The following piece of information is an excerpt from Casey (2011).
Section 3.6 (Casey, 2011)

“In short, a formal report of forensic findings should give readers all of the information they need to evaluate the evidence and associated conclusions. The following is a sample report structure:

- Introduction: Provide an overview of the case, the relevance of the evidential media being examined, who requested the forensic analysis, and what was requested. In addition, the introduction should provide the bona fides of those who performed the work, including a summary of relevant experience and training. A full CV can be provided as an attachment to the report.
- Evidence Summary: Describe the items of digital evidence that were analyzed, providing details that uniquely identify such as make, model, and serial number. Also consider including MD5 values, photographs, laboratory submission numbers, details of when and where the evidence was obtained, from whom the evidence was obtained and its condition (note signs of damage or tampering), and processing methods and tools.
- Examination Summary: Provide an overview of the critical findings relating to the investigation. Think of this as the executive summary, with any recommendations or conclusions in short form. This section is intended for decision makers who may not have time to read the full report and just need to know the primary results of the forensic analysis. In certain situations, it is advisable to summarize tools used to perform the examination, how important data were recovered (e.g., decryption and undeletion), and how irrelevant files were eliminated (e.g., using NSRL hash sets). Whenever feasible, use the same language in the examination summary as is used in the body of the report to avoid confusion and to help the attentive reader associate the summary with the relevant section in the detailed description.
- File System Examination: When dealing with storage media, provide an inventory of files, directories, and recovered data that are relevant to the investigation with important characteristics such as path names, date-time stamps, MD5 values, and physical sector location on disk. Note any unusual absences of data that may be an indication of data destruction, such as mass deletion, reformatting, or wiping.
- Forensic Analysis and Findings: Provide a detailed description of the forensic analysis performed and the resulting findings, along with supporting evidence. Any detailed forensic analysis of particular items that requires an extensive description can be provided in a separate subsection. The report should clearly specify the location where each referenced item was found, enabling others to replicate and verify the results in the future. In addition to describing important findings in the report, it can be more clear and compelling to show a photograph, screenshot, or printout of the evidence. Describe and interpret temporal, functional, and relational analysis and other analyses performed such as evaluation of source and digital stratigraphy.
- Conclusions: A summary of conclusions should follow logically from previous sections in the report and should reference supporting evidence. It is important not to jump to conclusions or make statements about innocence or guilt. Conclusions must be objective and be based on fact. Let the evidence speak for itself and avoid being judgmental.”

Casey, E., 2011. *Digital evidence and computer crime: Forensic science, computers, and the internet.* Academic press.

Section 16.7 (Casey, 2011)

“A sample report structure is provided here:

- Introduction: case number, who requested the report and what was sought, and who wrote the report, when, and what was found.
- Evidence Summary: summarize what evidence was examined and when, MD5 values, laboratory submission numbers, when and where the evidence was obtained and from whom, and its condition (note signs of damage or tampering).
- Examination Summary: summarize tools used to perform the examination, how important data were recovered (e.g., decryption or undeletion), and how irrelevant files were eliminated.
- File System Examination: inventory of important files, directories, and recovered data that are relevant to the investigation with important characteristics such as path names, date-time stamps, MD5 values, and physical sector location on disk. Note any unusual absences of data.
- Analysis: describe and interpret temporal, functional, and relational analysis and other analyses performed such as evaluation of source and digital stratigraphy.
- Conclusions: summary of conclusions should follow logically from previous sections in the report and should reference supporting evidence.
- Glossary of Terms: explanations of technical terms used in the report.
- Appendix of Supporting Exhibits: digital evidence used to reach conclusions, clearly numbered for ease of reference.”

Ideas for Report Structure (these are just ideas, not a proposed template!)

Following this structure, here are some ideas about what to include in the report:
(Do not forget that you also have to submit your contemporaneous notes, your timeline, and your opinion except from the report)

- Introduction
- Evidence summary
- Examination Summary (Executive summary)
- File system examination and Analysis:
    - User profiling
    - System Profiling
    - Related to the case - important evidence items. You can include references to the Appendix in order to avoid putting a lot of information (e.g. timestamps, hashes, complete file paths) on the actual document.
      - Maybe you want to include separate subsections for the following areas: e.g. Images, Emails, Messaging Activity, Internet Activity, Relevant documents, relevant software found in the evidence, link files and recycle bin files, Print artefacts, Any external drives used, any network connections or connections to external devices that might be relevant to the case.
- Conclusions
- (Optional) Glossary of Terms
- Appendix of Supporting Exhibits: The Examination Report created by EnCase, or a similar list of the Evidence items and their provenance.

In other words, you are describing your findings in a formal way. Your language should be neutral, impartial, and you should only refer to the evidence found. You can provide pointers to the Examination Report and the timeline if you want to give a visual identity to your report.

Things to avoid:

Informal language, speculations, simplifications, erroneous provenance, erroneous interpretation of the timestamps, discrepancies among the report, timeline and contemporaneous notes.

Additional information: Sections 3.6, 16.7 (Casey, 2011)

Other References:

http://www.rnyte-cyber.com/uploads/9/8/5/9/98595764/exampledigiforensicsrprt_by_ryan_nye.pdf

http://www.adfmedia.org/files/CoalfireCMPvideosReport.pdf

https://www.legalexecutiveinstitute.com/understanding-digital-forensics-report/

https://www.geeksforgeeks.org/computer-forensic-report-format/

https://prodigital4n6.com/four-tips-for-effective-forensic-report-writing/

https://info.publicintelligence.net/NITROstudentV2.pdf

https://allegiantinvestigation.com/writing-a-forensics-expert-report/

https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

https://ao.gl/cyber-forensic-investigative-reports/

https://www.sans.org/blog/intro-to-report-writing-for-digital-forensics/

https://www.sans.org/blog/report-writing-for-digital-forensics-part-ii/

Cheers,
Panos