



Heirloom Software

The Idjits Guide to
Evidence Triage

Read-only incident response collection from a USB stick.

Volatile data, persistence, event logs, hives, hashes and a sector map -
with a hash manifest and a printable chain-of-custody report.

Disclaimer and Hold Harmless Agreement

The Idjits Guide to Evidence Triage • October 2026 edition • Heirloom Software LLC

In plain words: This guide explains how to use the tool. Use it only on computers your organization owns or that you are authorized in writing to examine. Follow your own organization's evidence policy where it differs from this guide. Check the results yourself before you rely on them.

COPYRIGHT

Copyright © 2026 Heirloom Software LLC. All rights reserved. You may keep copies of this guide and print it for your own personal use. You may not resell it, share it publicly, or reproduce any part of it for others without written permission from Heirloom Software LLC.

TRADEMARKS

Product names, logos, and brands mentioned in this guide (including Microsoft, Windows, Linux, Ubuntu, Python, and the others named inside) are the property of their respective owners and are used only to identify their products. Heirloom Software LLC is not affiliated with, sponsored by, or endorsed by any of them, or by the publishers of any other book series.

DISCLAIMER

This guide is for general information and education only. It is provided "as is," without warranties of any kind, express or implied, including warranties of accuracy, completeness, merchantability, or fitness for a particular purpose. Software, websites, prices, and menus change often; the information was believed accurate in October 2026 but may be out of date or incorrect when you read it. Nothing in this guide is professional, legal, financial, or security advice. For important systems or data, consult a qualified professional.

YOUR RESPONSIBILITY

Installing operating systems, changing settings, typing commands, and working with computer hardware can erase data, make a computer unable to start, void warranties, or expose a computer or network to security risks. **Back up your data before you follow any instructions in this guide.** You alone decide whether to follow them, and you do so at your own risk. Always follow the manufacturer's and software maker's own instructions where they differ from this guide.

LIMITATION OF LIABILITY

To the fullest extent permitted by law, Heirloom Software LLC and its owners, authors, employees, and agents will not be liable for any direct, indirect, incidental, special, consequential, or punitive damages, or for any loss of data, profits, use, equipment, or business, arising out of or related to this guide or your use of it, even if advised of the possibility of such damages. If any liability is found despite this, it is limited to the amount you paid for this guide.

HOLD HARMLESS AGREEMENT

By reading or using this guide, you agree to release, hold harmless, defend, and indemnify Heirloom Software LLC and its owners, authors, employees, and agents from and against any and all claims, demands, losses, damages, liabilities, costs, and expenses (including reasonable attorneys' fees) arising out of or related to your use of this guide, your following or failing to follow any of its instructions, or your use of any software, hardware, website, or service it mentions.

THIRD PARTIES

This guide mentions software, websites, and services made by others. Heirloom Software LLC does not control them and is not responsible for their content, safety, availability, or terms. Your use of them is governed by their own terms and policies.

AGREEMENT

If any part of this notice is found unenforceable, the rest remains in effect. **If you do not agree to these terms, do not use this guide.** Using it means you accept them.

What's Inside

1. What It Collects	4
2. The Read-Only Promise	5
3. Setting Up the USB Stick	7
4. Running It on Windows	8
5. Running It on Linux	10
6. File Listing, Hashes and the Sector Map	11
7. Registry Hives and Prefetch	13
8. Chain of Custody	14
9. Troubleshooting	15
Cheat Sheet	16
Glossary	17

Read this first

Heirloom Evidence Triage collects evidence from a live computer without changing it. You plug in a USB stick, run one program, and walk away with an **Evidence** folder: what was running, who was logged on, what starts automatically, the recent security events, copies of the registry hives and prefetch files, a full file listing with hashes, a map of the exact disk sectors each file uses, and a printable chain-of-custody report.

It runs on **Windows 7 through Windows 11** and on **Linux**. Nothing is installed. The same folder works from a USB stick or from a folder on a desktop.

WATCH OUT

Use it only on computers your organization owns, or that you have written permission to examine. Collecting from someone else's computer without permission can be a crime.

CHAPTER 1

What It Collects

Every run makes one new folder named for the computer and the time (in UTC), so runs never mix. Inside it the evidence is grouped like this:

Folder	What is inside
1_Volatile	System time and time zone, uptime, network connections with the program that owns each one, DNS cache, ARP table, routes, every running process with its owner, parent and command line, logged-on users and logon sessions
2_Persistence	Scheduled tasks, startup programs, Run keys for every user, Winlogon, AppInit, Image File Execution Options debuggers, services, drivers, WMI event subscriptions
3_EventLogs	Last 50 (you choose) successful logons, failed logons, credential use and lockouts, account and policy changes, log-cleared events, system errors, service installs, Remote Desktop sessions, PowerShell script blocks
4_Artifacts	Prefetch files and registry hives (SYSTEM, SOFTWARE, SAM, SECURITY, DEFAULT, Amcache, every user's NTUSER.DAT and UsrClass.dat) with their .LOG1/.LOG2 files
5_Disk	Physical drives, volumes, partition tables, a full file listing with timestamps and SHA-256/MD5 hashes, and the sector map
(top level)	Report.txt, CollectionLog.txt, Manifest_SHA256.csv, ChainOfCustody.txt and ChainOfCustody_Report.pdf

Every table is saved as a **CSV** file you can open in Excel or load into a timeline tool. **Report.txt** puts the important parts together in one readable file.

CHAPTER 2

The Read-Only Promise

Evidence only counts if you can show you did not change it. The tool follows a strict look-don't-touch rule, and the rule is written at the top of every script so an auditor can check it.

How it stays read-only

- **Only read commands.** Every PowerShell command aimed at the computer is a **Get-** command (Get-WmiObject, Get-WinEvent, Get-ItemProperty, Get-ChildItem, Get-Process) or Test-Path. Nothing that sets, creates, removes, stops or starts anything is used.
- **Windows tools in listing mode only:** netstat -ano, ipconfig /all, arp -a, route print, quser, schtasks /query.
- **Disks are opened with read access only.** Files are opened with **read-attributes** access only. That kind of access cannot read or change what is in a file.
- **Hashes and copies come straight from the disk.** The tool finds a file's clusters and reads them through the read-only disk handle. The file itself is never opened for reading, so Windows never changes its last-access time. This is also how locked files like registry hives get copied.
- **Cloud placeholders are skipped.** OneDrive-style files that live online are not opened, because opening one could start a download that writes to the disk.
- **One gate for every write.** All output goes through a guard that refuses any path outside the evidence folder.
- **No temp files on the computer.** PowerShell's compiler normally drops temporary files in the computer's TEMP folder. The tool points it at the USB stick instead.

What no live collection can avoid

Running any program on a live computer leaves a small, known footprint. Write these in your case notes:

- Windows may record that Heirloom Evidence Triage.exe and powershell.exe ran (Prefetch, event 4688, and PowerShell script-block event 4104 when those are turned on).
- Plugging in a USB stick is recorded by Windows.

- Listing a folder can update that folder's last-access time if NTFS last-access updates are turned on. The report shows that setting (look for **NTFS last-access updates**).
- Turning on the backup privilege for the tool's own process may log event 4672/4673 when privilege auditing is on.

REMEMBER

Run it from the USB stick. If you save the evidence on the computer's own Windows drive, you are writing to the drive you are examining. The tool warns you and asks first.

CHAPTER 3

Setting Up the USB Stick

1. Use a USB stick or external drive with plenty of free space. 64 GB or more is a good start; hive copies and file listings of a big drive can take several gigabytes.
2. Format it **exFAT** or **NTFS** (FAT32 cannot hold files over 4 GB).
3. Copy the whole **Heirloom Evidence Triage** folder onto it.
4. Write down the SHA-256 of **HeirloomTriage.ps1** and **engine\HeirloomEngine.cs**. Every report prints both, so you can prove later that the tool was not changed.

Heirloom Evidence Triage\	
Heirloom Evidence Triage.exe	<- opens the window (no black box)
Run Triage (command line).cmd	<- command-line mode
HeirloomTriage.ps1	<- the collector (Windows)
HeirloomTriage-GUI.ps1	<- the window
engine\HeirloomEngine.cs	<- read-only disk engine
Agreements\	<- license and hold harmless agreements
linux\heirloom_triage.sh	<- the collector (Linux)
linux\heirloom_ro.py	<- read-only helper (Linux)
Evidence\	<- made on the first run

TIP

Want to run it from a desktop folder instead? Copy the same folder there. Then use **Save evidence to** (or **-OutputPath**) to send the evidence to an external drive.

CHAPTER 4

Running It on Windows

With the window

1. Plug in the USB stick and open the **Heirloom Evidence Triage** folder.
2. Double-click **Heirloom Evidence Triage.exe**. Click **Yes** when Windows asks for Administrator rights.
3. The first time (and when the agreements change), read the **License Agreement** and the **Hold Harmless Agreement** to the bottom, check the box, and click **I Have Read and Agree**. Your answer is saved on the USB stick, not on the computer.
4. Type the **Case number** and your **Examiner name**.
5. Check **Save evidence to**. It starts as the USB stick's tool folder.
6. Pick the **Drives to list and map** (C, or C,D, or All) and the hash size limit.
7. Click **Start Collection**. The log fills in as each part finishes.
8. When it says **Finished**, click **Open Evidence Folder**.

The green line under the check boxes tells you the tool has Administrator rights. Without them, the Security log, hashes, hives and the sector map are skipped.

From the command line

```
"Run Triage (command line).cmd" -CaseNumber IR-2026-114 -Examiner "J. Smith"

powershell -ExecutionPolicy Bypass -File HeirloomTriage.ps1 -CaseNumber IR-114 ^
-Examiner "J. Smith" -Volumes C,D -HashMaxMB 0 -ExportEvtx -NoPause
```

In the background (no window at all)

Give **Heirloom Evidence Triage.exe** the same options and it runs the whole collection hidden, then exits with the result code (0 = all collected, 1 = partial). Use it from an Administrator prompt or a scheduled task set to run with highest privileges. A hidden run cannot show the agreements, so agree once with the window first, or add **-AcceptAgreements** to say you have read and agree to both. Without either, it stops before collecting anything.

```
"Heirloom Evidence Triage.exe" -CaseNumber IR-114 -Examiner "J. Smith" -
OutputPath E:\
```

Option	What it does
-CaseNumber, -Examiner	Printed on every report and the PDF
-OutputPath FOLDER	Where the Evidence folder goes (default: the tool's folder)
-Volumes C,D All	Drives to list, hash and sector-map (default: the Windows drive)
-HashMaxMB N	Hash files up to N MB; 0 = every file (default 100)
-NoHash	List and map files without hashing them
-MaxFiles N	Stop each drive's listing after N entries (quick look)
-SkipDiskMap / -SkipArtifacts	Leave out the disk listing / the hives and prefetch
-EventCount N	Entries from each event-log query (default 50)
-ExportEvtx	Also export the whole Security, System and Application logs
-AllowLocalOutput	Allow saving on the computer's own Windows drive
-NoPause	Do not wait for Enter at the end (for scripts)

Exit codes for scripts: **0** everything collected, **1** finished but a section had a problem, **2** stopped before collecting.

TIP

Need a fast first look? Run with **-MaxFiles 20000 -NoHash** to get everything except the full drive listing in a few minutes. Run the full listing afterward.

CHAPTER 5

Running It on Linux

USB sticks usually do not keep the Linux "run" permission, so start the script with bash:

```
cd "/media/$USER/USBSTICK/Heirloom Evidence Triage/linux"
sudo bash heirloom_triage.sh -c IR-2026-114 -e "J. Smith"
```

Option	What it does
-c CASE -e NAME	Case number and examiner
-o FOLDER	Where the Evidence folder goes (default: the script's folder)
-m /,/home	Mount points to list, hash and map (default: /)
-H MB / -N	Hash size limit (0 = every file) / do not hash
-x COUNT	Stop each listing after COUNT entries
-n COUNT	Entries from each log query (default 50)
-S / -A	Skip the disk listing / skip the artifact copies
-L	Allow saving on the computer's own root disk

On Linux, files and folders are opened with **O_NOATIME**, so reading them does not change their access times. Login records (wtmp and btmp) are copied first, and **last** reads the copy. The block map comes from the kernel's **FIEMAP** query. The sector map, hashes and PDF need **python3**, which nearly every Linux system has.

CHAPTER 6

File Listing, Hashes and the Sector Map

For each drive you map, **5_Disk** gets four files:

File	What is in it
FileListing_C.csv	One row per file and folder: attributes, size, created, modified, accessed and MFT-changed times (UTC), MFT record, fragment count, first disk sector, SHA-256 and MD5
SectorMap_C_Fragments.csv	One row per piece (extent) of every file: start sector, sector count and end sector on the physical drive
SectorMap_C_Regions.csv	Every used and unused stretch of the drive, in sectors
SectorMap_C_Summary.txt	Drive layout, totals, a picture of used vs. unused space, the most fragmented files and the self-check

Reading the sector numbers

- **DiskStartSector** counts from the first sector of the physical drive (LBA 0). Open the drive image at that sector and you are at the start of the file's data.
- **VolumeStartSector** counts from the start of the partition.
- **MFT-resident** means a small file is stored inside its own MFT record. Its sector is the MFT record's sector.
- **Sparse/compressed** pieces use no disk clusters.
- Files are stored in whole clusters, so the last sector of a file can hold **slack space** past the end of the file.

The self-check

The summary ends with a **SECTOR TRANSLATION SELF-CHECK**. The tool reads the boot sector and the first MFT record two ways, through the volume and through the raw physical drive at the sector the map predicts, and compares them. **PASS** proves the sector numbers point at the right place on the disk.

About the hashes

Hashes are read from the disk clusters, so the file is never opened. NTFS-compressed and EFS-encrypted files are marked **Not hashed** because their clusters hold compressed or encrypted data, not the file's real contents. Files bigger than your hash limit are also marked. Use `-HashMaxMB 0` to hash everything.

WATCH OUT

On a running computer, a file that is being written at that moment can change while it is read. For a court-grade copy of a whole disk, make a full image with a hardware write blocker. This tool is for triage.

CHAPTER 7

Registry Hives and Prefetch

Windows keeps its registry hives locked while it runs, so ordinary copying fails. The tool reads each hive's clusters straight from the disk, the same way it makes hashes, and saves an exact copy under **4_Artifacts\Files**, keeping the original folder names.

- Each hive comes with its **.LOG1** and **.LOG2** files. Registry tools use them to bring the hive fully up to date. Load them together.
- **4_Artifacts\Artifacts_Copied.csv** lists every source path, its timestamps, the SHA-256 and MD5 of the copy, and the method used.
- Prefetch files show which programs ran and when. Open them with any prefetch parser.

TIP

If Windows refuses to say where a file's clusters are, the tool reads the cluster list from the file's own MFT record instead. The CSV says when that happened.

CHAPTER 8

Chain of Custody

When collection ends, the tool hashes every evidence file into **Manifest_SHA256.csv** and prints the manifest's own SHA-256 on the screen. **Write that number on your custody form.**

ChainOfCustody_Report.pdf is ready to print. It holds the case details, the computer's details, the tool and manifest hashes, what was collected, the SHA-256 of each evidence file, and signature lines for everyone who takes possession of the evidence.

Checking the evidence later

Run this in the evidence folder (PowerShell 4 or newer). It prints nothing if every file still matches:

```
Import-Csv Manifest_SHA256.csv | ForEach-Object {  
    if ((Get-FileHash $_.File -Algorithm SHA256).Hash -ne $_.SHA256) { "CHANGED:  
    " + $_.File }  
}
```

On Linux:

```
tail -n +2 Manifest_SHA256.csv | while IFS=, read -r f s h m; do  
    [ "$(sha256sum "$f" | cut -d' ' -f1 | tr a-f A-F)" = "$h" ] || echo "CHANGED:  
    $f"  
done
```

CHAPTER 9

Troubleshooting

What you see	What to do
NOT running as Administrator	Close the window and open it again. Click Yes when Windows asks for permission.
Security log sections FAILED	Needs Administrator. On a domain computer, Group Policy may also limit who can read the Security log.
"running scripts is disabled"	Start the tool with the .exe or .cmd files. They run PowerShell with -ExecutionPolicy Bypass for that run only and change no settings.
Could not open (Win32 error 32)	The page file, hibernation file and swap file are held by Windows itself. They are listed but not mapped.
Cloud/offline placeholder: not opened	The file lives online (OneDrive and similar). It was skipped on purpose.
The full listing takes a long time	A full drive with hashing reads every file once. Expect roughly a minute per 5 GB hashed, more on spinning disks and slow USB sticks.
Linux: hashes or sector map missing	Install or allow python3, and run with sudo.

QUICK REFERENCE

Cheat Sheet

To do this	Do this
Collect everything (window)	Heirloom Evidence Triage.exe, fill in the case, Start Collection
Collect everything (script)	Run Triage (command line).cmd -CaseNumber X -Examiner Y
Quick first look	-MaxFiles 20000 -NoHash
Hash every file	-HashMaxMB 0
Several drives	-Volumes C,D or -Volumes All
Whole event logs too	-ExportEvtx
Linux	sudo bash heirloom_triage.sh -c X -e Y
Prove nothing changed	Re-hash with the manifest (Chapter 8)

QUICK REFERENCE

Glossary

Word	What it means
Chain of custody	The signed record of who held the evidence and when.
Cluster	The smallest piece of disk space a file system hands out (often 4 KB).
Extent / fragment	One unbroken stretch of clusters that holds part of a file.
Hash (SHA-256, MD5)	A fingerprint of a file. Change one byte and it changes.
Hive	One of the files that holds the Windows registry.
LBA / sector	A numbered 512- or 4096-byte block on a disk, counted from 0.
Manifest	The list of every evidence file and its hash.
MFT	NTFS's Master File Table: one record for every file.
O_NOATIME	A Linux way to open a file without changing its access time.
Persistence	The ways a program arranges to start again after a reboot.
Prefetch	Windows files that record which programs ran and when.
Slack space	The unused end of a file's last cluster.
Volatile data	Information that disappears at shutdown, like connections and running processes.