HORIZONSHIELD

*Securing Your Digital Future, Today.*

THREAT INTEL SERIES · BOOK 13 OF 16

# Malware Analysis Guide

## Static, Dynamic & Advanced Techniques — 2026

Practitioner guide to malware analysis covering static analysis, dynamic sandbox analysis, memory forensics, and reverse engineering basics. Covers ransomware, RATs, rootkits, fileless malware, and IOC extraction.

| ANALYSIS TYPES | TOOLS | MALWARE FAMILIES | LEVEL |
|---|---|---|---|
| 4 | 40+ | 20+ | Advanced |

# Contents

MALWARE ANALYSIS 2026

CHAPTER 01

# Malware Analysis Lab Setup

*A properly isolated analysis environment is non-negotiable. Malware that escapes the lab infects the corporate network.*

ISOLATED NETWORK | REMnux | FlareVM | SNAPSHOTS



## Malware Analysis Lab Architecture

- **Host-only or isolated network ONLY** — analysis VMs must NEVER have internet access during dynamic analysis. Use FakeNet-NG or INetSim to simulate network services.
- **Snapshot before every analysis** — always revert to clean snapshot after analysis. Never analyse from a used/dirty state.
- **FakeNet-NG or INetSim** — simulate DNS, HTTP, SMTP, IRC to capture C2 behaviour without actual internet access.
- **REMnux** — Linux-based malware analysis distro with 100+ pre-installed tools: YARA, ClamAV, Volatility, Zeek, NetworkMiner.
- **FlareVM** — Windows-based analysis VM: Ghidra, IDA Free, x64dbg, OllyDbg, PEStudio, PEView, Wireshark, Process Monitor, Process Hacker.
- **No shared clipboard** — disable VM integration features during analysis. Disable drag-and-drop, copy-paste, shared folders.
- **Separate network adapters** — analysis VM on host-only network, REMnux as simulated internet gateway. No bridge to real network.

LINUX ANALYSIS

**REMnux**

Pre-built Ubuntu-based VM with 100+ malware analysis tools. Network analysis: Wireshark, Zeek, Suricata. Malware tools: Cuckoo, YARA, ssdeep, PEframe. Memory forensics: Volatility 3, LiME. Static: strings, binwalk, xxd. Available at: remnux.org

WINDOWS ANALYSIS

**FlareVM**

Windows-based analysis distro from Mandiant FLARE team. Reverse engineering: Ghidra (NSA), IDA Free, Binary Ninja demo, x64dbg. PE analysis: PEStudio, PEView, Dependency Walker. Dynamic: Process Monitor, Process Hacker, Regshot, Fakenet-NG. Install on Windows 10 VM.

| Tool | Category | Purpose | Platform |
|---|---|---|---|
| PEStudio | Static | PE header analysis, imports/exports, strings, entropy, VirusTotal lookup | Windows |
| FLOSS | Static | Extract obfuscated strings (not just plain strings command) | Windows/Linux |
| ExifTool | Static | File metadata extraction — compile time, author, suspicious timestamps | Both |
| Process Monitor | Dynamic | Real-time file, registry, network, process operations monitoring | Windows |
| Process Hacker | Dynamic | Process memory, handles, threads, loaded DLLs, network connections | Windows |
| Regshot | Dynamic | Registry snapshot diff — before/after malware execution | Windows |
| Wireshark | Dynamic | Full packet capture of all network traffic during execution | Both |
| x64dbg | Reverse Engineering | Open-source Windows debugger with plugin ecosystem | Windows |
| Ghidra | Reverse Engineering | NSA-developed disassembler/decompiler — free alternative to IDA Pro | Both |
| Volatility 3 | Memory | Memory forensics — process lists, network connections, injected code, credentials | Both |

CHAPTER 03

# Dynamic Analysis

*Executing malware in a controlled environment and monitoring all system interactions reveals behaviour that static analysis misses.*

PROCESS MONITOR | BEHAVIOURAL INDICATORS | NETWORK TRAFFIC | PERSISTENCE



## Dynamic Analysis Methodology

1. **Prepare Environment**

   BEFORE EXECUTION

   Verify network isolation (host-only adapter, FakeNet-NG running). Take CLEAN snapshot. Start monitoring tools: Process Monitor (all events, max buffer), Regshot (take snapshot 1), Wireshark (capture on host-only adapter), Process Hacker.

2. **Execute Sample**

   T+0

   Execute malware sample. For suspicious scripts: run with appropriate interpreter (python, PowerShell, cmd). For packers/crypters: wait 30-60 seconds for unpacking to complete before dumping memory.

3. **Observe & Document**

   T+0 TO T+10 MINUTES

   Document every observable action: new processes created, network connections attempted, files written/modified, registry changes. Look for anti-analysis checks (VM detection, debugger detection, sleep calls > 5 minutes).

4. **Take Snapshot 2 & Compare**

   T+10 MINUTES

   Regshot snapshot 2 — compare to snapshot 1 for registry and file changes. Filter Process Monitor output for suspicious operations. Export Wireshark pcap. Dump process memory for strings.

5. **Memory Analysis**

   T+10 MINUTES

   Dump memory of suspicious processes with Process Hacker. Scan with YARA rules. Extract strings. Look for injected code segments (RWX memory regions containing PE headers — malfind indicator).

6

**Document & Revert**

**END OF ANALYSIS**

Export all evidence (pcap, ProcMon log, Regshot diff, memory dumps, screenshots). REVERT to clean snapshot before removing from isolation. Never allow analysis VM to touch real network.

| Behavioural Indicator | What It Suggests | Data Source | Follow-Up Action |
| --- | --- | --- | --- |
| Process spawning cmd.exe or powershell.exe with encoded commands | Command execution, lateral movement preparation | Process Monitor, 4688 event | Decode encoded commands, identify C2 infrastructure |
| Scheduled task creation or service installation | Persistence mechanism | Registry: HKLM\SYSTEM\CurrentControlSet\Services, 4698 event | Document persistence location, determine trigger |
| LSASS process access (OpenProcess/ReadProcessMemory) | Credential harvesting | Process Monitor, Sysmon Event 10 | Extract credentials accessed, assume full credential compromise |
| HTTP/HTTPS connections to IP addresses (not hostnames) | C2 communication (bypasses DNS filtering) | Wireshark, FakeNet-NG | Extract IP, check threat intel, extract User-Agent |
| DNS queries to DGA-like domains (random strings) | DGA-based malware C2 | FakeNet-NG DNS log | Collect DGA domains, extract seed/algorithm if possible |
| File writes to temp directories + execution from temp | Dropper deploying payload | Process Monitor | Capture dropped files, analyse independently |

HS

**HORIZONSHIELD**

*Securing Your Digital Future, Today.*

## Malware Analysis Guide 2026

Part of the HorizonShield Security Series — 16 comprehensive professional cybersecurity manuals covering every domain of modern enterprise security.