

Law enforcement agencies are overwhelmed with the growth and complexity of digital evidence. Whether you're triaging mobile devices and computers in the field or working through a backlog of evidence back in the lab, time to evidence is critical. With Magnet OUTRIDER, examiners and nontechnical stakeholders can quickly and easily find information that is imperative to their case.

# **OUR SOLUTION**

### Rapid Triage

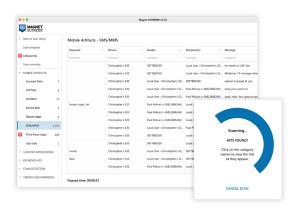
Uncover CSAM and other illicit content from mobile devices, computers and hard drives in the field or in the lab in under 6 minutes\* without having to perform a full extraction.

# **Actionable Insights**

Quickly identify apps and other key insights on a phone, computer, or hard drive, at the outset of an investigation to give your team real-time intel for interviews, warrants and seizures.

### No More Manual Scans

Start running OUTRIDER in less than three steps by using preconfigured artifact categories that automatically count and display the number of hits during scans.





OUTRIDER is becoming the most efficient thing we could ever dream up in an ideal world. It saves so much measurable time while also allowing us to focus only on devices that need it. It is possible in some cases to only use this tool."

### FORENSIC EXAMINER

Large police agency in the USA

# **MAGNET** OUTRIDER

# **FEATURES**

Triage devices for illicit content such as CSAM in the field or the lab with automated insights, enabling examiners and non-technical stakeholders to use Magnet OUTRIDER with confidence.

#### Scan Android Devices

- No more manual scans: Automatically search SMS/MMS messages, device ID, recently used apps, contact list, call logs, and more, to find actionable evidence in minutes, leaving a minimal footprint on the device.
- Detect the presence of secure folders and multiple user accounts.
- Scan multiple devices at once to save time in the field.

## Search Using Customizable Keyword Lists & NCMEC Reports

- Edit OUTRIDER's existing keyword list or import your own keywords, like account names, device ID's, browser terms, and URLs to find evidence quickly.
- CSAM has indicative file names, leveraging common or known keywords is an extremely fast and effective way to locate contraband.
- Scan internet browser history for keywords using a NCMEC CyberTip report to bring in URLs and file names as keywords.

## Live System Scans Including RAM Capture

• Collect valuable Windows operating system artifacts, capture RAM, take a screenshot of the desktop, and obtain the external IP address for the system.

### Preserve & Report Evidence

- Once scans are complete, a report is generated including details about the scan, what keywords were used, and any files of interest from the device that were saved.
- Create separate reports for each device when parallel scans are completed.
- Compatible with Magnet AXIOM and other third-party forensic tools that can be used to analyze evidence further.

# **Identify Devices**

• Obtain the external IP address of a live computer to cross-reference with other intelligence systems like the Child Protection System (CPS) or ICACCOPS.

Learn more at magnetforensics.com

Speak to an expert today, call us at 1-844-638-7884 or email sales@magnetforensics.com

