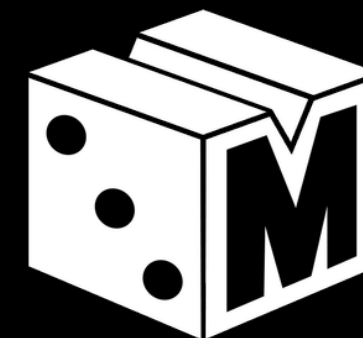




Salerno, 15/07/2026

Memory Forensics collaborativa nelle CTF

Analisi di dump di memoria con VolWeb e Volatility 3

About Me

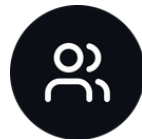
Marco Ferrara / bOru / <https://imbOru.github.io>

set 2022



Mntcrl Lab

gen 2025



Cyber Security Instructor, CyberChallenge.IT

mag 2025



Locked Shields 2025, NATO CCDCOE

ott 2025



MSc Cybersecurity, UniBa

ott 2025



Cyber Incident Responder, Deloitte



Team MNTCRL



Memory Forensics

CPU > Cache > **RAM** > Virtual Memory



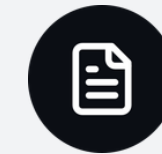
Processi e thread



Malware in esecuzione



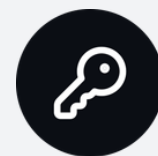
Connessioni e IP



File aperti



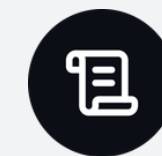
Password e clipboard



Chiavi di cifratura



Configurazioni HW/SW



Registry e log



Volatility 3

Cos'è

- Framework open source per memory forensics multi-OS
- Standard dal 2007, ora v3
- 100+ plugin di analisi

Limiti Operativi

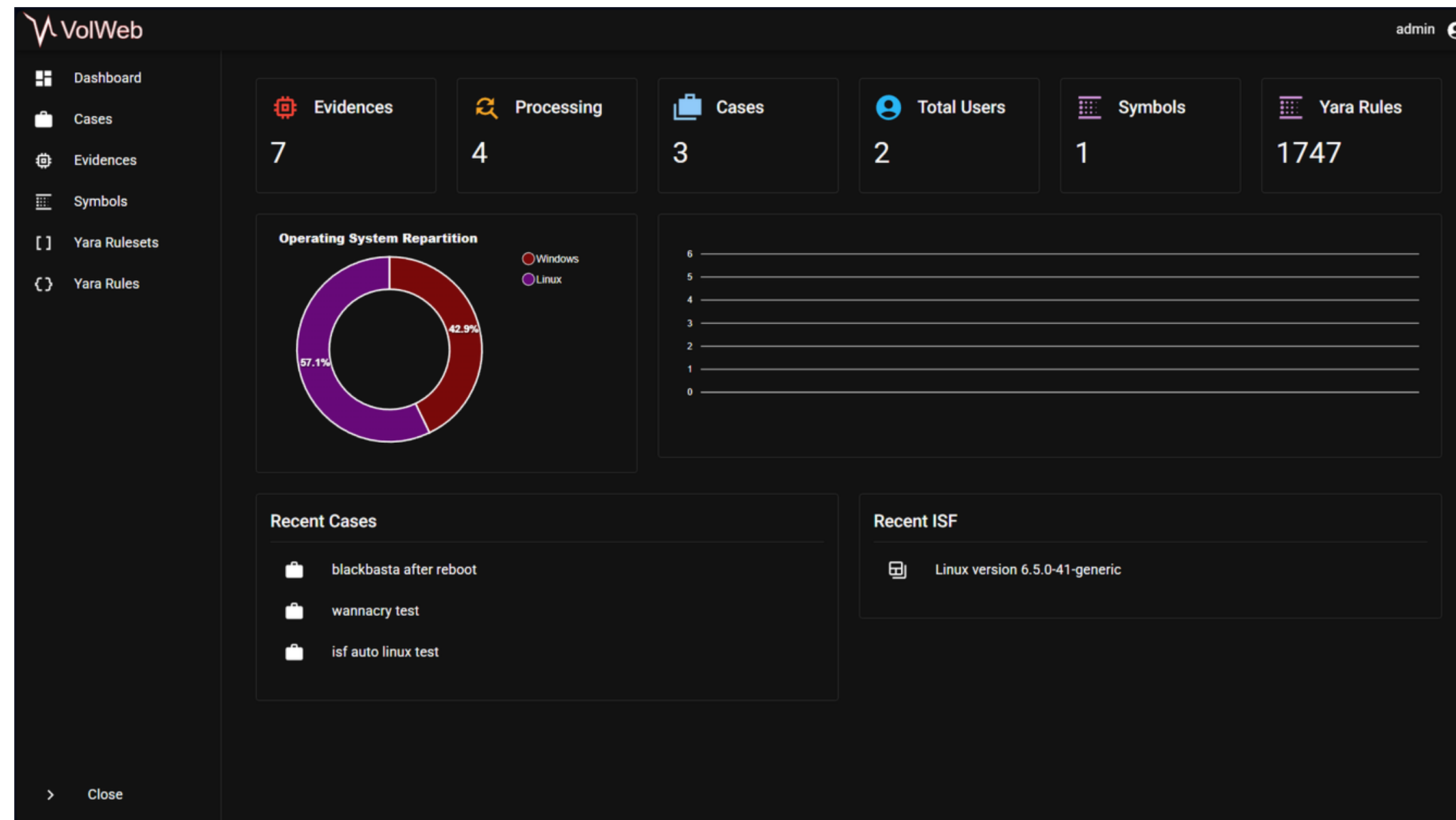
- Solo CLI: 100+ comandi da memorizzare
- Output grezzo: tabelle testuali difficili da interpretare e correlare
- Zero automazione: analisi manuale processo per processo, plugin per plugin

```
(.volatility3ENV)-(root@kali)-[~/Desktop/Tools/volatility3]
# ./vol.py -f /root/Desktop/victim.raw windows.handles --pid 268
Volatility 3 Framework 2.7.1
Progress: 100.00 PDB scanning finished
PID Process Offset HandleValue Type GrantedAccess Name
268 smss.exe 0xfa800232ccb0 0x4 File 0x100020
268 smss.exe 0xfa800232ca60 0x8 EtwRegistration 0x8
268 smss.exe 0xfa800232c910 0xc File 0x1f01ff
268 smss.exe 0xfa800232c7c0 0x10 File 0x1f01ff
268 smss.exe 0xfa800232c670 0x14 File 0x1f01ff
268 smss.exe 0xfa8002328070 0x18 File 0x1f01ff
268 smss.exe 0xfa8002328f20 0x1c File 0x1f01ff
268 smss.exe 0xfa8002328dd0 0x20 File 0x1f01ff
268 smss.exe 0xfa8002328c80 0x24 File 0x1f01ff
268 smss.exe 0xfa8002328b30 0x28 File 0x1f01ff
268 smss.exe 0xfa800232c580 0x2c IoCompletion 0x1
268 smss.exe 0xfa8002328a10 0x30 TpWorkerFactory 0xf
268 smss.exe 0xfa8002328250 0x34 ALPC Port 0x1
268 smss.exe 0xfa8002a93940 0x38 Event 0x1f0003
268 smss.exe 0xf8a003a12060 0x3c Section 0x6
268 smss.exe 0xf8a000219870 0x40 Directory 0xf
268 smss.exe 0xf8a0000061c0 0x44 Directory 0xf
268 smss.exe 0xfa8002addb60 0x48 Event 0x1f0003
268 smss.exe 0xf8a000224060 0x4c KeyedEvent 0xf
268 smss.exe 0xfa8002264550 0x50 Process 0x101441
268 smss.exe 0xfa800229d070 0x54 ALPC Port 0x1
```

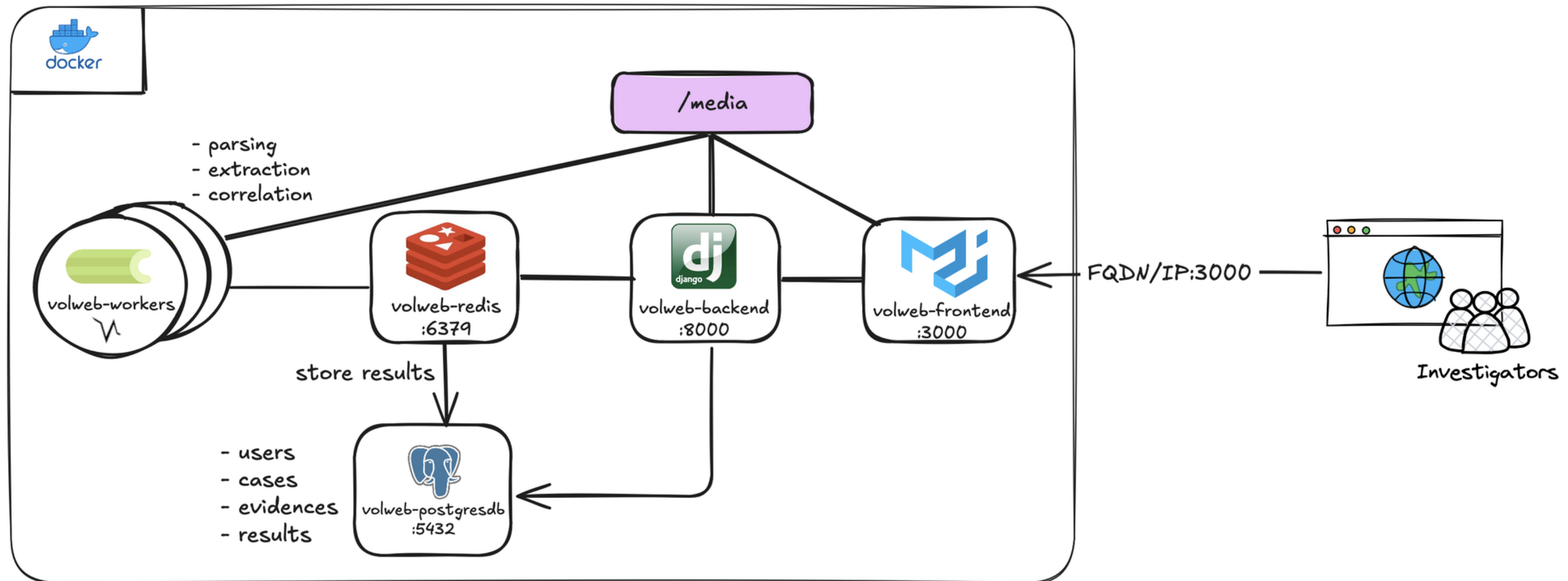


VolWeb

VolWeb è un'interfaccia web open source per Volatility3 che rende l'analisi della memoria accessibile e collaborativa: gestione di casi ed evidenze, esecuzione dei plugin Windows/Linux con risultati visuali (tabelle, grafo dei processi, timeline), scanning YARA, risoluzione automatica dei simboli ISF Linux ed estrazione di IOC con export STIX, il tutto condivisibile tra team distribuiti.



VolWeb



Demo

Team MNTCRL



CTF vs Real World

ASPETTO	IN CTF	IN INCIDENT RESPONSE
Evidenze	Un solo dump di memoria, di solito pochi GB.	Centinaia di GB o TB: dump di memoria di decine di endpoint, oltre a disco, log e telemetria.
Obiettivo	Ricostruire la challenge e trovare la flag.	Ricostruire l'accaduto, estrarre IOC e IOA, documentare la attack chain e, a compromissione in corso, dare subito elementi per il contenimento.
Tempistiche	Il tempo della gara, uguale per tutti.	SLA contrattuali e un attaccante che magari e' ancora dentro: le prime ore decidono il contenimento.
Ambiente	Un dump costruito ad hoc: tutto cio' che e' strano e' voluto.	Un sistema di produzione pieno di software legittimo che sembra sospetto: serve una baseline per separare rumore e segnale.
Analisti	In gara la piattaforma velocizza, ma di rado hai piu' player forensics sulla stessa challenge.	Piu' analisti sullo stesso caso e sugli stessi host, spesso su turni: lavorare sugli stessi dati non e' un extra, e' il metodo.



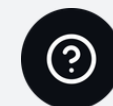
Piu' analisti, un caso

Il dump sta sulla piattaforma: ognuno lancia i suoi plugin senza passarsi file da decine di GB.



Risultati persistenti

L'output dei plugin resta salvato e consultabile: niente risultati persi nei terminali.



Copertura visibile

Vedi cosa e' gia' stato analizzato e cosa manca: nessuna ipotesi verificata due volte.



Handover rapido

Chi subentra riparte dai risultati, non dal dump: sui turni di un caso lungo vale ore.

\$ la piattaforma condivisa: in gara un vantaggio, su un caso un requisito



Q&A / Feedback

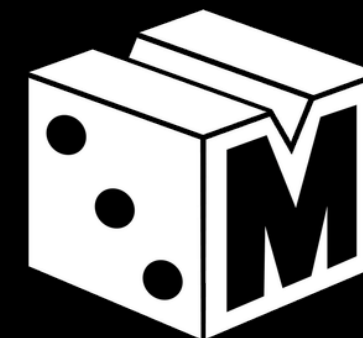
VolWeb GitHub repo



<https://github.com/k1nd0ne/VolWeb>

Team MNTCRL





Salerno, 15/07/2026

Grazie!

