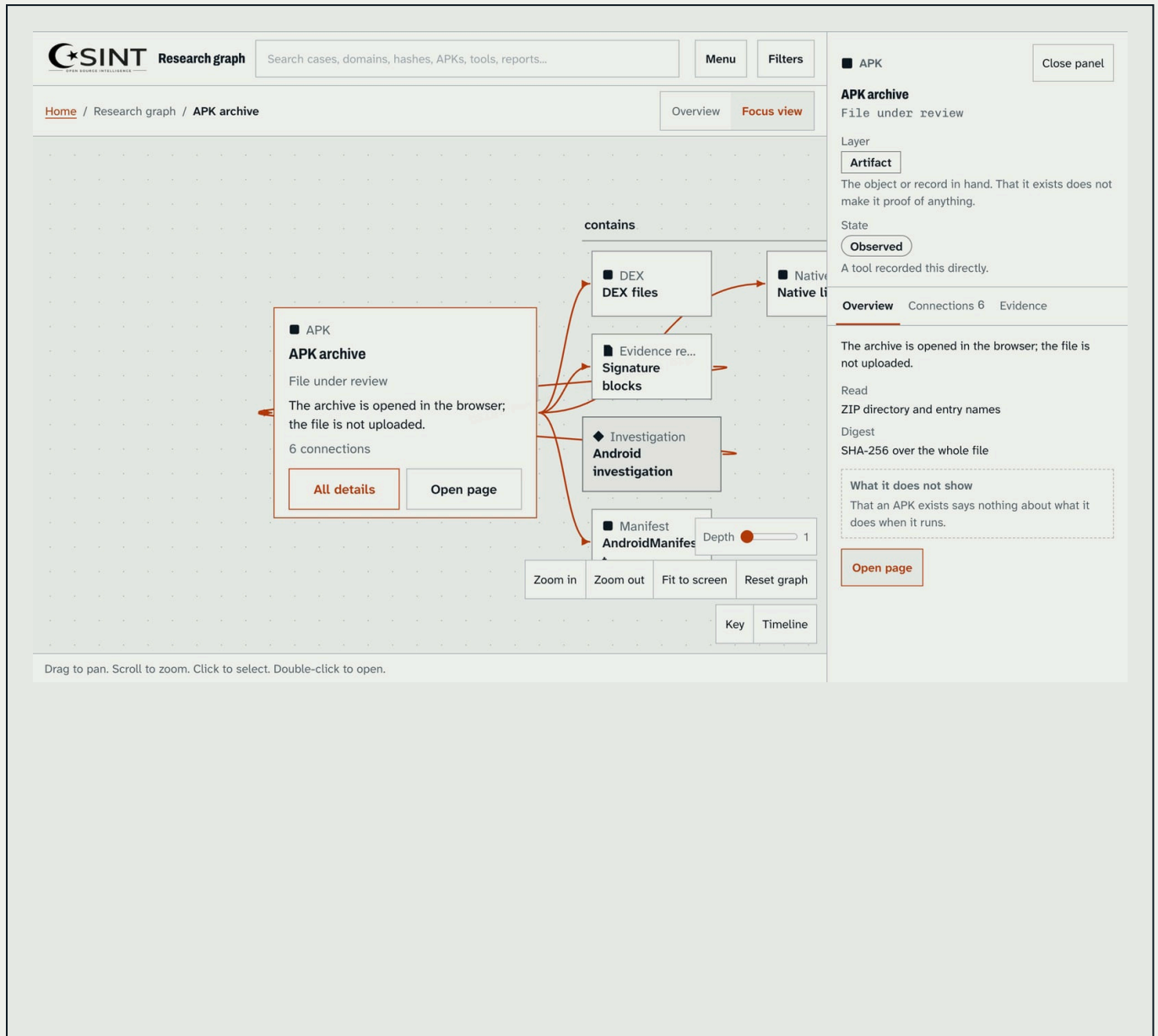




How the research graph is built

The research graph shows the investigations, artifacts, observations, evidence and interpretations I published on the site as one connected map. This handbook explains where the data comes from, where the graph is built and why I keep the layers apart.

1 What the graph is for

On the site, case files, tools, method pages and investigation chains sit on separate pages. To see which tool an APK review used, or which source a case rests on, you had to visit several pages. The graph shows those links in one place.

When you select a node, the nodes linked to it open. Every node states which layer it sits at and how sure we are. The graph does not create new information. It only links what the site has already published.

A few words

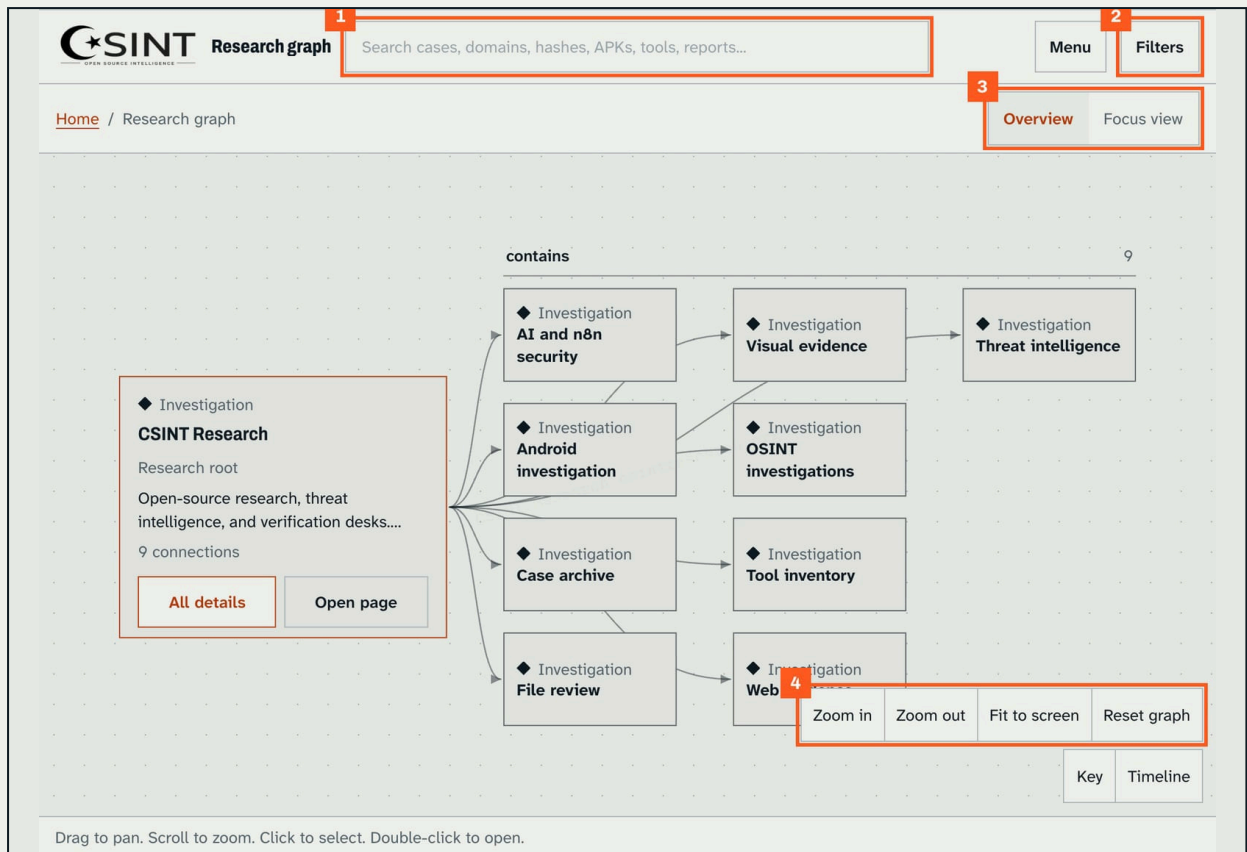
Node	A box on the graph. It can be a case, a file, a tool, a source or a finding.
Edge	The line between two nodes. It carries a relation name such as contains, uses or rests on.
Layer	The node's place in the chain. It can be investigation, artifact, observation, evidence or interpretation.
Record state	How the information was obtained. The value is observed, inferred, not recorded or unknown.

2 What runs where

The graph is built entirely in the browser. Opening the page sends no request to any server, stores nothing in the browser and needs no account.

			
1. The site's own data	2. Build	3. Browser	4. You
The case archive, the tool catalogue, the method graph and hand-written investigation chains. All in the site's source code.	This data is packed into the static site. No separate data file is downloaded.	When the page opens, the graph is computed once, the nodes are placed and drawn.	You search, filter, select a node, read its details or open the linked page.
Data source	Content published on the site. No live feed or outside service is read.		
Drawing	The open-source React Flow library. The layout is computed by the site's own layout code.		
Stored	Nothing. The node or filter you picked resets when the page reloads.		
Updates	When a new case or tool is published, the site is rebuilt and the graph grows by itself.		

3 Overview



The research-graph page, overview. The research root on the left, the main collections on the right.

1 Search

Searches by case, domain, hash, APK, tool or report name. Results open in the overview.

2 Filters

Opens the panel for filtering by type and layer.

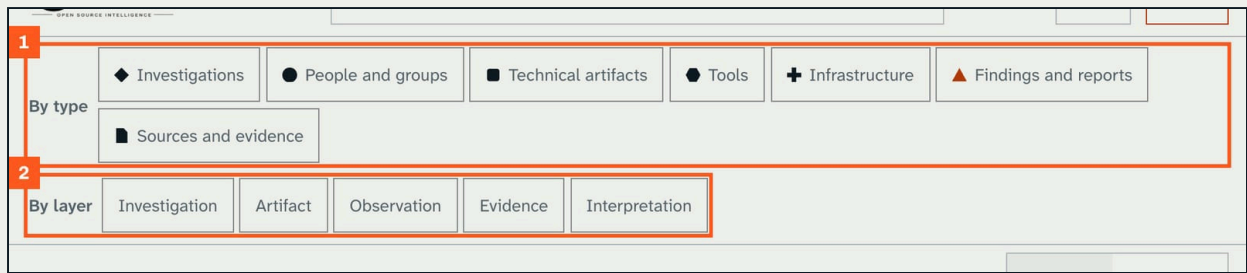
3 View

Overview shows the root and the main collections. Focus view shows only the selected topic and what it connects to.

4 Canvas buttons

Zoom in, zoom out, fit to screen and reset. Below them are the key and the timeline button.

4 Type and layer



The filter panel open.

1 By type

There are seven groups. They are investigation, people and groups, technical material, tools, infrastructure, finding and report, source and evidence.

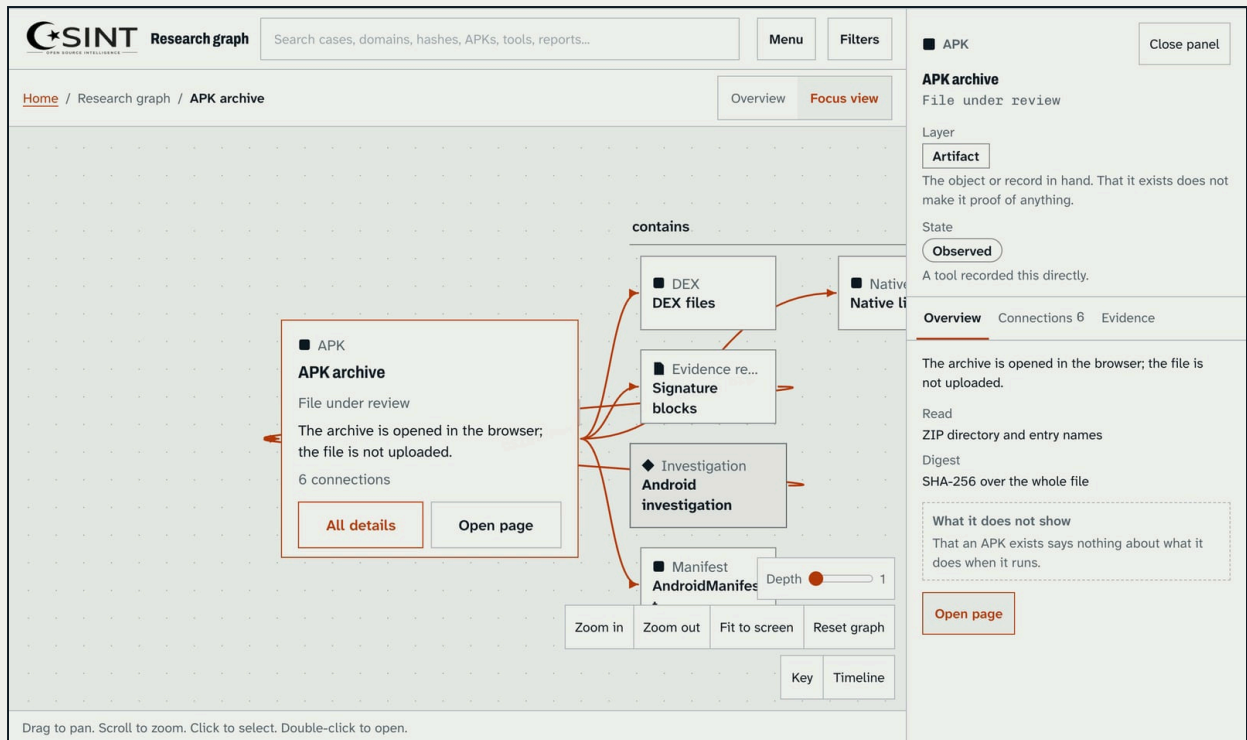
2 By layer

There are five layers. In reading order they are investigation, artifact, observation, evidence and interpretation.

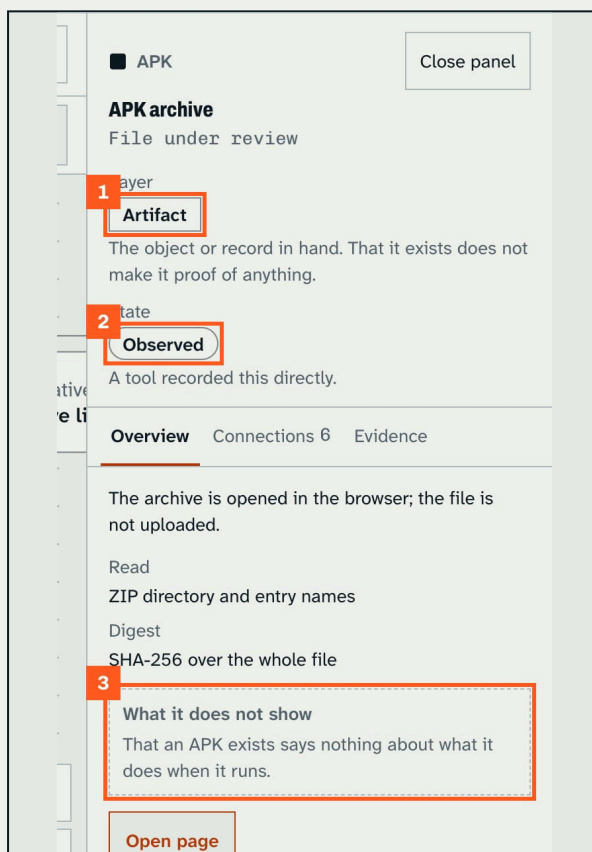
I keep the layers apart on purpose. Nothing in the interface moves a node up a layer by itself. Turning something a tool recorded into a finding is the analyst's call, not the drawing's.

5 A node in detail

In the example below I selected the APK archive node in the Android investigation chain and opened all its details. On a wide screen the panel sits on the right. On a narrow screen it becomes a sheet that opens from the bottom.



The APK archive node, focus view and details panel.



The details panel up close.

The panel always has a summary and a connections tab. If the node has an evidence record, an evidence tab opens, and if it has a date, a time tab opens too. The open page link goes to the page the node comes from, here the file review tool.

- 1 Layer**
This node is in the artifact layer. The note beside it warns that having an object does not mean it proves anything.
- 2 Record state**
Observed, meaning a tool recorded it directly. The state not recorded does not mean absent, it only says there is no record.
- 3 What it does not show**
Many nodes have this field. Here it says that an APK existing does not show what it does when it runs.

6 What it does not do

- ✗ It is not a complete case record. It only links what the site has published.
- ✗ It does no live tracking. It watches no person, domain or system and sends no outside queries.
- ✗ It gives no guarantee of accuracy. A line between two nodes shows what the source of that relation says. It does not prove on its own that the relation is right.
- ✗ It does not guess links from keywords. Every edge comes from a relation written in the data.

Use the graph like a table of contents. Find a topic, look at its links, then open its own page and read it there.