IDR IFPS Tools - Proof of Concept (PoC)

Tool Name:

IDR IFPS Tools

History:

IDR IFPS Tools were developed as part of an initiative to assist digital forensic investigators in collecting, analyzing, and reporting memory and file system artifacts from compromised or suspect systems. Initially designed for internal use by forensic professionals, the toolset evolved into a versatile and modular framework for both research and enterprise environments.

Description:

IDR IFPS Tools is a free, modular forensic toolkit for Windows and Linux that enables in-depth investigation of memory images, file systems, and process activities. It allows analysts to extract volatile data, detect persistence mechanisms, and uncover evidence of intrusion.

What Is This Tool About?

The toolset focuses on incident detection and response (IDR), specifically targeting memory (volatile) forensics and file system parsing (IFPS). It allows investigators to detect anomalies, parse system artifacts, and generate evidence-friendly outputs for further analysis or court proceedings.

Key Characteristics / Features:

1. RAM dump parsing and analysis
2. File system parsing (NTFS, FAT32, EXT4)
3. Timeline generation from file metadata
4. Process and DLL tracking
5. MFT (Master File Table) parsing
6. Shellbag and Jumplist extraction
7. Persistence detection (services, registry, startup folders)
8. Memory string and IOC searching
9. Export of reports in JSON, CSV, and PDF
10. Built-in YARA integration
11. Volatility plugin support

12. Lightweight CLI interface
13. Modular plugin architecture
14. Support for live or image-based analysis
15. Chain-of-custody logging

Types / Modules Available:

- Memory Parser
- File System Analyzer
- Persistence Finder
- Timeline Generator
- IOC Scanner
- Report Generator

How Will This Tool Help:

- Uncover malware indicators in memory and disk
- Parse system timelines for event correlation
- Identify persistence via registry, services, and files
- Extract deleted file traces and shell artifacts
- Automate forensic triage for faster response

PoC Screenshots to Capture:

1. Main IFPS Interface
2. Memory Scan Output
3. Timeline Graph
4. Registry Key Parser
5. IOC Detection Result
6. Chain-of-Custody Report
7. File System Artifact Viewer
8. Plugin Loader Interface
9. Volatility Plugin Integration
10. YARA Match Display

15-Liner Summary:

1. Modular forensic toolkit
2. Focused on memory and file systems
3. Works with live and image-based input
4. Integrates YARA, Volatility
5. Lightweight command-line interface
6. Cross-platform (Windows & Linux)
7. Generates detailed forensic timelines
8. Parses system artifacts: MFT, Shellbags
9. Detects persistence techniques
10. Extracts and logs volatile data
11. Supports chain-of-custody logs
12. Friendly JSON and PDF reports
13. Fast processing speed
14. Plugin-based design
15. Useful for forensic triage & IR

Time to Use / Best Case Scenarios:

- Post-breach forensic investigation
- During volatile memory capture
- When analyzing deleted or modified files
- For detecting rootkits or fileless malware
- Timeline generation during breach reporting

When to Use During Investigation:

- Initial triage phase
- After acquiring memory or disk image
- When persistence or data exfiltration is suspected
- Before handing over evidence to legal
- During IOC-based threat hunting

Best Person to Use This Tool & Required Skills:

Best User: Digital Forensics Examiner / Incident Response Analyst

Required Skills:

- Familiarity with Windows/Linux internals
- Volatile memory concepts
- Knowledge of file system structures
- Scripting or command-line usage
- Ability to read IOC and YARA rules
-

Flaws / Suggestions to Improve:

- No GUI version yet
- Limited automation with external SIEMs
- Requires separate acquisition tools
- Minimal documentation for new users
- Better visualization for timelines could help

Good About the Tool:

- Cross-platform support
- Rich forensic artifact parsing
- Lightweight and fast
- Compatible with industry standards
- Modular and extensible