AYI NEDJIMI Consultants

Volatility 3 : Framework Forensics Mémoire O

10 mai 2026 • Mis à jour le 17 mai 2026 • 17 min de lecture • 377 mo

> Volatility 3 est le framework open source de référence pour l'analyse foren
> Guide complet : architecture ISF, plugins Windows/Linux/macOS, détection
> workflow DFIR, alternatives Rekall et MemProcFS.

Volatility est le framework open source de référence mondiale pour l'**analyse fore**
forensics), maintenu depuis 2007 par la Volatility Foundation, organisation à but n
Écrit en **Python 3**, Volatility 3 (sortie initiale en 2020, version stable 2.7.0 publiée e
2.x après une réécriture totale du moteur, abandonnant le système de profils statiq
modulaire fondée sur les *symbol tables* (ISF — Intermediate Symbol File) et le méc
automatique du système d'exploitation analysé. Le framework prend en charge l'e
modules kernel, connexions réseau, registres Windows, hooks SSDT, injections de
(historique bash, command line, clipboard) et credentials hachés, à partir de captu
crash dump Microsoft, hibernation file, ELF core, LiME ou VMware snapshot. Utilis
laboratoires d'expertise judiciaire numérique, les ana ERT, SOC n
cybersécurité (SANS FOR508, FOR526, FOR610), Vo u le standar

post-mortem de la mémoire volatile sur Windows 7-11, Linux noyaux 2.6 à 6.x, et m
first présente exhaustivement l'architecture, les plugins majeurs, les workflows DF
les alternatives concurrentes (Rekall, MemProcFS) du framework Volatility en 202

À RETENIR

Points clés à retenir

Volatility 3 est un framework Python 3 open source d'analyse forensique d
la Volatility Foundation.

Successeur de Volatility 2.x, il abandonne les profils statiques au profit des
Files) et de l'*automagic*.

Plus de 200 plugins couvrent Windows, Linux et macOS pour processus, r
credentials.

Workflow DFIR standard : acquisition → triage → analyse approfondie → re

Alternatives modernes : Rekall (fork archivé), MemProcFS (live memory, pe

Licence : Volatility Software License (VSL), dérivée GPLv2, gratuite et libre

Définition : qu'est-ce que Volatility ?

Volatility est un **framework Python d'analyse forensique de mémoire vive** (memo
permettant l'examen post-mortem du contenu de la [illegible] d'exploitat
Conçu pour les enquêteurs forensiques numériques [illegible] éponse à in

Réponse sous 24h

Devis gratuit →