Volatility3 - MCP Bridge

- Kiran Dawadi

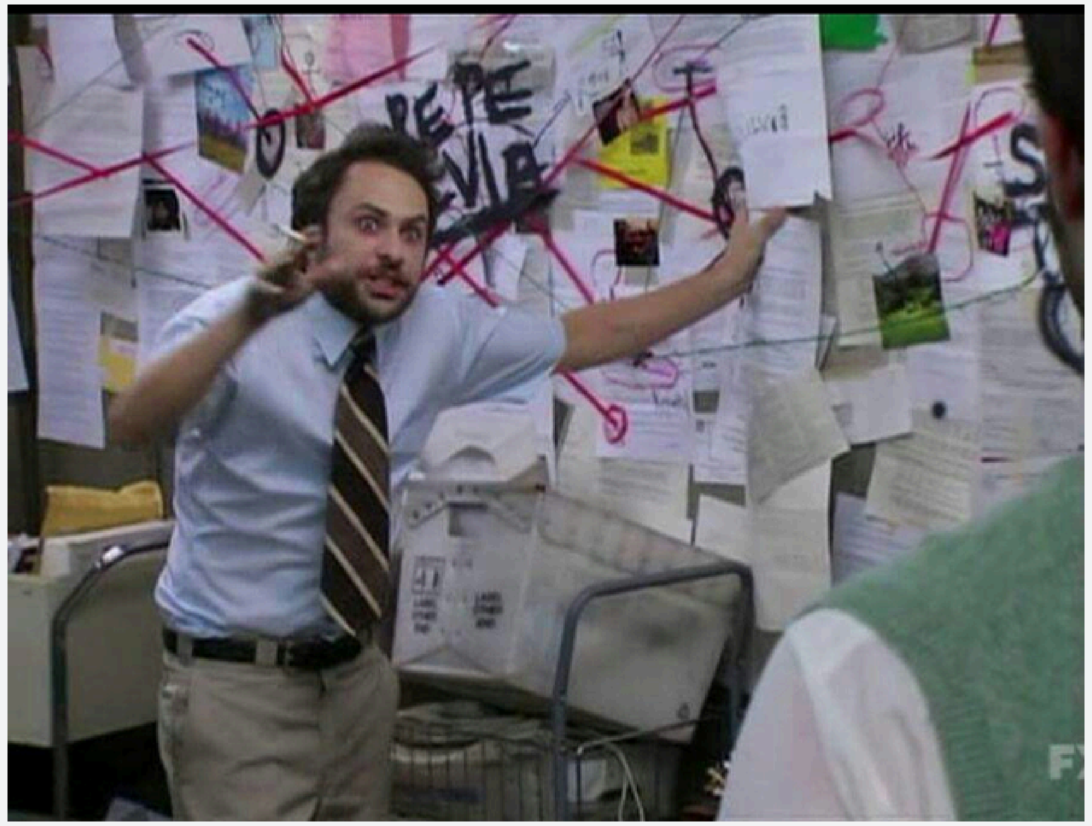
Apr 20

Introduction - The Big Picture

- Memory forensics is complex field requiring specialized expertise and technical knowledge
- Volatility3 MCP Bridge connects advanced memory forensics capabilities with AI assistants through the Model Control Protocol (MCP)
- Transforms complex forensic workflows into natural language conversations
- Imagine asking an AI assistant:

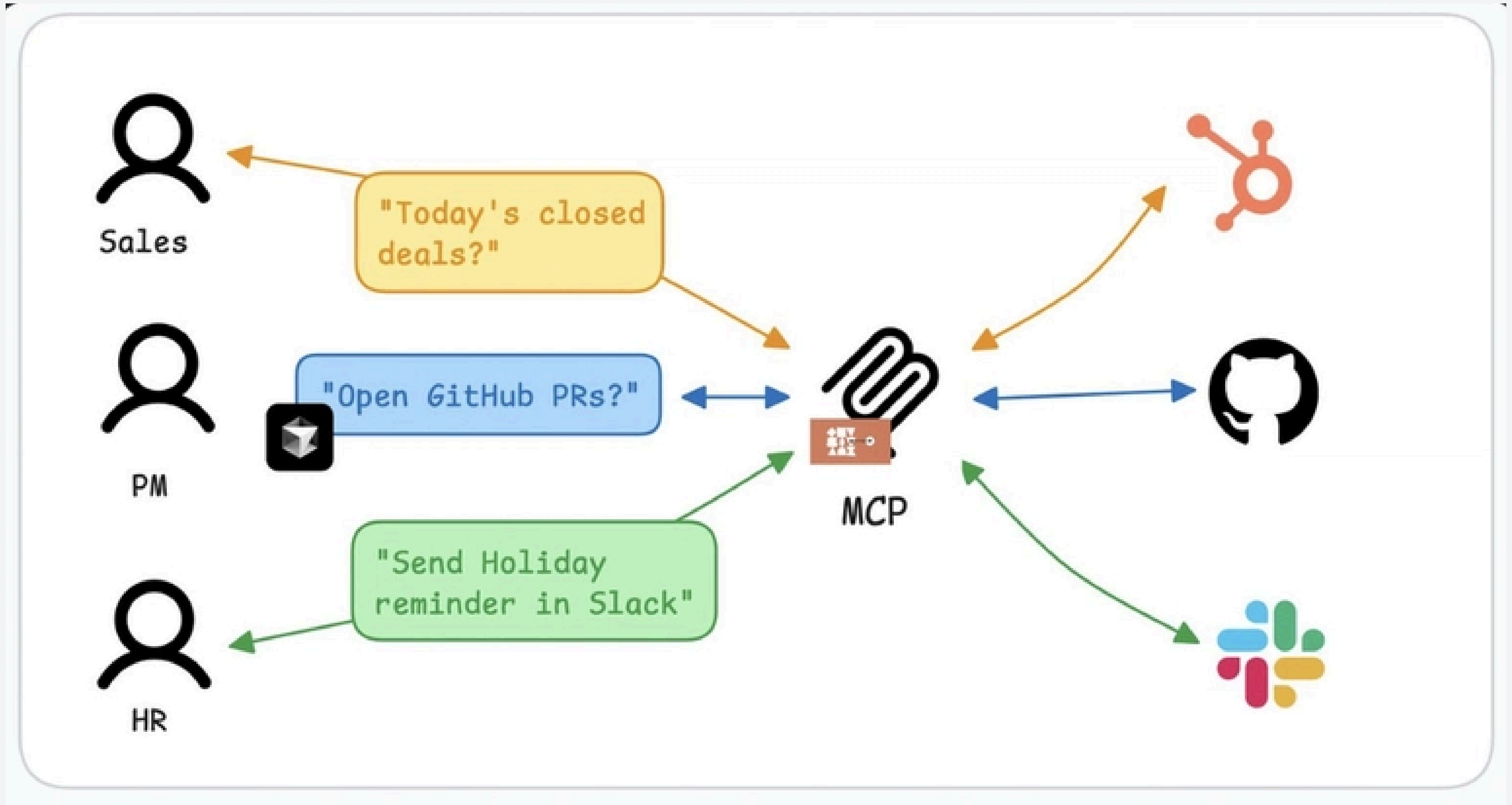
  Analyze this memory dump and tell me if there's any malware
- Bridge between two worlds:

  depth of memory forensics + the accessibility of conversational AI



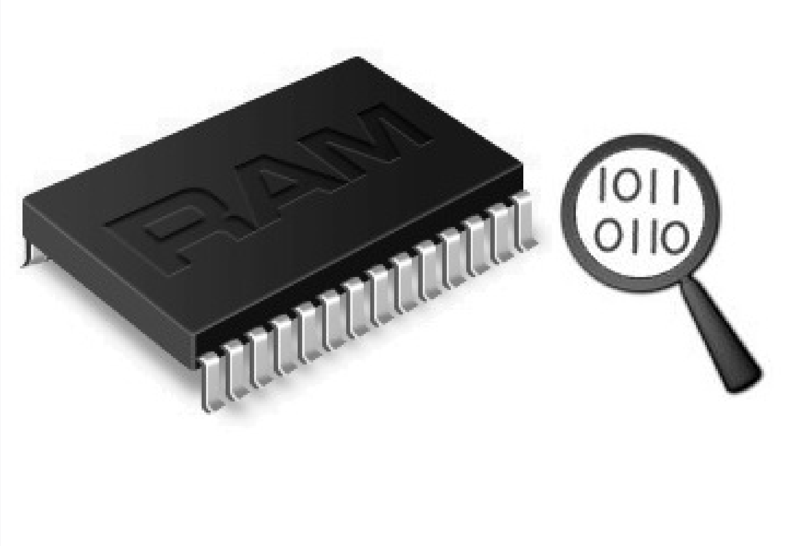
What is MCP?

- An emerging standard that enables AI models to interact with external tools and services
- Developed by Anthropic in 2023 and rapidly adopted across the AI ecosystem
- Claude Desktop and Cursor are leading MCP clients currently supporting this protocol
- Fundamentally changes AI capabilities by allowing models to:
    - Execute code
    - Access specialized tools
    - Interact with external systems



Introduction to Volatility3

- Volatility3 is the industry-standard open-source memory forensics framework
- Used by security professionals worldwide for incident response and digital forensics
- Essential for detecting sophisticated malware that hides from disk-based analysis
- Core capabilities include:
  - Process enumeration and analysis
  - Network connection detection
  - Registry examination
  - Malware identification
  - Hidden code detection

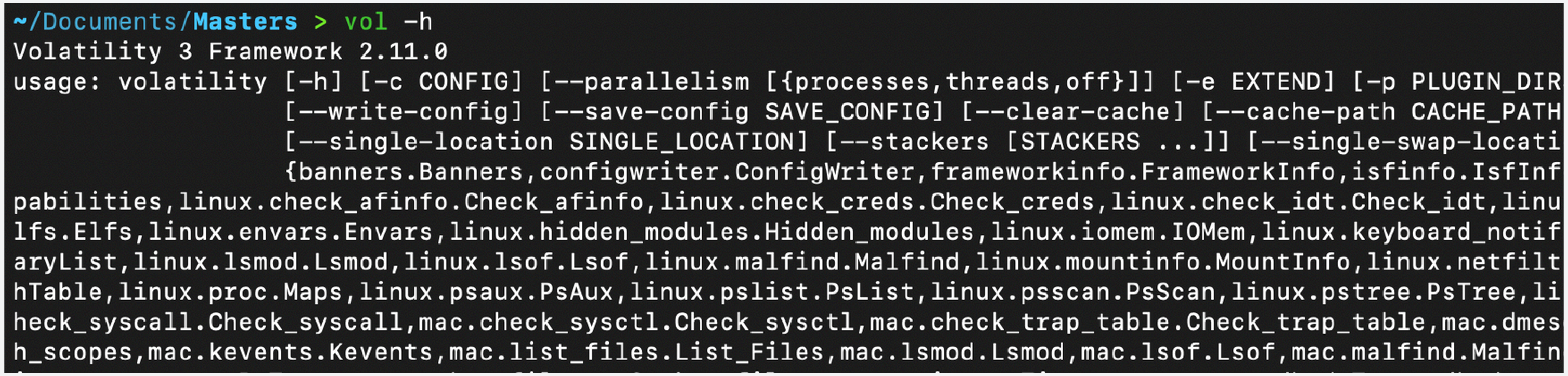


The Problem Space

- Memory forensics expertise is rare - Most organizations lack dedicated specialists
- Volatility requires comprehensive plugins knowledge to play around:

  vol -f memory.dmp windows.pslist.PsList

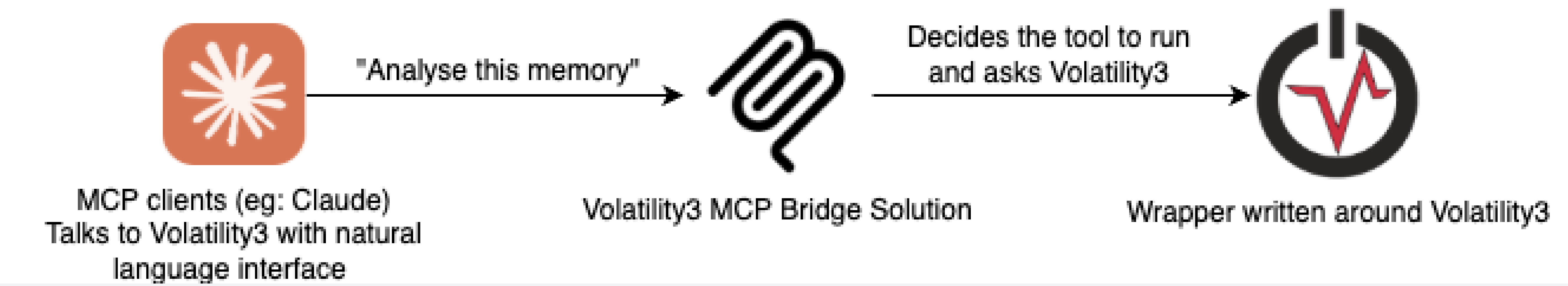
- Documentation and complex parameters for over 80+ plugins add to the learning curve
- Limited accessibility prevents wider adoption of this essential security technique



```
~/Documents/Masters > vol -h
Volatility 3 Framework 2.11.0
usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIR
                  [--write-config] [--save-config SAVE_CONFIG] [--clear-cache] [--cache-path CACHE_PATH
                  [--single-location SINGLE_LOCATION] [--stackers [STACKERS ...]] [--single-swap-locati
                  {banners.Banners,configwriter.ConfigWriter,frameworkinfo.FrameworkInfo,isfinfo.IsfInf
pabilities,linux.check_afinfo.Check_afinfo,linux.check_creds.Check_creds,linux.check_idt.Check_idt,linu
lfs.Elfs,linux.envars.Envars,linux.hidden_modules.Hidden_modules,linux.iomem.IOMem,linux.keyboard_notif
aryList,linux.lsmod.Lsmod,linux.lsof.Lsof,linux.malfind.Malfind,linux.mountinfo.MountInfo,linux.netfilt
hTable,linux.proc.Maps,linux.psaux.PsAux,linux.pslist.PsList,linux.psscan.PsScan,linux.pstree.PsTree,li
heck_syscall.Check_syscall,mac.check_sysctl.Check_sysctl,mac.check_trap_table.Check_trap_table,mac.dmes
h_scopes,mac.kevents.Kevents,mac.list_files.List_Files,mac.lsmod.Lsmod,mac.lsof.Lsof,mac.malfind.Malfin
```

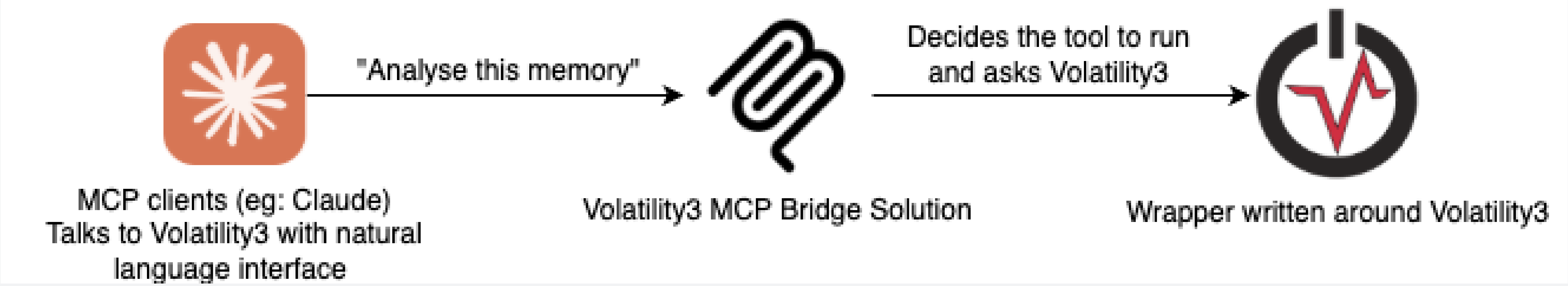
Volatility3 MCP Bridge Solution

- Natural language interface to sophisticated memory forensics:
  - "Find evidence of process injection in this memory dump"
  - "Show me all processes with suspicious network connections”
- Contextual understanding of memory forensics concepts by the AI assistant
- Bridges the expertise gap by guiding users through the investigation process
- Automates common forensic workflows that typically require multiple manual steps


"Analyse this memory"
Decides the tool to run and asks Volatility3
MCP clients (eg: Claude) Talks to Volatility3 with natural language interface
Volatility3 MCP Bridge Solution
Wrapper written around Volatility3

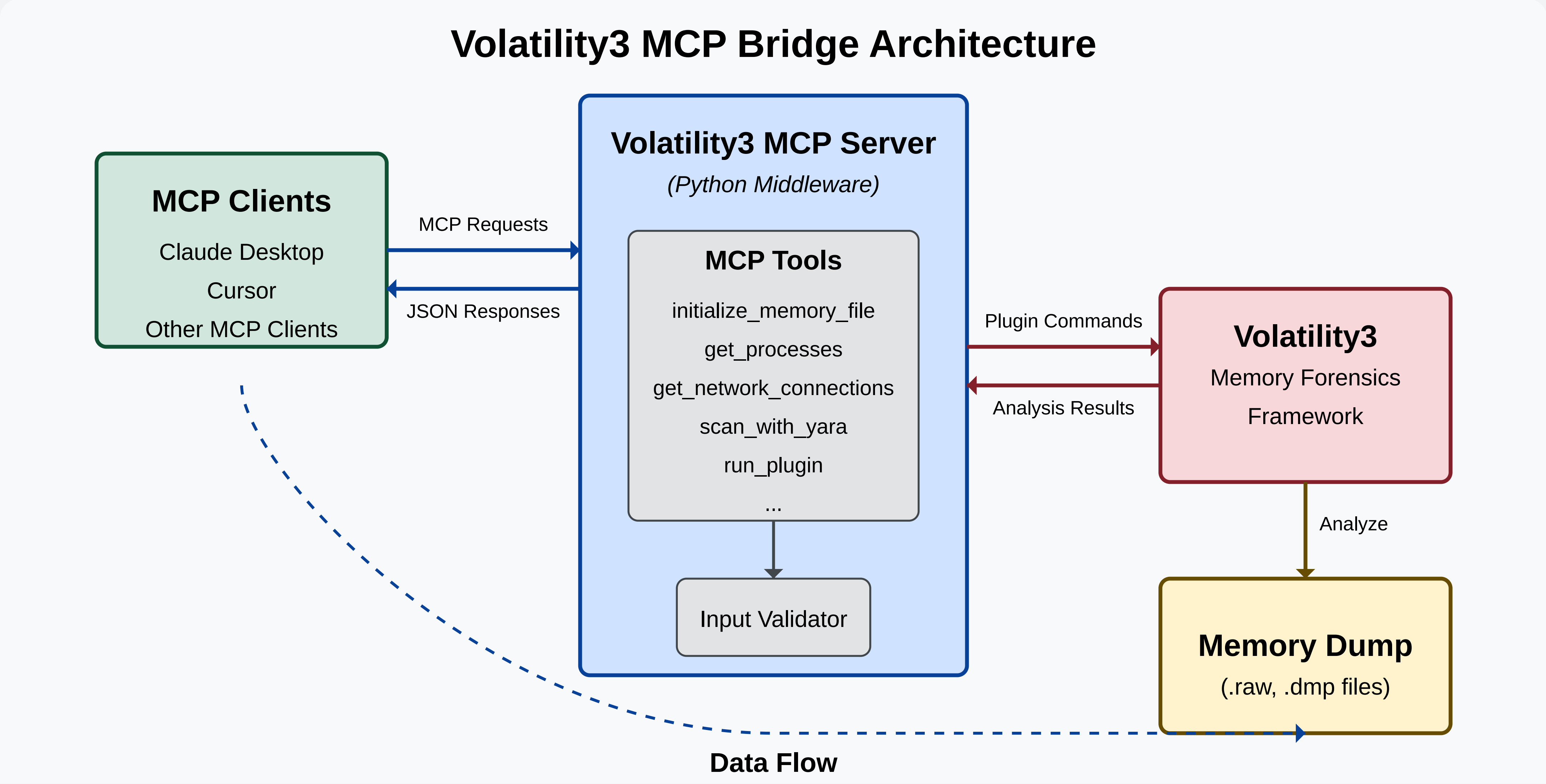
Core Features

- Cross-platform memory analysis of Windows and Linux dumps (macOS coming soon)
- Network connection analysis to identify command and control servers
- Hidden processes detection
- Process relationships and hierarchies
- Timeline creation for forensic reconstruction of events
- Highlight feature: Malware detection integration with YARA rules


"Analyse this memory"
Decides the tool to run and asks Volatility3
MCP clients (eg: Claude) Talks to Volatility3 with natural language interface
Volatility3 MCP Bridge Solution
Wrapper written around Volatility3

Technical Architecture

- Three-tier architecture:
  - MCP Client (Claude Desktop/Cursor)
  - Bridge Server (Python-based middleware)
  - Volatility3 Framework Wrapper (written in Python)



Available Tools

- initialize_memory_file: Set up a memory dump file for analysis
- detect_os: Identify the operating system of the memory dump
- list_plugins: Display all available Volatility3 plugins
- get_plugin_info: Get detailed information about a specific plugin
- run_plugin: Execute any Volatility3 plugin with custom arguments
- get_processes: List all running processes in the memory dump
- get_network_connections: View all network connections from the system
- list_process_open_handles: Examine files and resources accessed by a process
- scan_with_yara: Scan memory for malicious patterns using YARA rules

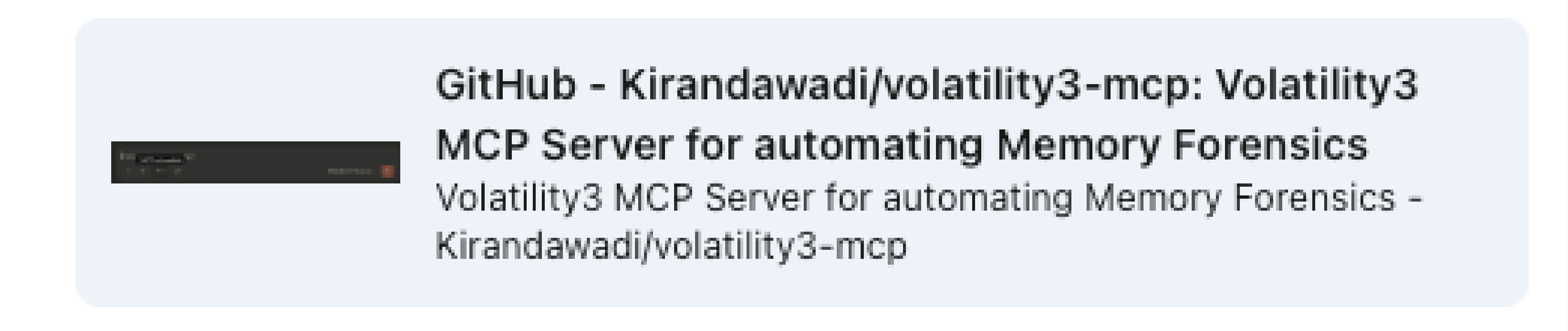
Let’s see a Demo

Watch how it is able to solve a medium-level difficulty challenge on memory forensics from BlueTeamLabs.

Demo Link

References

- https://github.com/Kirandawadi/volatility3-mcp



GitHub - Kirandawadi/volatility3-mcp: Volatility3 MCP Server for automating Memory Forensics

Volatility3 MCP Server for automating Memory Forensics - Kirandawadi/volatility3-mcp

- https://modelcontextprotocol.io/introduction
- https://volatilityfoundation.org/

Thank You!