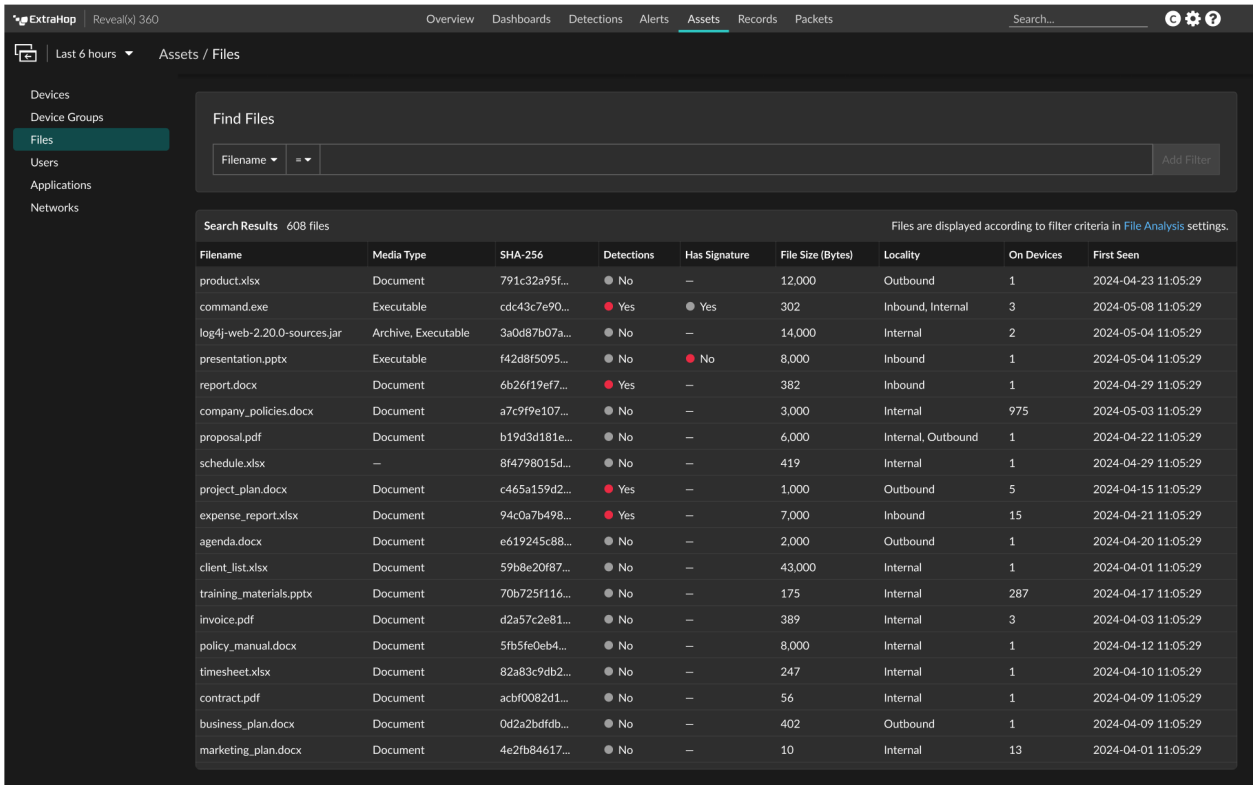
Files

Published: 2024-10-23

Metadata from hashed files are a valuable tool for identifying malware and risks in your network. For example, files downloaded by several devices, files with an extension that does not match the media type, unsigned files, or large outbound or inbound file transfers are observations worth investigating. The Files page displays a table of hashed files and associated file details that you can filter and search. To view the Files page, click **Assets** from the top navigation menu and then click the **Files** chart.

Files are hashed with the SHA-256 hashing algorithm and displayed in the Files table according to filter criteria configured from the File Analysis settings. You can add filters in the Find Files section to refine results in the Files table.

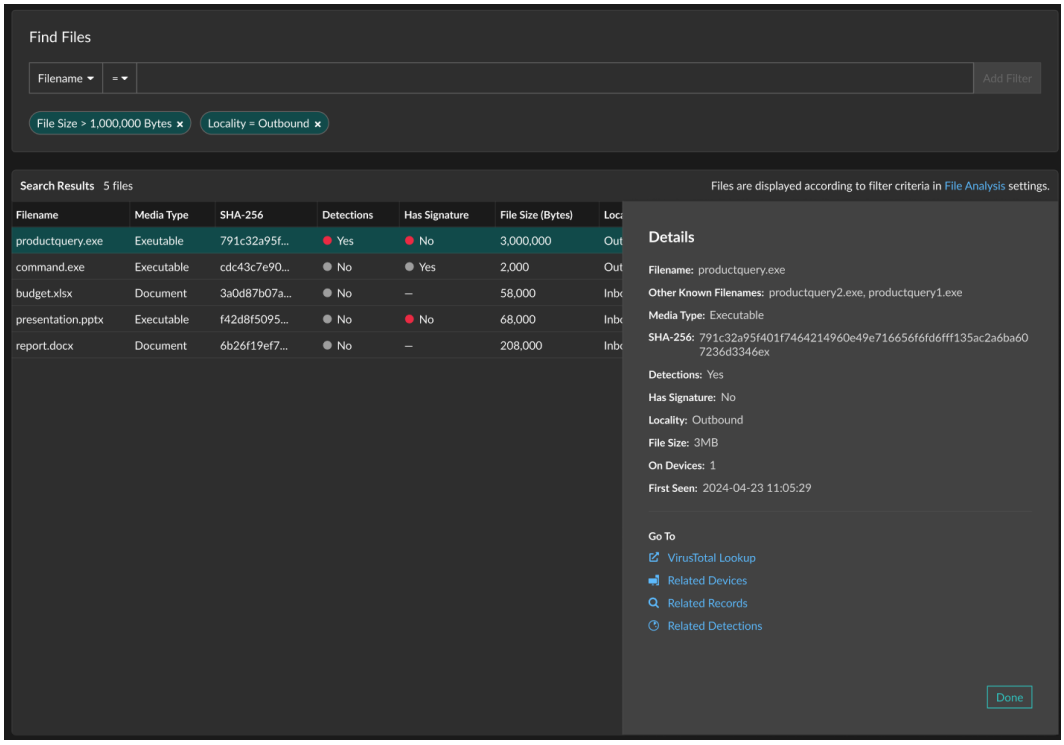


The Files table displays the following details for each file.

File Detail	Description
Filename	The name of the hashed file. Other filenames returned by the same SHA-256 hashing algorithm are displayed on the Details pane.
Media Type	The media type of the hashed file. Supported file types are Document, Archive, and Executable. The ExtraHop system determines the file media type by analyzing patterns in the header and initial bytes of the file payload.
SHA-256	The SHA-256 file hashing algorithm applied to the file.

File Detail	Description
	Tip: You can find devices associated with specific hashed files by adding the SHA-256 filter to a device search.
Detections	Indicates whether the hashed file was involved in a detection that matched an indicator in a threat collection, such as a malicious file transfer. (Only available on a console connected to an Intrusion Detection System (IDS) sensor for users with NDR module access)
Has Signature	Indicates whether a signature on the hashed file was observed, but does not verify whether the signature is valid.
File Size	The size of the hashed file, in bytes.
Locality	The locality, or flow direction, of the hashed file. Supported localities are Inbound, Outbound, and Internal.
On Devices	The number of devices on which the hashed file was observed.
First Seen	The timestamp when the hashed file was first observed.

Click a file in the table to open the Details pane and display several links that enable you to investigate the SHA-256 file hash.



- Click **VirusTotal Lookup** to navigate to the VirusTotal site and check the file hash for malicious content.
- Click **Related Devices** to filter devices by the file hash and view results on the Devices page.

- Click **Related Records** to filter records by the file hash and view results on the Records page.
- Click **Related Detections** to filter detections by the file hash and view results on the Detections page. (Only available on a console connected to an Intrusion Detection System (IDS) sensor for users with NDR module access.)