HANNES SOFTWARE / PCAP SURGERY SAMPLE EVIDENCE REPORT

Large capture trimmed to the failure window

A sample handoff for reducing a large PCAP to the packets that explain the failure while preserving timing and packet context.

SCENARIO

Incident evidence reduction

LIKELY CAUSE

Support or incident response needs a focused artifact rather than a full network trace.

FAILURE BOUNDARY

The full capture is too large and noisy for review; the failure is isolated to a specific packet window and endpoint pair.

RAW EVIDENCE EXCERPT

```
Time range selected; endpoint filters applied;
unrelated packets excluded; subset export
preserves the failure sequence.
```

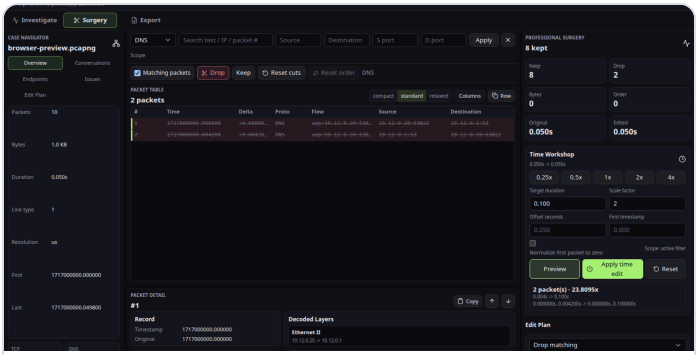
Evidence table

LAYER	FINDING	IMPLICATION
Filter scope	The failure window is isolated by time and endpoint filters.	Reviewers do not need the full capture to understand the case.
Subset export	The export keeps packet order and timing inside the selected window.	The reduced PCAP remains useful for debugging and replay-oriented analysis.
Handoff	The smaller file is easier to attach, review, and archive.	Support can move a case forward without exposing unrelated traffic.

Recommended fix

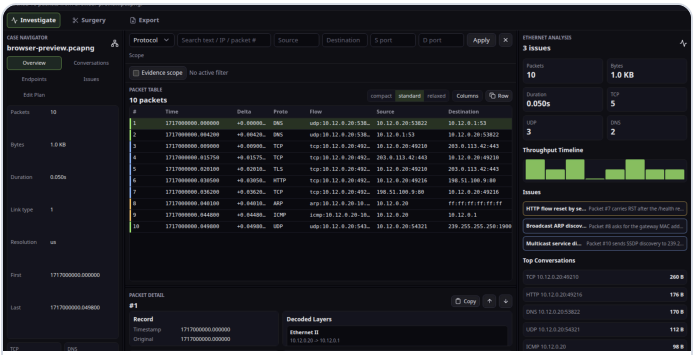
1. Preserve a private copy of the original capture before trimming.
2. Document the time window and filters used for the exported handoff.
3. Attach the subset PCAP and the export report together.

Evidence screenshots



Time workshop

The time workflow helps isolate a capture window before export.



Packet detail

Decoded packet context remains available while deciding what belongs in the subset.

This sample is static marketing evidence. Real reports are generated locally from the case data inspected in PCAP Surgery.