Strategic Rebranding and Maintenance Report: Transitioning Cado-Batch to "Host Evidence Runner"

1. Executive Summary: The Strategic Value of Forensic Tool Maintenance

The landscape of Digital Forensics and Incident Response (DFIR) is in a perpetual state of flux, driven not only by the evolving sophistication of threat actors but also by the consolidation of the cybersecurity market. The acquisition of Cado Security by Darktrace [1] represents a typical lifecycle event in the industry: a specialized cloud investigation vendor is absorbed into a larger autonomous defense ecosystem. While such acquisitions often bolster enterprise capabilities, they frequently leave a vacuum in the open-source community. Tools that were once freely available "community editions" or utility scripts—such as "Cado-Batch" [2]—often face archiving, deprecation, or restricted access as the parent company realigns its intellectual property strategy.

For an aspiring forensic practitioner, this transition presents a high-value opportunity. The archiving of "Cado-Batch" is not a dead end; it is a genesis point for a professional portfolio project. By executing a strategic fork, rebranding, and independent maintenance of this utility, a practitioner demonstrates far more than simple scripting ability. They demonstrate a nuanced understanding of software governance, open-source licensing compliance (specifically Apache 2.0) [4], trademark de-confliction, and the forensic integrity of evidence collection.

This report serves as a comprehensive operational blueprint for transforming the archived "Cado-Batch" script into **"Host Evidence Runner" (HER)**. This transformation—colloquially termed "De-Cadoing"—involves stripping the tool of its commercial affiliations while preserving its core forensic utility. The objective is twofold: to provide the community with a legally unencumbered, maintained legacy collection tool, and to construct a "flagship" portfolio asset that serves as incontrovertible proof of competence for hiring managers in the DFIR sector.

The analysis begins with a rigorous brand risk assessment, rejecting proposed names like "Responder Grab" and "HostSweep" due to critical conflicts with offensive security tools and network nomenclature, effectively reducing the risk of professional embarrassment during interviews. It proceeds to a granular technical refactoring guide, detailing how to modernize the batch architecture for Windows 10/11 compliance while maintaining backward compatibility. Finally, it culminates in a career strategy module, outlining exactly how to leverage "Host Evidence Runner" on resumes and GitHub to secure employment in forensic investigations.

2. Brand Identity and Nomenclature Analysis

In the domain of cybersecurity, naming is an exercise in precision. A tool's name serves as its first line of documentation, signaling its function, scope, and intent. For a forensic professional, using ambiguous or conflicted terminology is a red flag. A hiring manager reviewing a portfolio will assess whether the candidate understands the distinction between "offensive" (Red Team) and "defensive" (Blue Team) terminology. The task of renaming "Cado-Batch" requires a name that is descriptively accurate, legally safe from trademark infringement, and distinct from existing well-known utilities.

The following analysis evaluates the user-proposed candidates against a matrix of risk factors, including trademark collision, offensive tool conflation, and scope inaccuracy.

2.1. Critical Evaluation of Candidate Names

The selection process eliminates candidates that introduce risk or confusion. The "De-Cado" objective [User Query] mandates a neutral name that avoids implying affiliation with Darktrace or Cado Security while establishing a distinct identity.

2.1.1. "Responder Grab" (Critical Failure: High Risk)

The proposal "Responder Grab" represents a significant terminological danger. In the information security community, **Responder** is a ubiquitous and highly recognizable offensive tool written in Python. It is used primarily for Link-Local Multicast Name Resolution (LLMNR), NBT-NS, and mDNS poisoning to capture NTLMv2 hashes and credentials.[5] It is a staple of penetration testing and adversary simulation workflows.[6]

If a defensive practitioner names a forensic collection tool "Responder Grab," it invites catastrophic confusion. An incident responder reviewing a system who sees a process named "Responder" or a directory named "Responder Grab" may assume the host is actively compromised or that a red team engagement is underway. Furthermore, listing a project named "Responder Grab" in a forensic portfolio suggests to an interviewer that the candidate is unaware of standard offensive toolsets.[8] This demonstrates a lack of situational awareness, which is fatal in an interview context.

2.1.2. "TraceKit Collector" (Rejected: Domain Conflict)

"TraceKit" is an established open-source library used for normalizing JavaScript stack traces across different web browsers.[10] While the overlap between web development and digital forensics is minimal, the namespace is polluted. Searching for "TraceKit" leads almost exclusively to debugging tools for web applications.[12]

In a forensic context, "trace" usually refers to "tracing a process" or "trace evidence." However, adopting the name of an existing popular library creates SEO (Search Engine Optimization) friction and implies a focus on application debugging rather than artifact acquisition. It lacks the gravitas required for a legal evidence collection utility.

2.1.3. "HostSweep Collector" (Rejected: Scope Inaccuracy)

Terminology in cybersecurity is specific. A "sweep" typically refers to a network-based reconnaissance activity, such as a "Ping Sweep" or "Port Sweep," used to identify live hosts across a subnet.[13] Palo Alto Networks, for example, defines "Host Sweep" explicitly as a reconnaissance protection metric for detecting vertical or horizontal scans.[15]

The tool in question is a local batch script designed to run on a single endpoint to collect local artifacts.[2] It does not scan the network; it does not "sweep" multiple hosts. Naming it "HostSweep Collector" implies a network capability that the tool possesses, leading to a mismatch between user expectation and tool reality. This technical inaccuracy would be scrutinized during a technical review of the portfolio.

2.1.4. "Forensic QuickCollect" (Rejected: Commercial Dilution)

The term "QuickCollect" is heavily utilized in commercial industries outside of IT. It is a trademarked brand for SKF's vibration monitoring sensors in industrial engineering [16] and Bell & Howell's automated grocery lockers.[18] While these trademarks do not directly compete with digital forensics, using such a generic commercial term dilutes the project's identity. It sounds like a consumer product rather than a specialized forensic utility. Furthermore, generic names often struggle to gain traction in the open-source community because they lack distinctiveness.

2.1.5. "Evidence Lift" (Rejected: Physical Forensics Association)

"Lift" is a term of art heavily associated with physical forensics, specifically the "lifting" of latent fingerprints.[19] Recently, it has also become associated with the "LIFT" system by Forensic Photonics, which deals with C2PA authentication of digital images and cryptographic sealing.[20] Using "Evidence Lift" creates an ambiguity regarding the tool's function. Does it lift fingerprints? Does it cryptographically seal images? Since the tool is a script for copying files and logs, "collection" or "acquisition" are more accurate descriptors than "lift."

2.1.6. "FleetForensics Collect" (Rejected: Infrastructure Implication)

"Fleet" implies centralized management and orchestration, similar to Osquery fleets or Google Rapid Response (GRR).[21] These systems involve agents deployed across thousands of endpoints reporting back to a central server. Cado-Batch is a standalone script intended for ad-hoc, manual execution on a single machine.[3] Naming it "FleetForensics" implies an infrastructure capability—a server, a database, a dashboard—that the script does not provide.

This oversells the tool and sets the user up for disappointment.

2.2. Selection and Rationale: "Host Evidence Runner"

The analysis identifies **"Host Evidence Runner" (HER)** as the optimal brand identity. This name satisfies all requirements for neutrality, accuracy, and professionalism.

Criteria	Assessment for "Host Evidence Runner"
Descriptive Accuracy	**High.** "Host" correctly scopes the tool to a single endpoint. "Evidence" accurately describes the output (MFT, Logs, Hives). "Runner" implies a lightweight execution method (Batch script).
Neutrality	**High.** It avoids conflict with offensive tools (Responder), network terms (Sweep), and physical forensics (Lift). It is a utilitarian name that sounds "safe" to run on a corporate asset.
Conflict Check	**Clear.** No significant open-source projects or commercial forensic tools currently dominate this namespace.
Acronym Potential	**Strong.** "HER" or "Host-ER" allows for easy referencing in documentation (e.g., "Deploy the HER script to the target").
Professionalism	**High.** It sounds like a standard utility in a DFIR toolkit, fitting alongside tools like "KAPE" or "Velociraptor."

Strategic Decision: The project will be rebranded as **"Host Evidence Runner"**. This name will be applied consistently across the repository, script headers, output filenames, and documentation. The rebranding strategy will focus on "running" acquisition tasks on the "host" to secure "evidence," a narrative that aligns perfectly with the tool's function.

3. Legal and Governance Framework: The "De-Cado" Strategy

Successfully "De-Cadoing" the project is not merely a technical task of finding and replacing text strings. It is a legal governance exercise. The original project is licensed under **Apache License 2.0**.[2] This is a permissive license that allows for broad freedom to modify and distribute the software, provided that strict attribution and notice requirements are met.[4] Failure to adhere to these requirements can render the fork illegitimate and potentially expose the maintainer to copyright claims, which would be disastrous for a portfolio intended to demonstrate professional responsibility.

3.1. Apache 2.0 Compliance for Derivative Works

The "Host Evidence Runner" is, in legal terms, a "derivative work" of Cado-Batch. To maintain the fork publicly on GitHub and use it in a portfolio, the following compliance steps are non-negotiable.

3.1.1. Preservation of the LICENSE File

The Apache 2.0 license explicitly states that you must give any other recipients of the Work or Derivative Works a copy of the License.[23]

- **Requirement:** The original LICENSE file from the Cado-Batch repository must remain in the root directory of the new repository. It cannot be deleted or modified.
- **Implication:** Even though the project is now "Host Evidence Runner," the license text remains the standard Apache 2.0 text.

3.1.2. Attribution and Copyright Notices

The license requires the preservation of all copyright, patent, trademark, and attribution notices from the Source form of the Work.[24]

- **Requirement:** You cannot remove the line Copyright (c) 2021 Cado Security (or similar) from the source files.
- **Solution:** You must *append* your own copyright notice to the existing one. This creates a chain of custody for the intellectual property.

3.1.3. The State of Changes

The license requires that you cause any modified files to carry prominent notices stating that you changed the files.[23]

- **Requirement:** The main batch script must include a header explicitly stating that it has been renamed and modified.
- **Implementation:** A "Modification Log" or "History" section in the script header is the standard method for satisfying this clause.

3.2. Brand Separation and Trademark De-Confliction

While the copyright (the code) allows for modification, the trademark (the name "Cado") is different. The user correctly identified that "Cado" implies affiliation.[1] To "De-Cado" the project is to remove the trademark while keeping the code.

- **Removal of Trade Names:** All user-facing text strings in the script (e.g., ECHO Starting Cado Batch...) must be replaced with ECHO Starting Host Evidence Runner....
- **Documentation Disclaimer:** The README must explicitly state that the tool is an independent fork. A standard disclaimer is: *"This project is a derivative of Cado-Batch, originally developed by Cado Security. Host Evidence Runner is independently maintained and is not affiliated with, endorsed by, or connected to Cado Security or Darktrace."*

3.3. Git Release Strategy: The Clean Switch Point

The user proposed a sophisticated release strategy: tagging a release before the rename. This is excellent practice and demonstrates advanced version control skills.

The Workflow:

1. **Clone and Mirror:** Clone the original repo.
2. **Tagging Legacy:** Before making *any* changes, create a git tag to mark the final state of the original code.
   - git tag -a v0.9.0-legacy -m "Final state of upstream Cado-Batch before fork"
   - This preserves the history. If anyone needs the exact original behavior, it is accessible via this tag.
3. **The "De-Cado" Commit:** Perform the renaming, refactoring, and license header updates. Commit these changes.
4. **Tagging New Release:** Create the first release of the new brand.
   - git tag -a v1.0.0 -m "Initial release of Host Evidence Runner"
   - git push origin --tags
5. **GitHub Release:** On the GitHub interface, draft a new release for v1.0.0. Attach the zipped tool as a binary asset. This gives users a clean "switch point" as requested.

3.4. Recommended License Header

The following header block should be placed at the very top of host_evidence_runner.bat to satisfy all legal requirements while establishing the new brand.

Code snippet

```
::
========================================================================
=========
:: HOST EVIDENCE RUNNER (HER)
:: A lightweight, standalone forensic acquisition utility for Windows endpoints.
::
:: Copyright (c) 2025
::
:: This software is a derivative work of "Cado-Batch"
(https://github.com/cado-security/Cado-Batch)
:: Copyright (c) 2021 Cado Security
::
:: Licensed under the Apache License, Version 2.0 (the "License");
:: you may not use this file except in compliance with the License.
:: You may obtain a copy of the License at
::
::     http://www.apache.org/licenses/LICENSE-2.0
::
:: Unless required by applicable law or agreed to in writing, software
:: distributed under the License is distributed on an "AS IS" BASIS,
:: WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
:: See the License for the specific language governing permissions and
:: limitations under the License.
::
========================================================================
=========
:: HISTORY & MODIFICATIONS:
:: - Forked from Cado-Batch. Renamed to Host Evidence Runner.
:: - Updated output naming convention to HER_%HOSTNAME%_%TIMESTAMP%.
:: - Removed proprietary Cado Response import cues.
::
========================================================================
=========
```

4. Technical Refactoring: Modernizing the Collector

The original Cado-Batch was designed for "older Windows systems" [2] and likely optimized for ingestion into the Cado Response platform.[3] To make "Host Evidence Runner" a viable modern portfolio piece, it must be refactored to be platform-agnostic, robust on Windows 10/11, and forensically sound.

4.1. File System and Directory Architecture

A professional tool requires a professional structure. The flat structure of the original repo should be reorganized to separate documentation, resources, and logic.

Proposed Directory Structure:

```
Host-Evidence-Runner/
├── LICENSE (Apache 2.0 Text)
├── NOTICE (Attribution requirements)
├── README.md (Project Documentation)
├── host_evidence_runner.bat (The Core Logic)
├── docs/
│  ├── artifact_manifest.md (Detailed guide on what is collected)
│  └── usage_guide.md (Instructions for Analysts)
└── resources/ (Formerly 'bins')
├── 7za.exe (7-Zip Command Line)
└── (RawCopy, etc.)
```

4.2. Script Modernization and Sanitization

The refactoring process involves three key technical improvements: Dynamic Naming, Output Sanitization, and Binary Verification.

4.2.1. Dynamic Output Naming

The original script outputted to collected_files.zip.[3] In a real investigation involving multiple machines, having every file named identically is a disaster. It leads to evidence overwrites and confusion.
Refactoring: The script must dynamically generate filenames based on the specific machine it is running on.
Code Implementation:

Code snippet

```
:: Get Hostname
FOR /F "usebackq" %%i IN (`hostname`) DO SET HOSTNAME=%%i

:: robust Timestamping (WMIC method for Windows compatibility)
FOR /F "skip=1 tokens=1-6" %%A IN ('WMIC Path Win32_LocalTime Get
Day^,Hour^,Minute^,Month^,Second^,Year /Format:table') DO (
   IF "%%~F"=="" (
      SET Year=%%F
      SET Month=%%D
      SET Day=%%A
      SET Hour=%%B
      SET Min=%%C
   )
)
```

```
:: Pad single digits with leading zeros for ISO 8601 compliance
IF %Month% LSS 10 SET Month=0%Month%
IF %Day% LSS 10 SET Day=0%Day%
IF %Hour% LSS 10 SET Hour=0%Hour%
IF %Min% LSS 10 SET Min=0%Min%

SET TIMESTAMP=%Year%-%Month%-%Day%_%Hour%-%Min%
SET ZIP_NAME=HER_%HOSTNAME%_%TIMESTAMP%.zip
```

Insight: This change alone demonstrates "forensic maturity" to a hiring manager. It shows you anticipate the chaos of an incident and build tools to mitigate it.

4.2.2. Removing Proprietary Hooks

The snippets mention the tool creates files for import into "Cado Response".[3] If the script generates a JSON manifest specific to Cado's schema, it should be generalized.

- **Action:** Review the script for any lines creating metadata.json or similar.
- **Modification:** If the JSON structure is proprietary (using Cado-specific keys), simplify it to a standard key-value pair text file (e.g., system_info.txt) or a generic JSON.
- **Rationale:** The tool should be vendor-neutral. A generic zip file can be ingested by Autopsy [26], generic SIEMs [21], or widely used tools like Zimmerman’s KAPE.

4.2.3. The resources (bins) Directory

Forensic scripts often rely on external binaries (e.g., RawCopy.exe to copy locked files like the Registry). The original repo likely contains outdated versions of these tools.

- **Risk:** Using outdated binaries can introduce vulnerabilities or fail on newer OS versions (e.g., Windows 11 Registry structures).
- **Update:** Replace the binaries in resources/ with the latest stable versions.
- **Verification:** In the README.md, list the SHA-256 hashes of the binaries included. This establishes a "Chain of Trust." An analyst downloading your tool needs to know the binaries inside haven't been backdoored.

5. Forensic Artifact Deep Dive: The "Why" Behind the Collection

To use this project as a demonstration of skills, the documentation must explain *why* these specific artifacts are being collected. This transforms the repository from a code dump into a knowledge base, showcasing the maintainer's expertise. The original Cado-Batch functionality targets high-value Windows artifacts.[25]

The following sections analyze the specific forensic value of the artifacts collected by Host Evidence Runner. This content should be integrated into the docs/artifact_manifest.md of the repository.

5.1. The Master File Table ($MFT)

- **Mechanism:** The script likely uses a raw copy tool to extract $MFT from the root of the NTFS volume. This file is locked by the OS and cannot be copied by standard copy commands.
- **Forensic Utility:** The MFT is the database of every file on the volume. It contains the $STANDARD_INFORMATION and $FILE_NAME attributes for every entry.
- **Investigation Use Case:**
  - **Timestomping Detection:** By comparing the creation timestamps in $SI vs $FN attributes, analysts can detect if a threat actor manually altered file times to hide their tracks.
  - **Deleted File Recovery:** The MFT retains records of deleted files (flagged as unallocated) until they are overwritten, allowing for recovery of file names and paths.

5.2. Windows Event Logs (EVTX)

- **Mechanism:** The script copies C:\Windows\System32\winevt\Logs\*.evtx.
- **Forensic Utility:** These logs act as the flight recorder of the operating system.
- **Key Event IDs to Document:**
  - **Security.evtx:**
    - *4624:* Successful Logon (Who logged in? When? Type 3 for Network, Type 10 for RDP).
    - *4672:* Special Privileges Assigned (Did they get Admin rights?).
  - **System.evtx:**
    - *7045:* Service Installed. This is a primary indicator of persistence. Attackers often install malware as a service to ensure it survives reboots.
  - **PowerShell/Operational:**
    - *4104:* PowerShell Script Block Logging. Captures the actual code executed by attackers, even if obfuscated.

5.3. Registry Hives (SYSTEM, SOFTWARE, SAM, NTUSER.DAT)

- **Mechanism:** These files are also locked and require raw extraction.
- **Forensic Utility:** The Registry is a goldmine of configuration and history.
- **Key Keys to Document:**
  - **SAM:** Contains user account information and NTLM hashes (if not scrubbed).
  - **SYSTEM:** *HKLM\SYSTEM\CurrentControlSet\Enum\USBStor* tracks every USB device ever connected to the machine. Critical for insider threat investigations.
  - **SOFTWARE:** *Microsoft\Windows\CurrentVersion\Run* shows programs set to auto-start.
  - **NTUSER.DAT:** Located in user profiles. Contains *Shellbags* (folder browsing history) and *UserAssist* (GUI execution history).

5.4. Prefetch (*.pf)

- **Mechanism:** C:\Windows\Prefetch\*.pf.
- **Forensic Utility:** Windows creates these files to speed up application launch.
- **Investigation Use Case:** Prefetch proves **execution**. The existence of CMD.EXE-12345678.pf proves cmd.exe was run. It stores the run count and the last 8 execution timestamps (on Win10+). This is vital for proving that a suspect actually ran a malicious tool, rather than just possessing it.

5.5. $UsnJrnl:$J (Update Sequence Number Journal)

- **Mechanism:** Alternate Data Stream (ADS) of the $Extend folder.
- **Forensic Utility:** Records changes to files (Create, Delete, Rename).
- **Investigation Use Case:** Provides a granular history of file operations. It is often used to reconstruct the activity of ransomware, which rapidly renames and modifies thousands of files in a short sequence.

6. Portfolio Integration Strategy: Getting Hired

The ultimate goal of this project is employment. A GitHub repository is passive; the narrative constructed around it determines its value in a job search. To effectively leverage "Host Evidence Runner," the user must present it not just as a script, but as a product of professional engineering.

6.1. Resume Engineering

The resume entry must highlight the *maintenance* and *governance* aspects, not just the coding. This signals maturity to hiring managers.

Draft Resume Entry:

> **Open Source Maintainer | Host Evidence Runner (HER)**
>
> - *Independent maintenance of a forensic acquisition utility derived from the archived Cado-Batch project.*
> - **Governance:** Refactored legacy codebase to ensure strict adherence to Apache 2.0 licensing, implementing proper attribution chains and trademark de-confliction.
> - **Engineering:** Modernized the batch architecture to support Windows 10/11 endpoints, implementing dynamic hostname resolution and timestamped output to prevent evidence collisions in multi-host investigations.
> - **Forensics:** Documented extensive artifact mappings (MFT, Prefetch, EVTX) to map tool capabilities to the MITRE ATT&CK framework, aiding junior analysts in understanding collection scope.
> - **DevOps:** Established a Git release workflow with semantic versioning to

manage the transition from the legacy codebase to the rebranded active branch.

6.2. GitHub Repository Presentation

The README.md is the "sales page" for the developer. It needs to look corporate-grade.

Recommended README Sections:

1. **Badges:** [License: Apache 2.0][Maintenance: Active].
2. **Introduction:** "Host Evidence Runner is a dependency-free, portable forensic triage tool designed for First Responders. It allows for the rapid preservation of volatile data and disk artifacts without requiring installation."
3. **The "Why":** Explain *why* a batch script is still relevant.
    - *Argument:* "In compromised environments, introducing complex dependencies (like Python or.NET) can alter the forensic footprint. HER runs on native Windows binaries, minimizing impact."
4. **Artifact Matrix:** A table listing the artifacts collected and their forensic relevance (derived from Section 5).
5. **Legal Disclaimer:** Explicit statement regarding the fork from Cado Security.

6.3. Interview Preparation

In an interview, the candidate should proactively bring up this project to answer behavioral questions.

- **Question:** "Tell me about a time you identified a process gap."
    - **Answer:** "I noticed a valuable open-source tool, Cado-Batch, was archived and at risk of obsolescence due to a commercial acquisition. I recognized the need for a lightweight, script-based collector for legacy systems, so I forked the project, rebranded it to avoid trademark issues, and updated the dependencies to keep it viable for the community."
- **Question:** "How do you handle open-source licensing?"
    - **Answer:** "I take it very seriously. When I forked Cado-Batch, I ensured I preserved the original Apache 2.0 license file and appended my own copyright notices rather than removing the original authors', ensuring full legal compliance for the derivative work."

7. Future Roadmap and Expansion

To demonstrate forward-thinking, the repository should include a "Roadmap" document. This shows the maintainer is not just preserving code, but planning for the future of forensics.

7.1. Phase 1: PowerShell Hybridization

Batch is limited. The roadmap should discuss a "Hybrid" mode where the Batch script detects if PowerShell is available and safe to run, then launches a child process to use PowerShell cmdlets for more advanced tasks (like interacting with the Azure CLI or hashing files in memory).

7.2. Phase 2: YARA Integration

Adding a step to scan the collected memory dump or specific process handles against a set of critical YARA rules. This moves the tool from "Collection" to "Triage," allowing it to flag potential threats immediately upon execution.

7.3. Phase 3: Cloud Upload

Integrating a secure upload mechanism (e.g., to an S3 bucket with a presigned URL) so that evidence can be exfiltrated directly from the host to a secure cloud repository, bypassing local USB storage which can be a vector for malware transmission.

8. Conclusion

The transformation of "Cado-Batch" into **"Host Evidence Runner"** is a strategic maneuver that elevates a simple technical task into a comprehensive demonstration of professional competency. By navigating the complexities of brand identity, legal compliance, software engineering, and forensic science, the maintainer proves they possess the multifaceted skillset required for modern Digital Forensics and Incident Response.

The choice of name—**Host Evidence Runner**—reflects a disciplined approach to risk management, avoiding the pitfalls of offensive terminology and trademark infringement. The meticulous refactoring of the code ensures the tool remains a reliable asset in the investigator's toolkit. Finally, the positioning of this project within a portfolio provides a compelling narrative of initiative, responsibility, and expertise that will resonate powerfully with hiring managers in the cybersecurity industry.

Report Metadata

- **Subject:** Forensic Tool Rebranding & Maintenance Strategy
- **Primary Tool Name:** Host Evidence Runner (HER)
- **License:** Apache 2.0
- **Target Audience:** DFIR Hiring Managers / Technical Leads

1

Works cited

1. Cado Security - GitHub, accessed December 12, 2025, https://github.com/cado-security
2. Repositories - Cado Security - GitHub, accessed December 12, 2025, https://github.com/orgs/cado-security/repositories

3. cado-security/Cado-Batch: A Batch script to collect forensic evidence from older Windows systems - GitHub, accessed December 12, 2025, https://github.com/cado-security/Cado-Batch
4. Licensing a repository - GitHub Docs, accessed December 12, 2025, https://docs.github.com/articles/licensing-a-repository
5. Responder: Tool for Network Exploitation - Hunt.io, accessed December 12, 2025, https://hunt.io/malware-families/responder
6. LLMNR & NBT-NS Poisoning and Credential Access - Cynet, accessed December 12, 2025, https://www.cynet.com/attack-techniques-hands-on/llmnr-nbt-ns-poisoning-and-credential-access-using-responder/
7. Capturing Hashes with Responder: A Practical Walkthrough | by CyberWarLab - Medium, accessed December 12, 2025, https://medium.com/@CyberWarLab/capturing-hashes-with-responder-49ff21177941
8. meirwah/awesome-incident-response - GitHub, accessed December 12, 2025, https://github.com/meirwah/awesome-incident-response
9. 11 Best Digital Forensics Tools For Evidence Management | Rev, accessed December 12, 2025, https://www.rev.com/blog/digital-forensics-tools
10. TraceKit.Dev: Home, accessed December 12, 2025, https://tracekit.dev/
11. Issues · csnover/TraceKit - GitHub, accessed December 12, 2025, https://github.com/csnover/TraceKit/issues
12. How do we track Javascript errors? Do the existing tools actually work? - Stack Overflow, accessed December 12, 2025, https://stackoverflow.com/questions/20810009/how-do-we-track-javascript-errors-do-the-existing-tools-actually-work
13. Host Sweep Triggering Method in Zone Protection Profile - Palo Alto Knowledge Base, accessed December 12, 2025, https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClZhCAK
14. PaloAlto Host Sweep - Detection rules | ManageEngine Log360, accessed December 12, 2025, https://www.manageengine.com/au/log-management/detection-rules/DETECTION_PALOALTO_PALOALTO_HOST_SWEEP.html
15. Configure Reconnaissance Protection - Palo Alto Networks, accessed December 12, 2025, https://docs.paloaltonetworks.com/ngfw/administration/zone-protection-and-dos-protection/zone-defense/zone-protection-profiles/configure-reconnaissance-protection
16. Field Of View - All Manufacturers - atlis, accessed December 12, 2025, https://atlis.etesters.com/see/11238/Field_Of_View/?page=20
17. FOV - All Manufacturers - 6tl, accessed December 12, 2025, https://6tl.etesters.com/see/11247/FOV/?page=20
18. A Review of Last-Mile Delivery Optimization: Strategies, Technologies, Drone Integration, and Future Trends - MDPI, accessed December 12, 2025,

https://www.mdpi.com/2504-446X/9/3/158

19. Stopping the Craigslist Killer with Digital Forensics: Expert Interview, accessed December 12, 2025, https://www.forensicscolleges.com/blog/forensics-casefile-craigslist-killer
20. AI Threatens Evidence. LIFT Neutralizes Doubt. - YouTube, accessed December 12, 2025, https://www.youtube.com/watch?v=LeAU1ANC5xI
21. Top 7 OSS Incident Response Tools [By Category] - Wiz, accessed December 12, 2025, https://www.wiz.io/academy/top-oss-incident-response-tools
22. The Power User's Guide to Open-Source Licenses - Heavybit, accessed December 12, 2025, https://www.heavybit.com/library/article/power-users-guide-open-source-licenses
23. The Complete Guide to Open Source Licenses | FOSSA Learning Center, accessed December 12, 2025, https://fossa.com/learn/open-source-licenses/
24. Complete guide to open source licenses for developers. Friendly licenses for proprietary software - DEV Community, accessed December 12, 2025, https://dev.to/oborys/complete-guide-to-open-source-licenses-for-developers-3j5e
25. What Log and Artifact Types Can / Forensic Acquisition and Investigation Process? - Cado Security, accessed December 12, 2025, https://docs.cadosecurity.com/cado/discovery-import/data-types/logs
26. Digital Forensics: Get Started with These 9 Open Source Tools - BlueVoyant, accessed December 12, 2025, https://www.bluevoyant.com/knowledge-center/get-started-with-these-9-open-source-tools
27. Forensic Evidence Collection From Windows Host Using Python Based Tool - IEEE Xplore, accessed December 12, 2025, https://ieeexplore.ieee.org/document/9989295/
28. EN - SKF Enlight ProCollect Brochure | PDF | Cloud Computing - Scribd, accessed December 12, 2025, https://www.scribd.com/document/784809405/18606-EN-SKF-Enlight-ProCollect-Brochure