POC of Tools

🛠️ Tool Name:

History

Description:

What Is This Tool About?

Key Characteristics / Features:

Types / Modules Available:

How Will This Tool Help?

Proof of Concept (PoC) Images:

15-Liner Summary:

Time to Use / Best Case Scenarios:

When to Use During Investigation:

Best person to use that tool and what skills required

flaws suggestion to improve in that tool

good about tools

🛠️ Tool Name:

History

📄 Description:

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

📌 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
- Browsing Timeline Builder
- Download History Extractor
- Bookmark Analyzer
- Session Reconstruction
- SQLite Parser Module

🎯 How Will This Tool Help?

- Maps browsing 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:

📸 *(Insert 10 screenshots showing timeline visualization, browser artifacts parsed, and keyword-based filtering)*

📄 15-Liner Summary:

1. Parses local browser databases
2. Supports multiple browsers and OS
3. Creates an activity timeline
4. Allows search/filter by keyword
5. Works with deleted artifacts
6. Portable execution supported
7. Ideal for LEA and corporate IR teams
8. Simple GUI and CLI available

9. Metadata and session data included
10. Visualization for easy reporting
11. Bookmark analysis module
12. Supports multiple export formats
13. Works with volatile memory dumps
14. Automatable with Python/Batch
15. Maintained and regularly updated

⏱️ Time to Use / Best Case Scenarios:

- During initial timeline reconstruction
- After drive acquisition/image parsing
- Before 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 not available
- Add hash validation for integrity
- Improve visualization with AI insight
- Add 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