YARAify | Data exposed through Real Time Intelligence Feed v. publicly available data

YARAify, provided by abuse.ch, is one of the largest repositories of YARA rules available. Users can scan suspicious files, such as malware samples or process dumps, against these rules to identify targeted attacks and threats, specific to their environment.

Users can access this data via the Real Time Intelligence Feed, or via publicly available APIs. These access methods provide different metadata outputs, as highlighted in this document.

The Real Time Intelligence Feed is the only access method to receive all observed threat signals.

Metadata field	Metadata description	Real Time Feed	Publicly available data
File Additions			
`_idx`	Is an integer representing the incremental number of the message.	✓	✗
`_ts`	Is the Unix timestamp, indicating when the message was received by the real time infrastructure.	✓	✓*
`uuid`	Is an internal, unique identifier for the message. This is the property that should be used to dedupe the incoming flows where necessary.	✓	✓*
`type`	Defines the type of message. It's always 'file_addition'.	✓	✗
`md5_hash`	Is the MD5 hash of the payload received.	✓	✓
`sha256_hash`	Is the SHA256 hash of the payload received.	✓	✓
`sha1_hash`	Is the SHA1 hash of the file.	✓	✓
`sha3_384_hash`	Is the SHA3-384 hash of the file.	✓	✓
`file_size`	Is the size (in bytes) of the payload received.	✓	✓
`imphash`	Is the imphash of the payload received.	✓	✓
`ssdeep`	Is the ssdeep of the payload received.	✓	✓
`tlsh`	Is the tlsh of the payload received.	✓	✓
`telfhash`	Is the telfhash of the payload received.	✓	✓
`gimphash`	Is the gimphash of the file.	✓	✓
`dhash_icon`	Is the dhash of the file icon.	✓	✓
`mime_type`	Is the Multipurpose Internet Mail Extensions (MIME) type of the payload received.	✓	✓
Task results			
`_idx`	Is an integer representing the incremental number of the message.	✓	✗
`_ts`	Is the Unix timestamp, indicating when the message was received by the real time infrastructure.	✓	✗
`uuid`	Is an internal, unique identifier for the message. This is the property that should be used to dedupe the incoming flows where necessary.	✓	✓*
`type`	Defines the type of message. It's always "task_result".	✓	✗
`task_id`	Task ID (UUID4).	✓	✓
`md5_hash`	Is the MD5 hash of the payload received.	✓	✓
`sha256_hash`	Is the SHA256 hash of the payload received.	✓	✓
`sha1_hash`	Is the SHA1 hash of the file.	✓	✓
`sha3_384_hash`	Is the SHA3-384 hash of the file.	✓	✓
`file_name`	Is the original file name.	✓	✓
`clamav_scan`	Boolean indicating whether the file has been scanned with ClamAV or not.	✓	✓
`unpack`	Is boolean value indicating whether the file has been processed by the Portable Executable (PE) unpacker.	✓	✓
`unpacked_files_cnt`	If `unpack` is `True`, number of unpacked files collected (if any).	✓	✓
`share_file`	Boolean indicating whether the user decided to share the sample or not.	✓	✓
`results.clamav`	Is the matching ClamAV signature.	✓	✓*
`results.yara_static`	Is an array indicating the static YARA rule matching results.	✓	✓*
`results.yara_unpack`	Is the array of the unpacker YARA rule matching results.	✓	✓*
Unpacker results			
`_idx`	Is an integer representing the incremental number of the message.	✓	✗
`_ts`	Is the Unix timestamp, indicating when the message was received by the real time infrastructure.	✓	✗
`uuid`	UUID identifying this message	✓	✓
`type`	Type of this message	✓	✓
`md5_hash`	MD5 hash of the unpacked file	✓	✗
`sha256_hash`	SHA256 hash of the unpacked file	✓	✗
`sha1_hash`	SHA1 hash of the unpacked file	✓	✓
`sha3_384_hash`	SHA3-384 hash of the unpacked file	✓	✗
`file_name`	File name of the unpacked file	✓	✗
`file_size`	Size (in bytes) of the unpacked file	✓	✗
`timestamp`	Unix timestamp of the message	✓	✗
`imphash`	imphash of the unpacked file	✓	✗
`ssdeep`	ssdeep of the unpacked file	✓	✗
`tlsh`	TLSH of the unpacked file	✓	✗
`telfhash`	telfhash name of the unpacked file	✓	✗
`gimphash`	gimphash of the unpacked file	✓	✗
`dhash_icon`	dhash of the unpacked file' icon	✓	✗
`mime_type`	MIME type of the unpacked file	✓	✗
`parent_file`	The original file (parent) from which this file (child) got unpacked from	✓	✗
`yara_matches`	YARA rules matching this unpacked file	✓	✓

*** Comparable data for this field is provided via publicly available data, however the field names are not an exact match.**
If you require the comparable field name, please speak with your Spamhaus contact.