CHAPTER 5

Acquiring Memory

Chapter Overview

01

Order of Volatility

What to collect first — the most perishable evidence

02

Local Memory Collection

Tools and procedures for on-site RAM acquisition

03

Remote Memory Collection

Capturing memory without physical access

04

Live Memory Analysis

Analyzing memory without a full dump

Order of Volatility

Collect the most perishable evidence first

Order of Volatility

Evidence is lost in order of volatility — collect fastest-changing first

1. **CPU registers,** cache, running processes (seconds)
2. **RAM** — full memory contents including encryption keys, credentials (minutes)
3. **Network state** — connections, ARP table, routing (minutes)
4. **Running processes** and open files (may persist until reboot)
5. **Disk contents** — non-volatile, survives reboot
6. **Remote logging** / monitoring data

Do NOT reboot before collecting RAM — volatile evidence is gone forever

What Lives in Memory — Evidence Types

Running processes: executable code, DLLs, heap contents, stack frames

Network state: active sockets, ARP table, routing cache, DNS resolver cache

Credentials: NTLM hashes, Kerberos tickets, cleartext passwords from SSP providers

Encryption keys: BitLocker VMK, TrueCrypt keys, SSL session keys — only in RAM

Injected code: shellcode, reflectively loaded DLLs that never touch disk

Registry hive cache: in-memory copy of registry — includes recently deleted keys

Clipboard contents: attacker may have copied credentials or commands to clipboard

Malware configuration: C2 servers, campaigns, encryption keys embedded in malware memory

Cold Boot Attack

Local Memory Collection

Tools and process for on-site acquisition

Preparing Media & Collection Tools

Preparing Storage Media

Use dedicated, sterile (wiped) external media

Verify media integrity before and after collection

Encrypt collected image at rest

Never write to the suspect system's local disk

Calculate hash of image immediately after capture

Collection Tools

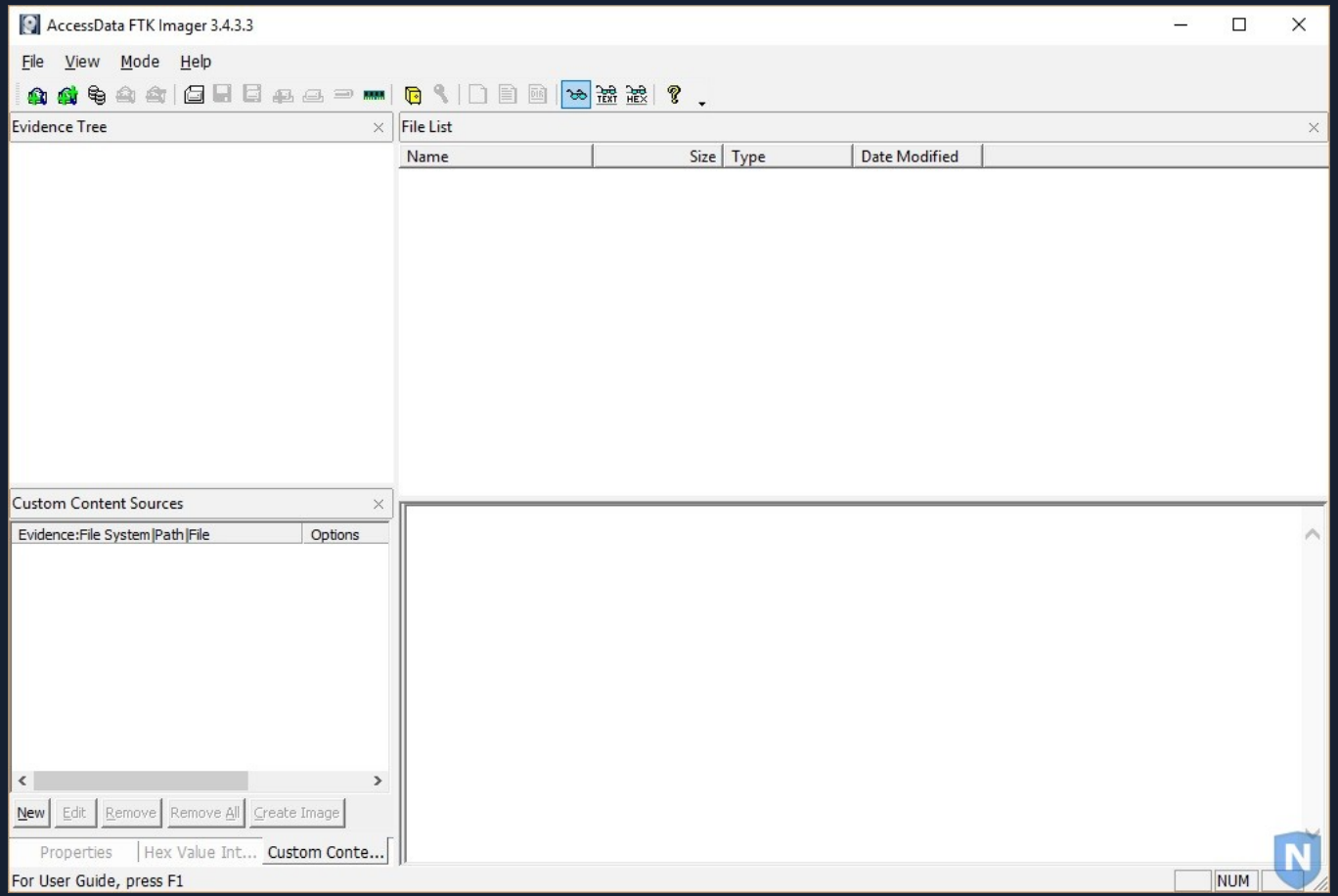
WinPmem: open-source, writes to file or stdout

Magnet RAM Capture: free, GUI-based

FTK Imager: commercial, also does disk imaging

DumpIt: single executable, minimal footprint

Belkasoft RAM Capturer: handles paged/non-paged pools



Memory acquisition — capturing volatile RAM contents before evidence is lost

Collection Process — Step by Step

Step 1 — Prepare media: verify sterile external drive or network share is available

Step 2 — Document the system: note time, uptime, logged-in users, and running processes

Step 3 — Copy acquisition tool to external media (do NOT install on suspect system)

Step 4 — Execute: winpmem -o D:\memory.raw (write to external media)

Step 5 — Hash the image: Get-FileHash D:\memory.raw -Algorithm SHA256

Step 6 — Record hash in case log with timestamp and examiner name

Step 7 — Verify after transfer: hash on destination must match source hash

Do NOT reboot the system until all volatile evidence is captured

Acquisition Tool Comparison

WinPmem: open-source, command-line, output to file or stdout — most flexible

DumpIt: single EXE, minimal footprint, outputs to current directory

Magnet RAM Capture: free GUI, beginner-friendly, progress bar

FTK Imager: commercial, also handles disk imaging, validated for legal proceedings

Belkasoft RAM Capturer: handles both 32-bit and 64-bit Windows including Vista+

Velociraptor: agent-based, no tool deployment — best for remote/fleet collection

All tools modify memory slightly by loading themselves — unavoidable; document tool used

Choose tool based on: environment (remote vs. local), legal requirements, and speed

Hash Verification & Chain of Custody

Hash Verification

Compute hash immediately after acquisition — before any transfer

Re-hash at destination — source hash == destination hash proves integrity

SHA-256 preferred (MD5 has known collision vulnerabilities)

certutil -hashfile memory.raw SHA256 (Windows built-in)

sha256sum memory.raw (Linux)

Hash mismatch: image was altered in transit — evidence is inadmissible

Chain of Custody

Document: who collected it, when, on what system, with what tool

Evidence bag or encrypted container: limit unauthorized access

Every person who handles evidence must sign the custody log

Digital signature: sign the hash log with examiner's key

Breaks in chain of custody: defense attorneys challenge admissibility

Good documentation protects the analyst even for internal IR

Remote Memory Collection

Capturing RAM without physical access

Remote Collection Methods

WMIC: wmic /node:HOST process call create 'winpmem -o \\share\output.raw'

PowerShell Remoting: copy collection tool, execute, retrieve image file

Caution: running tools over the network may impact performance

Agent-based: Velociraptor, GRR — best for large-scale remote collection

Agents minimize interaction with target OS (less evidence contamination)

Bandwidth: a 16 GB RAM image is ~16 GB — plan collection window carefully

Prioritize systems with highest likelihood of active compromise

Remote Collection — Challenges & Planning

Bandwidth: 16 GB RAM image at 1 Gbps LAN ≈ 2 minutes; WAN much slower

Prioritize: collect highest-risk systems first; triage by known indicators

Compression: gzip reduces image size ~20–30% for unencrypted memory regions

Encryption in transit: use SCP or HTTPS — memory images contain credentials

Agent-based collection: significantly reduces risk of detection vs. WMI/PS commands

Scheduling: memory acquisition is I/O and CPU intensive — plan for performance impact

Documentation: log all remote actions — commands run, times, target IPs, analyst name

Partial image: if bandwidth is limited, prioritize kernel + process memory over all pages

Live Memory Analysis

Analyze without a full dump when needed

Live Memory Analysis Techniques

Full dump preferred — but live analysis is faster when scope is large

Local: Volatility or Rekall pointed at \\.\PhysicalMemory (admin required)

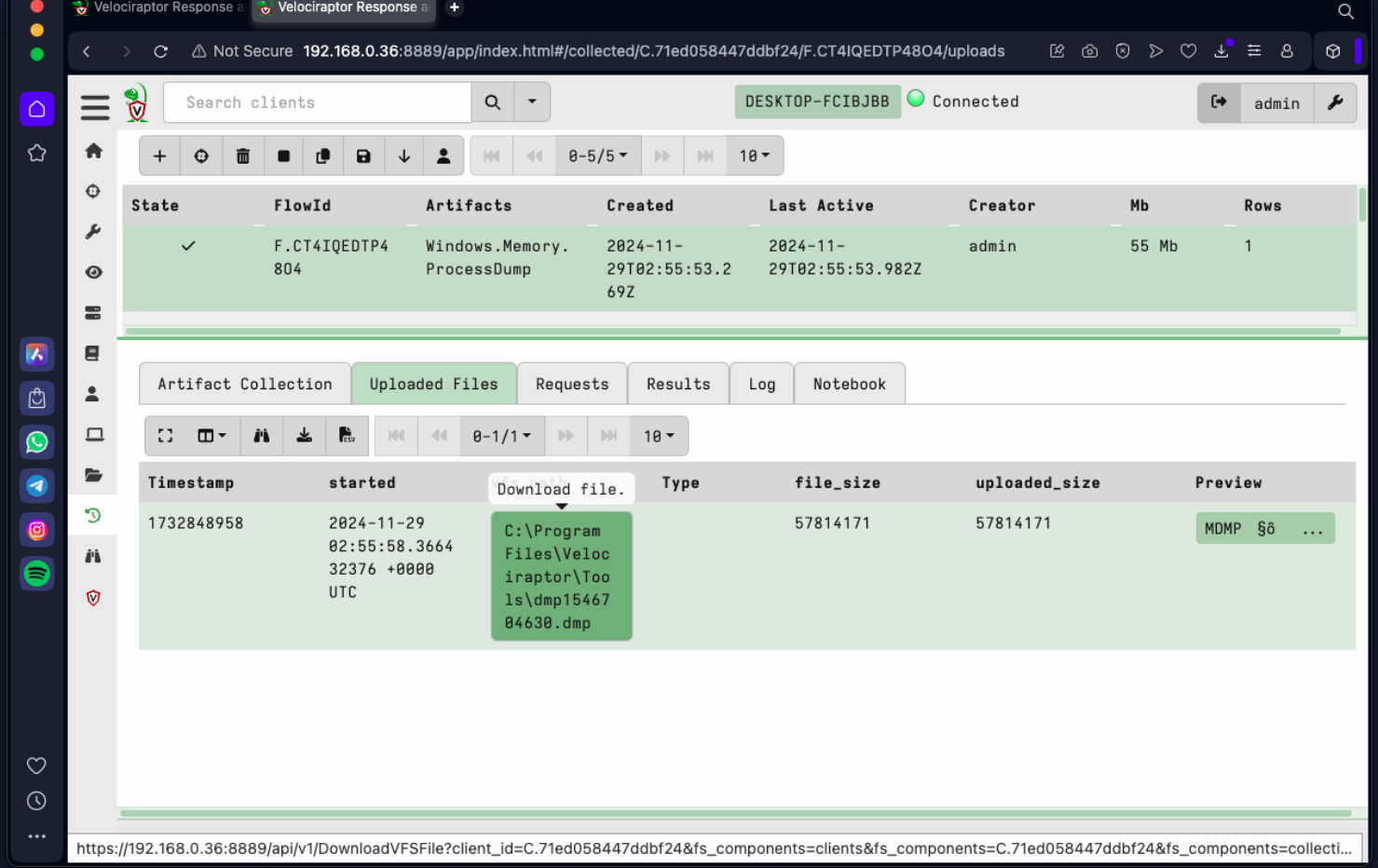
Remote: PowerShell Get-Process, Get-NetTCPConnection for quick triage

EDR platforms provide live memory introspection without separate tools

Velociraptor: live memory artifacts without full dump via VQL queries

Trade-off: speed vs. completeness — live analysis may miss injected code

Follow up live analysis with full dump on highest-priority systems


Velociraptor Response
Velociraptor Response
Not Secure 192.168.0.36:8889/app/index.html#/collected/C.71ed058447ddbf24/F.CT4IQEDTP48O4/uploads
Search clients
DESKTOP-FCIBJBB
Connected
admin
0-5/5
10
State
FlowId
Artifacts
Created
Last Active
Creator
Mb
Rows
F.CT4IQEDTP4804
Windows.Memory.ProcessDump
2024-11-29T02:55:53.269Z
2024-11-29T02:55:53.982Z
admin
55 Mb
1
Artifact Collection
Uploaded Files
Requests
Results
Log
Notebook
0-1/1
10
Timestamp
started
Download file.
Type
file_size
uploaded_size
Preview
1732848958
2024-11-29 02:55:58.366432376 +0000 UTC
C:\Program Files\Velociraptor\Tools\dmp1546704630.dmp
57814171
57814171
MDMP §ô ...
https://192.168.0.36:8889/api/v1/DownloadVFSFile?client_id=C.71ed058447ddbf24&fs_components=clients&fs_components=C.71ed058447ddbf24&fs_components=collecti...

Hibernation File & Page File as Memory Sources

hiberfil.sys: compressed copy of RAM written when system hibernates

Located: C:\hiberfil.sys — readable after mounting volume without booting

hiberfil.sys can be converted with volatility's imagecopy or specialized tools

Useful when: system was hibernated by attacker to avoid full acquisition

pagefile.sys: swapped-out memory pages — contains fragments from all processes

Located: C:\pagefile.sys — not a complete RAM image but supplements full dump

Pagefile analysis: strings, yara, and memory parsers can extract artifacts

SWAP on Linux: /dev/swapX — may contain encryption keys if system was running

Memory Acquisition on Modern Systems

Windows 10/11 HVCI (Hypervisor-Protected Code Integrity): kernel isolated in VSM

Secure Boot: limits which drivers can run — some acquisition tools need signing

Kernel patch guard (PatchGuard): blocks kernel-mode hooks used by older tools

WinPmem solution: uses a legitimate kernel driver signed by Microsoft

macOS: memory acquisition requires disabling SIP or booting to Recovery

Linux: /proc/kcore (kernel memory), /dev/mem (physical — usually restricted)

LiME (Linux Memory Extractor): loadable kernel module, streams image to file or network

Cloud VMs: no physical memory access; use hypervisor snapshot APIs instead

Containers: Must prepare monitoring tools in advance, like **Sysdig**


sysdig
Home
2 Accounts
3 Projects
3 Subscriptions
24 Agents
VULNERABILITIES
Vulnerability Findings Prioritization
88.84 K
Total
Critical
High
sysdig
Welcome to cloud security, the right way.
Sysdig helps security and development teams prevent, detect, and respond to threats, instantly and precisely.
You've landed on our CNAPP tour! Ready to see it in action?
Let's dig in.
GET STARTED
Powered by Navattic
88.8 K
Total
6,078
82,764
0
Registry Unique Vuln. Detections
800
600
400
200
0
1.08 K
Total
27
286
771
High
Medium

Conclusion

Volatile memory contains encryption keys, credentials, injected code, and network state

Collect RAM before rebooting — this evidence is gone forever after shutdown

Follow order of volatility: RAM before disk, network state before processes

Hash all collected images immediately to establish chain of custody

Remote and agent-based collection enables scale across the enterprise

hiberfil.sys and pagefile.sys extend memory analysis to offline and hibernated systems

Knowledge Check