HANNES SOFTWARE / PCAP SURGERY SAMPLE EVIDENCE REPORT

Checksum-safe IP and port rewrite for a lab fixture

A sample report for rewriting endpoints in a PCAP while preserving protocol structure and repairing IPv4, TCP, and UDP checksums.

SCENARIO

Reproducible test fixture

LIKELY CAUSE

The capture was collected in a customer network and needs deterministic test-lab addresses without invalidating checksums.

FAILURE BOUNDARY

The useful packet sequence is valid, but endpoint values must be rewritten before the capture can become a repeatable lab fixture.

RAW EVIDENCE EXCERPT

```
IPv4 endpoints selected; TCP/UDP ports rewritten; checksum fields repaired; exported fixture reparses cleanly.
```

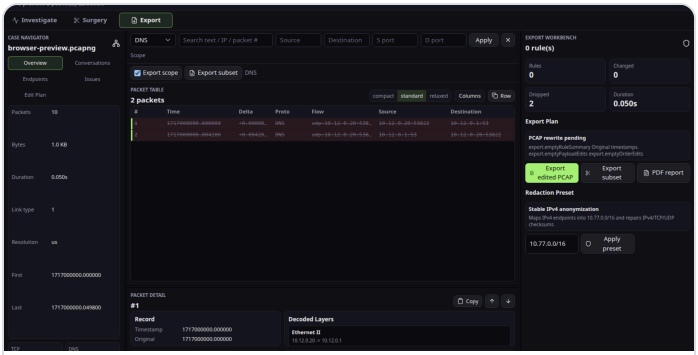
Evidence table

LAYER	FINDING	IMPLICATION
Rewrite scope	Only selected IP addresses and ports are changed.	The test fixture keeps the original packet sequence and timing.
Checksum repair	IPv4/TCP/UDP checksum repair is part of the export path.	The fixture can be consumed by packet tools without immediate checksum noise.
Fixture handoff	The exported PCAP can be shared with QA or regression tests.	A customer-only trace becomes a repeatable engineering artifact.

Recommended fix

1. Rewrite only the fields required for lab isolation.
2. Keep a note of the original-to-lab endpoint mapping outside the shared PCAP.
3. Re-open the exported fixture and verify parser and checksum status before committing it.

Evidence screenshots



Export readiness

Export warnings and checksum readiness are reviewed before writing the handoff file.

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