What a defensible forensic report contains

A section-by-section checklist for the written part of an investigation, usable as a template for students and as a grading guide for instructors. The order is the order a reader needs it: conclusion first, proof after, detail last.

1. Front matter

- [ ] Case identifier, report date, report version
- [ ] Examiner name, role and contact; organization
- [ ] Requesting party and the question they asked, in their words
- [ ] Classification or handling marking if any

2. Executive summary (half a page)

- [ ] What was examined, in one sentence
- [ ] Each conclusion as a plain statement with a confidence level
- [ ] What couldn't be determined and why
- [ ] No tool names, no hashes, no jargon the requester wouldn't use

3. Scope and authority

- [ ] Items received, each with number, description and hash
- [ ] Who collected them, when, and the chain of custody reference
- [ ] Questions in scope; questions explicitly out of scope
- [ ] Authority to examine (consent, warrant, policy, course assignment)

4. Methodology

- [ ] Tools with versions; verification that the image hash matched before analysis
- [ ] Write-blocking or working-copy procedure
- [ ] Time zone used throughout, and how it was established
- [ ] Any deviation from standard procedure, with the reason

5. Findings

- [ ] One finding per heading, each answering one question from the scope
- [ ] Every factual claim tied to a specific artifact: path, record, offset or event, and a timestamp
- [ ] Screenshots or extracts only where they prove something; captioned
- [ ] Observation and interpretation kept in separate sentences
- [ ] Alternative explanations considered and, where possible, ruled out

6. Timeline

- [ ] Chronological table: time (one zone), source artifact, event, significance
- [ ] Only events that support a finding; the full export goes in an appendix
- [ ] Gaps and clock problems called out, not smoothed over

7. Conclusions

- [ ] Restate each question and answer it directly
- [ ] Confidence stated and justified by the findings section
- [ ] Limitations: missing evidence, anti-forensics, time
- [ ] Recommendations only if asked for them

8. Appendices

- [ ] Evidence manifest with hashes; chain of custody forms
- [ ] Full tool output referenced in the findings
- [ ] Glossary for the non-technical reader
- [ ] Examiner qualifications

Common ways student reports lose marks. Conclusions that aren't in the findings. A finding with no artifact behind it. Mixed time zones. "The malware" when the evidence shows "an executable named". A summary written last and longest instead of first and shortest. Screenshots of a whole screen when one line was the point.

The Competence Collective, LLC