

**Intern ID: 211**

**Name: Rudra Rajendra Sawant**

**Tool Name: Chaos and Cenysys**

## **History**

A digital forensics tool used for extracting and analyzing browser history, user activities, and artifact timelines from various sources.

Description: What Is This Tool About?

History parsing tools recover and reconstruct web activity data from browsers, helping investigators trace user behavior and access patterns.

## **Key Characteristics / Features:**

- \* Extracts history from Chrome, Firefox, Edge, Safari.
- \* Supports Windows, macOS, and Linux.
- \* Timeline reconstruction.
- \* Supports SQLite, JSON, and proprietary formats.
- \* Keyword-based filtering.
- \* Export in CSV, HTML, or JSON.
- \* Supports bookmark and download extraction.
- \* Session-based sorting.
- \* Multilingual URL detection.
- \* Timestamps with timezone correction.
- \* Visualization charts.
- \* Portable, no installation required.
- \* Command-line and GUI options.
- \* Supports automation scripts.
- \* Metadata enrichment features.

## **Types / Modules Available:**

- \* BrowserHistory Viewer.
- \* Browse Timeline Builder.
- \* Download History Extractor.
- \* Bookmark Analyzer.
- \* Session Reconstruction.
- \* SQLite Parser Module.

## **How Will This Tool Help?**

- \* Maps Browse behavior.
- \* Links user intent and digital trails.
- \* Tracks specific keyword or domain-based access.
- \* Supports cross-device and cross-platform investigation.
- \* Reconstructs user session lifecycle.
- \* Evidence gathering for legal/compliance audits.

Proof of Concept (PoC) Images:

- http.tls.certificates.leaf\_data.tbs.fingerprint
- http.response.headers.Set-Cookie.headers
- http.body\_hash

Nov 09, 2023 07:36 PM UTC

Hurricane Electric

Service Added

80/TCP/HTTP

Nov 09, 2023 04:27 PM UTC

Hurricane Electric

Service Observed

443/TCP/HTTP

Changed Fields

- http.response.body
- http.response.body\_hashes
- banner
- banner\_hashes
- http.response.headers.Set-Cookie.headers
- http.body\_hash

Nov 08, 2023 08:03 PM UTC

Location Updated

Nov 08, 2023 08:03 PM UTC

Routing Updated

Nov 08, 2023 08:03 PM UTC

Hurricane Electric

Service Added

443/TCP/HTTP

Nov 07, 2023 06:47 PM UTC

Service Removed

443/TCP/HTTP

Reason

Expired

Nov 05, 2023 08:35 PM UTC

DNS Name Resolved to Host

www.daftar.pt-aab.my.id [AAAA]

Nov 02, 2023 06:30 PM UTC

DNS Name Resolved to Host

daftar.pt-aab.my.id [AAAA]


Oct 25, 2023 07:27 PM UTC

DNS Name Resolved to Host

nt-aah mv id [AAAA]

SHOW ALL OBSERVATIONS

COMPARE



Hosts

2001:df0:27b:2::6:14b

Search

RH

- http.tls.certificates.leaf\_data.tbs\_fingerprint
- http.response.headers.Set-Cookie.headers
- http.body\_hash

Nov 09, 2023 07:36 PM UTC

Hurricane Electric

Service Added

80/TCP/HTTP

Nov 09, 2023 04:27 PM UTC

Hurricane Electric

Service Observed

443/TCP/HTTP

Changed Fields

- http.response.body
- http.response.body\_hashes
- banner
- banner\_hashes
- http.response.headers.Set-Cookie.headers
- http.body\_hash

Nov 08, 2023 08:03 PM UTC

Location Updated

Nov 08, 2023 08:03 PM UTC

Routing Updated

Nov 08, 2023 08:03 PM UTC

Hurricane Electric

Service Added

443/TCP/HTTP

Nov 07, 2023 06:47 PM UTC

Service Removed

443/TCP/HTTP

Reason

Expired

Nov 05, 2023 08:35 PM UTC

DNS Name Resolved to Host

www.daftar.pt-aab.my.id [AAAA]

Nov 02, 2023 06:30 PM UTC

DNS Name Resolved to Host

daftar.pt-aab.my.id [AAAA]

Oct 25, 2023 07:27 PM UTC

DNS Name Resolved to Host

nt-aah mv id [AAAA]

SHOW ALL OBSERVATIONS

COMPARE

## 15-Liner Summary:

- \* Parses local browser databases.
- \* Supports multiple browsers and OS.
- \* Creates an activity timeline.
- \* Allows search/filter by keyword.
- \* Works with deleted artifacts.
- \* Portable execution supported.
- \* Ideal for LEA and corporate IR teams.
- \* Simple GUI and CLI available.
- \* Metadata and session data included.
- \* Visualization for easy reporting.
- \* Bookmark analysis module.
- \* Supports multiple export formats.
- \* Works with volatile memory dumps.
- \* Automatable with Python/Batch.
- \* Maintained and regularly updated.

## **Time to Use / Best Case Scenarios:**

- \* During initial timeline reconstruction.
- \* After drive acquisition/image parsing.
- \* Before the browser cache is cleared.
- \* Early in threat actor profiling.
- \* During internal HR investigations.

## **When to Use During Investigation:**

- \* Post breach timeline reconstruction.
- \* Insider threat tracking.
- \* Child exploitation cases.
- \* Phishing investigation.
- \* Employee misuse of resources.
- \* Malware Command & Control tracking.

## **Best Person to Use This Tool & Required Skills:**

- \* Best User: Digital Forensics Examiner / Cybercrime Analyst.
- \* Required Skills:
  - \* Understanding of browser internals.
  - \* Basic SQL and JSON parsing.
  - \* Familiarity with timeline reconstruction.
  - \* Use of forensic suites like Autopsy/X-Ways.

## **Flaws / Suggestions to Improve:**

- \* Lacks cloud-sync history parsing.
- \* Real-time monitoring is not available.
- \* Add hash validation for integrity.
- \* Improve visualization with AI insight.

- \* Add a plug-in for encrypted browser profiles.

## **Good About the Tool:**

- \* Lightweight and portable.
- \* High compatibility across platforms.
- \* Easy export and reporting.
- \* Fast parsing with minimal resource usage.
- \* Detailed forensic insights on browser usage.

## **For each tool (Chaos and Censys):**

- \* Tool Name: Clearly state the name (Chaos, Censys).
- \* History:
  - \* When was it developed?
  - \* By whom?
  - \* What problem was it designed to solve?
  - \* Key milestones in its development.
- \* Description: What Is This Tool About?
  - \* Provide a clear, concise explanation of the tool's primary purpose.
  - \* What kind of data does it collect or analyze?
  - \* What industry/field is it primarily used in (e.g., cybersecurity, threat intelligence, asset discovery)?
- \* Key Characteristics / Features:
  - \* List all major features.
  - \* What are its unique selling points compared to similar tools?
  - \* Mention supported protocols, data types, integration capabilities, etc.
- \* Types / Modules Available:
  - \* Does the tool have different versions (e.g., community, enterprise)?
  - \* Are there specific modules or functionalities that can be used independently or in conjunction?
- \* How Will This Tool Help?
  - \* Describe the benefits and use cases for individuals or organizations.
  - \* How does it improve efficiency, security, or decision-making?
- \* Proof of Concept (PoC) Images:



- \* Crucially, you need to find or create screenshots that demonstrate the tool in action. For Chaos, this might be showing subdomains found. For Censys, it could be search results, vulnerability reports, or asset inventory.

- \* Aim for 5-10 clear screenshots for each tool.

- \* Add captions to explain what each screenshot illustrates.

- \* 15-Liner Summary:

- \* Condense the most important aspects of the tool into 15 bullet points, covering its function, benefits, and key features.

- \* Time to Use / Best Case Scenarios:

- \* When is the tool most effective or necessary?

- \* Provide specific examples of scenarios where it would be the ideal choice.

- \* When to Use During Investigation:

- \* In which phases of a cybersecurity investigation or incident response would this tool be leveraged?

- \* Give concrete examples (e.g., initial reconnaissance, vulnerability assessment, post-compromise analysis).

- \* Best Person to Use This Tool & Required Skills:

- \* Who is the ideal user (e.g., Security Analyst, Penetration Tester, Red Teamer, Blue Teamer, Threat Hunter)?

- \* What technical skills (e.g., networking, scripting, OS knowledge, specific domain expertise) are required to effectively use the tool?

- \* Flaws / Suggestions to Improve:

- \* Identify any limitations, weaknesses, or areas where the tool could be enhanced.

- \* Think critically about user experience, data accuracy, coverage, or integration.

- \* Good About the Tool:

- \* Highlight its strengths and advantages.

- \* Why would someone choose this tool over alternatives?

Formatting Tips for your actual report (which you'll create in Word/PDF):

- \* Page Numbers: Ensure page numbers are added to the bottom right or top right corner of each page.

- \* Professional Layout: Use clear headings, subheadings, and bullet points. Maintain consistent formatting throughout.

- \* Images: Embed your PoC images directly into the document and ensure they are clearly visible and captioned.
- \* Table of Contents: For a 10-page report, a table of contents would be beneficial.
- \* Introduction and Conclusion: Add a brief introduction and conclusion to tie everything together.