RHOMBUS · USE-CASE BRIEF · DFIR

Digital forensics & IR

Examine host evidence where the incident happened

The Rhombus console deploys forensic workstations for digital forensics and incident response (DFIR) onto the kit itself. Analysts collect triage evidence from endpoints, examine disk images and Windows artifacts, and build a timeline without shipping evidence off site.

01 · WHY IT MATTERS

- An alert says something happened; host evidence shows what, where and for how long.
- Disk images and artifacts often cannot leave the network where they were collected.
- Teams need the same forensic workflow in training and on a live mission.

02 · HOW IT WORKS ON RHOMBUS

- Autopsy and command-line Windows artifact parsers install on the analyst workstation from the kit's own mirror.
- Parsers cover event logs, registry hives, Prefetch, shortcut files, the master file table and volume shadow copies.
- Velociraptor builds an offline triage collector for each engagement, so endpoints the kit doesn't manage can be collected without a full disk image. Windows collectors can also capture a memory image.
- Magnet Forensics AXIOM, optional and licensed separately, deploys as its own examination workstation.

FIG · 01 FROM DEPLOYMENT TO RESULTS

01	02	03	04
Deploy the forensic workstation from the console.	Run a Velociraptor triage collector on each endpoint, or bring the case's disk images onto the workstation.	Examine disk images in Autopsy and parse Windows artifacts.	Build the case timeline in Autopsy and report findings.

03 · DEFENSE & GOVERNMENT

- Defensive cyber operations (DCO) examination of the host evidence behind a Security Onion alert.
- Incident response on a disconnected network where images must stay in the enclave.
- Forensics training on lab disk images.

04 · COMMERCIAL & ENTERPRISE

- Enterprise incident response teams examining images on site.
- Banks and financial services investigations where evidence must stay in house.
- Critical infrastructure sites investigating hosts without outside connectivity.

05 · OUTCOMES

- Deleted files, persistence and execution evidence are recovered from disk images on the kit.
- Evidence stays on the kit from intake to report.

06 · CONSIDERATIONS

- Collection is offline. Triage collectors run on each endpoint and their results are brought back to the kit.
- Magnet Forensics AXIOM is optional and licensed separately. You supply the license.

INTEGRATED TOOLS

Autopsy | Velociraptor | Magnet Forensics COMMERCIAL

Commercial products licensed separately · Trademarks of their owners; no endorsement implied