MAGNET OUTRIDER™

USER GUIDE

CONTENTS

What's new 5

About Magnet OUTRIDER 7

Getting started with Magnet OUTRIDER 9

Understanding system changes 9

Windows 9

macOS 10

Android and iOS 10

Preparing a Mac device to be scanned 11

Step 1: Allow full disk access for Terminal 11

Step 2: Run the Magnet OUTRIDER admin script 12

Preparing a mobile device to be scanned 13

Preparing an Android device 13

Turn on Developer mode 13

Turn on USB Debugging 13

Preparing an iOS device 14

Scanning a target 15

Connect the device 15

Start the scan 15

Encryption detection 16

Supported evidence sources 16

Reviewing scan results 19

Understanding "No hits found" results 19
View the scan report 20
Scan report folder contents 20
Configuring a scan template 23
Configure a scan template 23
Scan option categories 23
Files and apps 23
Artifacts 29
Live system 29
Mobile 31
CSAM detection technology 32
Reporting options 33
Scan and report settings 35
Scan settings 35
Report settings 35
Supported applications 36
Anti-forensic files 36
Built-in file collection 37
Cloud storage apps 38
Cryptocurrency apps 38
Dark web apps 39
Encryption Apps 39
Gaming Apps 40
Messaging Apps 40
Peer-to-Peer (P2P) Apps 41

Virtual Machine Apps 42
Virtual private network (VPN) Apps 42
Web Browsers 43

WHAT'S NEW

Version	Description
4.1	• Updated About Magnet OUTRIDER and Configuring a scan template with information about MAG24 hash matching, VICS and CAID hash lists deduping and conversion to MAG24, and Android Gallery and Download hash matching • Updated Scan and report settings with information about the blur media option.
4.0	• All topics have been updated due to Android MMS support, iOS Support, MD5 Custom Hashes, NCMEC PDF Scraping, and support for Windows To Go
3.5.1	• There are no documentation updates for this release
3.5.0	• There are no documentation updates for this release
3.4.0	• There are no documentation updates for this release
3.3.0	• There are no documentation updates for this release
3.2.0	• All topics have been updated and reorganized to accommodate new features introduced by the updated user interface for both Windows and macOS versions of Magnet OUTRIDER. • Updated Configuring a scan template with new scan options and more information about adding keywords. • Updated Supported applications with more VPN applications and information about which versions of applications are detected.
3.1.0	• Added Preparing a Mac device to be scanned. • Updated Configuring a scan template with new scan options. • Updated Supported applications with supported web browsers.

Version	Description
3.0.0	• All topics have been updated and reorganized to accommodate new features introduced by the macOS version of Magnet OUTRIDER.
2.2.0	• Updated with information about the option to display or hide thumbnails for potential CSAM hits. • Updated Scanning a target with information about using the Disk Manager in bootable environments.
2.1.0	• Updated with information about scanning connected networks, new supported operating system artifacts, and customizing case and report locations.
2.0.0	• Updated Reviewing scan results with information about new supported apps. • Updated Scanning a target with information about scanning specific folders. • Updated with information about regex keywords and NCMEC report data. • Updated Reviewing scan results with information about reporting false positive hits using CRC CSAM detection technology. • Updated Viewing and exporting scan reports with information about new features in scan reports. • Updated and reorganized with information about new configuration options. • Updated Getting started with Magnet OUTRIDER with current system requirements.
1.5.0	• Initial version

ABOUT MAGNET OUTRIDER

Use Magnet OUTRIDER at the beginning of your investigation to triage Windows and macOS computers, external drives, and mobile devices by quickly scanning target devices for contraband content and applications.

- Search for potential dark web, P2P, cloud storage, encryption, anti-forensics, gaming, messaging, virtual machine, VPN, and cryptocurrency apps and files.
- Enhance your scans by loading keywords, regex keywords, and NCMEC CyberTip reports.
- Search browser history for URLs and keywords.
- For Windows scans, collect operating system artifacts, capture RAM, scan for drive encryption, take a screenshot of the desktop, search running processes, scan the connected network for devices, and obtain the IP address from the live system.
- For macOS scans, search running processes and obtain the IP address from the live system.
- For Android scans, collect device and user info artifacts; list third-party apps and recently used apps; obtain account data, call logs, and contacts; search SMS/MMS for keywords; and match known hash lists against MMS, Gallery, and downloaded media.
- For iOS scans, view Safari history and recent Safari searches; collect device and user info artifacts; list third-party apps; obtain account data, call logs, and contacts; search SMS/MMS for keywords and hash matches.

Law enforcement customers can use technology from the Child Rescue Coalition (CRC) to quickly identify known CSAM content even if no keyword hits were found in file names. This technology analyzes all of the files scanned by Magnet OUTRIDER (not including files found in ZIP files) using hashes from international law enforcement CSAM databases.

Using the ProjectVicToFlatFile tool included with Magnet OUTRIDER, you can deduplicate VICS and CAID hash files and convert the files to a MAG24 flat file hash list via Command Prompt. Note that only MD5 hashes with media sizes are added to the flat file.

After a scan completes, you can review the items of interest in the app, export evidence, and view a summary report generated by the app.

GETTING STARTED WITH MAGNET OUTRIDER

If your organization has purchased Magnet OUTRIDER, you'll receive the product on a USB dongle that you can take with you on your investigations. If you're using a trial license of Magnet OUTRIDER, you'll receive an email from Magnet Forensics , which includes an installation file and license key.

See the Knowledge Base articles below for information about running and activating Magnet OUTRIDER on your system:

- System requirements for Magnet OUTRIDER
- Install Magnet OUTRIDER
- Activate Magnet OUTRIDER
- Updating Magnet OUTRIDER

Understanding system changes

When you run Magnet OUTRIDER, some changes might be made to the system, depending on the operating system.

Windows

Magnet OUTRIDER does not modify or create any files on the system where it is run. However, a few files are created automatically by the Windows system. If you run Magnet OUTRIDER on a system and then examine evidence from the system more closely using a forensic tool such as Magnet AXIOM, you'll find registry keys and prefetch files in the evidence that were created when you connected the USB drive and ran Magnet OUTRIDER.

- Registry keys are created when Magnet OUTRIDER is run from a USB dongle. These registry keys match the hardware ID of the USB drive.

- Prefetch files, such as MAGNET OUTRIDER.EXE-<value>.pf, are created in C:\Windows\Prefetch when Magnet OUTRIDER is run on a computer.

macOS

When you first run Magnet OUTRIDER, dynamic libraries are extracted to the installed location folder and remain there for subsequent runs of the product. Files are created, modified, and deleted from the Logs, Resources, and Reports folders in the Magnet OUTRIDER X.X macOS folder. These files remain between runs.

Temporary files are created in a few locations. These files are removed upon graceful exit of the application. However, if Magnet OUTRIDER terminates unexpectedly, these files may remain. These locations include:

- /System/Volumes/Data/private/var/folders/cl/
- /System/Volumes/Data/Users/[username]/Library/Saved Application State/-com.magnetforensics.outrider.savedState

Examples of the temporary files created in these locations include:

- CASESENSITIVETESTf3be3efe5b8447bda29e003a8905d265
- dotnet-diagnostic-8334-1634696265-socket
- clr-debug-pipe-8334-1634696265-in
- clr-debug-pipe-8334-1634696265-out

To access folders on the system, entries are added to the Transparency, Consent and Control (TTC) database. The bundle ID is com.magnetforensics.outrider.

Android and iOS

Magnet OUTRIDER does not modify or create any files on the target device.

PREPARING A MAC DEVICE TO BE SCANNED

By default, Magnet OUTRIDER does not have permissions to scan protected system paths and private user folders. You must allow full disk access for Terminal and run the Magnet OUTRIDER admin script. For more information on granting full disk access, see Controlling app access to files in macOS.

Step 1: Allow full disk access for Terminal

Consider running an initial scan of the device without full disk access to detect all running applications.

Before you begin: Close any instances of Terminal that are open.

1. Open **System preferences**, and then click **Security and privacy** > **Privacy**.
2. Select **Full disk access**, and then click the lock icon.
3. Enter an admin account's username and password.
4. Complete one of the following actions:
   - If **Terminal** is in the list of allowed apps, select the checkbox next to the application.
   - If **Terminal** is not in the list of allowed apps, click the **Add** button **+** and navigate to **Applications/Utilities/Terminal**. Click **Open**.
5. Close the window.

If you need to return the device to its previous state, remove full disk access from the terminal after you have scanned the device.

Step 2: Run the Magnet OUTRIDER admin script

1. In your Magnet OUTRIDER installation folder, double-click **Start OUTRIDER for macOS (admin).command**.
2. In the Terminal window that opens, enter the root password and press **Enter**.
3. Keep the Terminal window open and use Magnet OUTRIDER as you normally would.
4. Close the Terminal window when you are done using Magnet OUTRIDER.

PREPARING A MOBILE DEVICE TO BE SCANNED

To scan a target mobile device, you can run Magnet OUTRIDER from one of the following storage devices on a Windows 10+ computer with minimum 2 GB of RAM:

- USB (minimum 32 GB)
- External SSD
- Fixed drive

Use a forensic workstation to scan the target mobile device. Do not perform the scan from the suspect's computer.

Preparing an Android device

You must enable developer mode and USB debugging before scanning an Android device. Developer mode and USB debugging settings are in different locations depending on the device manufacturer and system version. If your screen does not match the following steps, see Configure on-device developer options for other options.

Turn on Developer mode

1. Go to **Settings** > **About phone** > **Software information**.
2. Tap **Build number** seven times and enter the device PIN, if requested.

Turn on USB Debugging

1. Turn on USB debugging in **Settings** > **System** > **Advanced** > **Developer Options** > **USB debugging**.
2. Connect the target device to the computer you're running Magnet OUTRIDER from.
3. When the device requests USB debugging, click **Allow**.

After turning on developer mode and USB debugging for the target device, click **Select evidence** > **Refresh all** in Magnet OUTRIDER, and follow the instructions for Scanning a target.

Preparing an iOS device

You must have the iTunes application installed on the computer running Magnet OUTRIDER before initiating an iOS device scan.

1. Unlock the target iOS device.
2. Connect the target iOS device to the computer you're running Magnet OUTRIDER from.
3. When the device requests to allow access, click **Allow**.

When the target device is ready, click **Select evidence** > **Refresh all** in Magnet OUTRIDER, and follow the instructions for Scanning a target.

SCANNING A TARGET

If this is your first time using Magnet OUTRIDER, consider configuring Scan and report settings.

Connect the device

- To scan Windows or macOS computers, connect your Magnet OUTRIDER dongle to the target computer.
- To scan external drives, connect to a forensic workstation using a forensic writer-blocker.
- To scan mobile devices, connect the target device using a device-appropriate cable to a forensics workstation.

Start the scan

1. Open Magnet OUTRIDER.
   - Windows: Double-click the **Start OUTRIDER for Windows.bat** file.
   - macOS: Double-click either the **Start OUTRIDER for macOS (admin).command** or **Start OUTRIDER for macOS.command** file, depending on whether you have the admin password or not.
2. Enter a case number.
3. Select or configure a scan template.
4. Select evidence to scan.
5. Start the scan.

If necessary, you can stop a scan at any time. When you stop a scan, Magnet OUTRIDER generates scan reports based on the evidence already scanned. These reports are saved to the Reports folder. For more information, see Reviewing scan results.

If Magnet OUTRIDER is running from a location that is either read-only or does not have write permission, reports cannot be saved to that location.

Encryption detection

This feature is available for Windows scans only.

When Magnet OUTRIDER launches, it loads the drives available to be scanned and automatically checks the computer and its attached drives for Bitlocker encryption. When configuring your scan template, you can optionally include information about encryption detection in your scan report. If Magnet OUTRIDER detects a drive that has been encrypted and password-locked using Bitlocker, you'll be notified of which drive has been detected as a Bitlocker locked drive.

If decryption is detected, you can choose to continue with the scan or close Magnet OUTRIDER. This report on encryption, including available recovery keys and passwords for detected Bitlocker drives, will be automatically placed in the case folder.

If Magnet OUTRIDER does not detect encryption, that doesn't guarantee that no encryption is present on the system. Magnet OUTRIDER may not be able to detect some types of encryption.

If encryption is detected, do not shut your device down unless you have the password to decrypt the encrypted containers or drives. Consider saving files or creating a live forensic image of the drive while the computer is on and you have decrypted access to the data.

Supported evidence sources

Target	Description	Windows	macOS
Computers	In addition to those options selected in your scan template, a computer scan includes: • File names of running processes	✓	✓

Target	Description	Windows	macOS
	• All files and drives attached to the system		
External drives	External drives include those that do not have a USB interface as well as USB drives that are not already connected to the target computer. To scan these devices, connect them to a forensic workstation using a forensic write-blocker that has the Magnet OUTRIDER dongle inserted. An external drive scan includes file names of all files on the selected drives in addition to any options selected in the scan template. By default, the system drive is not selected.	✓	✓
Android devices	Scan Android devices running Android 12.0 and above. To scan these devices, connect them to a forensic workstation running Magnet OUTRIDER using a device appropriate USB cable. Android devices typically use USB-C or Micro-USB. In addition to those options selected in your scan template, an Android device scan includes: • Account data, user data, and device info • Any third-party apps installed on the device and a list of recently used apps • Contacts list • Call logs • SMS/MMS logs	✓	

Target	Description	Windows	macOS
	• Hashing of media from Gallery app and downloads		
iOS devices	Scan iOS devices running iOS 4 and above. To scan these devices, connect them to a forensic workstation running Magnet OUTRIDER using a device appropriate USB cable. iOS devices typically use Lightning cables. In addition to those options selected in your scan template, an iOS device scan includes: • Account data, user data, and device info • Any third-party apps installed on the device • Safari history and recent searches • Contacts list • Call logs • SMS/MMS logs	✓	
Bootable drives	Bootable environments, such as Windows To Go or WinPE/FE, drives are offline by default and not visible to other applications such as Magnet OUTRIDER. Drive Manager in Magnet OUTRIDER can be used to bring these drives online in a read-only state for scanning.	✓	

REVIEWING SCAN RESULTS

As Magnet OUTRIDER scans a device, you can view the scan progress, including how many artifacts have been processed and how many items have been scanned in real time. As the scan progresses, you can start to review hits:

- Click an application category to view new hits or to refresh a category. When hits have been found, category names are highlighted in bold.
- Review critical hits marked an exclamation mark next to the title.
- Right-click a file result to open the source location of the file or to save the source file.

Warning: Opening files on a live system can change timestamps or modify data associated with the accessed files.

Understanding "No hits found" results

If Magnet OUTRIDER returns a result of *No hits found*, the drive isn't necessarily clear of relevant apps, keyword matches, or CSAM content. Some users are capable of hiding files from the application. However, scanning devices with Magnet OUTRIDER helps you prioritize between multiple target devices.

It is also possible that Magnet OUTRIDER was not able to recover hits if the file names on the scanned device do not match any of the loaded keywords. Magnet OUTRIDER reports whole word keyword hits to help reduce the chance of false positives.

Positive hits in Magnet OUTRIDER is a good indication that you'll want to take a closer look at a particular device, but negative hits don't necessarily mean there's nothing to be found.

View the scan report

When Magnet OUTRIDER finishes scanning a computer, view a complete report to gain insight into the results of the scan. If you cancel your scan, your report includes items that were scanned up until the point that the scan was canceled.

To view your report, complete one of the following actions:

- In Magnet OUTRIDER, click **Open report**.
- Browse to **Magnet OUTRIDER_<X.X.X.XXX>\Reports**.

Scan report folder contents

Depending on the scan options that you enabled, you might not have some of the files or folders listed below.

Windows

File / folder	Description
Collected_OS_Artifacts	Contains .txt files with collected operating system artifacts.
thumbnails	Contains thumbnails of CSAM hits.
Desktop.png	The captured screenshot of the desktop.
Live System Encryption Report.txt	Lists the details of encryption detected during the scan.
pathlist.txt	Contains a list of saved paths.
ramcapture.bin	The live system's RAM captured using the Magnet RAM Capture tool.
computer.html	Lists information about the hits that were found during the scan, in HTML format.
SavedFiles.zip	Contains the files that you chose to save after the

File / folder	Description
	scan completed. You can save files from the Filename Keyword Hits and CRC CSAM Hits categories.
styles.css	The stylesheet used to format the HTML report.

macOS

File / folder	Description
computer.html	Lists information about the hits that were found during the scan, in HTML format.
styles.css	The stylesheet used to format the HTML report.
thumbnails	Contains thumbnails of CSAM hits.

Android

File / folder	Description
<device identifier>.html	Lists information about the hits that were found during the scan, in HTML format. The device identifier will change based on the target device's model and serial number.
styles.css	The stylesheet used to format the HTML report.

iOS

File / folder	Description
<device identifier>.html	Lists information about the hits that were found during the scan, in HTML format. The device identifier will change based on the target device's model and serial number.

File / folder	Description
styles.css	The stylesheet used to format the HTML report.

CONFIGURING A SCAN TEMPLATE

Scan templates contain pre-configured options for you to choose from in order to quickly and easily scan a target. Scan options can be operating system specific. If you're configuring a scan template for a certain operating system, you can filter the options to pick from by setting the operating system type before you start to configure the template.

Configure a scan template

1. Complete one of the following actions:
   - To create a new template, from the **Scan setup** page, click **Add new template**.
   - To edit a template, select an existing scan template, and then click **Edit template**.
2. Add or modify the name for the scan template.
3. Set the operating system you want to view the scan options for.
4. Configure the options to include in the scan.

Scan option categories

- Files and apps
- Artifacts
- Live system
- CSAM detection technology
- Reporting options

Files and apps

Setting	Description	Windows	macOS	Android	iOS
Locate files	Add an MD5 hashset in a	✓	✓	✓	✓

Setting	Description	Windows	macOS	Android	iOS
with MD5 hashes matching the source hashes	flat file. MD5 and MAG24 hash files will be listed for selection or deletion. You can use the ProjectVicToFlatFile tool included with Magnet OUTRIDERto deduplicate VICS and CAID hash files and convert the files to a MAG24 flat file hash list. Note that only MD5 hashes with media sizes are added to the flat file. Note: Support for iOS is limited to media that was shared through iMessages/SMS/MMS. No other media in iOS is hash matched.				
Search files using a keyword list	Enter individual keywords or add keyword lists to locate file name-based keyword hits by scanning for file name matches. Magnet OUTRIDER includes a default list of CSAM-related keywords for law enforcement agencies to help identify	✓	✓	✓	

Setting	Description	Windows	macOS	Android	iOS
	files that contain CSAM or other content. Keyword lists must be in .txt files and each keyword must be on a separate line. Keyword lists are applied to the following categories: • File names • Running processes • Browser search history • Contacts • SMS/MMS logs • Call logs Keyword lists are not shared between scan templates.				
Match on whole word	Search for whole word matches rather than partial instances of keywords. Matching on a whole word reduces the number of false positive hits	✓	✓	✓	

Setting	Description	Windows	macOS	Android	iOS
	as system or program files could be matched as partial hits on keywords. For example, the file name "msg_qwihr35yowlji90.dat" would be considered a hit for the keyword "5yo" if you don't match on a whole word. Make sure that word bounding characters exist on either side of the keyword. The following file names would be matched for the keyword "5yo": "5yo.jpg", "downloaded 5yo.mp4", "5yo_new.png", "first_5yo-file.avi". However, "msg_qwihr35y-owlji90.dat" would not be matched as it does not have word boundary characters surrounding the keyword.				
Search files using a regex keyword list	Enter individual regex keywords or add regex keyword lists lists to locate file name-based keyword hits by scanning	✓	✓	✓	

Setting	Description	Windows	macOS	Android	iOS
	for file name matches. Regex keyword lists must be in .txt files and each regular expression must be on a separate line. Regex keyword lists are not shared between scan templates.				
Locate apps of interest	Search for known application executable files to locate apps of interest in categories such as dark web apps, encrypted apps, VPN apps, and more. For a complete list of supported apps, see Supported applications.	✓	✓	✓	
Locate files of interest for optional collection purposes	Locate files of interest such as cryptocurrency wallet files, cloud storage decryption key files, and more. For a complete list of supported files, see Supported applications and review the Built-in file col-	✓	✓	✓	

Setting	Description	Windows	macOS	Android	iOS
	lection list.				
Scan the first tier of file names within ZIP files	Scan files that are stored within a ZIP archive file to locate keyword or regex keyword hits, even if the .zip file is password-protected. Only file names are scanned. The file content within .zip files is not analyzed (using the CRC CSAM Detection or otherwise).	✓	✓		
Search priority paths	Scan the following directories first for every user listed on the device: • Browser history directories • Documents • Downloads • Desktop • Pictures • Movies You must select this option to collect Safari browser history. If you choose not to	✓	✓		

Setting	Description	Windows	macOS	Android	iOS
	search priority paths, Documents, Downloads, Desktop, Pictures and Movies will still be searched, but later in the search process.				
Locate files using a NCMEC tip	Use the loaded NCMEC tip to locate file-name, URL's, and IP addresses based on keyword hits. Both .xml and PDF are supported.	✓	✓	✓	

Artifacts

Setting	Description	Windows	macOS
Search browser history for URLs for keywords	Search browser history for URLs and keywords included in your keyword lists.	✓	✓

Live system

Setting	Description	Windows	macOS
Collect operating system artifacts	Collect operating system artifacts, including: • USB device history • Recently accessed logged-on users • Extended drive info, routing, firewall settings, saved Wi-Fi networks	✓	

Setting	Description	Windows	macOS

	• Mapped network drives (persistent only)
	• User accounts and info
	• Operating system information
	  ◦ Installed date
	  ◦ Saved Wi-Fi passwords
	  ◦ Registered owner
	  ◦ Time zone setting
	• List of installed apps
	• Active network connections
	• List of scheduled tasks
	• List of Windows services
	• Prefetch files (basic information)
	• Running processes
	• List of Wi-Fi networks currently visible		

Collect RAM	Capture the live system's RAM prior to starting the scan. The capture is saved to the report folder as a file named "RAMCapture.bin".	✓	
Scan for drive encryption	Include information about drive encryption in your scan report. For more information about how Magnet OUTRIDER checks for encryption, see Encryption screening.	✓	
Save a screenshot of the desktop	Prior to starting the scan, but after capturing RAM, capture a screenshot of the desktop. The screenshot is saved to the report folder as a PNG file named "Desktop.png".	✓	

Setting	Description	Windows	macOS
Minimize the OUTRIDER window before capturing the screenshot	Minimize just the Magnet OUTRIDER application before capturing a screenshot of the desktop. Otherwise, all windows are minimized to capture the entire desktop and its background photo and desktop icons.	✓	
Search running processes	Search the names of all applications that are running on the device.	✓	✓
Scan connected network for devices	If the live system is currently connected to a network (Wi-Fi or wired), Magnet OUTRIDER scans the network to locate devices and determine their IP address, MAC address, hostname (if applicable), and the device manufacturer.	✓	
Obtain IP address	Obtains the external IP address of the device that Magnet OUTRIDER is running on.	✓	✓

Mobile

Setting	Description	Android	iOS
Include user data without a keyword	Perform a search without keyword match. Searching without a keyword list will display all discovered contacts, Accounts info, Knox Accounts, Device info, and SMS/MMS logs. You can select this option in addition to other scan options. For a list of items included in the scan, see Android devices or iOS devices.	✓	✓
Include all MMS attachments without a keyword match	Searching without a keyword list displays all discovered MMS media in the Magnet OUTRIDER UI. If you do not select this option, only media with	✓	✓

Setting	Description	Android	iOS
	keyword matches will be displayed in the Magnet OUTRIDER UI. Right-click a source option and click **Save** to include attachments in the savedfiles.zip file. **Requires Save MMS attachments to be selected**.		
Save MMS attachments	Must be selected, otherwise no MMS media will be retrieved.	✓	✓
Calculate MD5 values for media files. Increases scan times.	This feature will capture MD5 or MAG24 values for media files from the phone and compare those with supplied hashsets. NOTE: At least one Hashset in "Locate files with MD5 hashsets matching the source hashes" must be selected for this option to be enabled.	✓	

CSAM detection technology

CRC CSAM detection technology is available to law enforcement customers only.

Setting	Description	Windows	macOS
After initial scan, run Child Rescue Coalition CSAM Detection.	Complete a secondary scan using CSAM detection technology from the Child Rescue Coalition (CRC). This scan can detect known CSAM—even if no keyword hits were found in file names. This scan analyzes all of the files scanned by Magnet OUTRIDER (not including files found in ZIP files) using hashes from law enforcement CSAM databases in the United States	✓	✓

Setting	Description	Windows	macOS
	and Canada. It's possible that Magnet OUTRIDER will be unable to recover all hits. Hits may not be returned if: • The file names do not match any of the loaded keywords. • Support isn't available for the detection of an application. • You may not have permissions to locations on the device.		
Scan all file types	Scan all file types using the CRC CSAM detection technology, regardless of extension. The following file types are supported: .jpg, .mp4, .png, .bmp, .gif, .avi, .mpg, . wmv, .jpeg, .mov, .m4v, and .flv. Depending on the number of files present on the computer or drive and the speed of the hardware, turning on this setting can significantly increase scan time. Consider turning on this option if you suspect that the user might be hiding files by changing the file extensions.	✓	✓

Reporting options

Setting	Description	Windows	macOS
Save thumbnails of	Include thumbnails of CSAM hits in your HTML report.	✓	✓

Setting	Description	Windows	macOS
CSAM hits			
Save path list to report folder	Save all file paths detected by Magnet OUTRIDER. This setting can increase scan time and the saved pathlist.txt file in your report can be large.	✓	✓

SCAN AND REPORT SETTINGS

To configure how data is displayed in your search results and in your reports, click **Manage** > **Manage settings**.

Scan settings

Setting	Description
Display CSAM thumbnail images	Displays CSAM thumbnails in your search results.
Display parsed timestamps in UTC	Converts parsed timestamps to UTC and displays the UTC time in your search results.
Blur thumbnail images	Blur CSAM thumbnails in your search results.
Send diagnostic information	Sends diagnostic data to Magnet Forensics, to help us improve the product.

Report settings

Setting	Description
Add a logo/crest to the header	Customize the logo or crest that appears in the header of reports.
Save case/report files to the following location	Sets where report and case information is saved.

SUPPORTED APPLICATIONS

Magnet OUTRIDER searches for all versions of the following applications:

Anti-forensic files

Application	Windows	macOS
Active@ KillDisk		✓
CCleaner	✓	✓
Eraser	✓	
File Shredder	✓	
Folder Lock	✓	
Kruptos 2 Professional	✓	
Mask Surf Pro	✓	
OpenPuff	✓	
Our Secret	✓	
Slacker	✓	
Spotflux	✓	
Steg	✓	
Steganos Privacy Suite	✓	
Permanent Eraser		✓
Timestomp	✓	
usbkill		✓
Winclear	✓	

Built-in file collection

This feature is available for Windows scans only.

These files will be located for evidence collection.

Category	Windows	macOS
Armory/Other Wallet File	✓	
Armory Wallet File	✓	
Bitcoin Key	✓	
Bitcoin Wallet File	✓	
BitPay Wallet Backup	✓	
Electron Private Keys	✓	
Electron Wallet File	✓	
Electrum Wallet File	✓	
EOS Wallet File	✓	
EOSIO Key	✓	
Ethereum Key	✓	
Exodus Wallet	✓	
Guarda Wallet Backup	✓	
Litecoin Wallet File	✓	
Mega.nz Recovery Key	✓	
Scatter Wallet File	✓	
Tron Key	✓	
Wasabi Wallet File	✓	

Cloud storage apps

Application	Windows	macOS
Amazon Drive	✓	
Dropbox	✓	✓
Box Drive	✓	✓
Google Drive	✓	✓
Google Drive File Stream	✓	
MEGAsync	✓	
Mega.nz		✓
OneDrive	✓	✓

Cryptocurrency apps

Application	Windows	macOS
Armory Client	✓	✓
Atomic Wallet Client	✓	
Bitcoin Core Client	✓	✓
Bither Client	✓	
BitPay Client	✓	
Electron Client	✓	
Electrum Client	✓	✓
Exodus Client	✓	
Guarda Client	✓	
Jaxx Liberty Client	✓	

Application	Windows	macOS
Litecoin Client	✓	
Monero Client	✓	
Scatter Client	✓	
Toast Wallet Client	✓	
Tron Wallet	✓	
Wasabi Wallet Client	✓	✓

Dark web apps

Application	Windows	Mac
Freenet	✓	✓
i2p	✓	
Isotoxin	✓	
qTox	✓	✓
Tor	✓	✓
TorChat	✓	✓
Toxygen	✓	
uTox	✓	

Encryption Apps

Category	Windows	macOS
AES Crypt	✓	✓
AxCrypt	✓	✓
BestCrypt	✓	✓

Category	Windows	macOS
Check Point Encryption	✓	
GPG	✓	✓
PGP	✓	
Sophos SafeGuard	✓	
Symantec Drive Encryption	✓	
TrueCrypt	✓	
Veracrypt	✓	✓

Gaming Apps

This feature is available for Windows scans only.

Category	Windows	macOS
Fortnite	✓	
Minecraft	✓	
Roblox	✓	

Messaging Apps

This feature is available for Windows scans only.

Category	Windows	macOS
Discord	✓	
Facebook Messenger	✓	
KaKaoTalk	✓	

Category	Windows	macOS
LINE	✓	
Microsoft Teams	✓	
Pidgin	✓	
Riot	✓	
Signal	✓	
Skype	✓	
Slack	✓	
Telegram	✓	
Viber	✓	
WeChat	✓	
WhatsApp	✓	
Wicker	✓	
Wire	✓	

Peer-to-Peer (P2P) Apps

Category	Windows	macOS
Ares	✓	
BitTorrent	✓	
BitTorrent Web		✓
eMule	✓	
FrostWire	✓	✓
qBitTorrent	✓	✓
Shareaza	✓	
uTorrent	✓	✓

Category	Windows	macOS
Vuze	✓	✓

Virtual Machine Apps

Category	Windows	macOS
Bluestacks	✓	✓
Genymotion	✓	✓
MEmu	✓	
Nox	✓	✓
Parallels Hard Disk Drive	✓	
QEMU Emulator/Virtualizer	✓	
Virtual Hard Disk	✓	
VirtualBox	✓	✓
VirtualBox Virtual Disk Image	✓	
VMware	✓	
VMware Fusion		✓
VMware Virtual Machine Disk	✓	
Windows Virtual PC	✓	

Virtual private network (VPN) Apps

Category	Windows	macOS
Cisco Anyconnect	✓	✓
CyberGhost VPN	✓	
Hotspot Shield	✓	

Category	Windows	macOS
IPVanish VPN	✓	
KeepSolid VPN Unlimited	✓	
NordVPN	✓	
Private Internet Access	✓	
ProtonVPN	✓	
proXPN	✓	
StrongVPN	✓	
Surfshark	✓	
TunnelBear	✓	
VyprVPN	✓	
Windscribe	✓	

Web Browsers

Category	Windows	macOS
Chrome	✓	✓
Edge	✓	✓
Firefox	✓	✓
Safari		✓ *

*Safari browsing history is only available with full disk access. See Preparing a Mac device to be scanned for more information.

Magnet Forensics

2220 University Ave. E., Suite 300

Waterloo, ON, N2K 0A8

1 (519) 342-0195

This document was published on 10/26/2023.