Official resource

Packet Capture Evidence and Escalation Sheet

SLUG	packet-capture-evidence-and-escalation-sheet
SUMMARY	Printable worksheet for planning, approving, collecting, storing, and escalating yacht network packet captures without over-collecting sensitive traffic.
RESOURCE TYPE	Worksheet
RESOURCE AREA	Connectivity, IT & cyber
INTENDED AUDIENCE	ETOs, AV/IT crew, IT providers, captains, yacht managers
ESTIMATED USE MINUTES	20
DOCUMENT LABEL	Download PDF
PDF	packet-capture-evidence-and-escalation-sheet-v1-0.pdf
VERSION	1.0
PUBLICATION STATUS	Published resource archive
IMPORTANT NOTE	This resource is practical operational guidance. It does not replace the vessel SMS, flag or class requirements, privacy advice, incident-response procedures, manufacturer manuals, competent network/security advice, or the authority of the Captain and responsible technical officers onboard.

YachtByte Official Resource

Capture approval

- [ ] Fault question written in plain language.
- [ ] Capture approved by responsible technical lead.
- [ ] Captain or management approval recorded where owner, guest, crew, security, bridge-adjacent or OT traffic may be involved.
- [ ] Vendor or support recipient named before collection.
- [ ] Data sensitivity reviewed before capture starts.
- [ ] Retention or deletion plan recorded.

Scope and boundary

- [ ] Affected network zone recorded.
- [ ] Affected device name and IP address recorded.
- [ ] Destination service, server or endpoint recorded.
- [ ] Capture point recorded.
- [ ] Capture duration recorded.
- [ ] Capture filter recorded.
- [ ] Networks explicitly excluded from capture recorded.
- [ ] Expected test action written before capture starts.

Collection record

- [ ] Capture tool recorded.
- [ ] Capture file name recorded.
- [ ] Start time recorded with time zone.
- [ ] Stop time recorded with time zone.
- [ ] Test action performed during capture recorded.
- [ ] Screenshots or logs captured at the same time.
- [ ] Device, firewall, switch, DNS or application logs preserved where relevant.
- [ ] Hash or file integrity note recorded where incident evidence is required.

Privacy and access control

- [ ] Capture file stored in restricted location.
- [ ] Unnecessary broad traffic avoided.
- [ ] Guest, owner, crew, CCTV, access-control, bridge-adjacent or OT exposure noted if present.
- [ ] Passwords, tokens or unencrypted sessions considered before sharing.
- [ ] Redaction or narrower recapture considered before external escalation.
- [ ] File recipients recorded.
- [ ] Sharing method recorded.

Support escalation

- [ ] Fault summary attached.
- [ ] Network/VLAN and capture point explained.
- [ ] Filter and test action explained.
- [ ] Relevant logs attached.
- [ ] Recent changes listed.
- [ ] What has already been ruled out recorded.
- [ ] Vendor question written clearly.
- [ ] Vendor response and next action recorded.

Closeout

- [ ] Root cause or current finding recorded.
- [ ] Corrective action recorded.
- [ ] Firewall, switch, DNS, DHCP, Wi-Fi or application change logged where applicable.
- [ ] Capture file archived or deleted according to the agreed plan.
- [ ] Captain or management plain-language summary provided where operational impact occurred.
- [ ] Follow-up review date assigned if the fault was not fully resolved.