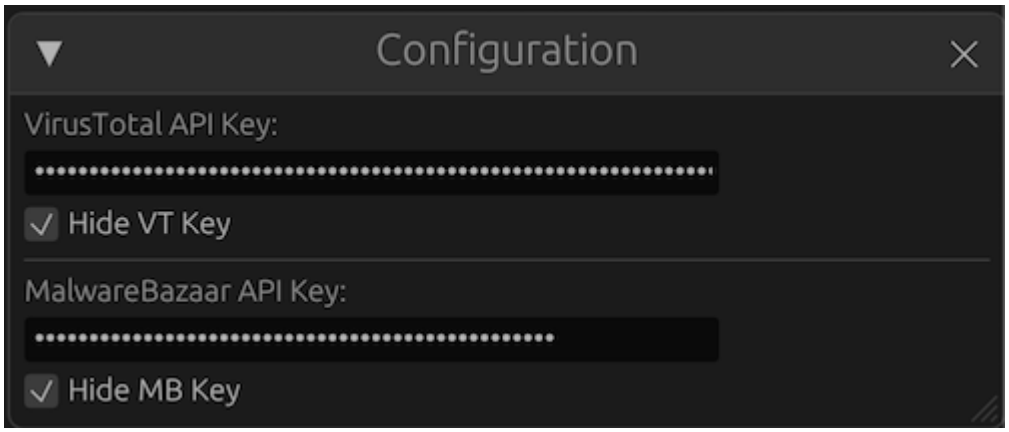

Figure 4: API Configuration Utility

4.2.3 Managing Your Keys with the Configuration Utility

The MalChela GUI includes a built-in Configuration Panel that lets you easily **Create or update API key files** without opening a text editor.

Look for the **API Key Management** section in the Configuration Panel. Changes take effect immediately and persist across sessions.

4.2.4 Best Practices

- **Keep these files private.** Do not commit them to Git or share them publicly.

If a tool requires an API key but none is found, it will log a warning and skip external requests.

5. Core Tools

5.1 Overview

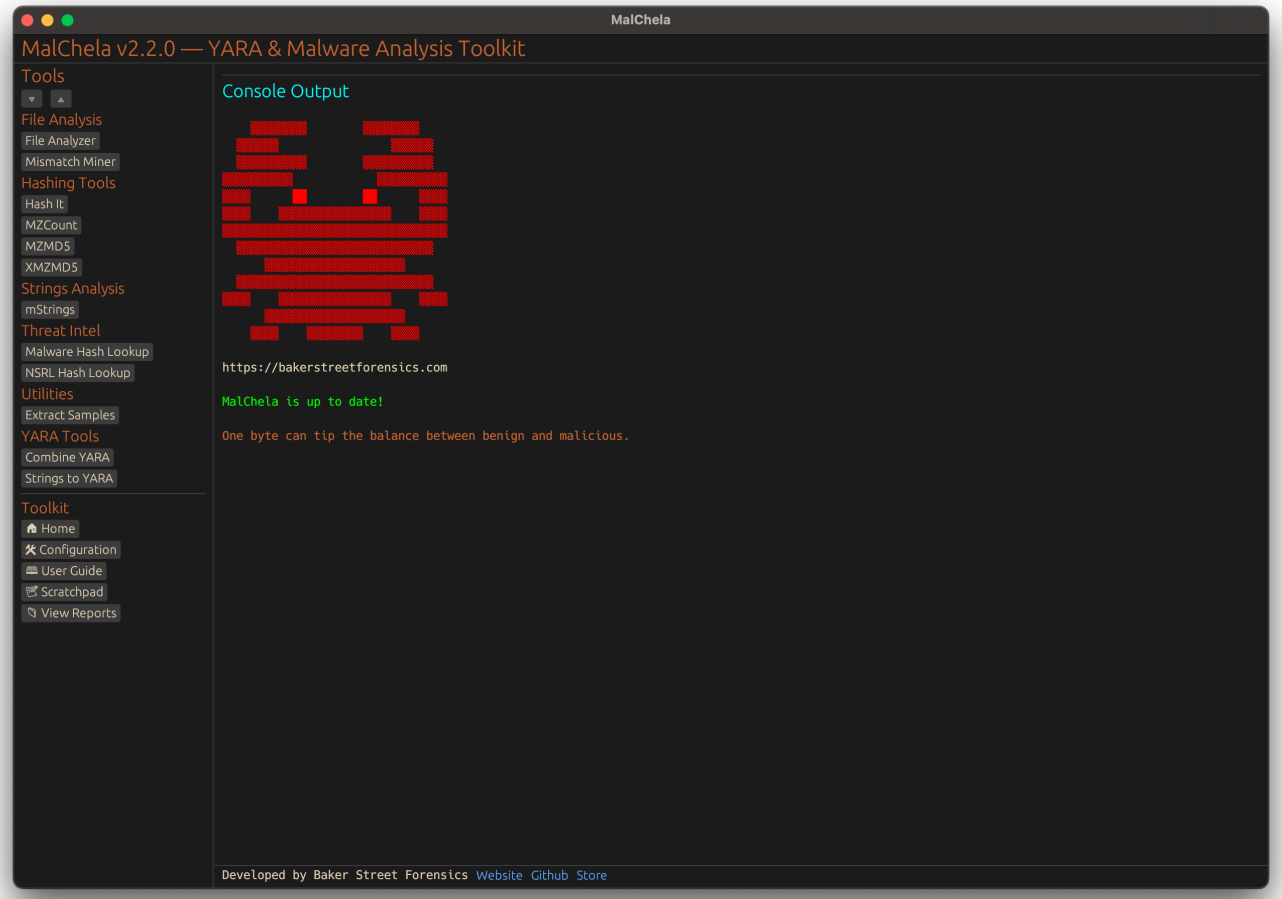

Figure 5: MalChela GUI

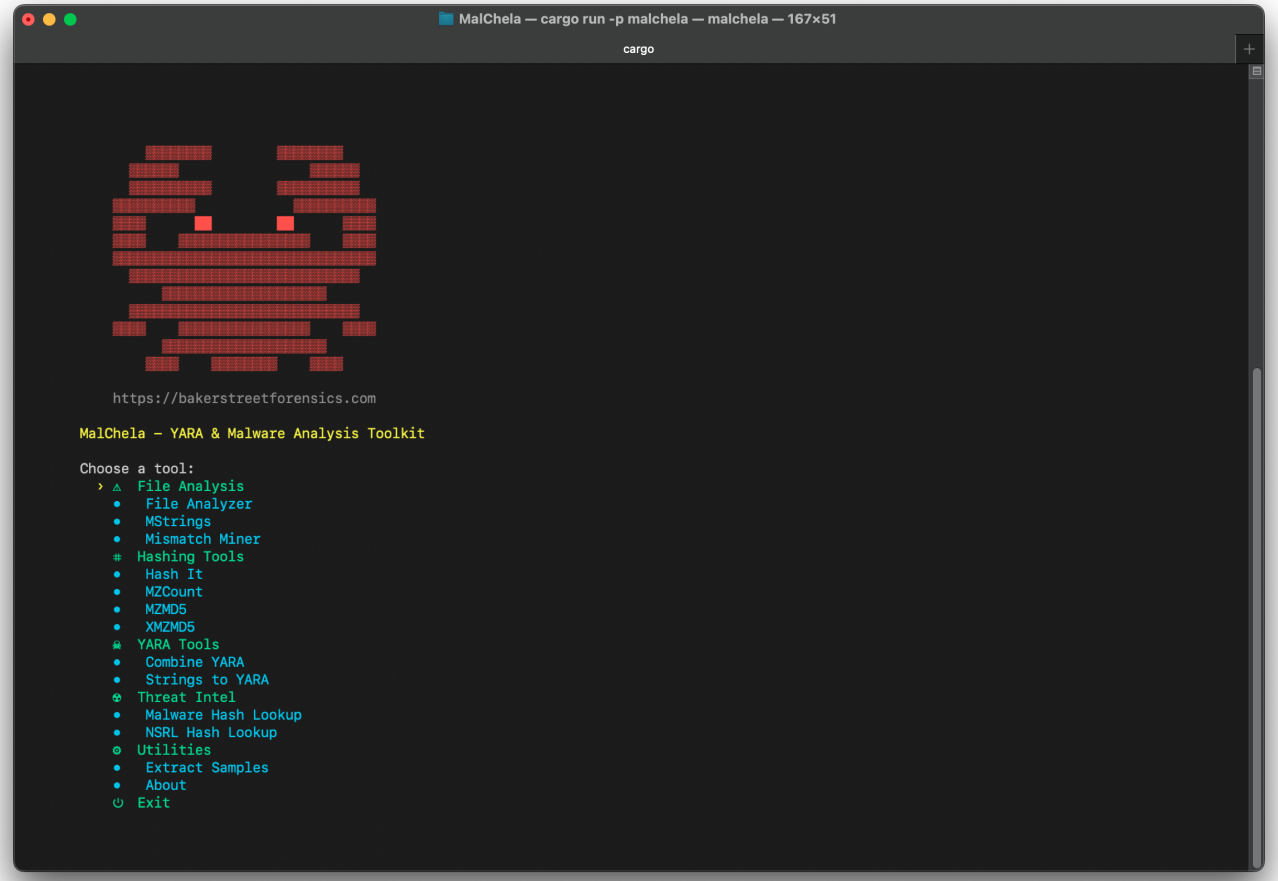

Figure 6: MalChela CLI

5.1.1 MalChela Core Tools

These built-in programs provide fast, flexible functionality for forensics and malware triage.

Program	Function
Combine YARA	Point it at a directory of YARA files and it will output one combined rule
Extract Samples	Point it at a directory of password protected malware files to extract all
File Analyzer	Get the hash, entropy, packing, PE info, YARA and VT match status for a file
Hash It	Point it to a file and get the MD5, SHA1 and SHA256 hash
Mismatch Miner	Hunts for exes disguised as other formats
mStrings	Analyzes files with Sigma rules (YAML), extracts strings, matches ReGex
MZMD5	Recurse a directory, for files with MZ header, create hash list
MZcount	Recurse a directory, uses YARA to count MZ, Zip, PDF, other
NSRL Query	Query a MD5 or SHA1 hash against NSRL
Strings to YARA	Prompts for metadata and strings (text file) to create a YARA rule
Malware Hash Lookup	Query a hash value against VirusTotal & Malware Bazaar*
XMZMD5	Recurse a directory, for files without MZ, Zip or PDF header, create hash list

***The Malware Hash Lookup requires an API key for VirusTotal and Malware Bazaar.** If unidentified, MalChela will prompt you to create them the first time you run the malware lookup function.

5.2 CombineYARA

Combine YARA merges multiple YARA rule files into a single consolidated rule set. It recursively scans a folder for .yar or .yara files and combines them into one output file. Ideal for organizing or deploying rule collections.

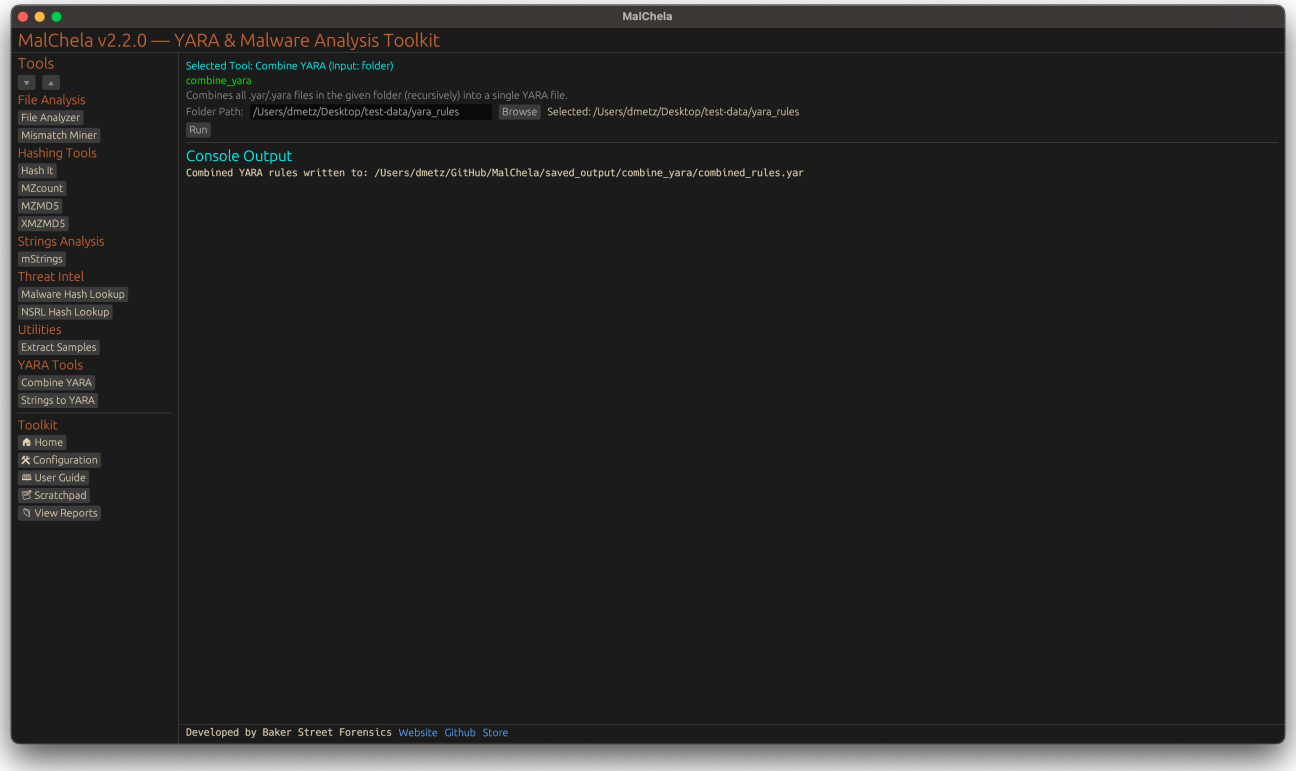

Figure 7: Combine YARA

5.3 ExtractSamples

Extract Samples recursively unpacks password-protected archives commonly used in malware sharing (e.g., .zip, .rar, .7z). It uses default malware research passwords like infected and malware to extract samples in bulk for analysis.

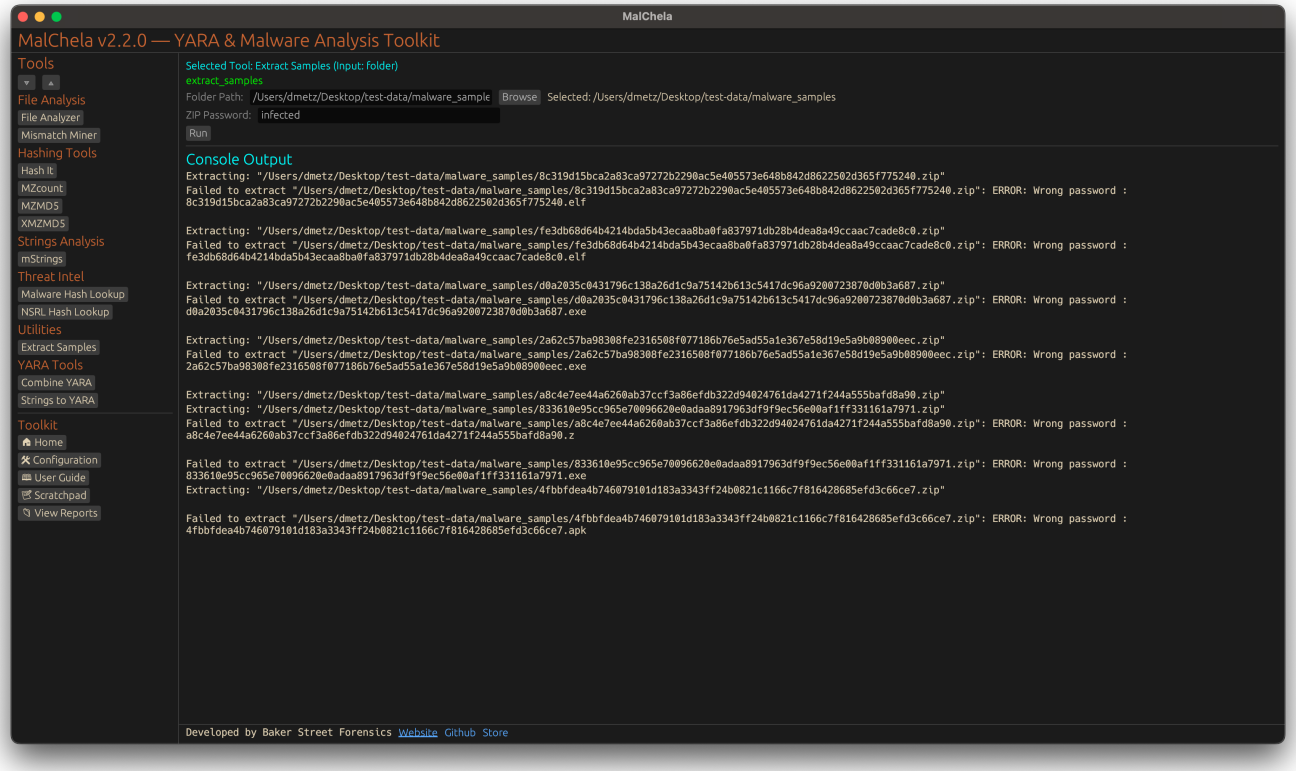

Figure 8: Extract Samples

5.4 FileAnalyzer

FileAnalyzer performs deep static analysis on a single file. It extracts hashes, entropy, file type metadata, YARA rule matches, NSRL validation, and — for PE files — rich header details including import/export tables, compile timestamp, and section flags. Ideal for triaging unknown executables or confirming known file traits.

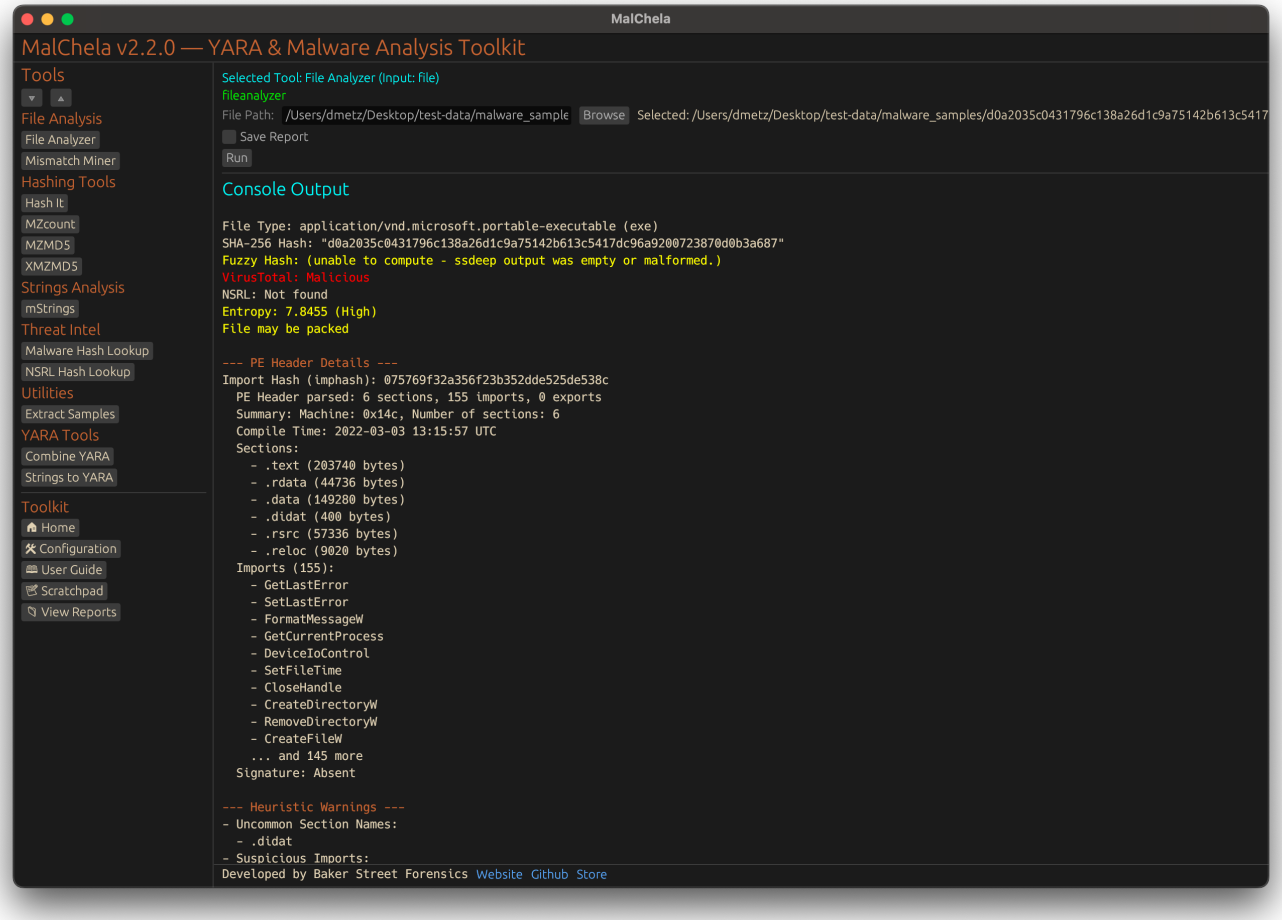

Figure 9: File Analyzer

- YARA rules for `fileanalyzer` are stored in the `yara_rules` folder in the workspace. You can modify or add rules here.

5.5 HashIt

Hash It generates cryptographic hashes (MD5, SHA1, and SHA256) for a given file. It's useful for file integrity checks, hash-based lookups, or comparing suspected duplicates across datasets.

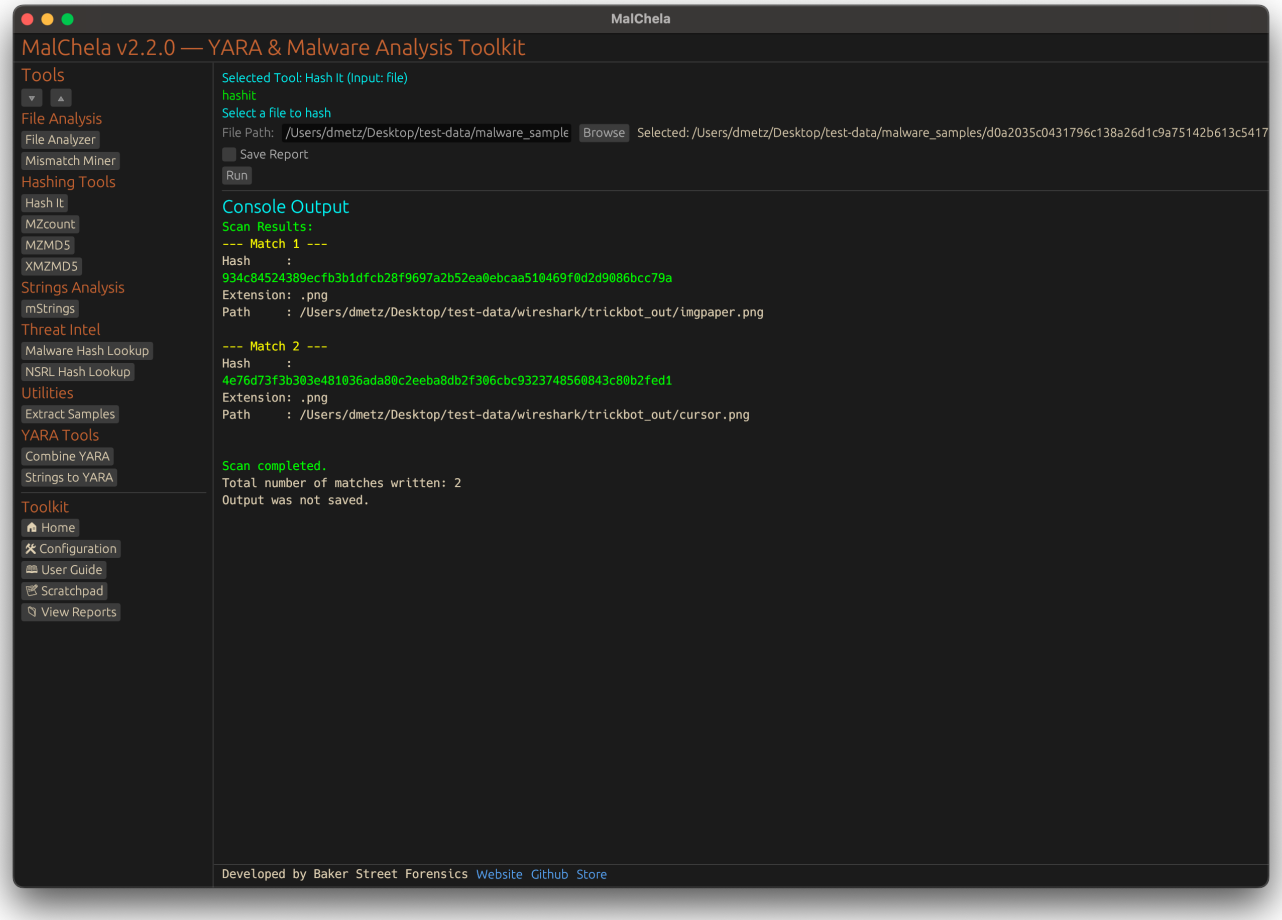

Figure 10: HashIt

5.6 MalHash

MalHash queries malware intelligence sources using a provided hash. It checks VirusTotal and MalwareBazaar for file metadata, threat labels, antivirus detections, and known associations. A quick way to enrich an unknown sample or confirm if a hash is already known and classified in the wild.

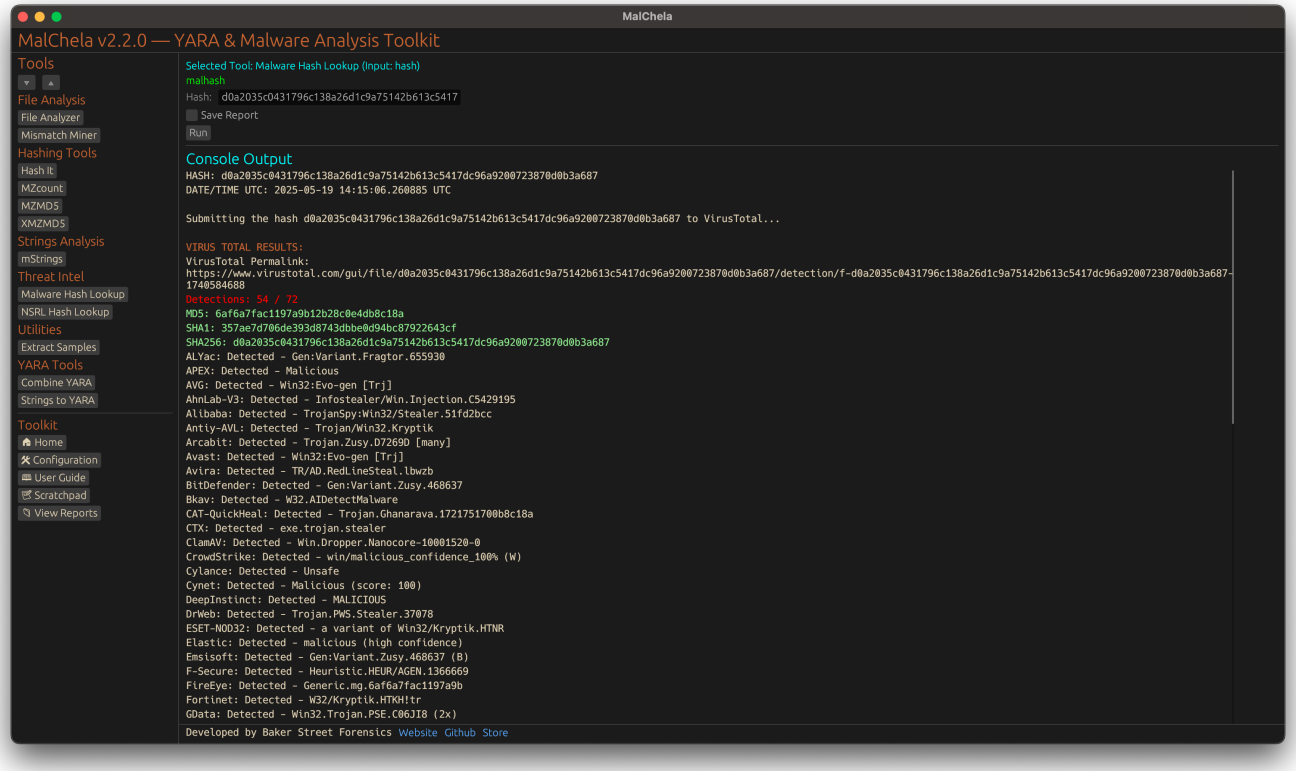

Figure 11: Malware Hash Lookup

The first time you run MalHash, you'll be prompted to configure API keys for VirusTotal and MalwareBazaar if they're not already set.

5.7 MismatchMiner

MismatchMiner scans directories for files whose extension does not match their internal file signature. It flags suspicious files like executables masquerading as documents or images, helping analysts quickly identify potentially malicious or obfuscated payloads.

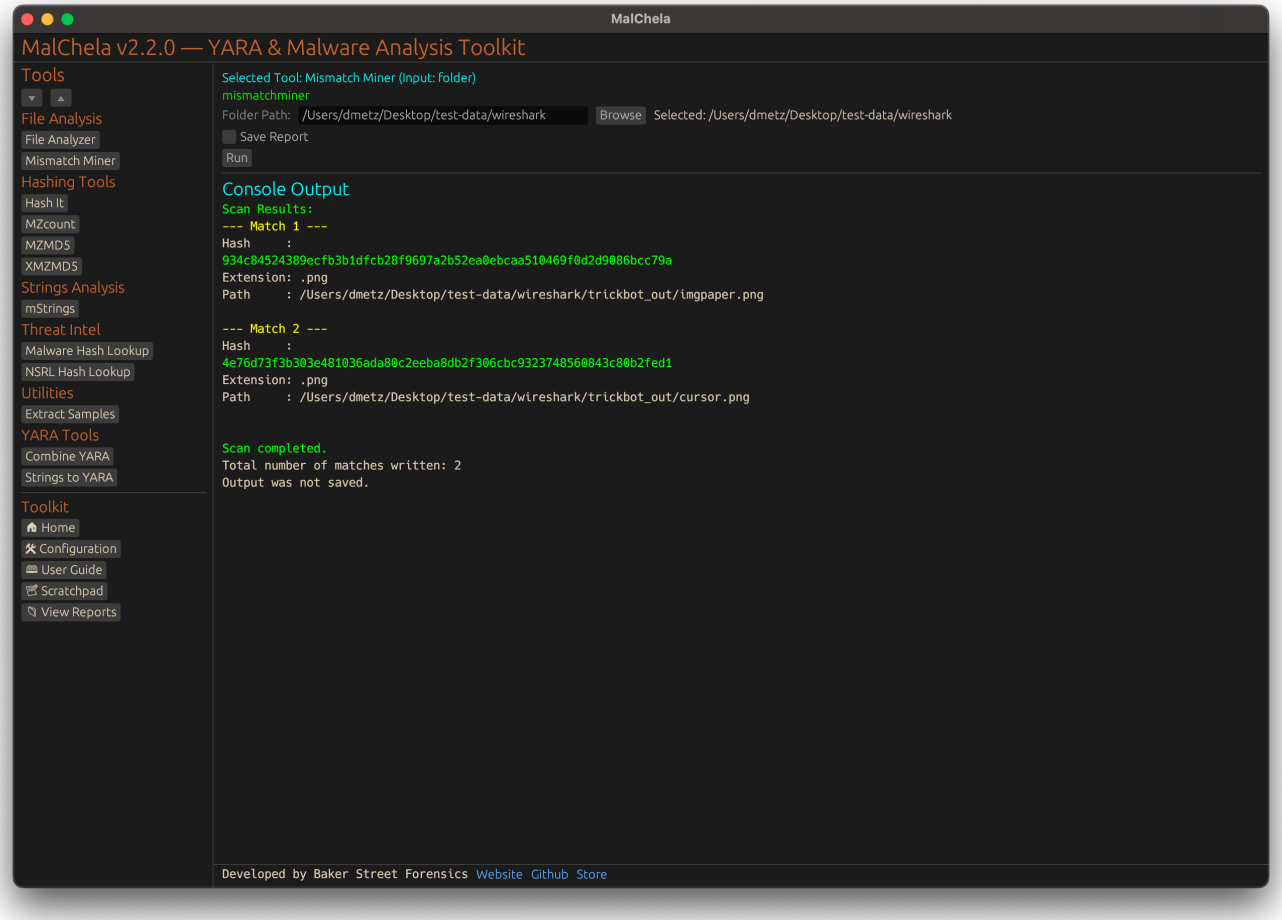

Figure 12: Mismatch Miner

5.8 MStrings

mStrings extracts strings from files and classifies them using regular expressions, YARA rules, and MITRE ATT&CK mappings. It highlights potential indicators of compromise and suspicious behavior, grouping matches by tactic and technique. Ideal for quickly surfacing malicious capabilities in binaries, scripts, and documents.

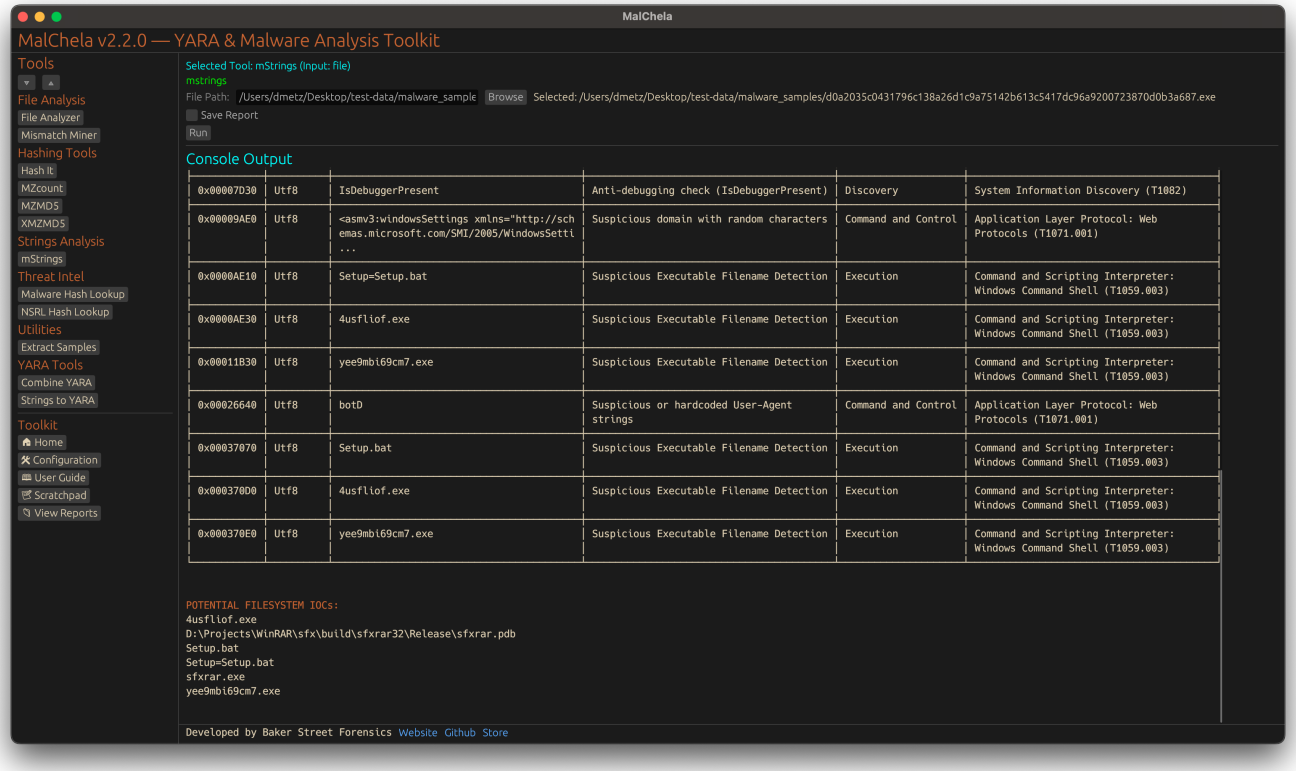

Figure 13: MStrings

5.9 MZCount

MZcount recursively scans a directory and counts the number of files that match key signatures like MZ (Windows executables), ZIP, PDF, and others. It uses lightweight YARA rules to classify files by type, giving a quick overview of the content breakdown within a dataset. Results can be displayed in either a detailed per-file view or a clean summary table, depending on your analysis needs.

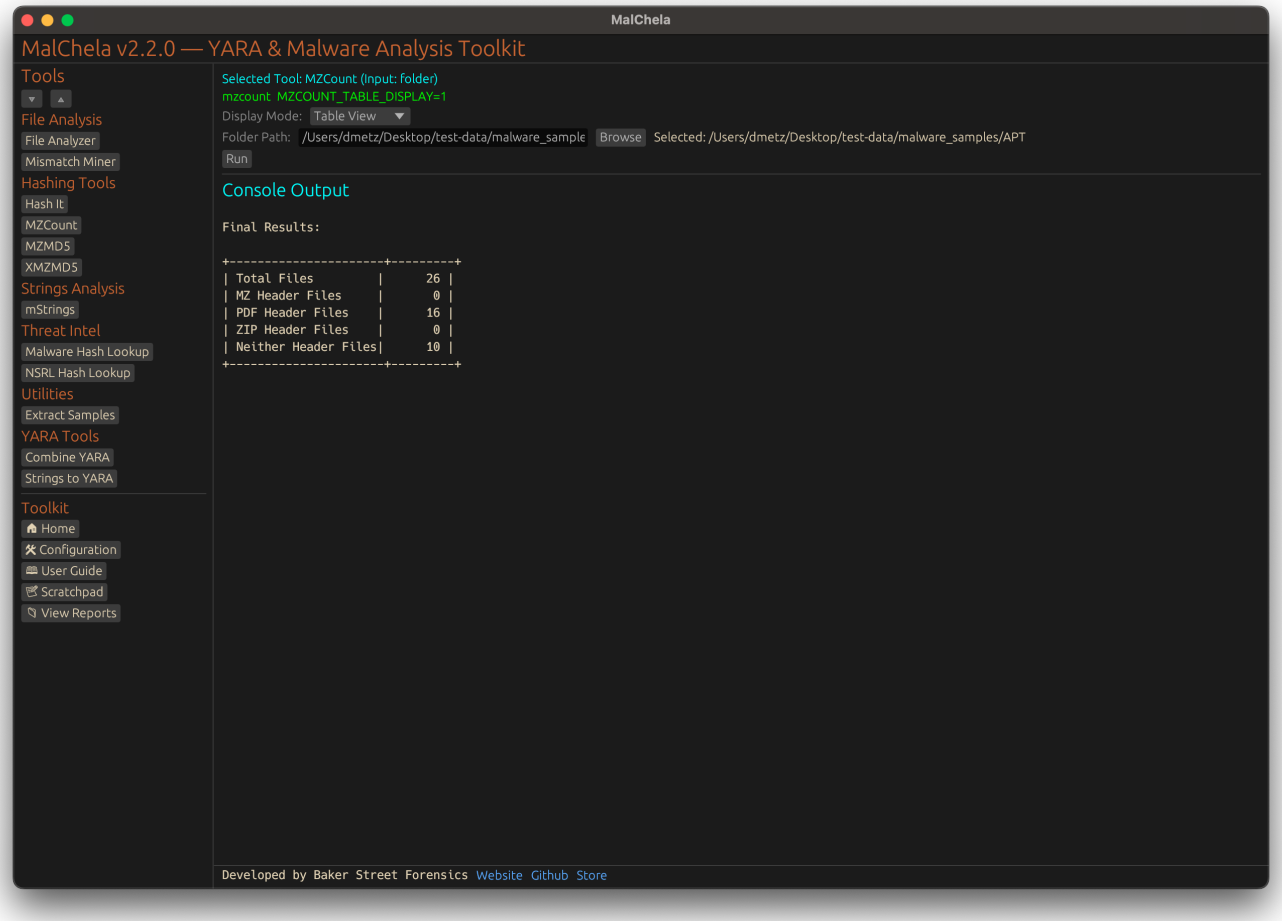

Figure 14: MZCount Table View

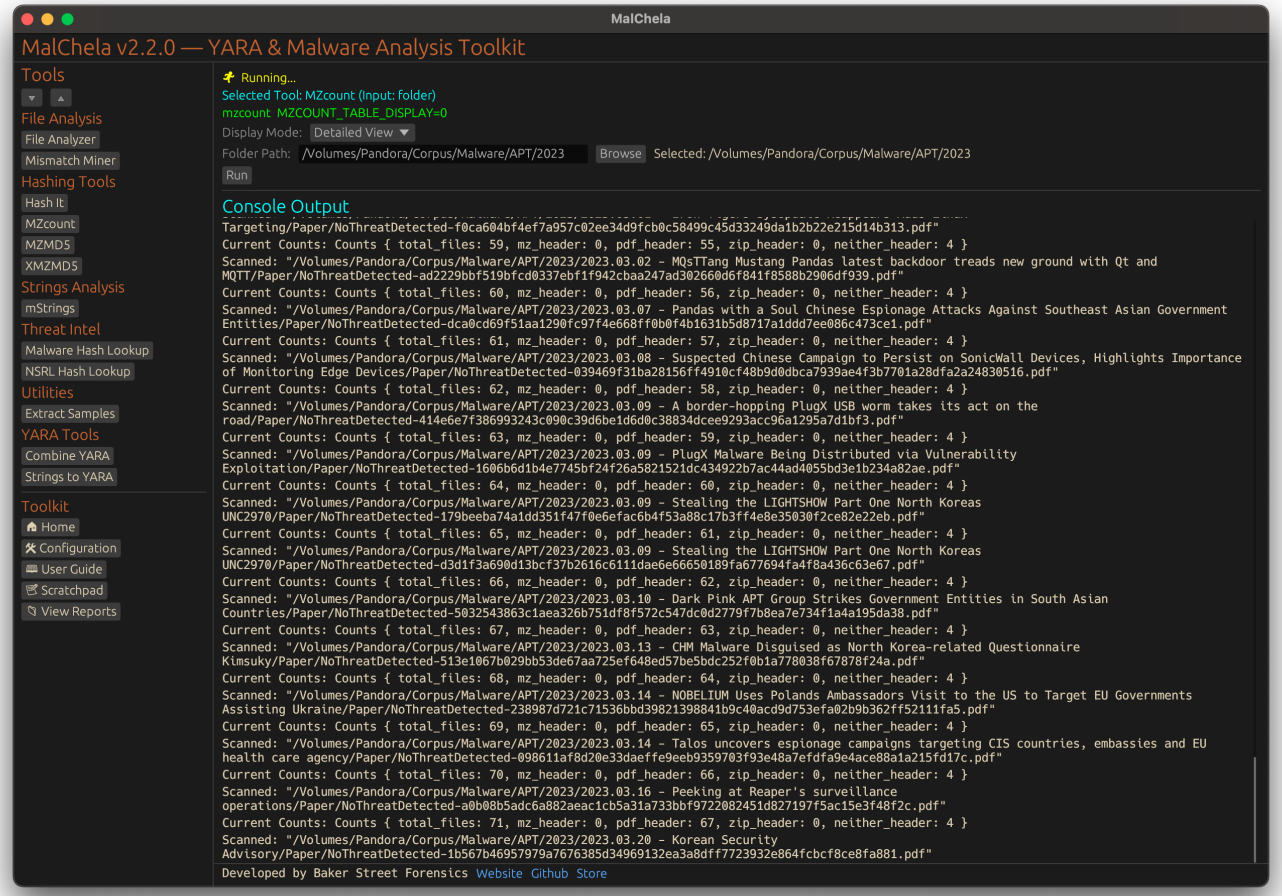

Figure 15: MZCount Detail View

5.10 MZMD5

MZMD5 recursively scans a folder and generates MD5 hashes for all files that start with an MZ header — the standard signature for Windows executables. It's useful for building hash sets of known-good or known-bad PE files during malware analysis or triage.

By default, hashes are saved to the saved_output/mzmd5/mzmd5.txt. If the file exists already you will be prompted to overwrite it.

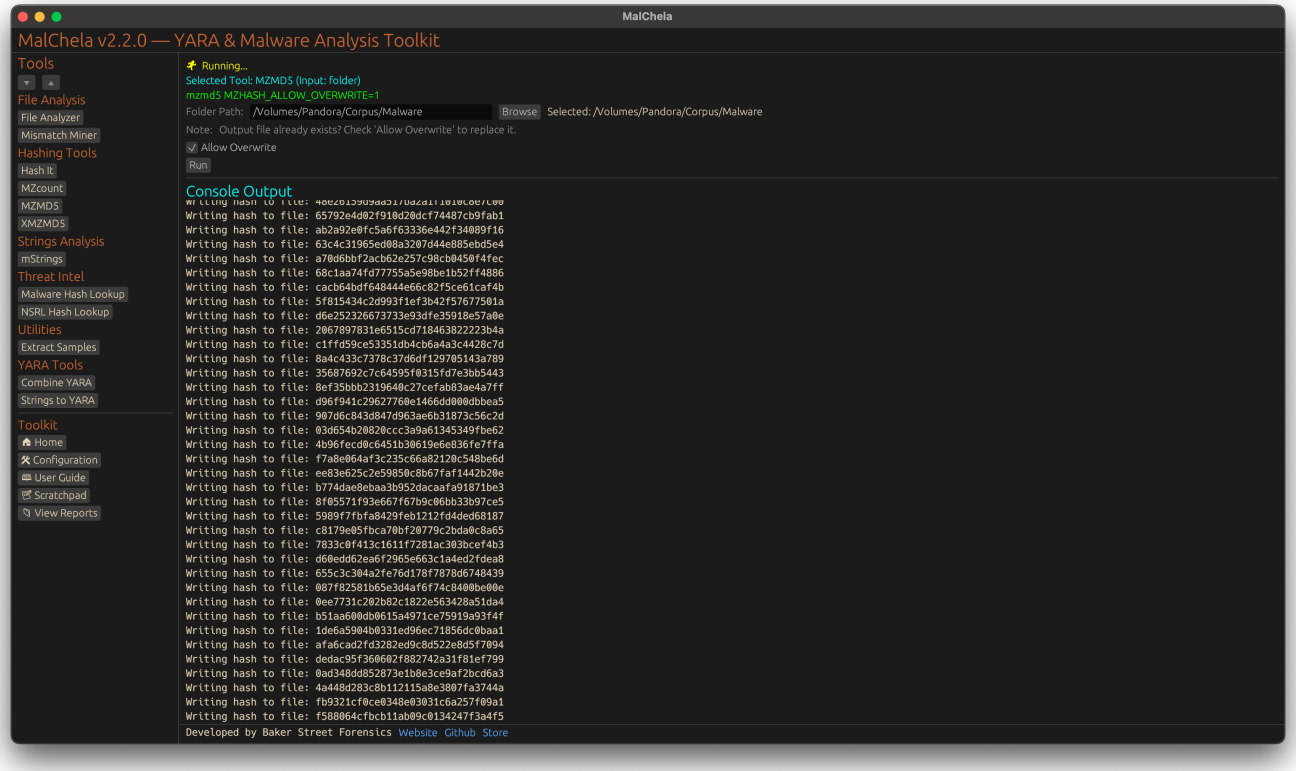

Figure 16: MZMD5

5.11 NSRLQuery

NSRL Query checks a file hash against the National Software Reference Library (NSRL) by querying the CIRCL hash lookup service. It helps identify known, trusted software — allowing analysts to filter out benign files and focus on unknown or suspicious ones during forensic triage.

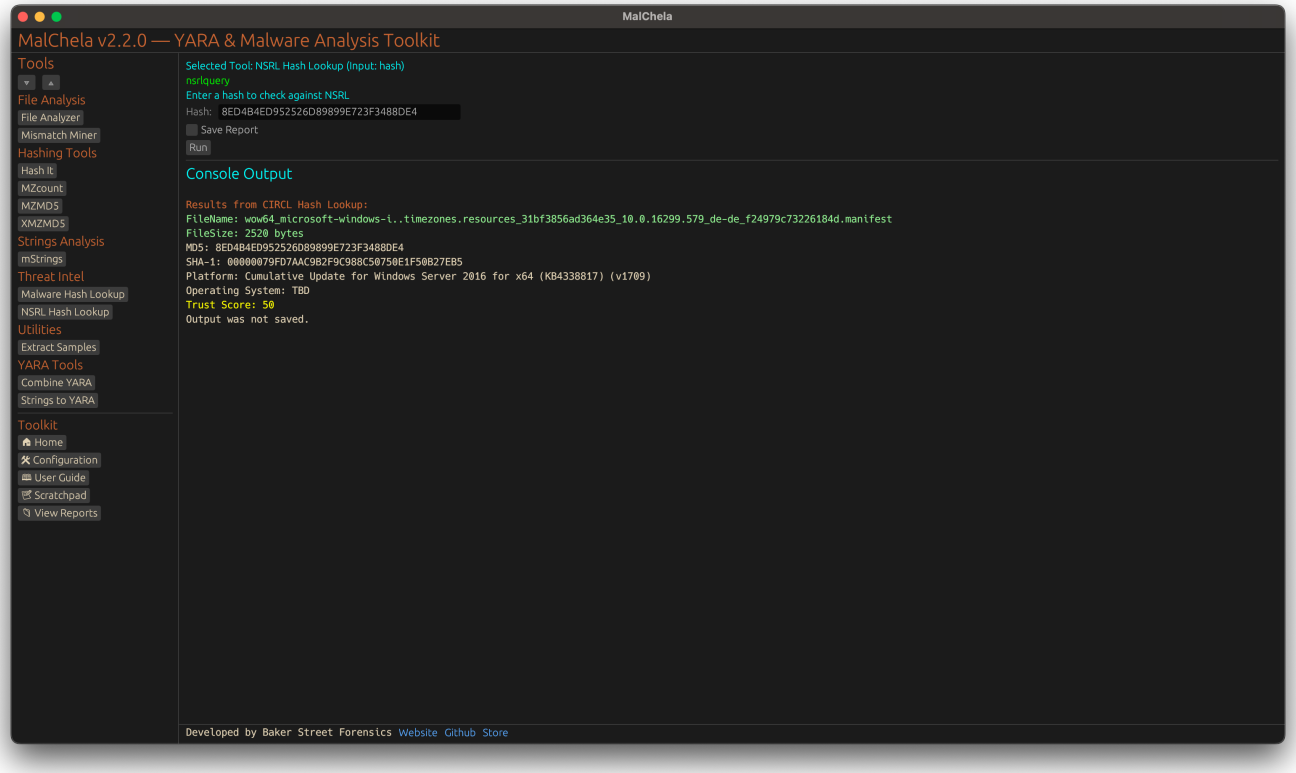

Figure 17: NSRL Hash Lookup

5.12 StringsToYARA

Strings to YARA helps you rapidly build custom YARA rules by prompting for a rule name, optional metadata, and a list of string indicators. It integrates with the MalChela scratchpad, allowing you to paste or collect candidate strings interactively.

Lines beginning with hash: are deliberately ignored during rule generation — this lets you use the scratchpad to track hashes alongside strings without polluting your YARA rule content.

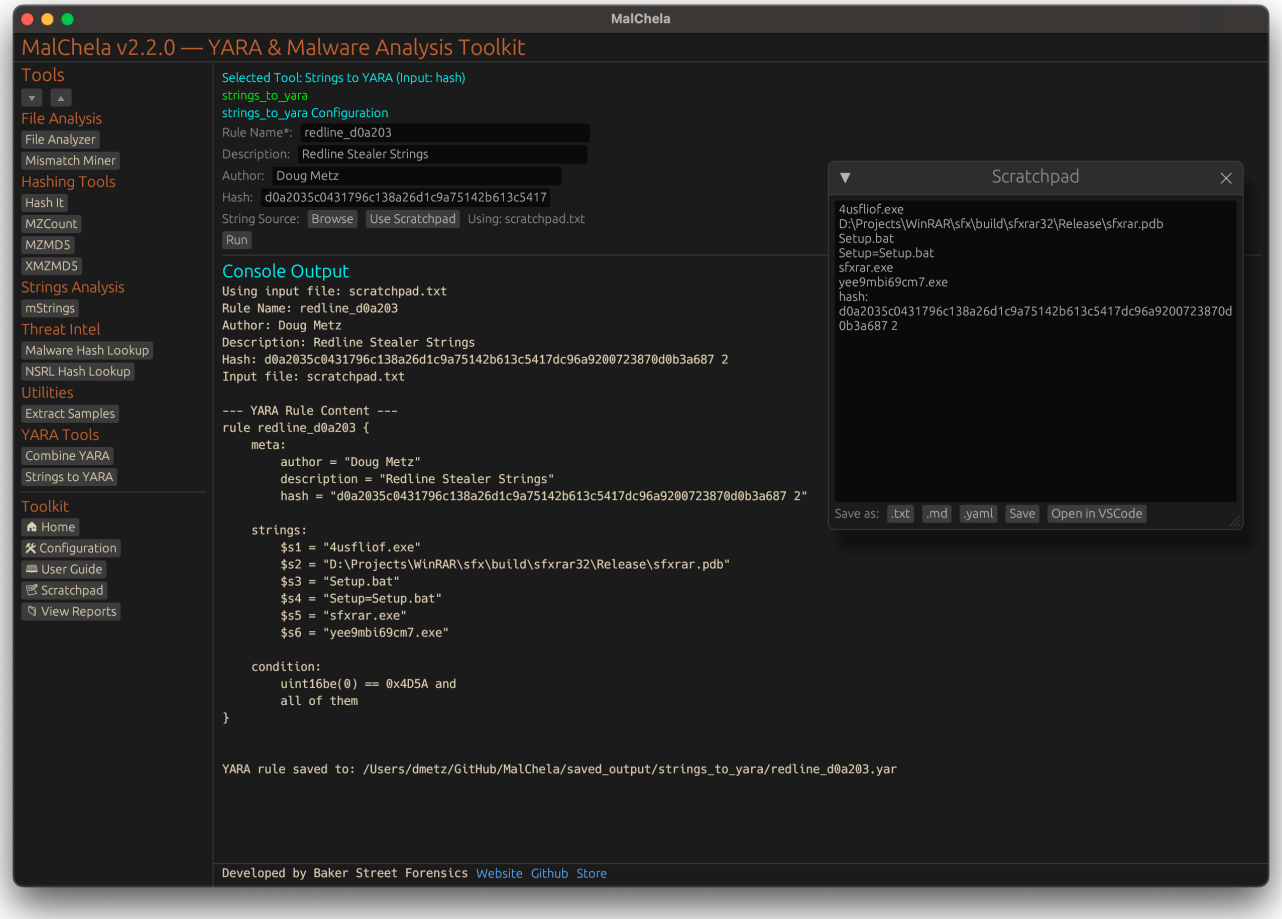

Figure 18: Strings to YARA

5.13 XMZMD5

XMZMD5 recursively scans a directory and generates MD5 hashes for all files that do not match common binary or archive signatures such as MZ, ZIP, or PDF. It's ideal for uncovering unusual or misclassified files that may require deeper inspection or reverse engineering. Use this on a malware corpus to help surface non-Windows malware samples.

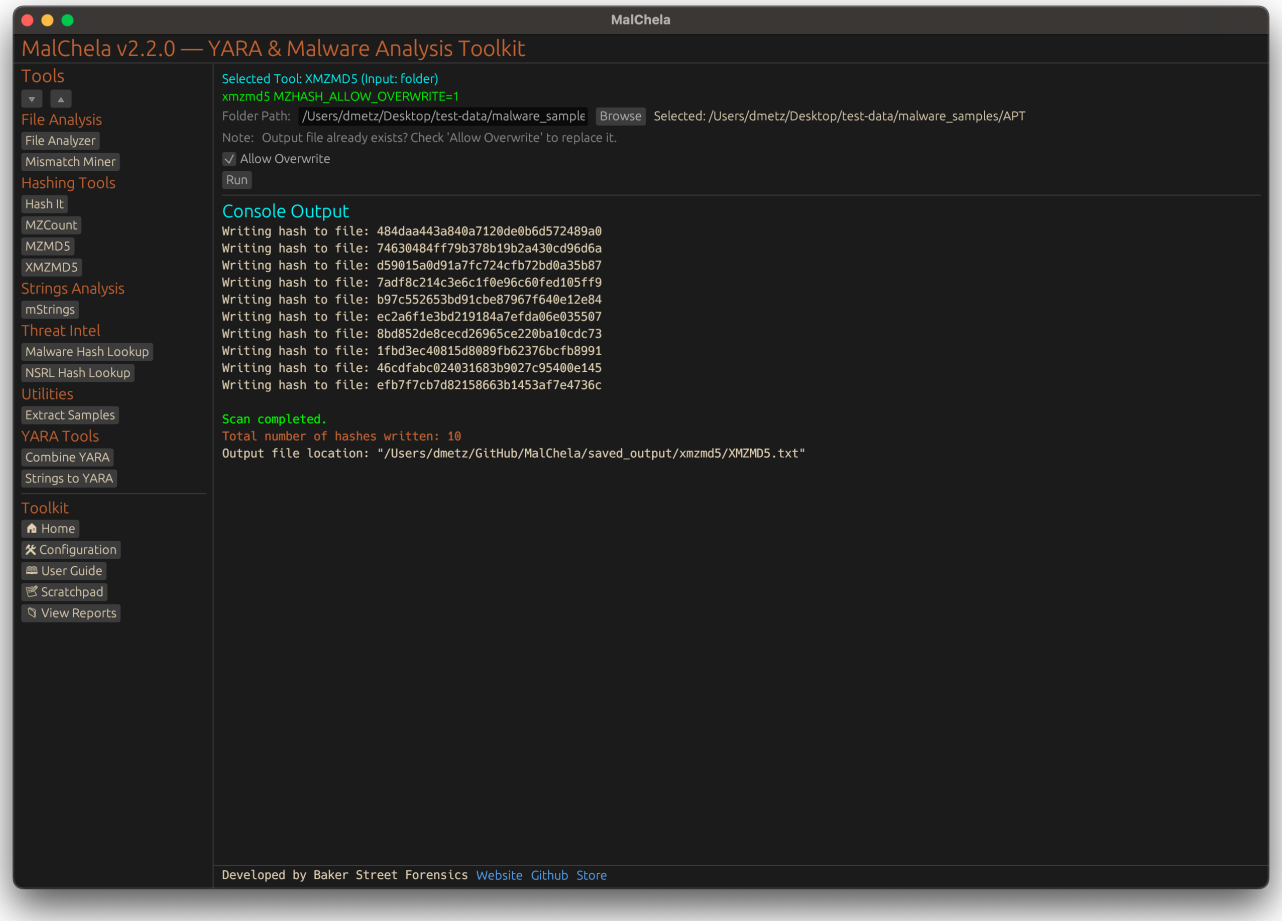

Figure 19: XMZMD5

6. Third-Party Tools

6.1 Integrating Third-Party Tools

MalChela supports the integration of external tools such as Python-based utilities (`oletools` , `oledump`) and high-performance YARA engines (`yara-x`). These tools expand MalChela's capabilities beyond its native Rust-based toolset.

Tools now require `exec_type` (e.g., `cargo` , `binary` , `script`) to define how they are launched, and `file_position` to clarify argument order when needed.

To integrate a new tool into the GUI, ensure the tool: - Accepts CLI arguments in the form `toolname [args] [input]` - Outputs results to stdout - Is installed and available in `$PATH`

```
- name: toolname
  description: "Short summary of tool purpose"
  command: ["toolname"]
  input_type: file  # or folder or hash
  category: "File Analysis"  # or other GUI category
  optional_args: []
  exec_type: binary  # or cargo / script
  file_position: last  # or first, if required
```

You can switch to a prebuilt `tools.yaml` for REMnux mode via the GUI configuration panel — useful for quick setup in forensic VMs.

6.2 Configuration Reference

6.2.1 Tool Configuration

MalChela uses a central `tools.yaml` file to define which tools appear in the GUI, along with their launch method, input types, categories, and optional arguments. This YAML-driven approach allows full control without editing source code.

Key Fields in Each Tool Entry

Field	Purpose
name	Internal and display name of the tool
description	Shown in GUI for clarity
command	How the tool is launched (binary path or interpreter)
exec_type	One of `cargo`, `binary`, or `script`
input_type	One of `file`, `folder`, or `hash`
file_position	Controls argument ordering
optional_args	Additional CLI arguments passed to the tool
category	Grouping used in the GUI left panel

⚠️ All fields except `optional_args` are required.

6.2.2 Swapping Configs: REMnux Mode and Beyond

MalChela supports easy switching between tool configurations via the GUI.

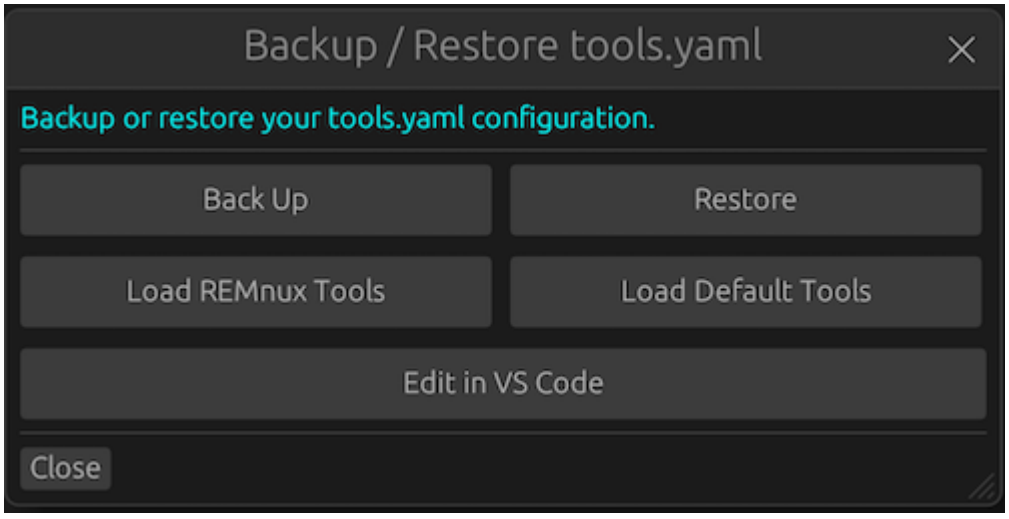

Figure 20: YAML Config Tool

To switch:

- Open the **Configuration Panel**
- Use **"Select tools.yaml"** to point to a different config
- Restart the GUI or reload tools

This allows forensic VMs like REMnux to use a tailored toolset while keeping your default config untouched.

A bundled `tools_remnux.yaml` is included in the repo for convenience.

KEY TIPS

- Always use `file_position: "last"` unless the tool expects input before the script
- For scripts requiring Python, keep the script path in `optional_args[0]`
- For tools installed via `pipx`, reference the binary path directly in `command`

6.2.3 Backing Up and Restoring tool.yaml

The MalChela GUI provides built-in functionality to back up and restore your `tools.yaml` configuration file.

Backup

To create a backup of your current `tools.yaml`:

- Open the **Configuration Panel**
- Click the **"Back Up Config"** button
- A timestamped copy of `tools.yaml` will be saved to the default location

You'll see a confirmation message when the operation completes successfully.

Restore

To restore from a previous backup:

- Click the **"Restore Config"** button in the Configuration Panel
- Select a previously saved backup file
- The selected file will overwrite the current configuration

This feature makes it easy to experiment with custom tool setups while retaining a safety net for recovery.

6.3 Enhanced Integrations

Enhanced configurations have been preconfigured for several third-party tools such as TShark and Volatility, enabling streamlined integration with MalChela. Additionally, dedicated setup instructions are provided for Python-based tools like oledump and olevba, as well as installation guidance for utilities like YARA-X to ensure consistent and reliable operation across environments.

6.4 FLOSS

- FLOSS extracts static, stack, tight, and decoded strings from binaries.
- The GUI supports all CLI flags (e.g., `–only`, `–format`, `-n`, etc.).
- Occasionally, FLOSS may print a multiprocessing-related error such as: `from multiprocessing.resource_tracker import main;main(6)` This is a known issue and does not affect output. It can be safely ignored.

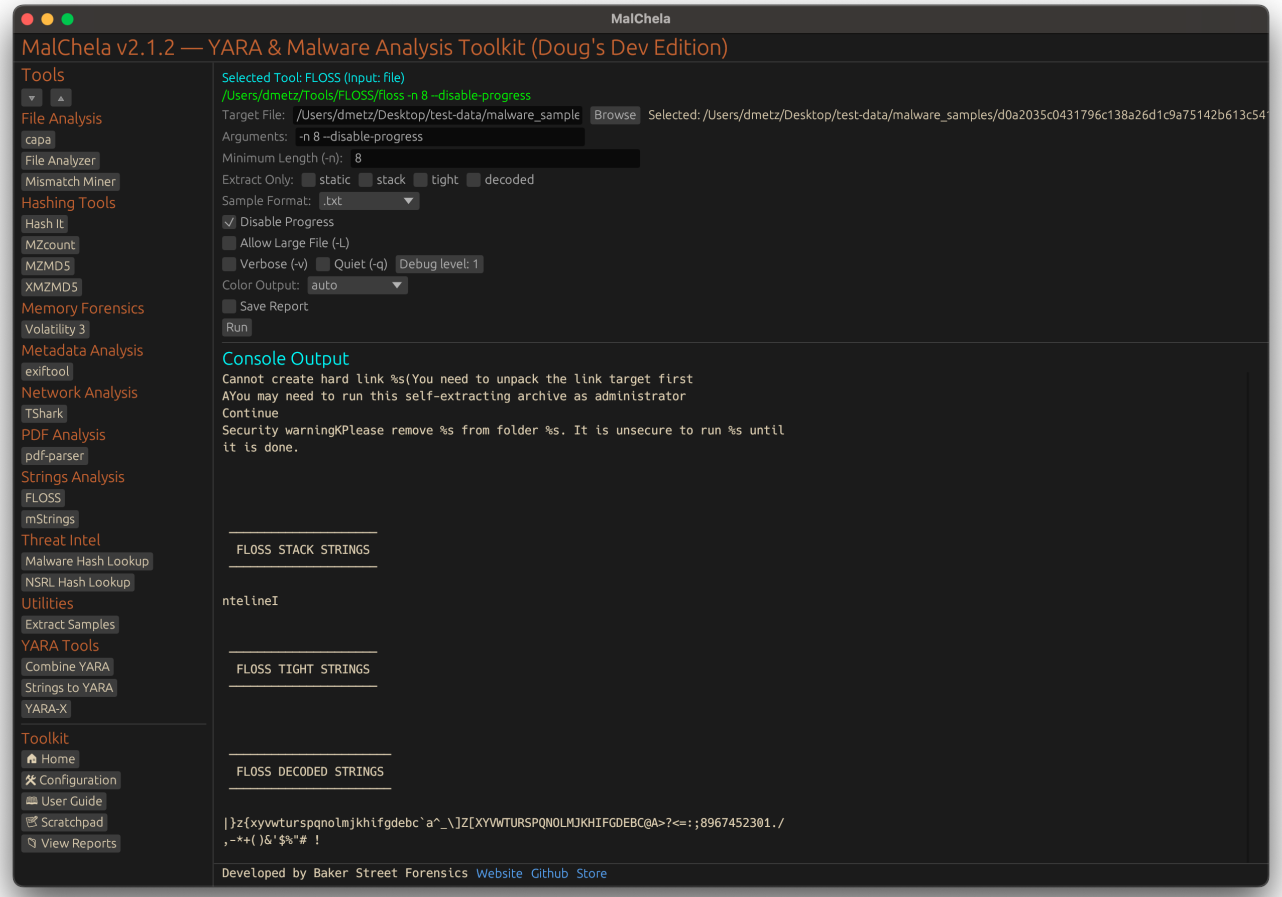

Figure 21: FLOSS

6.5 TShark

TShark Field Reference Panel

If TShark is included in your `tools.yaml` (or if you're using the REMnux configuration), the GUI offers a powerful set of tools to assist with display filter creation and usage. This includes both an integrated filter builder and a TShark Field Reference panel.

- The filter builder allows users to construct and modify complex TShark display filters directly within the GUI, with real-time syntax support and validation.
- The "?" icon next to filter fields launches the Field Reference panel, which provides searchable field definitions, examples, tooltips, and a copy-to-clipboard feature.
- Together, these tools help analysts visually explore and test filter syntax without needing to memorize protocol-specific field names.

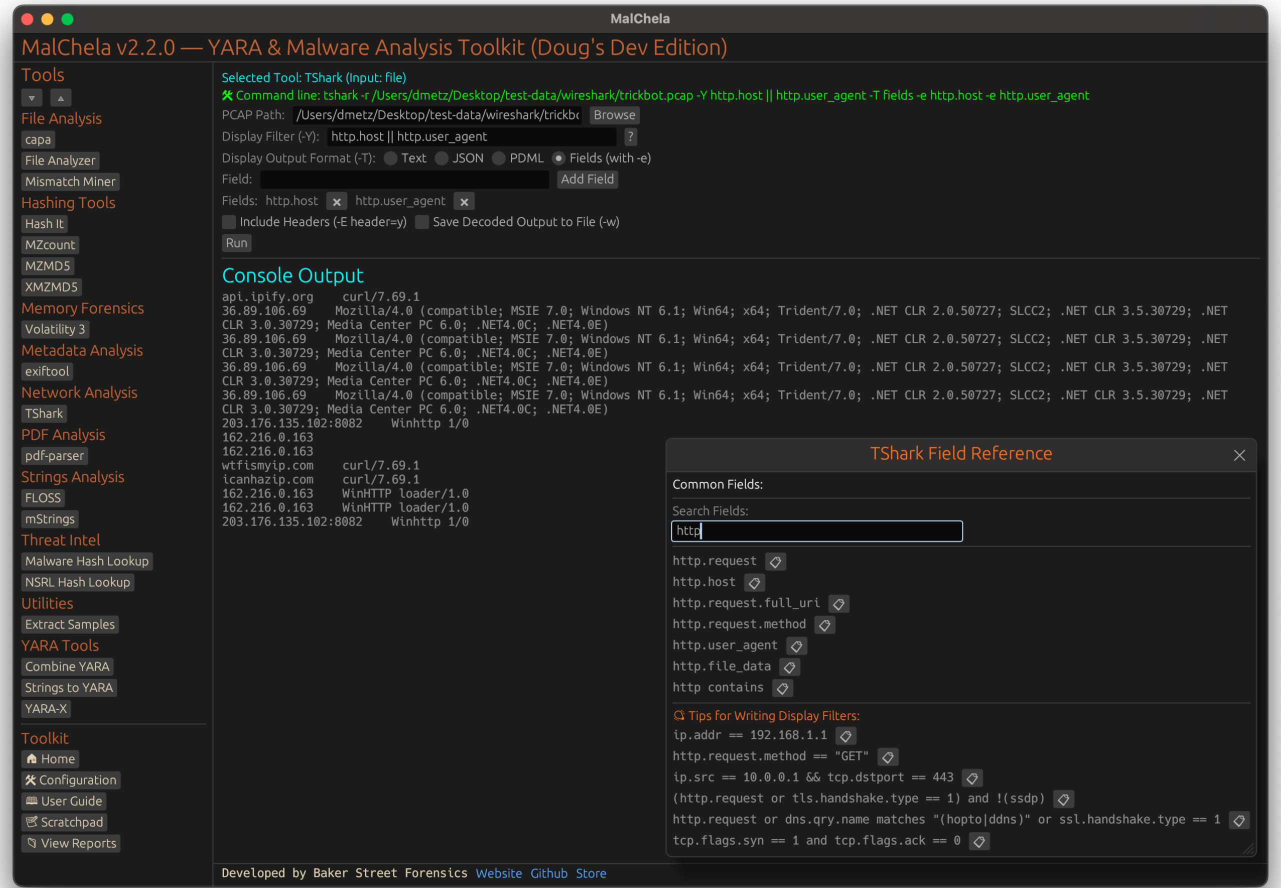

Figure 22: TShark

6.6 Volatility 3

MalChela integrates support for **Volatility 3**, a powerful memory forensics framework. This tool enables analysts to examine memory dumps for signs of compromise, persistence mechanisms, and malicious activity.

6.6.1 Integration Overview

Volatility 3 is available in MalChela as an enhanced third-party tool. The GUI provides a dedicated interface for selecting plugins, supplying arguments, and reviewing results — all within a structured panel that mimics the CLI workflow but adds quality-of-life improvements like:

- Live search and categorized plugin reference
- Plugin-specific argument helpers
- Color-coded output for easier review
- Output saving and file dump options

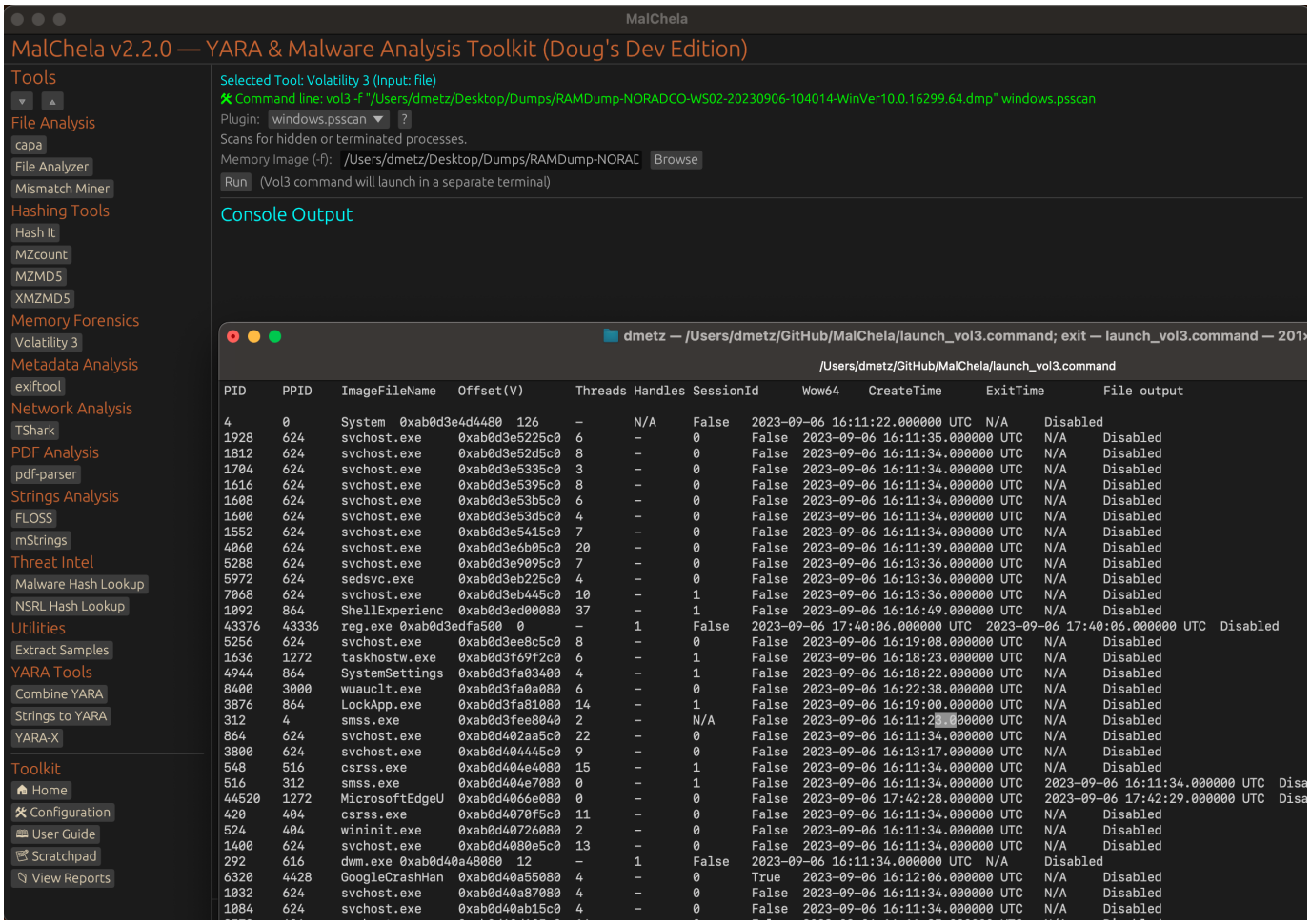

Figure 23: Volatility (launches in separate terminal)

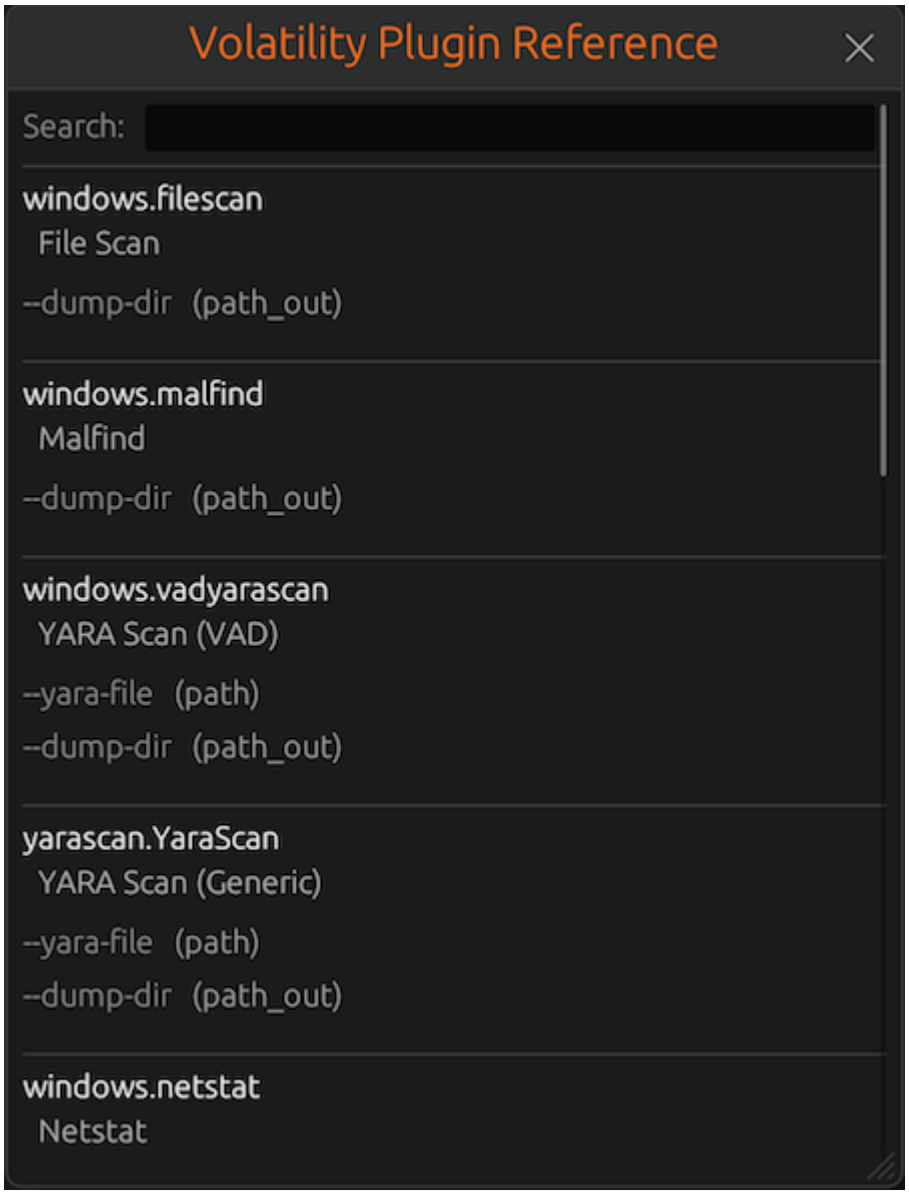

Figure 24: Volatility Plugin Reference

6.6.2 Requirements

To use Volatility 3 within MalChela:

- You must have `vol3` (Volatility 3 CLI) installed and accessible in your system `$PATH`.
- On REMnux, `vol3` is preinstalled and configured automatically.
- On macOS or Linux, you can install it via pip: `pip install volatility3`

6.6.3 tools.yaml Configuration

To use Volatility 3 with the GUI launcher, ensure the correct `command` value is defined in your `tools.yaml` configuration. Depending on your environment, the binary may be installed under different names or locations.

Two common examples:

```
- name: Volatility 3
  description: "Memory analysis using Volatility 3"
  command: ["/Users/dmetz/.local/bin/vol3"]
  input_type: "file"
  file_position: "first"
  category: "Memory Forensics"
  gui_mode_args: []
  exec_type: binary

- name: Volatility 3
  description: "Memory analysis using Volatility 3"
  command: ["vol3"]
  input_type: "file"
  file_position: "first"
  category: "Memory Forensics"
  gui_mode_args: []
  exec_type: script
```

Make sure that the specified binary path or command is accessible in your system's `$PATH`.

6.6.4 Example Use Cases

- Enumerate processes: `windows.pslist`
- Dump suspicious files from memory: `windows.dumpfiles --dump-dir /output/path`
- Detect injected code: `windows.malfind`
- YARA scanning on memory: `windows.vadyarascan --yara-file rules.yar`

6.6.5 Output and Reports

All plugin results are streamed to the GUI console with formatting preserved. Where supported, plugins that produce dumped files will output to a user-specified folder.

6.6.6 Known Limitations

- Some plugins require symbol files (`.pdb`) to function correctly. Volatility will display a warning if missing.
- Ensure sufficient system memory when analyzing large memory dumps.

6.6.7 Additional Resources

- Volatility 3 GitHub
- Official Documentation

6.7 Installing and Configuring YARA-X

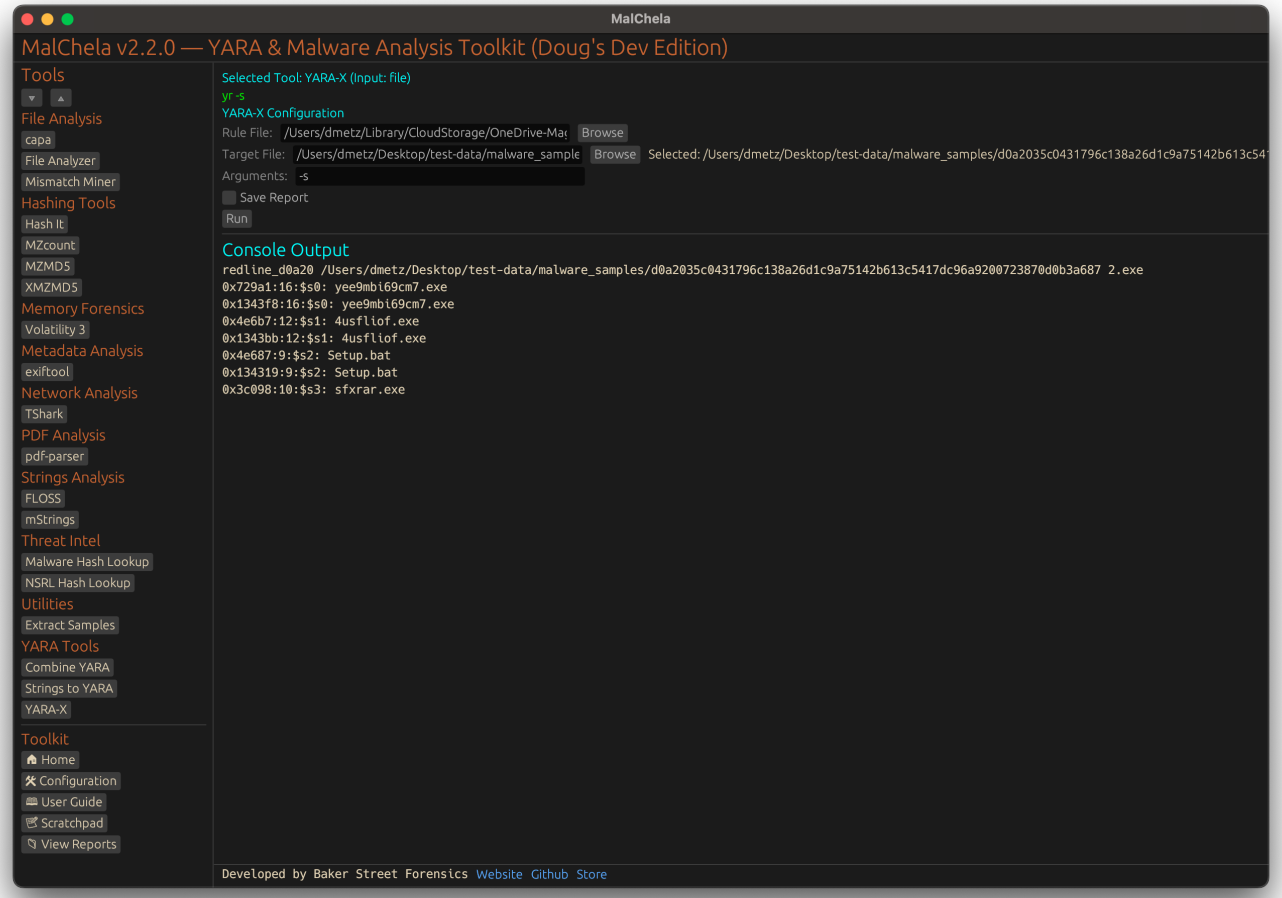

Figure 25: YARA-X

YARA-X is an extended version of YARA with enhanced performance and features. To integrate YARA-X with MalChela, follow these steps:

6.7.1 Installation

- **Download the latest release:**
  Visit the official YARA-X GitHub releases page at https://github.com/Yara-Rules/yara-x/releases and download the appropriate binary for your platform.
- **Extract and install:**
  Extract the downloaded archive and place the `yara-x` binary in a directory included in your system's `$PATH`, or note its absolute path for configuration.
- **Verify installation:**
  Run the following command to confirm YARA-X is installed correctly:

```
yara-x —version
```

6.7.2 Configuration in MalChela

To use YARA-X within MalChela tools, update your `tools.yaml` with the following example entry:

```
- name: yara-x
  description: "High-performance YARA-X engine"
  command: ["yara-x"]
  input_type: "file"
  file_position: "last"
  category: "File Analysis"
  optional_args: []
  exec_type: binary
```

6.7.3 Using YARA-X Rules

- Place your YARA rules in the `yara_rules` folder within the workspace.
- YARA-X supports recursive includes and extended features; ensure your rules are compatible.
- The MalChela GUI and CLI will invoke YARA-X when configured as above, providing faster scans and improved detection.

6.7.4 Tips

- For advanced usage, consult the YARA-X documentation for command-line options and rule syntax.

6.8 Python Integrations

Configuring Python-Based Tools (oletools & oledump)

MalChela supports Python-based tools as long as they are properly declared in `tools.yaml`. Below are detailed examples and installation instructions for two commonly used utilities:

🔧 `olevba` (FROM `oletools`)

Install via `pipx`:

```
pipx install oletools
```

This installs `olevba` as a standalone CLI tool accessible in your user path.

`tools.yaml` configuration example:

```
- name: olevba
  description: "OLE document macro utility"
  command: ["/Users/youruser/.local/bin/olevba"]
  input_type: "file"
  file_position: "last"
  category: "Office Document Analysis"
  optional_args: []
  exec_type: script
```

Notes:

- `olevba` is run directly (thanks to pipx)
- No need to specify a Python interpreter in `command`
- Ensure the path to `olevba` is correct and executable

—

`oledump` (STANDALONE SCRIPT)

Manual installation:

```
mkdir -p ~/Tools/oledump
cd ~/Tools/oledump
curl -O https://raw.githubusercontent.com/DidierStevens/DidierStevensSuite/master/oledump.py
chmod +x oledump.py
```

Make sure the script path in `optional_args` is absolute, and that the file is executable if it's run directly (not through a Python interpreter in `command`).

Dependencies:

```
python3 -m pip install olefile
```

Alternatively, create a virtual environment to isolate dependencies:

```
python3 -m venv ~/venvs/oledump-env
source ~/venvs/oledump-env/bin/activate
pip install olefile
```

`tools.yaml` configuration example:

```
- name: oledump
  description: "OLE Document Dump Utility"
  command: ["/usr/local/bin/python3"]
  input_type: "file"
  file_position: "last"
  category: "Office Document Analysis"
  optional_args: ["/Users/youruser/Tools/oledump/oledump.py"]
  exec_type: script
```

Notes:

- The GUI ensures correct argument order: `python oledump.py <input_file>`
- `command` points to the Python interpreter
- `optional_args` contains the path to the script

7. REMnux Mode

MalChela includes built-in support for running in **REMnux Mode**, a configuration designed specifically for seamless operation within the REMnux malware analysis distribution.

7.1 How REMnux Mode Works

REMnux Mode is a configuration profile that aligns MalChela's behavior with the REMnux malware analysis distribution. It adjusts paths, tool definitions, and GUI presentation to match the REMnux environment.

This mode is manually enabled by selecting **"Load REMnux"** from the tools.yaml Configuration Panel in the GUI. Once selected, a REMnux-specific `tools.yaml` file is loaded and remains active until you replace it with another configuration.

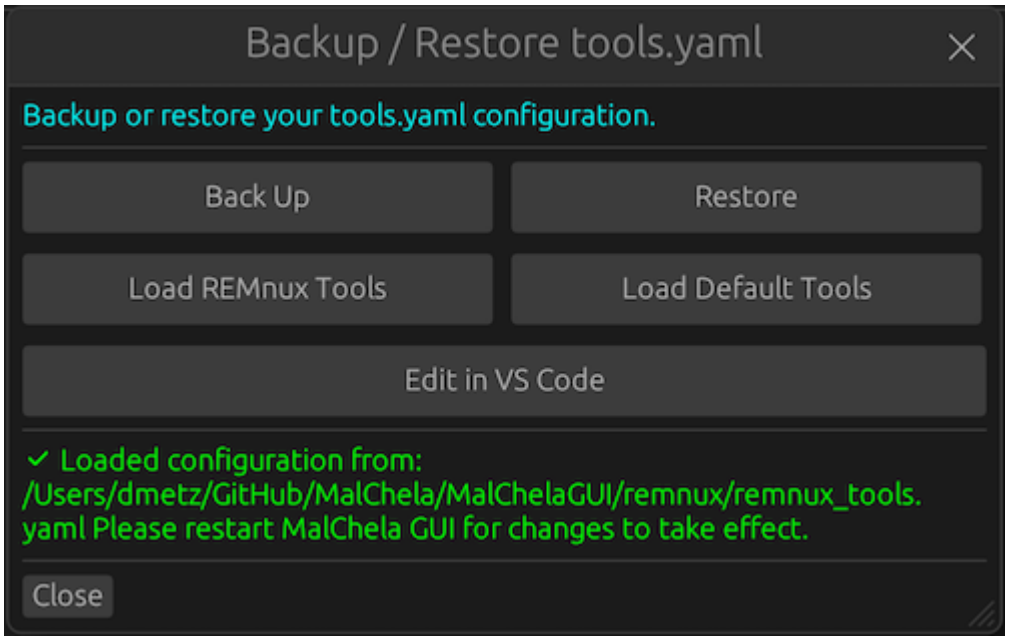

Figure 26: Enabling REMnux mode

Note: Whenever you change the tools.yaml, you need to restart the GUI for it to take effect.

7.2 Preconfigured Tools in REMnux Mode

The following tools will appear in the GUI when REMnux Mode is enabled. Each is preconfigured with known-good paths for the REMnux environment:

7.2.1 File Analysis

Tool	Description	Command
binwalk	Scan binary files for embedded files	`binwalk`
capa	Detects capabilities in binaries via rules	`capa`
FLOSS	Extract obfuscated strings from binaries	`floss`
radare2	Scan binary files	`/usr/bin/r2 -i`

7.2.2 Memory Forensics

Tool	Description	Command
Volatility 3	Memory analysis using Volatility 3	`vol3`

7.2.3 Metadata Analysis

Tool	Description	Command
exiftool	Extract metadata from files	`exiftool`

7.2.4 Network Forensics

Tool	Description	Command
TShark	Analyze network traffic	`tshark`

7.2.5 Office Document Analysis

Tool	Description	Command
mraptor	Detect auto-executing macros in Office docs	`mraptor`
oledump	Dump streams from OLE files	`oledump.py`
oleid	Analyze OLE files for suspicious indicators	`oleid`
olevba	Extract VBA macros from OLE files	`olevba`
rtfobj	Extract embedded objects from RTF files	`rtfobj`
zipdump	Parses and analyzes suspicious PDF structures	`zipdump.py`

7.2.6 PDF Analysis

Tool	Description	Command
pdf-parser	Parse structure and objects of a PDF file	`python3 /usr/local/bin/pdf-parser.py`

7.2.7 Utilities

Tool	Description	Command
clamscan	Antivirus scan using ClamAV	`clamscan`
strings	Extracts printable strings from binary files	`strings`

7.3 Benefits

- Tools like **Volatility 3**, **FLOSS**, **oledump**, and **olevba** are preconfigured and ready to go
- `tools.yaml` is auto-tailored to the REMnux environment
- You can still customize your tool entries, but defaults are optimized for REMnux paths and permissions
- Useful for education, triage labs, and portable analysis setups

7.4 Customizing the REMnux Experience

Although REMnux Mode provides sane defaults, you can still:

- Override tool entries in `tools.yaml`
- Add new third-party tools via the GUI or YAML
- Use the Configuration Panel to backup/restore your configuration

For more information about REMnux, visit REMnux.org.

8. Support

8.1 Support & Contribution

The MalChela project is open source and actively maintained. Contributions, feedback, and bug reports are always welcome. You can find the project on GitHub, where issues and pull requests are encouraged.

8.2 Known Limitations & Platform Notes

MalChela is designed to be cross-platform but has some current limitations:

- The **CLI** runs well on macOS, Linux, and WSL environments.
- The **GUI** is supported on macOS and Linux. It may also work under WSLg on Windows 11, but this is not officially tested.
- File paths must use **POSIX-style formatting** (e.g., `/home/user/file.txt`). Windows-style paths are not supported.
- If the `exec_type` field is missing or misconfigured in `tools.yaml`, GUI execution may fail or behave incorrectly.
- The `category` field in `tools.yaml` no longer impacts GUI execution behavior—it is only used for grouping in the interface.