Evaluating Red Herrings for a forensics or incident response program

A one-page summary for a chair, curriculum committee or purchasing office. It covers what the software does, how to check it in a free trial, what a purchase involves, and the answers security and procurement reviewers usually need.

What it is

A desktop application for Windows, macOS and Linux that generates digital forensics and incident response lab exercises. Each case ships evidence in the real formats (disk images, registry hives, Windows event logs, Windows crash dumps and Linux LiME memory images, packet captures, mobile extractions, cloud audit logs, EDR and SIEM exports) with a worksheet, an answer key and a grading rubric.

The distinguishing feature is that **every student receives a different variant of the same case**: names, timestamps, hashes, addresses and answers all change per student from one seed. A copied answer is a wrong answer, and an anti-collusion report shows which submissions look alike. Every answer key is re-derived from the generated files by an independent parser before the lab is released.

What the trial lets you check

- [ ] Install without an account, generate a three-student First Look lab, and open the evidence in Autopsy, Registry Explorer, EvtxECmd, Wireshark or Volatility.
- [ ] Confirm two students' packages differ, and that the answer key for each matches its own evidence.
- [ ] Grade a submission and read the per-answer explanation; export the scores as a CSV your LMS imports.
- [ ] Open the 14-week forensics and 8-week incident response syllabi and map them to your catalog.
- [ ] Filter the library by certification-prep track (aligned to GIAC, CompTIA, EnCE and Cellebrite objectives) and by MITRE ATT&CK tactic.
- [ ] Run the student portal on the instructor's machine and submit answers as a student would.

First Look cases run free with no key. The 30-day trial key adds a medium and a hard case in each discipline, for up to five students per lab, with watermarked documents. CTF mode and the Scenario Editor need a license.

How a purchase works

- Card checkout on the website, or a purchase order sent to sales@redherrings.app. A W-9 and a vendor form are available on request.
- Licenses are annual and renew unless canceled. A license key arrives by email and is activated inside the app; air-gapped machines can activate by file.
- Department licenses cover three instructors; ask us about larger programs.
- Full refund within 14 days of purchase; see redherrings.app/refund.html.

Plans

Educator

One instructor and their classes

- Up to 40 students per lab
- Auto-grader, rubric and LMS export
- Student portal, timed exams and LTI grade passback
- Anti-collusion report and term analytics

Department

Programs with several instructors

- Three instructors included, 150 students per lab
- Every case, including the Expert capstones
- CTF mode and the Scenario Editor for authoring your own cases
- Institution logo on documents, priority support

Personal and student plans, current pricing and the free trial: **redherrings.app/#pricing**

For security and procurement review

QUESTION	ANSWER
Where does student data live?	On the instructor's computer. Generation, grading, rosters and submissions never leave it. No telemetry.
What network access is needed?	License activation and a periodic refresh with the license server; a missed refresh has 14 days' grace, and air-gapped machines activate by file. Optional, off by default: a once-daily version check and connected LMS (LTI 1.3) mode.
Does the vendor hold student records?	No. The only records held are the purchaser's email, license and payment status (card processing by Stripe).
Accessibility	Accessibility statement and VPAT at redherrings.app/accessibility.html.
Software integrity	Windows builds are code-signed (The Competence Collective, LLC). Licenses are Ed25519-signed.
Legal	EULA, privacy policy and terms at redherrings.app. Security questionnaires completed on request.