HANNES SOFTWARE / PCAP SURGERY SAMPLE EVIDENCE REPORT

Customer PCAP redacted for a support ticket

A sample PCAP Surgery handoff that removes sensitive addresses and payload context while preserving packet timing and protocol evidence.

SCENARIO

Support evidence handoff

LIKELY CAUSE

Support workflows need a defensible redaction step between customer capture collection and external vendor handoff.

FAILURE BOUNDARY

The original capture contains useful protocol evidence, but it cannot be sent to a vendor until sensitive endpoints and payload bytes are removed.

RAW EVIDENCE EXCERPT

```
Original capture includes private endpoints and
payload preview; rewrite plan masks addresses;
subset export keeps the failure window;
checksums are repaired before export.
```

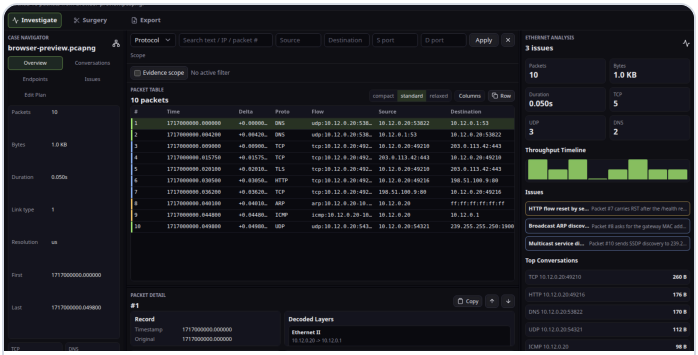
Evidence table

LAYER	FINDING	IMPLICATION
Original capture	The PCAP contains the packet window needed for vendor support but also exposes sensitive endpoint data.	Sending the raw file creates avoidable privacy and customer-trust risk.
Rewrite plan	Address and payload handling are explicit before export.	The handoff can be reviewed instead of hidden behind a one-line CLI command.
Export	The focused output retains protocol timing and repaired checksums.	The vendor receives a smaller file that is still useful for reproduction.

Recommended fix

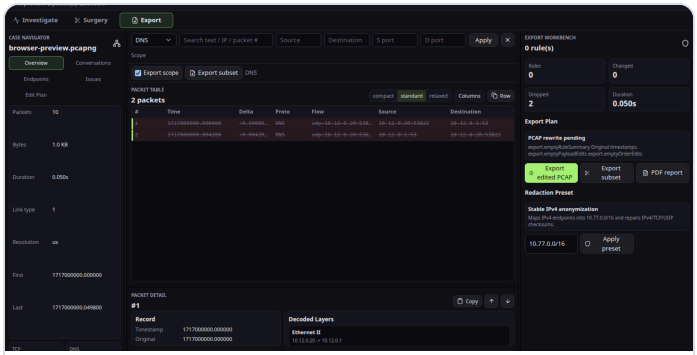
1. Keep the raw customer capture internal and attach only the redacted export to external tickets.
2. Document every rewrite rule used for the handoff file.
3. Verify checksum repair before sending the fixture to a vendor or QA system.

Evidence screenshots



Packet detail evidence

Decoded layers and raw bytes stay inspectable before the capture is changed.



Export plan

The export plan keeps redaction, warnings, and readiness visible before handoff.

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