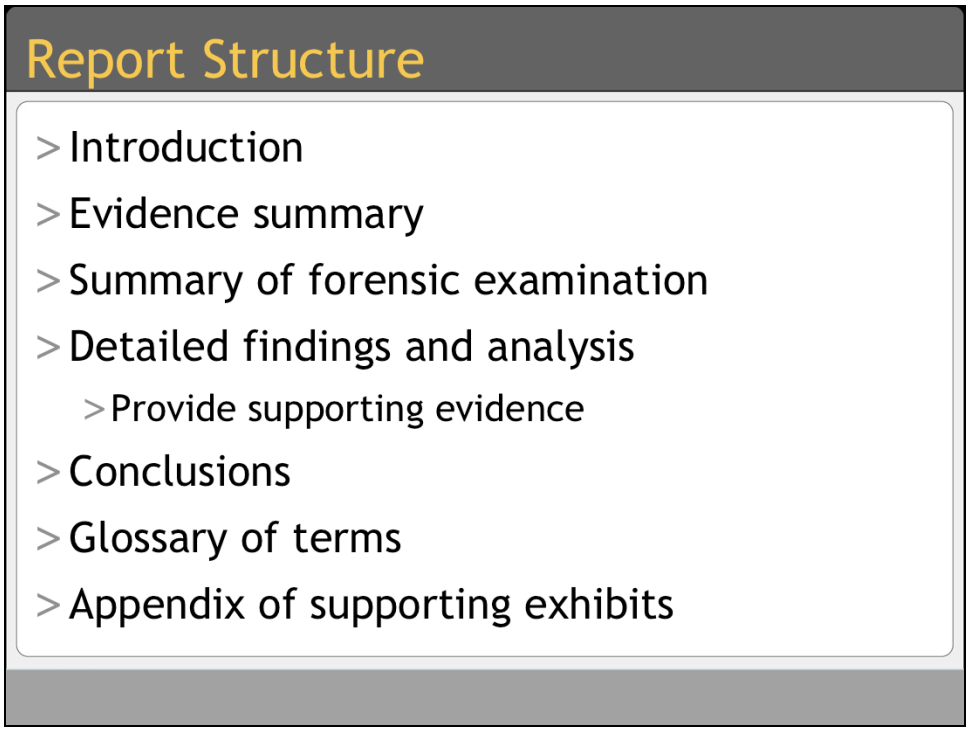
Report Writing Guidelines

General guidelines

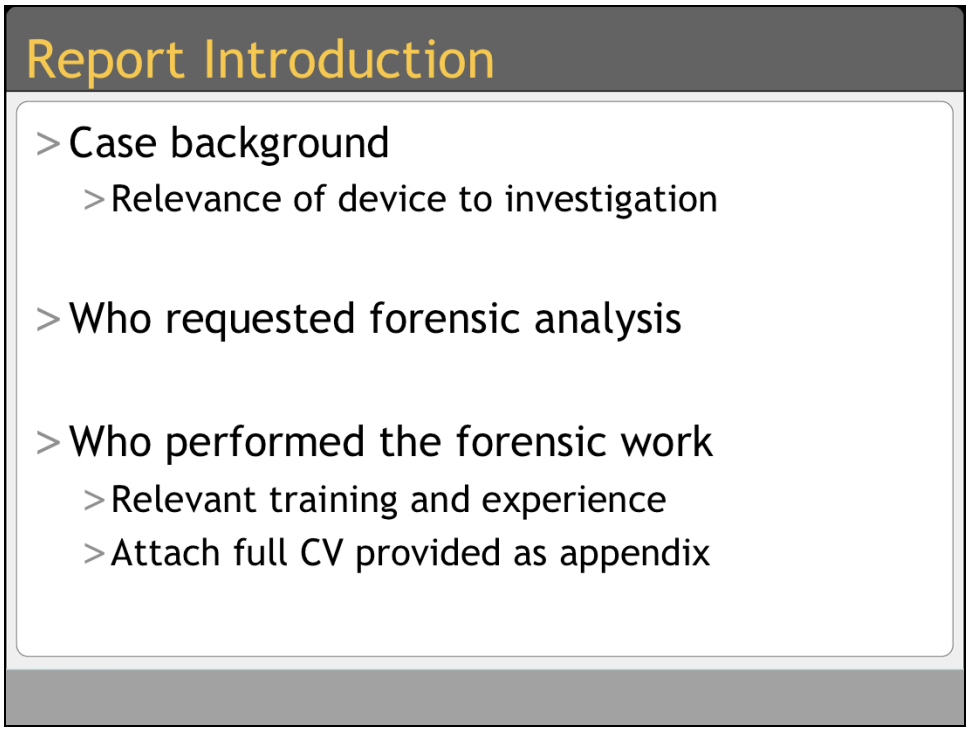
Presented by Dr. Eoghan Casey

31.05.2018



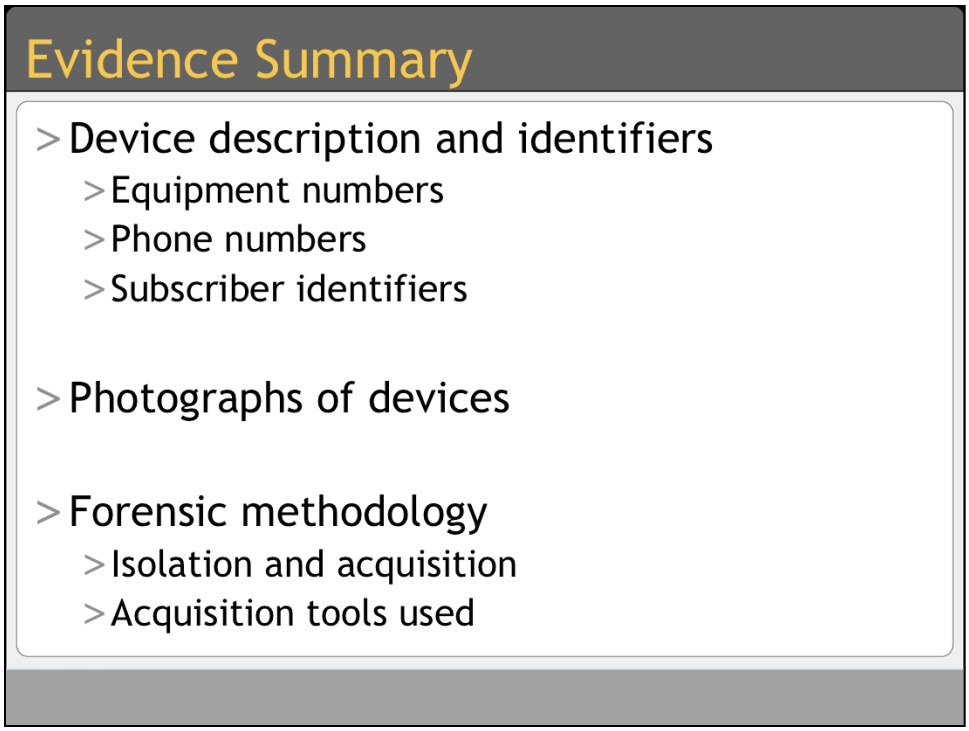
A forensic report should give readers all of the information they need to evaluate your work and the evidence. This should include the case background, your credentials, a summary of evidence you examined, and details about the evidence. Any additional forensic analysis should be described, and all conclusions may be summarized at the beginning and clearly stated at the end of the report.

Supporting items and a glossary of terms may be attached at the end if they are too cumbersome to include in the body of the report.



The report introduction should be short and sweet, providing an overview of the case, the relevance of the data being examined, and who requested the examination. In addition, the introduction should provide the credentials of those who performed the work, including a summary of relevant experience and training.

A full CV or resume can be provided as an attachment to the report.



Here is a sample evidence summary section:

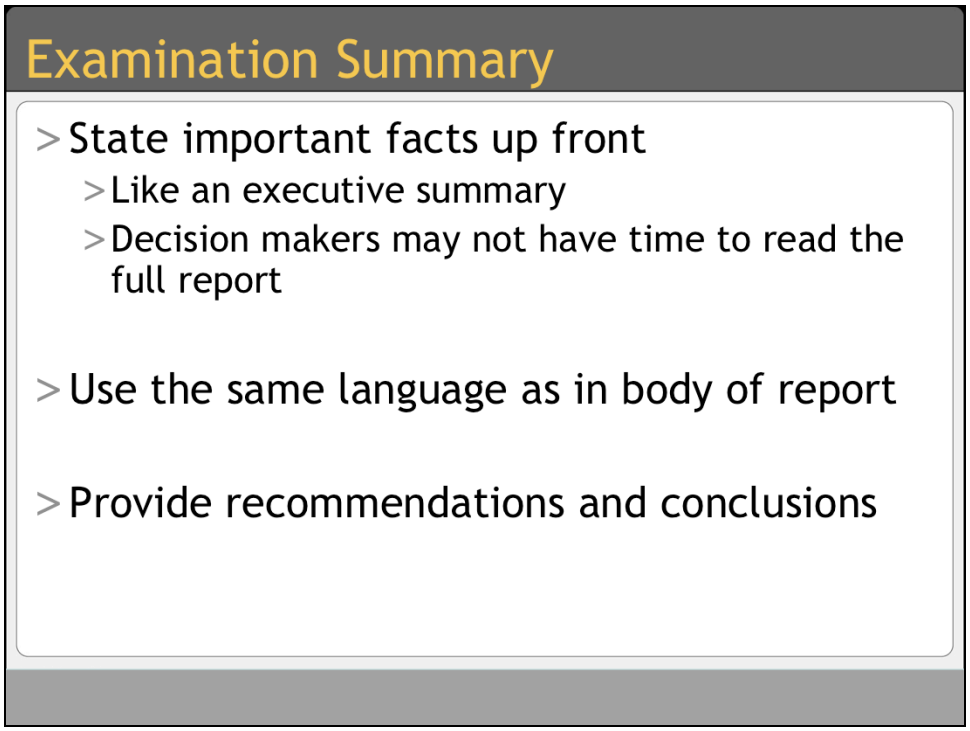
Evidentiary Media (Data)

The items listed below are not necessarily all evidence submitted in the case, but reflect the media where the reported evidence was found / located.

MD-001-001 (Person, Device Type 1)
HTC Dash (GSM), model S620
FCC-ID: NM8EXCA
IMEI: 355634020485402
S/N: SZ830FE01566
IMSI: 234545647568
ICCID: 98645634246

MD_001-002 (Person, Device Type 2)
Motorola RAZR (CDMA), model V3m
ESN: 02003591013
Phone number: 5405553322

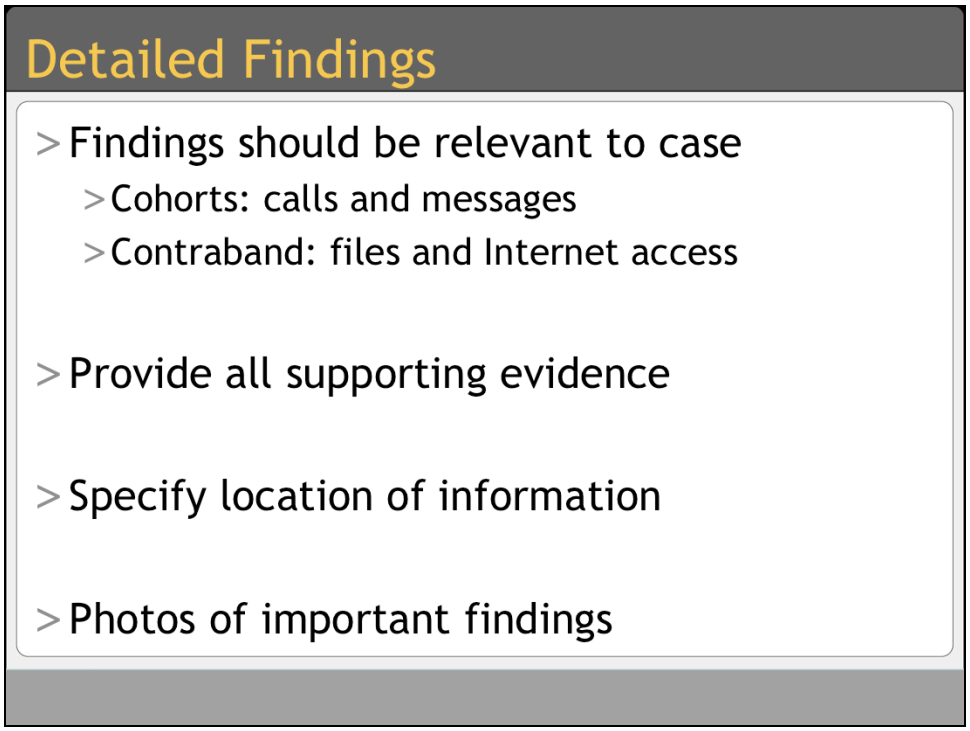
The mobile devices were labeled with reference numbers (MD_001-001 & MD_001-002). The report will refer to this designation when talking about information found on said storage media. Both devices were acquired in a forensic laboratory environment that prevented the devices from communicating with the network. Forensic acquisitions of MD_001_001 were performed using .XRY, Cellebrite, and XACT. Forensic acquisitions of MD_001_002 were performed using BitPim and MobileForensics. Whenever feasible, all findings were verified by performing a manual examination



The examination summary provides an overview of the critical findings relating to the investigation. This is intended for decision makers who may not have time to read the full report and just need to know the primary results of your forensic examination. Think of this as the executive summary. It should be a couple of brief paragraphs that fit onto one page.

It is important to describe key findings in clear terms that are comprehensible to a less-technical person. Use the same language in the examination summary as you use in the body of the report to avoid confusion and to help the attentive reader associate the summary with the relevant section in your detailed description.

The examination summary can include any recommendations or conclusions in short form.

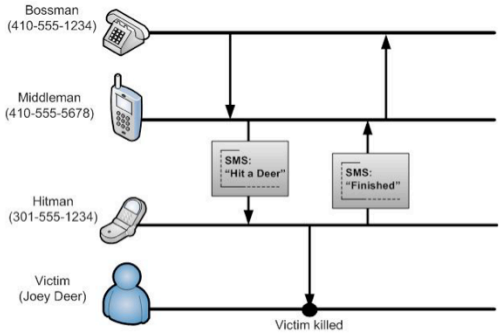


The section of findings from your forensic examination should contain all supporting evidence. If large amounts of information are involved, such a full listing of SMS or emails, put them in Appendices and reference them in the detailed findings.

The report should clearly specify the location where each trace was found, enabling others to find it and replicate your findings in the future. In addition to describing important findings in your report, it can be more clear and compelling to show a photograph or screenshot of the evidence as it is displayed on the device itself or seen during forensic examination. This can be important to show evidence in context or to show details of the evidence that are more meaningful when seen in a visual form.

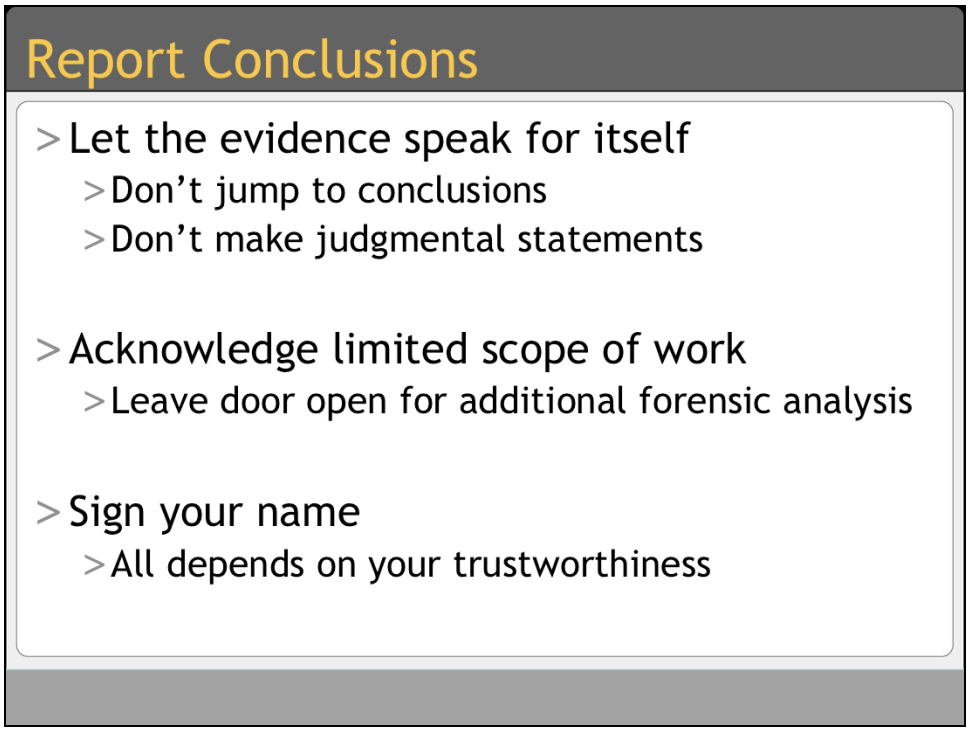
Forensic Analysis Examples

- Temporal
  - Chronology of events
- Relational
  - Link diagram
- Functional
  - Testing environment and results
- Evaluation of source



The analysis section should contain details about important insights you gained into the evidence, and how you conducted your analysis. This can be as simple as creating a timeline or link diagram and making observations about the events and relationships between entities.

This section could also include setup and configuration details for any functional analysis you performed (testing smartphone apps, dynamic analysis of malware). Any detailed analysis of particular items that requires an extensive description, such as characteristics of a photograph and their comparison with the subject mobile device, can be provided in a separate subsection. This section should provide sufficient detail to enable others to repeat and validate your analysis.



As a forensic practitioner, your conclusions must be objective and based in fact. Therefore, it is important not to jump to conclusions or make statements about innocence or guilt. Let the evidence speak for itself and avoid being judgmental. It is not your job to advocate the case – leave that to the lawyers.

To leave room for further analysis, say something like "Further review and examination of any of this information is available upon request."

Finalize your report with your signature and the date.