SURGE Beta – Triage Artifact Collection Guidance

Overview

SURGE analyzes **forensic artifacts**, not telemetry. To ensure consistent results, all uploads must follow the SURGE Artifact Profile below. Customers must collect artifacts using their own DFIR workflows and licensed tools. SURGE only defines what the resulting ZIP archive must contain.

---

1. Supported OS (Beta)

Windows only.
Linux and macOS support will be added later.

---

2. Required Artifacts

Please gather the following artifacts

MFT
/$MFT

Windows Tasks
/Windows/System32/Tasks/*

System Registry Hives
/Windows/System32/config/SYSTEM
/Windows/System32/config/SOFTWARE
/Windows/System32/config/SAM
/Windows/System32/config/SECURITY

Hosts File
/Windows/System32/drivers/etc/hosts

SRUM DB
/Windows/System32/sru/SRUDB.dat

PCA Launch Items
/Windows/appcompat/pca/PcaAppLaunchDic.txt

EVTX logs
/Windows/System32/winevt/Logs/*.evtx

Prefetch Files
/Windows/Prefetch/*.pf

Windows Defender
/ProgramData/Microsoft/Windows Defender/Scans/History/*.log|*.dat
/ProgramData/Microsoft/Windows Defender/Support/*.log|*.dat

App Compatibility logs
/ProgramData/Microsoft/Windows/Application Compatibility/*.xml|*.log

Browser Histories
/User/<user>/AppData/Local/Google/Chrome/User Data/Default/History
/User/<user>/AppData/Local/Microsoft/Edge/User Data/Default/History
/User/<user>/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat
/User/<user>/AppData/Roaming/Opera Software/Opera Stable/Default/History
/User/<user>/AppData/Roaming/Mozilla/Firefox/Profiles/places.sqlite

User Registry Hive
/User/<user>/NTUSER.DAT

Automatic/Custom Dest
/User/<user>/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations/*.automaticdestinations-ms
/User/<user>/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations/*.customdestinations-ms

In the future, we will consider a different level of analysis that will include files like the Master File Table. If this is something that would be beneficial, or you have additional use cases for analysis, please make a feature request in the Discord.

---

3. ZIP Archive Requirements

- **ZIP file only** (no RAR/7z/tar)
- Do **not** password-protect
- 300 MB max upload
- Preserve original artifact filenames

Folder Structure Guidance

Any folder structure is accepted, **but preserving the original Windows file path structure inside the ZIP is strongly recommended.**

Doing so gives the analysis engine additional context and helps improve artifact classification, correlation, and timeline reconstruction.

Example of path-preserving layout (not required):

```
C:/Windows/System32/config/SYSTEM
C:/Windows/System32/config/SOFTWARE
C:/Windows/System32/config/SAM
C:/Windows/System32/winevt/Logs/Security.evtx
C:/Windows/System32/winevt/Logs/System.evtx
```

SURGE will still process artifacts regardless of layout—this is a best practice, not a requirement.

---

4. General Collection Principles (Vendor-Agnostic)

- Collect artifacts from a **consistent point in time**
- Avoid modifying artifacts prior to collection
- Preserve original filenames
- Use your organization's **approved DFIR tools**
- Ensure compliance with all tool **license terms**

SURGE does **not** provide instructions for specific collectors.