



SURGE Beta Tester Walkthrough Guide

For early SURGE beta participants

1. Welcome to the SURGE Beta

Thank you for participating in the SURGE beta program. This guide walks you through everything you need to begin testing SURGE, including account access, running forensic analyses, reviewing results, submitting bugs, providing feedback, using SURGE credits, and navigating the SURGE Discord.

The goal is to make this experience simple and predictable. If anything feels confusing, unclear, or unexpected, message us in Discord.

2. What SURGE Is

SURGE automates host-based digital forensics. Instead of relying on logs or assumptions, SURGE analyzes real forensic artifacts such as registry hives, file system metadata, event logs, and execution traces to determine what actually occurred on a system.

SURGE provides two primary capabilities:

Automated Forensics

SURGE performs triage forensic analysis on systems where you collect artifacts. SURGE reconstructs system activity, highlights anomalies, identifies persistence mechanisms or compromise indicators, and produces clear, evidence-backed results in minutes.

Automated Forensic Assurance (AFA)

SURGE continuously verifies the integrity of critical systems. By repeatedly analyzing forensic evidence, SURGE enables security teams to maintain ongoing assurance that high-value assets like domain controllers, identity infrastructure, and build servers remain uncompromised.

The outcome is fast, scalable forensic truth available across every investigation.

3. What This Beta Is

This beta program allows us to validate the following areas:

- Quality and clarity of triage forensic analysis
- Ease of the upload and analysis workflow
- Usefulness of report content including timelines, evidence summaries, and recommendations
- The types of bugs and edge cases encountered in real-world testing
- General product usability and user expectations

This is an early-stage beta, so bugs or rough edges are expected. The user interface is not at its end state.

Please report any issues in the Discord. Please see below in Section 5

4. Getting Started Checklist

Before you begin, confirm the following:

- ☐ You have your SURGE beta login details
- ☐ You have access to the SURGE Discord community
- ☐ You are able to generate test forensic collections
- ☐ You are using a modern browser such as Chrome or Edge

5. Discord Workflow

The SURGE Discord community is where beta testers collaborate, report issues, request features, learn how the platform works, and track their contributions. You will get a private Discord invite link in email.

When you join the server, you will see several channels that support different parts of the beta program.

The **general** channel is a place for open discussion about SURGE, DFIR, and anything related to the product or security operations.

The **support** channel is where you can ask questions; each time you post there, a dedicated support thread is automatically created for you.

All follow-up conversation should happen inside your own thread. If another user provides a helpful answer, you can react with 🌟 to reward them, and when your question is resolved you can react with 🟡 to mark the thread as solved.

The **bug-reports** channel is reserved for submitting issues using the `/bug` command. The **feature-requests** channel is where you can share product ideas or enhancements using the `/feature_request` command.

A dedicated **leaderboard** channel displays the top contributors in the community, updated automatically. Finally, the **how-to-guides** channel contains walkthroughs and educational materials to help you make the most of the platform.

To make Discord participation productive, several slash commands are available. The `/bug` command submits an official bug report to the SURGE team. The `/feature_request` command submits a new feature idea and makes it eligible for community voting. The `/points` command shows your personal point total and current tier. The `/my_issues` command lists your submitted bugs and feature requests, and `/top_features` shows the highest-voted feature ideas across the community.

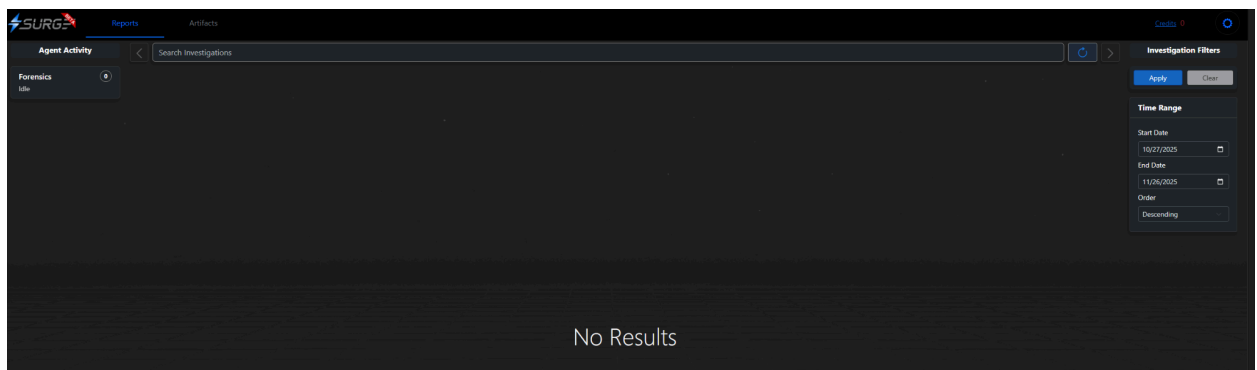
The community uses a point system to recognize valuable contributions. An approved bug report earns 100 points. An approved feature request earns 50 points. Helping another user in a support thread, validated by a moderator using the 🌟 reaction, earns 25 points. Voting on a feature request grants 5 points to the creator of that feature. As points accumulate, you unlock tiers that appear both in Discord and in the leaderboard. The **Seeker** tier begins at 200 points, **Analyst** at 500, **Forensic Lead** at 1000, **Hunter** at 2500, and **Master** at 5000. These roles update automatically based on your total points.

Feature voting is an important part of shaping the product roadmap. In the feature-requests channel, you can react with 📝 to indicate interest in an idea. Each vote contributes points to the user who created that feature request, allowing the community to collectively elevate the most valuable improvements. Helping other testers works the same way: in the support channel, moderators can react with ⭐ on a helpful message to award points to the user who assisted.

Your standing in the program is visible through the **leaderboard** channel, where the top 25 contributors are displayed in real time. You can check your own ranking and tier at any time using the `/points` command. The combination of helpful contributions, bug discovery, and product ideas all feed into your total point score.

6. Account Access

1. Open the SURGE login page included in your invite email. It will come from support@surge.security.
2. Enter your email address and create a password
3. Accept the legal terms and conditions
4. You will land on the SURGE Dashboard.

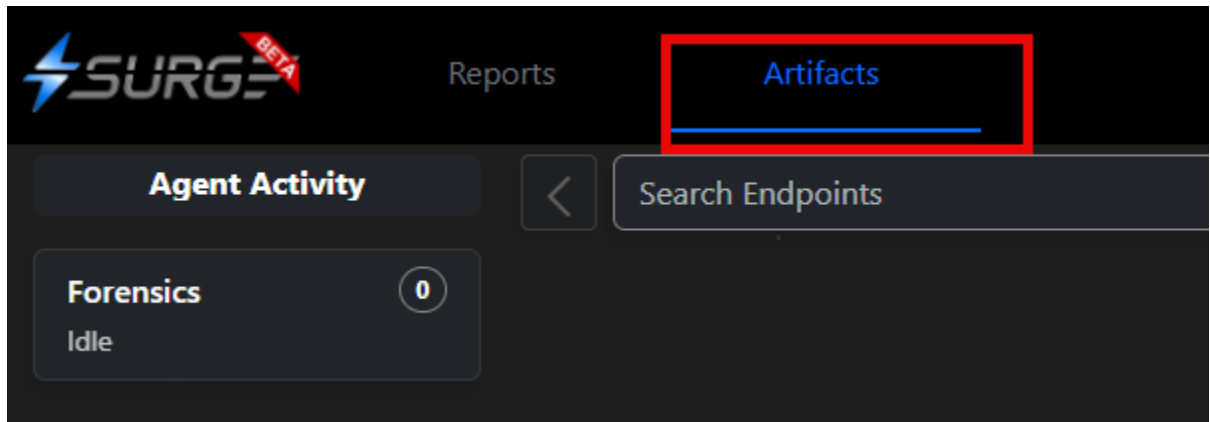


5. If you have access issues, message the SURGE Team in the Discord.
-

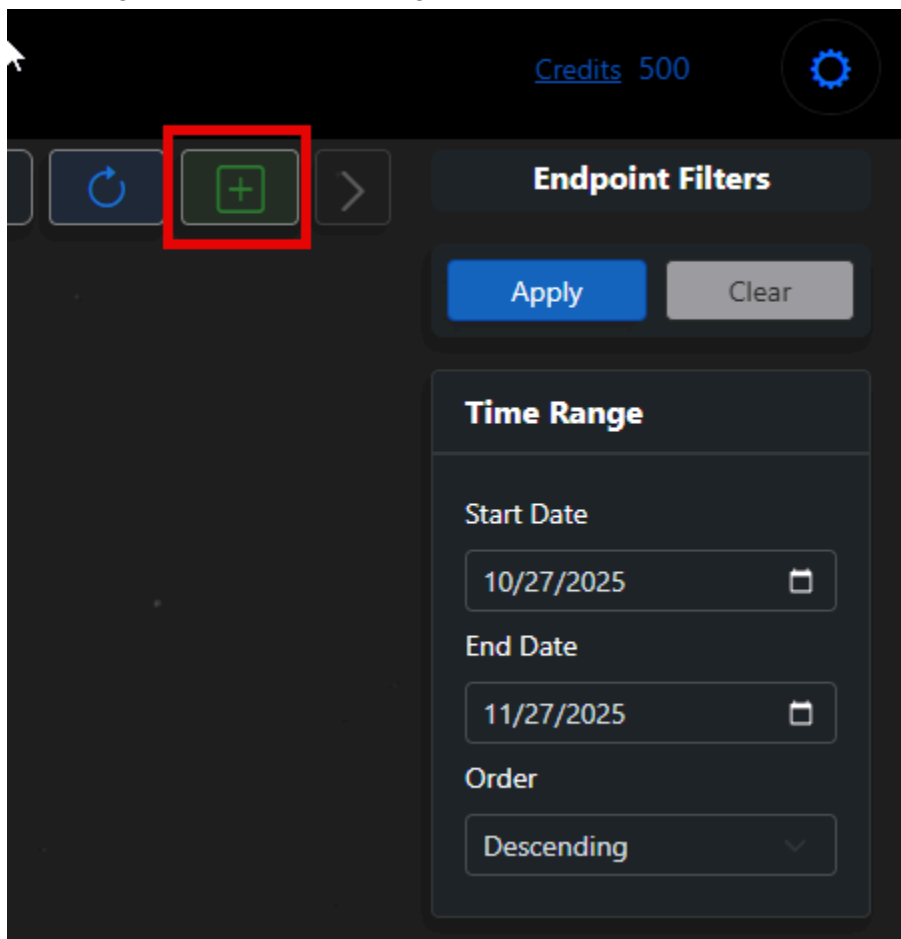
6. Uploading Forensic Collections

SURGE will accept zip files of artifacts. Retaining the original file path structure in the zip file is ideal.

1. Navigate to Artifacts



2. On the right hand side, find the green add button



- 3.

4. Upload your forensic package zip file. Enter a Hostname representative of the endpoint that you are uploading the forensic package from.

Add Endpoint

Hostname

Hostname Goes Here


Hostname

Windows

OS

Triage - 10 Credits - 10-15 Minutes

Effort

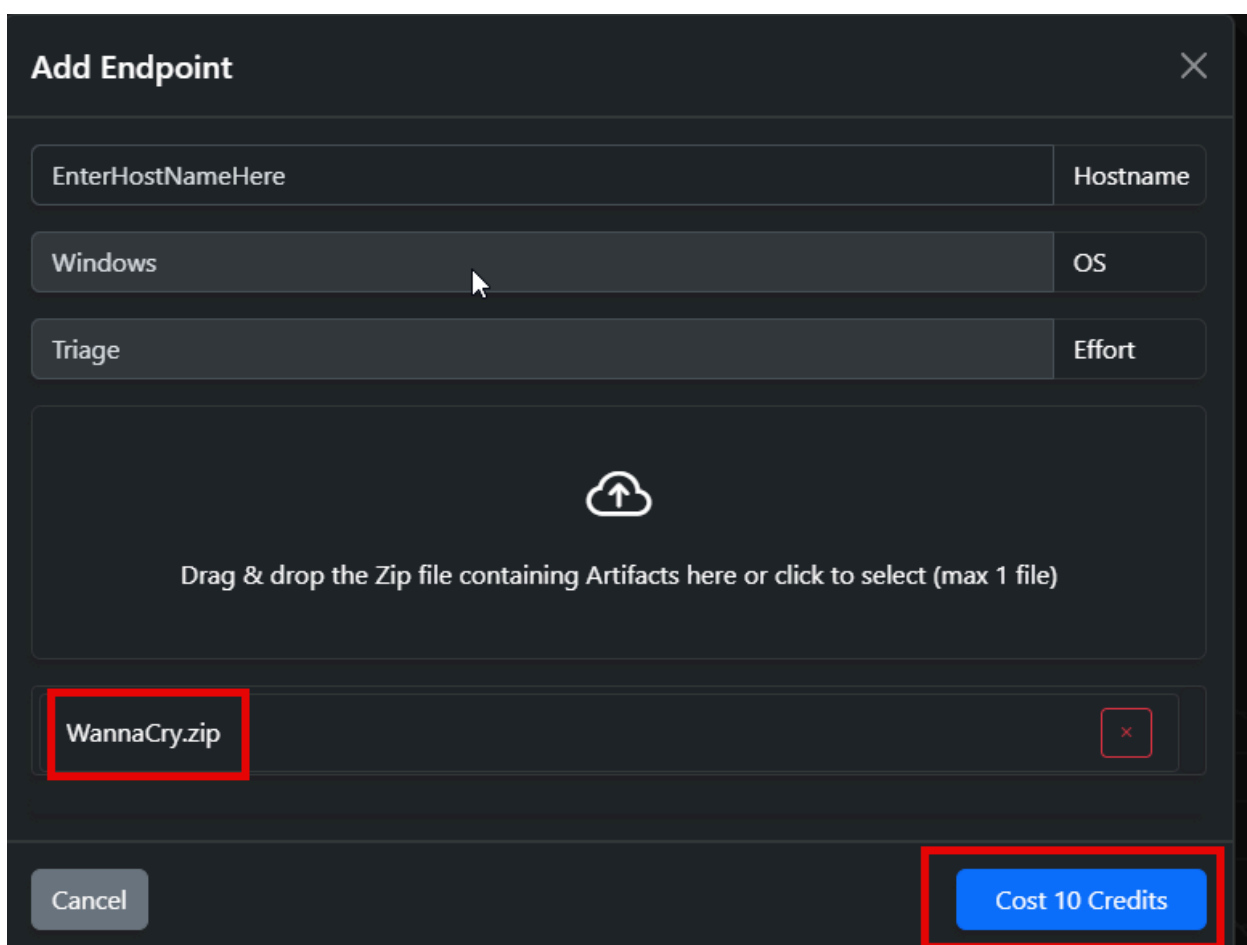
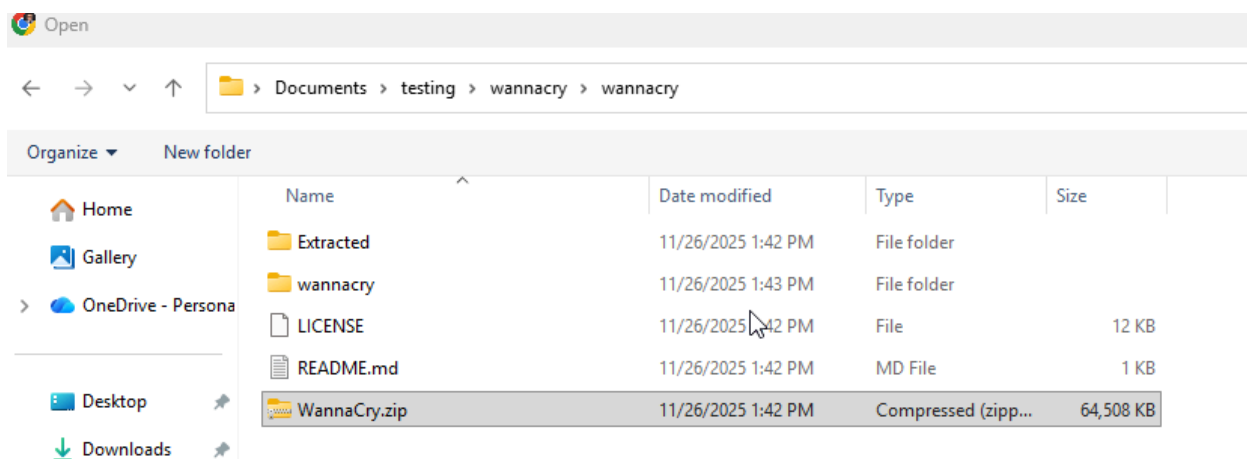


Drag & drop a Zip archive file containing Windows Artifacts here or click to select.
The archive **must** contain:

- SYSTEM Registry Hive
- SOFTWARE Registry Hive
- SAM Registry Hive
- Security.evtx XML Event Log
- System.evtx XML Event Log

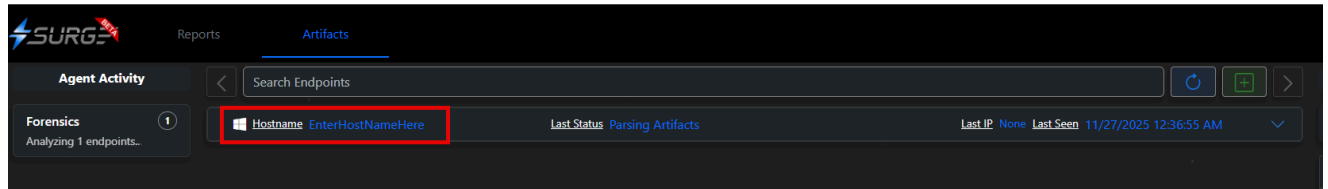
Cancel

Cost 10 Credits



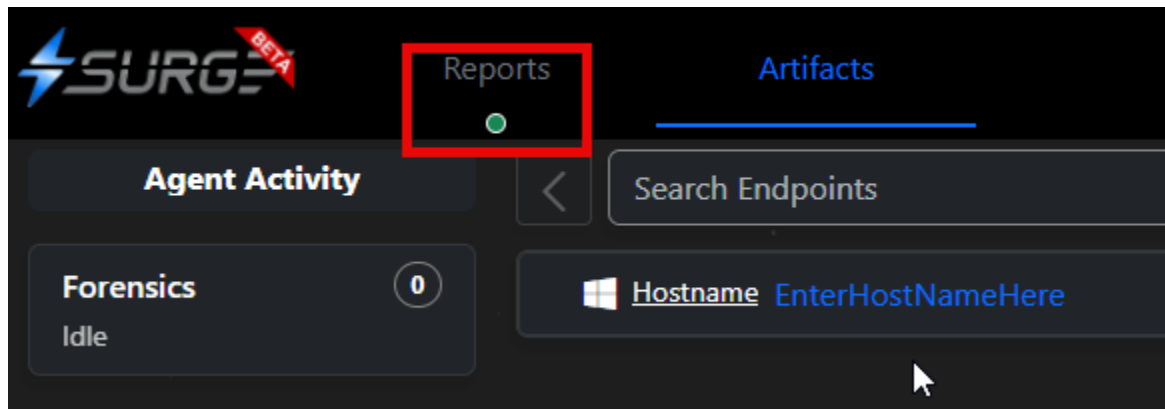
In the above example, WannaCry.zip has the forensic artifacts. It will cost 10 credits to run.

You will now see the entered hostname in the list under “artifacts”

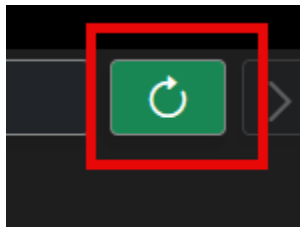


You may add another host, as many as you would like. Just be mindful of credits. You will not be able to upload and analyze once credits have been exhausted.

When the report has been generated you will notice a little green indicator under “Reports”

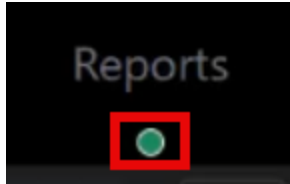


When pivoting over, hit the refresh button

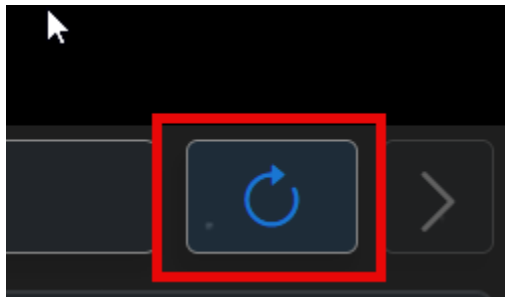


7. Reviewing Results in SURGE

Once you upload your artifacts collection, SURGE automatically begins processing. You are free to work on other things during analysis. After about 10 minutes you may see a green notification under “Reports”, indicating one of the investigations is done.



Pivot over to the reports tab, and hit the refresh button:



You will now see corresponding reports that have completed. Clicking on one of them will expand it

Hostname EC2AMAZ-D47M9TJ Last Timestamp 11/28/2025 9:29:53 PM

Remote desktop session with mi...
AMI Build Process Cleanup

EC2AMAZ-D47M9TJ

OS: Windows
IP: 10.0.19.151
Start UTC: 3/24/2023 12:26:40 PM
End UTC: 3/24/2023 12:37:20 PM
Effort: Triage
Classification: Remote desktop session with mixed activity

[Executive Summary](#) [Summary](#) [Analysis](#) [Timeline Events](#)

Executive Summary

Key Observations and Findings

On March 24, 2023, between 12:26 UTC and 12:37 UTC, a remote desktop session was established from external IP address 79.173.135.242 to the Windows Server 2022 system EC2AMAZ-D47M9TJ. The Administrator account was accessed via remote interactive login. During this session, a file named OpenMe.exe located in a directory called OpenMeTotallyLegit on the Administrator's desktop was executed. Concurrent with this execution, a text file named @Please_Read_Me@.txt from the same directory was accessed. Additionally, the forensic acquisition tool gkape.exe was executed from the desktop during the same timeframe.

The timeline shows:

- Remote desktop connection established from 79.173.135.242 at 12:26:50 UTC
- Administrator login via remote interactive session at 12:26:57 UTC

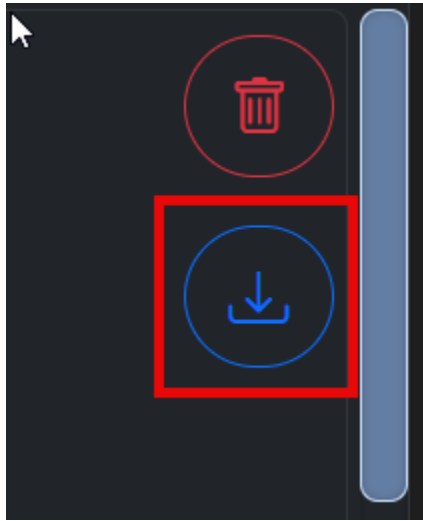
There are different observable grouping of activities on the left that you can review. You will then have different types of analysis.

Highlighted items in pink are evidence pulled from the host artifacts.

The executive summary has Recommended Next Steps that would be congruent with a forensic analyst drafting a report.

There are more detailed evidence collections in the Summary and Analysis tabs, along with a timeline in the Timeline Events tab.

Reports are downloadable with the download button



8. Using SURGE Credits

SURGE Credits allow beta testers to perform the triage analysis, in parallel if so desired.

During the beta:

- You will receive an initial number of credits
- Credits are consumed each time SURGE processes an artifact collection
- Paying users may request an invoice to purchase additional credits

Credits help manage system load while still giving you freedom to test different scenarios.

9. Reporting Bugs

To report a bug during the beta, you will use the dedicated bug-reports channel in Discord. This channel does not allow normal typing, and all issues must be submitted through the `/bug`

command. Begin by navigating to the bug-reports channel, then type `/bug` to open the bug submission form. The form will prompt you for a title, a description of the problem, the steps required to reproduce it, the expected result, and the actual result you observed. You may optionally attach screenshots or logs if they do not include sensitive information. The more specific your explanation is, the easier it is for the SURGE team to reproduce and validate the issue.

Once you submit the form, the SURGE bot will automatically generate an embedded bug entry inside the bug-reports channel. This includes creating a linked entry in our Notion bug database with the status set to “Submitted.” The SURGE team then reviews the report. If the bug is valid, an administrator will react to your submission with the ladybug emoji (🐞). This reaction signifies approval of the report. When the bug is approved, its status changes to “Accepted,” you automatically receive 100 SURGE points, and your tier updates if applicable. You will also receive a confirmation message from the system.

You can track the progress of all of your submitted bugs at any time by using the `/my_issues` command. This will show every bug and feature request you have filed along with the current status of each.

10. Submitting Feature Requests

To suggest new ideas or improvements for SURGE, you will use the feature-requests channel in Discord. This channel does not allow normal typing, and all feature ideas must be submitted through the `/feature_request` command. Start by opening the feature-requests channel, then type `/feature_request` to launch the submission form. The form will ask for a title, a clear problem statement, your proposed solution, the value this improvement would bring to investigators, and optionally any workaround you are currently using. You may include any additional details that help us understand the intent behind your request. Providing specific, thoughtful input ensures the SURGE team can accurately assess the idea.

After submitting the form, the SURGE bot will automatically post your request in the feature-requests channel and create a linked entry in our Notion database with the status set to “Submitted.” A SURGE administrator will then review the request. If the idea is valid and meets the program criteria, an admin will react to your submission with the pencil emoji (✎). This reaction confirms that the request has been accepted. When approved, the status changes to “Accepted,” you receive 50 SURGE points, and your tier updates automatically. You will also receive a confirmation message.

Feature voting helps prioritize the most valuable ideas. Anyone in the community can vote by reacting with the pencil emoji in the feature-requests channel. To track all of your submitted feature requests and bug reports, you can use the `/my_issues` command, which displays every issue you have created along with its current status.

11. Known Beta Limitations

As this is SURGE's beta release, there are items we are aware of that we'd like to disclose:

- Very large packages may take longer than expected
- Some results may have minor formatting issues
- The timeline view may expand in future iterations
- Certain artifact families may not have full interpretation yet
- The user interface will continue to evolve, and is not finished yet.

These limitations will be updated as the beta progresses.

12. FAQ

1. What artifacts can I upload?

SURGE analyzes real forensic artifacts, including:

- EVTX event log files
- Windows Registry Hives
- SRUM Database
- PCA Launch Items List
- Windows Prefetch
- Scheduled Tasks
- Automatic Destinations Jumplists
- Chrome and Edge browser history
- LNK Files

SURGE supports multiple collection methods. You may use the SURGE Collector (in

development) or Velociraptor. If your organization already uses another Windows artifact collector, such as KAPE, we can ingest the resulting ZIP. SURGE does not provide guidance or instructions on the use of these third party tools. Customers are responsible for ensuring their use of any third party tool complies with that tool's licensing terms..

2. How long does analysis take?

Investigations on average take about 10 minutes for a triage forensic analysis.

3. What does SURGE do with my data?

SURGE collects and analyzes forensic artifacts you submit to produce a triage forensic report similar to a human. It will parse the evidence you provide, and display evidence in a resulting report, highlighting evidence in pink. Your data is segregated and not shared with any other individuals other than the SURGE team.

4. How long is data retained?

SURGE retains **raw forensic artifacts for 7 days**, after which they enter **soft delete**. This means the data is no longer accessible to users but can still be restored within the cloud provider's soft-delete window.

5. Does SURGE require an agent?

SURGE does not require an agent. We support artifact collection through other means. In the very near future SURGE will have its own collector, which will be a "dissolveable", non-permanent agent similar to other industry collection tools.

A zip file of artifacts is accepted, retaining the original file path structure in the zip file is ideal.

6. How do credits and billing work?

SURGE credits are the currency that is consumed in order to get forensic analysis done. Beta customers get a predefined amount of credits to help with testing as a thank you for joining the

program. Paying customers will get a certain amount of credits based on the tier that they will purchase.

7. Where do I submit bugs or feature requests?

Feedback related to SURGE should be discussed in the SURGE Discord where it will be logged and addressed by the SURGE team asap.

Bugs can be submitted here—

<https://discord.com/channels/1438299656164479006/1441113801335378111>

Feature requests can be submitted here —

<https://discord.com/channels/1438299656164479006/1441113803499507932>

8. Where do I get support?

Support for SURGE should be requested in the SURGE Discord. This allows the SURGE team to keep track of requests, and allows the community to answer if possible.

Instructions on support can be found here —

<https://discord.com/channels/1438299656164479006/1442158595700559915>

The support channel is here —

<https://discord.com/channels/1438299656164479006/1441572299328327814>

9. Can I upload real production data?

Yes, but redact identifiable details. Do not upload regulated data such as PHI or PCI.

10 Can I share the reports with my team?

Yes, the outputs are designed for internal sharing.

13. Thank You

Your testing and feedback directly shape the future of SURGE. We appreciate your involvement and encourage you to share everything you notice, whether big or small. We're excited you're working with us, and this would not be possible without you!