

Key Legal Precedents in Digital Forensics

Australian Jurisprudence: *R v. May* (2020)

Australian federal and state courts enforce stringent standards for expert witness testimony and reporting under the Evidence Act 1995. Failure to translate complex technical methodologies into accessible narratives can result in severe judicial penalties.

Australia: *R v. May* (2020)

In the landmark case of *R v. May* (2020), the court addressed the standards required for expert witness reports submitted in digital forensics and technical investigations.

Exclusion of Evidence Due to Missing Plain-Language Summary: The court ruled that forensic expert reports must include a clear, accessible, plain-language summary. In *R v. May*, critical digital evidence and its corresponding expert testimony were excluded because the report failed to provide a 1-page plain-language summary adequate for judges and juries without technical backgrounds to comprehend.

Strategic Impact for Forensic Practitioners

A technically flawless forensic analysis is rendered legally worthless if judicial stakeholders cannot understand its core conclusions. Practitioners must bridge the gap between deep artifact parsing and legal clarity.

Application for Forensic Workflows

To ensure full compliance with the precedent established in *R v. May* (2020), forensic examiners operating within Australian jurisdictions must:

- **Draft Executive Summaries First:** Always compose a concise, non-technical 1-page summary at the outset of report generation to articulate findings clearly for legal counsel and the bench.
- **Demystify Technical Artifacts:** Avoid opaque jargon when describing hex values, memory offsets, or packet timelines without accompanying plain-language explanations.
- **Validate Report Completeness:** Implement a peer-review checklist confirming that all mandatory reporting elements under the Evidence Act 1995 are fully met prior to final submission.

