BSIDES MUMBAI

VOLATILITY MCP SERVER

MUMBAI

About me

- Researcher at BharatGen, Indian Institute of Technology Bombay
- Author & part of AI Red teaming at OWSAP AI Exchange (AI Security)
- Fusion of Large Language Model (LLM) with Cybersecurity.
- Speaker at FOSS Mumbai, DEFCON Delhi and BSides Bangalore
- FOSS enthusiast
- VERY passionate about National security

Role of memory forensics in incident response workflow

Incident Triggered (Alert, Suspicious Activity)

Live Response or Image Acquisition

MEMORY ACQUISITION PHASE

MEMORY FORENSICS ANALYSIS

CORRELATE WITH DISK & LOGS

REPORTING & MITIGATION

Importance of memory forensics

Reveals volatile data and processes

Helps identify malicious activities

Provides insights into system state at a specific point in time

Assists in identifying root causes of system issues

Supports incident response and digital investigations

Provides context for understanding system events

Information available in RAM

Processes and Drivers

Loaded Modules

Network Socket Info

Passwords

Encryption Keys

Decrypted files

Order of execution

Runtime State Information

Rootkits

Configuration Information

Logged in Users

Open Files

Unsaved Documents

Live Registry

Video Buffers – screen shots

BIOS Memory

VOIP Phone calls

Advanced Malware

Instant Messenger chat

Memory IMAGE Information (imageinfo)


```
root@kali:/opt/volatility# python2 vol.py -f memory.vmem imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/opt/volatility/memory.vmem)
                      PAE type : PAE
                           DTB : 0x319000L
                          KDBG : 0x80545ae0L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2011-06-03 04:31:36 UTC+0000
     Image local date and time : 2011-06-03 00:31:36 -0400
```

Volatility Plugins - pslist


```
root@kali:/opt/volatility# python2 vol.py -f memory.vmem --profile=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.6.1   3      133      0      0 2010-10-29 17:12:03 UTC+0000
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x823c8830 System                    4      0     59      403 ------      0
0x820df020 smss.exe                376      4      3       19 ------      0 2010-10-29 17:08:53 UTC+0000
0x821a2da0 csrss.exe               600    376     11      395      0      0 2010-10-29 17:08:54 UTC+0000
0x81da5650 winlogon.exe            624    376     19      570      0      0 2010-10-29 17:08:54 UTC+0000
0x82073020 services.exe            668    624     21      431      0      0 2010-10-29 17:08:54 UTC+0000
0x81e70020 lsass.exe               680    624     19      342      0      0 2010-10-29 17:08:54 UTC+0000
0x823315d8 vmacthlp.exe            844    668      1       25      0      0 2010-10-29 17:08:55 UTC+0000
0x81db8da0 svchost.exe             856    668     17      193      0      0 2010-10-29 17:08:55 UTC+0000
0x81e61da0 svchost.exe             940    668     13      312      0      0 2010-10-29 17:08:55 UTC+0000
0x822843e8 svchost.exe            1032    668     61     1169      0      0 2010-10-29 17:08:55 UTC+0000
0x81e18b28 svchost.exe            1080    668      5       80      0      0 2010-10-29 17:08:55 UTC+0000
0x81ff7020 svchost.exe            1200    668     14      197      0      0 2010-10-29 17:08:55 UTC+0000
0x81fee8b0 spoolsv.exe            1412    668     10      118      0      0 2010-10-29 17:08:56 UTC+0000
0x81e0eda0 jqs.exe                1580    668      5      148      0      0 2010-10-29 17:09:05 UTC+0000
0x81fe52d0 vmtoolsd.exe           1664    668      5      284      0      0 2010-10-29 17:09:05 UTC+0000
0x821a0568 VMUpgradeHelper        1816    668      3       96      0      0 2010-10-29 17:09:08 UTC+0000
0x8205ada0 alg.exe                 188    668      6      107      0      0 2010-10-29 17:09:09 UTC+0000
0x820ec7e8 explorer.exe           1196   1728     16      582      0      0 2010-10-29 17:11:49 UTC+0000
0x820ecc10 wscntfy.exe            2040   1032      1       28      0      0 2010-10-29 17:11:49 UTC+0000
0x81e86978 TSVNCache.exe           324   1196      7       54      0      0 2010-10-29 17:11:49 UTC+0000
0x81fc5da0 VMwareTray.exe         1912   1196      1       50      0      0 2010-10-29 17:11:50 UTC+0000
0x81e6b660 VMwareUser.exe         1356   1196      9      251      0      0 2010-10-29 17:11:50 UTC+0000
0x8210d478 jusched.exe            1712   1196      1       26      0      0 2010-10-29 17:11:50 UTC+0000
0x82279998 imapi.exe               756    668      4      116      0      0 2010-10-29 17:11:54 UTC+0000
0x822b9a10 wuauclt.exe             976   1032      3      133      0      0 2010-10-29 17:12:03 UTC+0000
0x81c543a0 Procmon.exe             660   1196     13      189      0      0 2011-06-03 04:25:56 UTC+0000
0x81fa5390 wmiprvse.exe           1872    856      5      134      0      0 2011-06-03 04:25:58 UTC+0000
0x81c498c8 lsass.exe               868    668      2       23      0      0 2011-06-03 04:26:55 UTC+0000
0x81c47c00 lsass.exe              1928    668      4       65      0      0 2011-06-03 04:26:55 UTC+0000
0x81c0cda0 cmd.exe                 968   1664      0 --------      0      0 2011-06-03 04:31:35 UTC+0000   2011-06-03 04:31:36 UTC+0000
0x81f14938 ipconfig.exe            304    968      0 --------      0      0 2011-06-03 04:31:35 UTC+0000   2011-06-03 04:31:36 UTC+0000
```

Volatility Plugins - pstree

```
root@kali:/opt/volatility# python2 vol.py -f memory.vmem --profile=WinXPSP2x86 pstree
Volatility Foundation Volatility Framework 2.6.1
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x823c8830:System                                      4      0     59    403 1970-01-01 00:00:00 UTC+0000
. 0x820df020:smss.exe                                 376      4      3     19 2010-10-29 17:08:53 UTC+0000
.. 0x821a2da0:csrss.exe                               600    376     11    395 2010-10-29 17:08:54 UTC+0000
.. 0x81da5650:winlogon.exe                            624    376     19    570 2010-10-29 17:08:54 UTC+0000
... 0x82073020:services.exe                           668    624     21    431 2010-10-29 17:08:54 UTC+0000
.... 0x81fe52d0:vmtoolsd.exe                         1664    668      5    284 2010-10-29 17:09:05 UTC+0000
..... 0x81c0cda0:cmd.exe                              968   1664      0 ------ 2011-06-03 04:31:35 UTC+0000
...... 0x81f14938:ipconfig.exe                        304    968      0 ------ 2011-06-03 04:31:35 UTC+0000
.... 0x822843e8:svchost.exe                          1032    668     61   1169 2010-10-29 17:08:55 UTC+0000
..... 0x822b9a10:wuauclt.exe                          976   1032      3    133 2010-10-29 17:12:03 UTC+0000
..... 0x820ecc10:wscntfy.exe                         2040   1032      1     28 2010-10-29 17:11:49 UTC+0000
.... 0x81e61da0:svchost.exe                           940    668     13    312 2010-10-29 17:08:55 UTC+0000
.... 0x81db8da0:svchost.exe                           856    668     17    193 2010-10-29 17:08:55 UTC+0000
..... 0x81fa5390:wmiprvse.exe                        1872    856      5    134 2011-06-03 04:25:58 UTC+0000
.... 0x821a0568:VMUpgradeHelper                      1816    668      3     96 2010-10-29 17:09:08 UTC+0000
.... 0x81fee8b0:spoolsv.exe                          1412    668     10    118 2010-10-29 17:08:56 UTC+0000
.... 0x81ff7020:svchost.exe                          1200    668     14    197 2010-10-29 17:08:55 UTC+0000
.... 0x81c47c00:lsass.exe                            1928    668      4     65 2011-06-03 04:26:55 UTC+0000
.... 0x81e18b28:svchost.exe                          1080    668      5     80 2010-10-29 17:08:55 UTC+0000
.... 0x8205ada0:alg.exe                               188    668      6    107 2010-10-29 17:09:09 UTC+0000
.... 0x823315d8:vmacthlp.exe                          844    668      1     25 2010-10-29 17:08:55 UTC+0000
.... 0x81e0eda0:jqs.exe                              1580    668      5    148 2010-10-29 17:09:05 UTC+0000
.... 0x81c498c8:lsass.exe                             868    668      2     23 2011-06-03 04:26:55 UTC+0000
.... 0x82279998:imapi.exe                             756    668      4    116 2010-10-29 17:11:54 UTC+0000
... 0x81e70020:lsass.exe                              680    624     19    342 2010-10-29 17:08:54 UTC+0000
 0x820ec7e8:explorer.exe                             1196   1728     16    582 2010-10-29 17:11:49 UTC+0000
. 0x81c543a0:Procmon.exe                              660   1196     13    189 2011-06-03 04:25:56 UTC+0000
. 0x81e86978:TSVNCache.exe                            324   1196      7     54 2010-10-29 17:11:49 UTC+0000
. 0x81e6b660:VMwareUser.exe                          1356   1196      9    251 2010-10-29 17:11:50 UTC+0000
. 0x8210d478:jusched.exe                             1712   1196      1     26 2010-10-29 17:11:50 UTC+0000
. 0x81fc5da0:VMwareTray.exe                          1912   1196      1     50 2010-10-29 17:11:50 UTC+0000
```

SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

Hunt Evil

POSTER

$25.00
DFPS_FOR508_v4.11_0624

Poster was created by Rob Lee and Mike Pilkington
with support of the SANS DFIR Faculty

dfir.sans.org

SANS DFIR CURRICULUM

SANSForensics | @SANSForensics | dfir.to/DFIRCast | dfir.to/LinkedIn

DIGITAL FORENSICS

FOR498 Digital Acquisition and Rapid Triage — GBFA

FOR500 Windows Forensic Analysis — GCFE

FOR518 Mac and iOS Forensic Analysis & Incident Response — GIME

FOR585 Smartphone Forensic Analysis In-Depth — GASF

INCIDENT RESPONSE & THREAT HUNTING

FOR508 Advanced Incident Response, Threat Hunting & Digital Forensics — GCFA

FOR509 Enterprise Cloud Forensics & Incident Response — GCFR

FOR528 Ransomware and Cyber Extortion

FOR572 Advanced Network Forensics: Threat Hunting, Analysis & Incident Response — GNFA

FOR577 LINUX Incident Response and Threat Hunting

FOR578 Cyber Threat Intelligence — GCTI

FOR589 Cybercrime Intelligence

FOR608 Enterprise-Class Incident Response & Threat Hunting — GEIR

FOR610 REM: Malware Analysis Tools & Techniques — GREM

FOR710 Reverse-Engineering Malware: Advanced Code Analysis

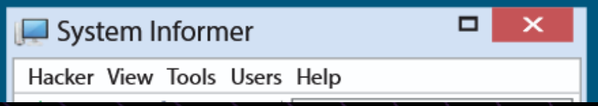
SEC504 Hacker Tools, Techniques & Incident Handling — GCIH

Find Evil – Know Normal

Knowing what's normal on a Windows host helps cut through the noise to quickly locate potential malware.
Use the information below as a reference to know what's normal in Windows and to focus your attention on the outliers.

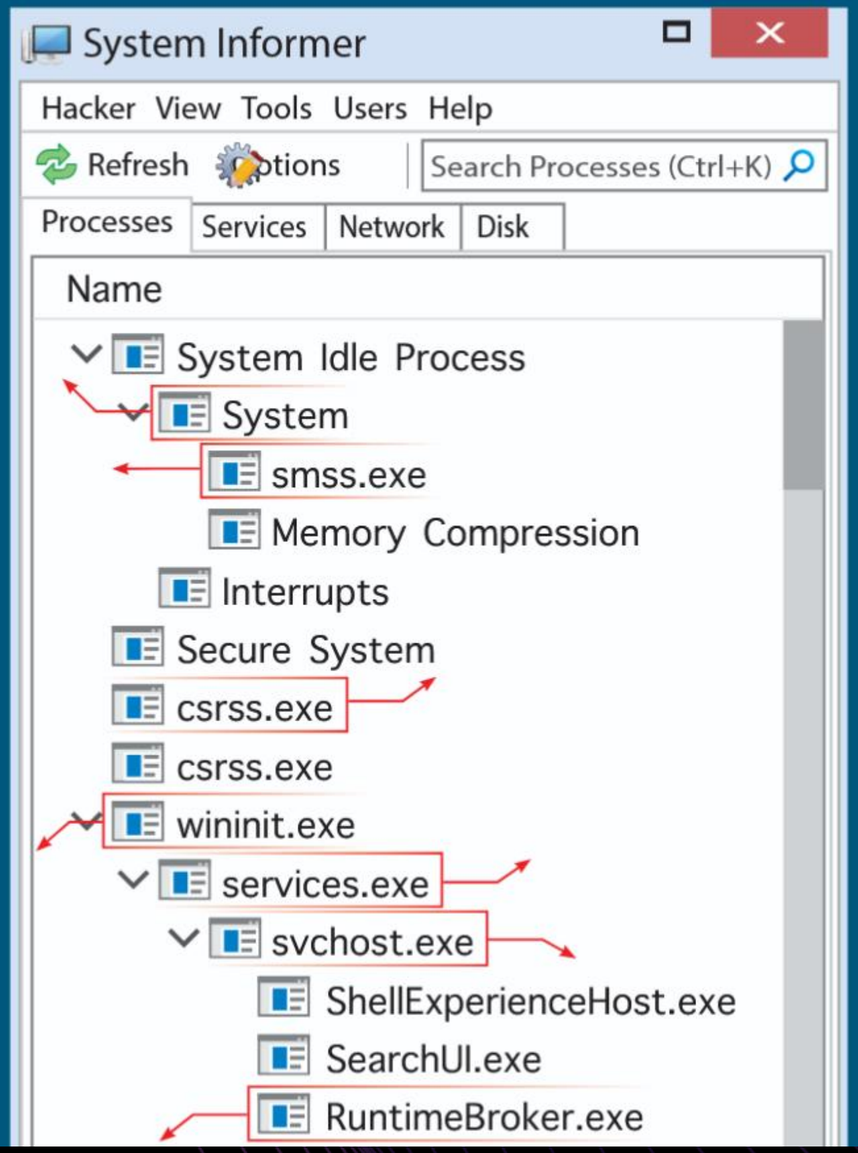
System

Image Path: N/A for `system.exe` – Not generated from an executable image



csrss.exe

Image Path: `%SystemRoot%\System32\csrss.exe`



csrss.exe

Image Path: `%SystemRoot%\System32\csrss.exe`

Parent Process: Created by an instance of `smss.exe` that exits, typically appearing as an orphan process.

Number of Instances: Two or more

User Account: Local System

Start Time: Within seconds of boot time for the first two instances (for Session 0 and 1). Start times for additional instances occur as new sessions are created, although often only Sessions 0 and 1 are created.

Description: The Client/Server Run-Time Subsystem is the user-mode process for the Windows subsystem. Its duties include managing processes and threads, importing many of the DLLs that provide the Windows API, and facilitating shutdown of the GUI during system shutdown. An instance of `csrss.exe` will run for each session. Session 0 is for services and Session 1 for the local console session. Additional sessions are created through the use of Remote Desktop and/or Fast User Switching. Each new session results in a new instance of `csrss.exe`.

services.exe

Image Path: `%SystemRoot%\System32\services.exe`

Parent Process: `wininit.exe`

Number of Instances: One

User Account: Local System

Start Time: Within seconds of boot time

Description: Implements the Unified Background Process Manager (UBPM), which is responsible for background activities such as services and scheduled tasks. `Services.exe` also implements the Service Control Manager (SCM), which specifically handles the loading of services and device drivers marked for auto-start. In addition, once a user has successfully logged on interactively, the SCM (`services.exe`) considers the boot successful and sets the Last Known Good control set (`HKLM\SYSTEM\Select\LastKnownGood`) to the value of the CurrentControlSet.

svchost.exe

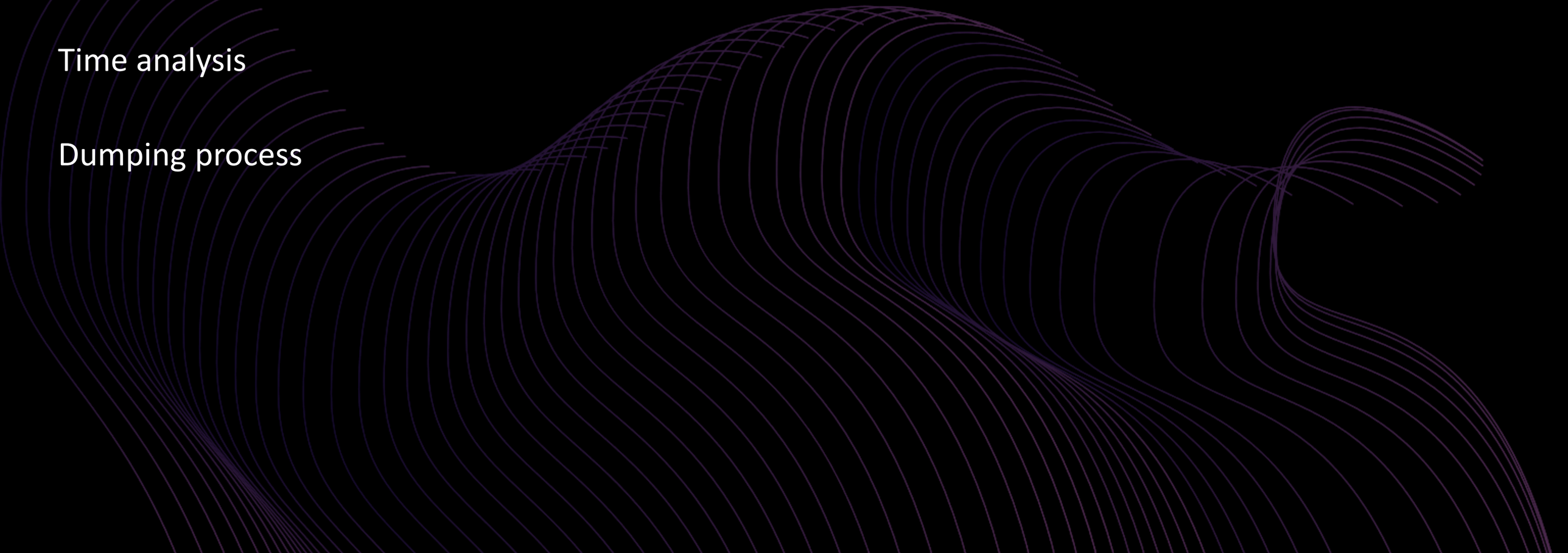
Investigating DLLs

Investigating Process Handles

Investigating Registry

Time analysis

Dumping process



Problem??

India’s digital forensic investigators are overwhelmed with thousands of pending cases

Limited resources, rising cybercrime, and complex technical requirements.

The backlog continues to grow (We need AI solutions)

Volatility MCP Server

It’s open source!!

Appreciation from CISO Hotstar (Now JioStar) & Monnappa K A

Beta testing in one of the top forensic company in India

Analyzes Windows, Linux and macOS memory.

Natural Language Memory Forensics: Ask Claude to analyze memory dumps using natural language

Currently runs over the internet. (BUT CAN RUN LOCALLY ALSO)

80% accuracy

MCP (Model Context Protocol)

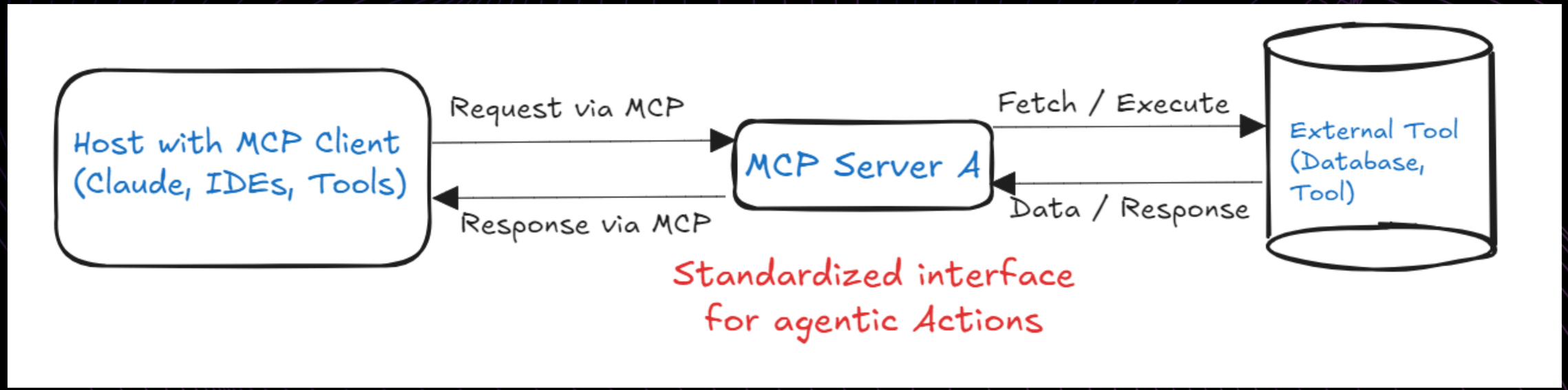
MCP is an open protocol that standardizes how applications provide context to LLMs.

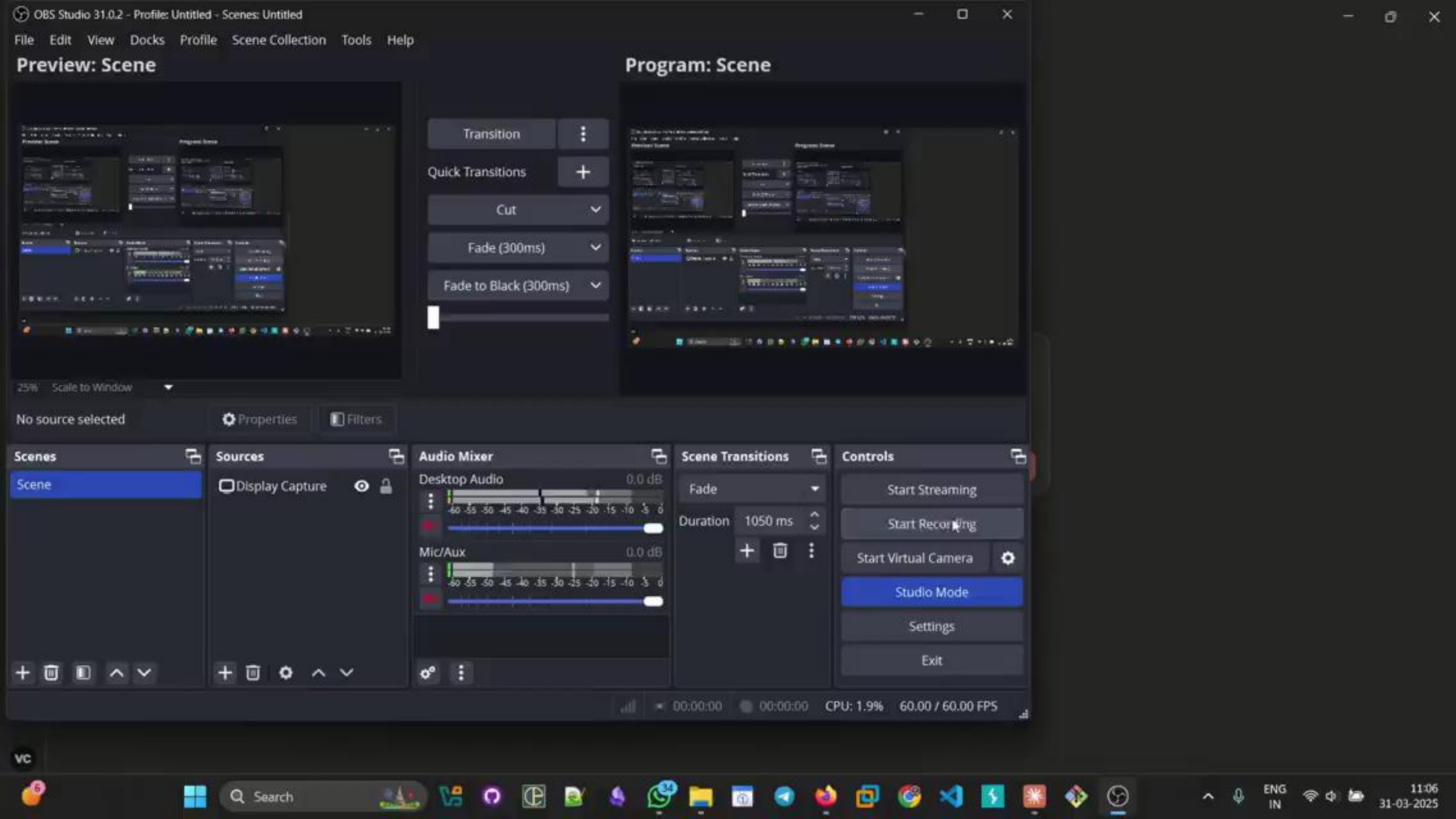
MCP provides a standardized way to connect AI models to different data sources and tools

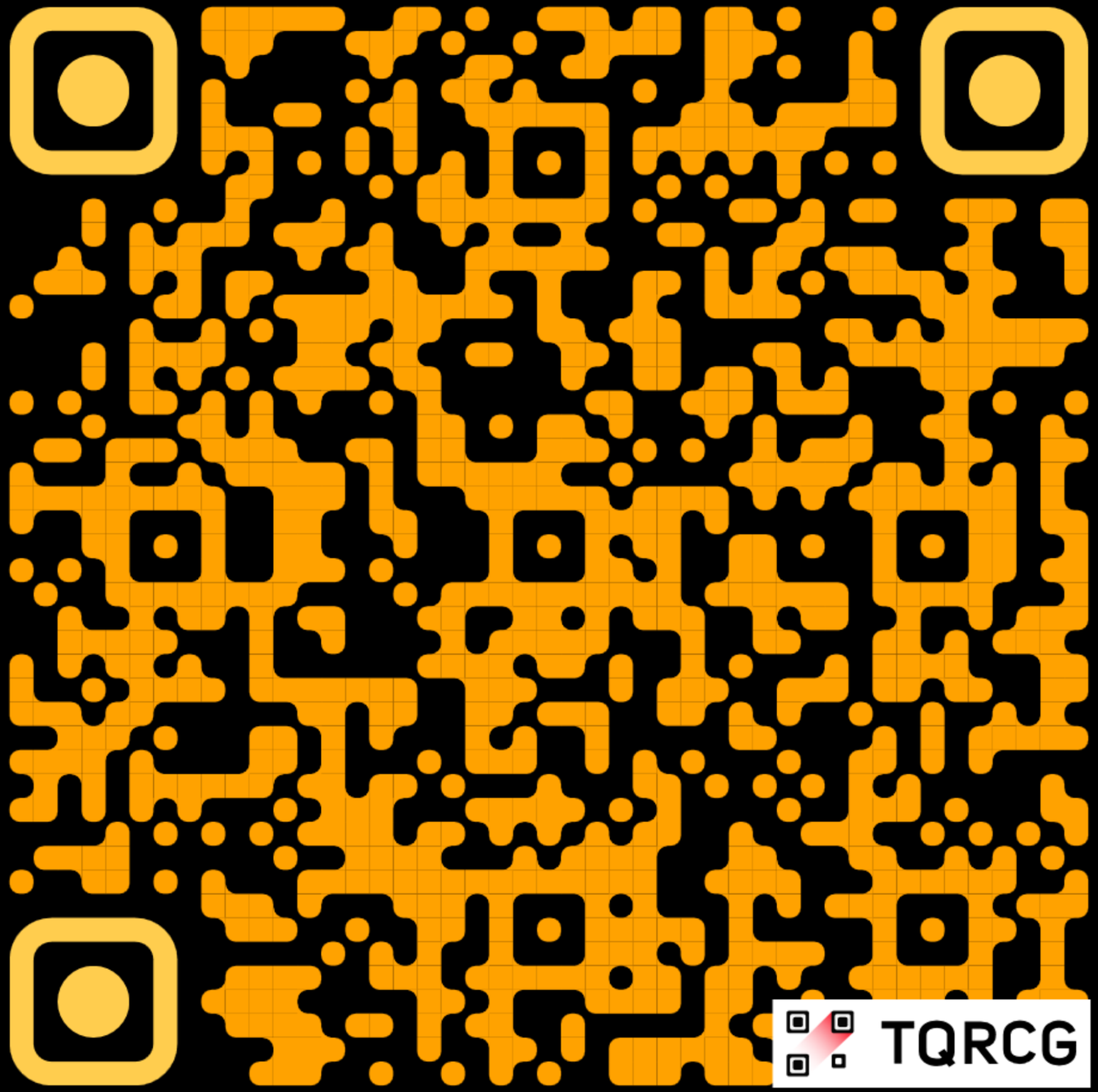
MCP operates on a client-server model where :

- Clients: Typically, AI models or applications embedding them.

- Servers: External system providing additional capabilities to the models




OBS Studio 31.0.2 - Profile: Untitled - Scenes: Untitled
File Edit View Docks Profile Scene Collection Tools Help
Preview: Scene
Program: Scene
Transition
Quick Transitions
Cut
Fade (300ms)
Fade to Black (300ms)
25% Scale to Window
No source selected
Properties
Filters
Scenes
Scene
Sources
Display Capture
Audio Mixer
Desktop Audio 0.0 dB
Mic/Aux 0.0 dB
Scene Transitions
Fade
Duration 1050 ms
Controls
Start Streaming
Start Recording
Start Virtual Camera
Studio Mode
Settings
Exit
00:00:00 00:00:00 CPU: 1.9% 60.00 / 60.00 FPS
Search
ENG IN
11:06 31-03-2025



BSIDES MUMBAI

THANKS

BSIDES MUMBAI