

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.

Search Results 608 files

Files are displayed according to filter criteria in [File Analysis settings](#).

Filename	Media Type	SHA-256	Detections	Has Signature	File Size (Bytes)	Locality	On Devices	First Seen
product.xlsx	Document	791c32a95f...	No	—	12,000	Outbound	1	2024-04-23 11:05:29
command.exe	Executable	cdc43c7e90...	Yes	Yes	302	Inbound, Internal	3	2024-05-08 11:05:29
log4j-web-2.20.0-sources.jar	Archive, Executable	3a0d87b07a...	No	—	14,000	Internal	2	2024-05-04 11:05:29
presentation.pptx	Executable	f42d8f5095...	No	No	8,000	Inbound	1	2024-05-04 11:05:29
report.docx	Document	6b26f19ef7...	Yes	—	382	Inbound	1	2024-04-29 11:05:29
company_policies.docx	Document	a7c9f9e107...	No	—	3,000	Internal	975	2024-05-03 11:05:29
proposal.pdf	Document	b19d3d181e...	No	—	6,000	Internal, Outbound	1	2024-04-22 11:05:29
schedule.xlsx	—	8f4798015d...	No	—	419	Internal	1	2024-04-29 11:05:29
project_plan.docx	Document	c465a159d2...	Yes	—	1,000	Outbound	5	2024-04-15 11:05:29
expense_report.xlsx	Document	94c0a7b498...	Yes	—	7,000	Inbound	15	2024-04-21 11:05:29
agenda.docx	Document	e619245c88...	No	—	2,000	Outbound	1	2024-04-20 11:05:29
client_list.xlsx	Document	59b8e20f87...	No	—	43,000	Internal	1	2024-04-01 11:05:29
training_materials.pptx	Document	70b725f116...	No	—	175	Internal	287	2024-04-17 11:05:29
invoice.pdf	Document	d2a57c2e81...	No	—	389	Internal	3	2024-04-03 11:05:29
policy_manual.docx	Document	5fb5fe0eb4...	No	—	8,000	Internal	1	2024-04-12 11:05:29
timesheet.xlsx	Document	82a83c9db2...	No	—	247	Internal	1	2024-04-10 11:05:29
contract.pdf	Document	acb0082d1...	No	—	56	Internal	1	2024-04-09 11:05:29
business_plan.docx	Document	0d2a2bdfb...	No	—	402	Outbound	1	2024-04-09 11:05:29
marketing_plan.docx	Document	4e2fb84617...	No	—	10	Internal	13	2024-04-01 11:05:29

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.

The screenshot shows the 'Find Files' interface. At the top, there is a search bar with 'Filename' and a dropdown arrow. Below it, two filters are applied: 'File Size > 1,000,000 Bytes' and 'Locality = Outbound'. The search results table shows 5 files. The first file, 'productquery.exe', is highlighted. To the right of the table, the 'Details' pane is open, showing information for 'productquery.exe', including its SHA-256 hash, detection status, and various links for further investigation.

Filename	Media Type	SHA-256	Detections	Has Signature	File Size (Bytes)	Locality
productquery.exe	Executable	791c32a95f...	Yes	No	3,000,000	Out
command.exe	Executable	cdc43c7e90...	No	Yes	2,000	Out
budget.xlsx	Document	3a0d87b07a...	No	—	58,000	Inb
presentation.pptx	Executable	f42d8f5095...	No	No	68,000	Inb
report.docx	Document	6b26f19ef7...	No	—	208,000	Inb

Details

Filename: productquery.exe
Other Known Filenames: productquery2.exe, productquery1.exe
Media Type: Executable
SHA-256: 791c32a95f401f7464214960e49e7166566fd6ff135ac2a6ba607236d3346ex
Detections: Yes
Has Signature: No
Locality: Outbound
File Size: 3MB
On Devices: 1
First Seen: 2024-04-23 11:05:29

Go To

- VirusTotal Lookup
- Related Devices
- Related Records
- Related Detections

Done

- 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.)