



Research files

Work

E-library

About

TR

EN

FILE ANALYSIS

Open the file. Inspect the record.

Choose one file. Identity, structure, findings, explicit observables, and relationships are produced from the real file bytes in the same workspace.

01 Review a file

02 Text, log, or email header

SPECIMEN INTAKE

Drop the file here

Images, PDF, Office, email, PCAP, APK, OCI, archives, scripts, and binaries.

[Choose file](#)

or drag and drop, Up to 64 MB. The file stays in memory and disappears when the page is refreshed.

PROCESSING BOUNDARIES

Analysis location This browser tab

The local report never moves the file out of the tab.

Upload to a server Only with explicit consent

For eligible types, optional deep analysis sends nothing until you start it.

File size 64 MB local, 25 MiB deep

Files above the limit are rejected.

Execution ...

How the file and document review is built

I review a file in your browser without running it and without uploading it anywhere. I pull out its identity, its structure and the indicators written plainly inside it, and I tie every finding to its source in the file. The result is not a verdict. It is a record you can check.

1 What this review is for

When a suspicious attachment arrives, the first habit is to upload it to an online scanner. But that means handing the file to someone else. It may contain client data or internal mail. I wanted the first look to never leave the device.

So the local review runs entirely in the browser tab. The file is read, parsed and reported on, and everything is gone when you reload the page.

1. Check at entry Size, format and readable structure. A file over the limit stops with a clear error.	2. Read in background The bytes are read in a separate browser Worker. The screen does not freeze.	3. Identity and type SHA-256 and the visible structure. The file name is not trusted.	4. Structure and indicators Supported fields, plus any URL, domain, IP, email, hash or CVE written plainly in the file.	5. Evidence pack Report, manifest, indicator records and graph. The reviewed file is not in the pack.
--	--	---	---	---

A few words

Static review	A review that only looks at the bytes of a file, without running it.
SHA-256	A fingerprint of the file. The same file always gives the same value.
Magic bytes	A few bytes at the start of a file that show its real type. An extension can lie, these are harder to fake.
Explicit indicator (IOC)	An address, domain, IP, email, hash or CVE that appears as plain text inside the file.
Browser Worker	A piece of work that runs apart from the page's main screen. It does the heavy lifting.

2 What runs where

Where it runs	This browser tab. The file never leaves it.
Engine	A separate browser Worker. One review may take at most 60 seconds.
Size	Up to 64 MB for the local review.
Network	None. No reputation lookup or outside service call is made.
Retention	None. The report is lost on reload and exists nowhere unless you download it.
Input	Images, PDF, Office, email, PCAP, APK, OCI, archives, scripts and binaries. Pasted text, logs or email headers too.

A file only goes to a server in the optional deep analysis, for eligible file types and with your clear consent. That step has its own handbook, HB-30 Deep Analysis.

3 Opening a file

The page opens on the intake screen. At the top there are two paths. Review a file, or paste text, a log or an email header. Pasted text that looks like an email is reviewed as an email. You choose or drop a file; the site ships no ready sample. The rules sit next to it, to be read before you start.



The processing limits and records produced, next to the intake screen.

1 Analysis location

This browser tab. The local report never moves the file out of the tab.

2 Upload to a server

Only with explicit consent. For eligible types, deep analysis sends nothing until you start it.

3 Retention

None. The report is lost on reload.

4 Records produced

The engine produces exactly hashes, parsed headers, a bounded string scan and an evidence pack without the reviewed file.

4 The work desk

Once a file is open, the top of the desk holds the file identity, the sections and the options. The site ships no sample file, so this part has no screenshot; I list the parts below.

File identity	Name, type, size and SHA-256. Click to copy the full value. The top right says "Local report ready" and "Local analysis".
Sections	Overview, findings and evidence. The "More" menu holds structure, indicators, graph and tools.
Download report	Downloads the full analysis record as JSON.
Evidence bundle	Puts the report, manifest, document text, IOC CSV and STIX, string list and graph.json into one ZIP.

The desk header says "Deep Analysis" because deep analysis is an optional step of the same desk. When the local report is ready, nothing has been sent.

5 Evidence and output

The Evidence tab opens after a file is reviewed and shows four things.

Four facts	Where it ran, whether the file was sent, execution and the number of network requests. The local report shows not sent, execution off and zero requests.
Boundary sentence	The report is not a security decision. A person must review it before delivery.
Evidence bundle (.zip)	All outputs in one pack. The reviewed file itself is never added.
Explicit indicators (.stix.json)	Only values plainly visible in the file. The engine adds no guesses and no reputation data.

6 Why I built it this way, and its limits

I give no risk score. Every finding is tied to the header, path or text that produced it. I do not look up the hash outside either, because even that tells someone what you are reviewing.

- ✗ The file is not run. Process, registry, memory and network behaviour are not observed.
- ✗ One signal does not prove a file is malicious. No findings does not mean the file is safe.
- ✗ A signature record is shown, but the signature chain is not verified. High entropy alone is not proof of bad intent either.
- ✗ The string scan is bounded. If it hits the limit, the report says so plainly.