



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Digital Forensics Analysis (ACCA7031_LON)

Lecture 6

Reporting Results of Cyber Forensics Investigations

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk

Content covered

- Explain the importance of reports
- Describe guidelines for writing reports
- Documenting and preparing evidence
- Understanding the importance of reports
- Guidelines for writing reports
- Generating report findings with forensic software tools

Objectives

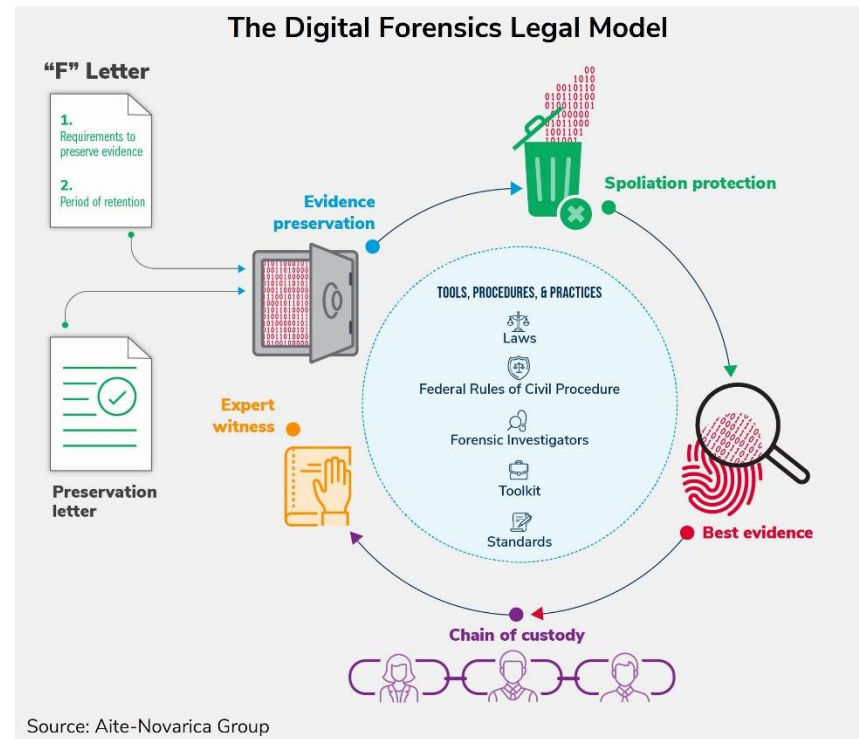
- Understand the purpose and structure cyber investigation report
- Understand the importance of finding reporting
- Differentiate between technical report and expert witness report
- Understand the structure of technical report and key components
- Understand the automation offered by DFIR tools in generating reports

Understanding the Importance of Reports

- Communicate the results of your investigation
 - Including expert opinion
- Courts require expert witness to submit written reports
- Written report must specify fees paid for the expert's services
 - And list all other civil or criminal cases in which the expert has testified
- Deposition banks
 - Examples of expert witness' previous testimonies

Digital Forensics Legal Model

- A reminder of the general legal model:

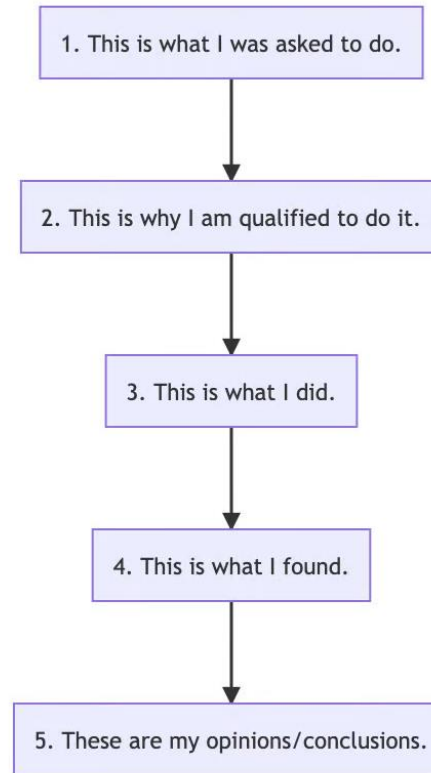


Limiting a Report to Specifics

- All reports to clients should start with the job mission or goal
 - Find information on a specific subject
 - Recover certain significant documents
 - Recover certain types of files
- Before you begin writing, identify your audience and the purpose of the report

Logical Flow of the Report

<https://www.forensicfocus.com/stable/wp-content/uploads/2021/02/Screenshot-2021-02-01-at-16.05.37.png>



Types of Reports

- Computer forensics examiners are required to create different types of reports
- Examination plan
 - What questions to expect when testifying
 - Attorney uses the examination plan to guide you in your testimony
 - You can propose changes to clarify or define information
 - Helps your attorney learn the terms and functions used in computer forensics

Types of Reports (cont.)

- Verbal report
 - Less structured
 - Attorneys cannot be forced to release verbal reports
 - Preliminary report
 - Addresses areas of investigation yet to be completed
 - Tests that have not been concluded
 - Interrogatories
 - Document production
 - Depositions

Types of Reports (cont.)

- Written report
 - Affidavit or declaration
 - Limit what you write and pay attention to details
 - Include thorough documentation and support of what you write

Types of Reports (cont.)

<https://guardian-forensics.com/wp-content/uploads/2017/07/Consent-Affidavit-Example-wording.pdf>

**AFFIDAVIT
AUTHORIZATION TO CONDUCT DIGITAL FORENSICS**

Comes now the affidavit, _____, and after begin duly sworn upon oath, states as follows;

I.

I am the affidavit, _____. I am above the age of 18 and competent to give this affidavit. I give this affidavit freely and here by warrant that the contents are based upon my personal knowledge.

II.

I hereby swear and affirm under penalty and perjury that I have authority to do any and all forensics, and hire any and all persons to conduct forensic examination on listed in the Description of Digital Evidence section delivery date of _____ to Guardian Forensics and Data Recovery, LLC consultant Alvey Matlock.

Description of Digital Evidence:

1) _____

2) _____

3) _____

4) _____

FURTHER, AFFIANT SAYETH NOT,

I, _____, begin first duly sworn, state under oath that I have read the above and foregoing affidavit, and the facts set forth herein are true and correct to the best of my knowledge, information, and belief.

'Name of Client/Law Firm' _____

Date: _____

Notary & Date:
Subscribed and sworn to before me this _____ day of _____, 2014

Notary Public

My commission expires: _____

Guidelines for Writing Reports

- Hypothetical questions based on factual evidence
 - Less favored today
 - Guide and support your opinion
 - Can be abused and overly complex
- Opinions based on knowledge and experience
- Exclude from hypothetical questions
 - Facts that can change, cannot be used, or are not relevant to your opinion

Guidelines for Writing Reports (cont.)

- As an expert witness, you may testify to an opinion, or conclusion, if four basic conditions are met:
 - Opinion, inferences, or conclusions depend on special knowledge or skills
 - Expert should qualify as a true expert
 - Expert must testify to a certain degree of certainty
 - Experts must describe facts on which their opinions are based, or they must testify to a hypothetical question

What to Include in Written Preliminary Reports

- Anything you write down as part of your examination for a report
 - Subject to discovery from the opposing attorney
- Considered high-risk documents
- Spoliation
 - Destroying the report could be considered destroying or concealing evidence
- Include the same information as in verbal reports

Report Structure

- Structure
 - Abstract
 - Table of contents
 - Body of report
 - Conclusion
 - References
 - Glossary
 - Acknowledgements
 - Appendixes

Writing Reports Clearly

- Consider
 - Communicative quality
 - Ideas and organization
 - Grammar and vocabulary
 - Punctuation and spelling
- Lay out ideas in logical order
- Build arguments piece by piece
- Group related ideas and sentences into paragraphs
 - Group paragraphs into sections

Writing Reports Clearly (cont.)

- Avoid jargon, slang, and colloquial terms
- Define technical terms
 - Consider your audience
- Consider writing style
 - Use a natural language style
 - Avoid repetition and vague language
 - Be precise and specific
 - Use active rather than passive voice
 - Avoid presenting too many details and personal observations

Designing the Layout and Presentation of Reports

- Decimal numbering structure
 - Divides material into sections
 - Readers can scan heading
 - Readers see how parts relate to each other
- Legal-sequential numbering
 - Used in pleadings
 - Roman numerals represent major aspects
 - Arabic numbers are supporting information

Designing the Layout and Presentation of Reports (cont.)

- Providing supporting material
 - Use material such as figures, tables, data, and equations to help tell the story as it unfolds
- Formatting consistently
 - How you format text is less important than being consistent in applying formatting
- Explaining examination and data collection methods
 - Explain how you studied the problem, which should follow logically from the purpose of the report

Designing the Layout and Presentation of Reports (cont.)

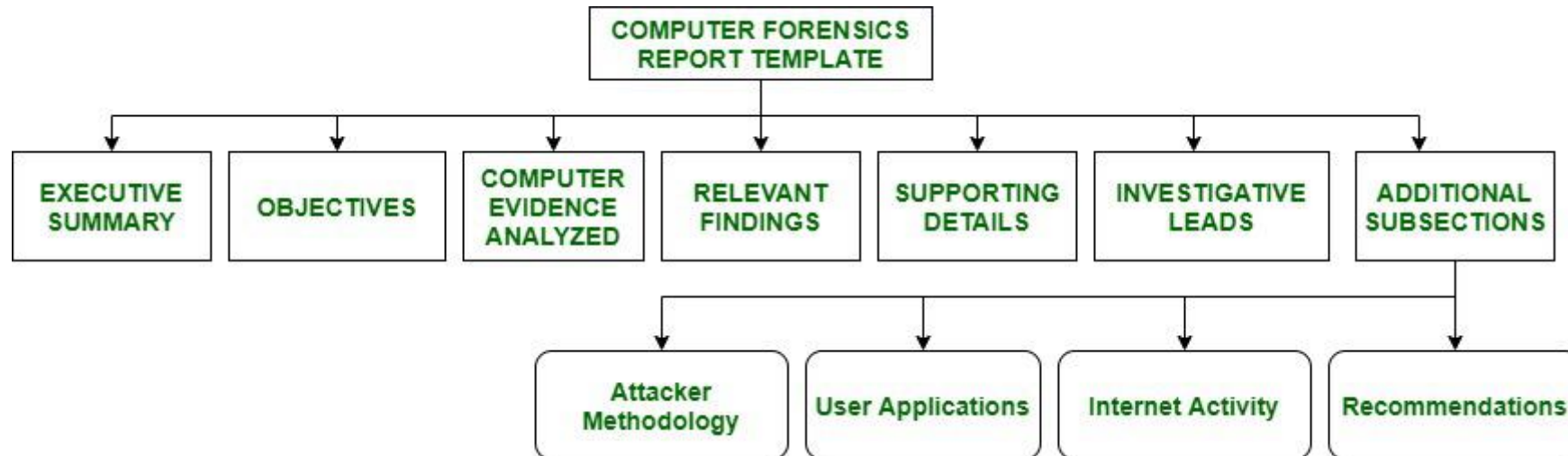
- Including calculations
 - If you use any hashing algorithms, be sure to give the common name
- Providing for uncertainty and error analysis
 - Protect your credibility
- Explaining results and conclusions
 - Explain your findings, using subheadings to divide the discussion into logical parts
 - Save broader generalizations and summaries for the report's conclusion

Designing the Layout and Presentation of Reports (cont.)

- Providing references
 - Cite references by author's last name and year of publication
 - Follow a standard format
- Including appendixes
 - You can include appendixes containing material such as raw data, figures not used in the body of the report, and anticipated exhibits
 - Arrange them in the order referred to in the report

Designing the Layout and Presentation of Reports (cont.)

- Example of the report format:



Designing the Layout and Presentation of Reports (cont.)

- Executive Summary
 - Provides background data of conditions that needs a requirement for investigation
 - Must contain short description, details and important pointers
- Objectives
 - Outline all tasks that an investigation has planned to complete
 - List should consist tasks undertaken and method undertaken by an examiner for each task and status of each task at the end of report
- Computer Evidence Analyzed
 - All gathered evidences and its interpretations are introduced. It provides detailed information regarding assignment of evidence's tag numbers, description of evidence and media serial numbers

Designing the Layout and Presentation of Reports (cont.)

- Relevant Findings
 - Summary of evidences found of probative value
 - Probative value of evidence can vary widely depending on way in which evidence is characterized and hypothesis of its interest
- Supporting Details
 - In-depth analysis of relevant findings is done
 - Contains table of vital files with a full path name, results of string searches, Emails/URLs reviewed, number of files reviewed and any other relevant data
 - Includes charts, tables and illustrations as it conveys much more than written texts. To meet outlined objectives, many subsections are also included
- Investigative Leads
 - Performs action items that could help to discover additional information related to the investigation of case
 - This section is very critical to law enforcement

Designing the Layout and Presentation of Reports (cont.)

- Additional Subsections

- Subsections are dependent on clients want and their need
- Examples include
 - Attacker Methodology
 - This section is useful in computer intrusion cases. Inspection of how attacks are done and what bits and pieces of attacks look like in standard logs is done here
 - User Applications
 - Discuss relevant applications that are installed on media analysed because it is observed that in many cases applications present on system are very relevant
 - Internet Activity
 - Browsing history is also useful to suggest intent, downloading of malicious tools, unallocated space, online researches, downloading of secure deleted programs or evidence removal type programs that wipe files slack and temporary files that often harbour evidence very important to an investigation
 - Recommendations
 - Gives recommendation to posture client to be more prepared and trained for next computer security incident

Designing the Layout and Presentation of Reports (cont.)

- Example of an excerpt from a report:

Analysis

File and Folder Analysis

There were a total of 29 folders residing on the flash drive. Each of the folders shows a modified, accessed, and created date of 2015-09-13 UTC with the modified and created time stamps between 2015-09-13 03:36:03 UTC and 2015-09-13 04:57:35 UTC. Copying a folder from a source drive to a destination drive results in the creation of a new modified and created date and time stamp on the destination drive. The date and time stamp from the source drive directory does not carry over to the directory created on the destination drive. This suggests that the date and time stamps for the folders located on the flash drive are indicative of when the folders were copied from the original source drive to the flash drive.

The root consisted of 5 directories which are listed below with their creation time and date stamps.

Directory Name	Created
[root]\052215Dyer dinner	2015-09-13 03:36:47 UTC
[root]\072514DebNucatola	2015-09-13 03:36:03 UTC
[root]\PPGC040915	2015-09-13 03:36:32 UTC
[root]\PPPSGV020615	2015-09-13 03:36:15 UTC
[root]\PPRM040715	2015-09-13 03:36:26 UTC

Directories contained within the root of the flash drive

Sources of Information for Reports

- Personal observations
- Applications
- Network/host devices
- Forensic tools

Audience for Reports

- Executives
- Information technology personnel
- Legal
- Marketing
- Regulators
- Law enforcement

Key Info to Include in a Forensics Report

- Examiner bio/background
- Tools utilized
- Evidence items
- Forensic analysis
- Tool output

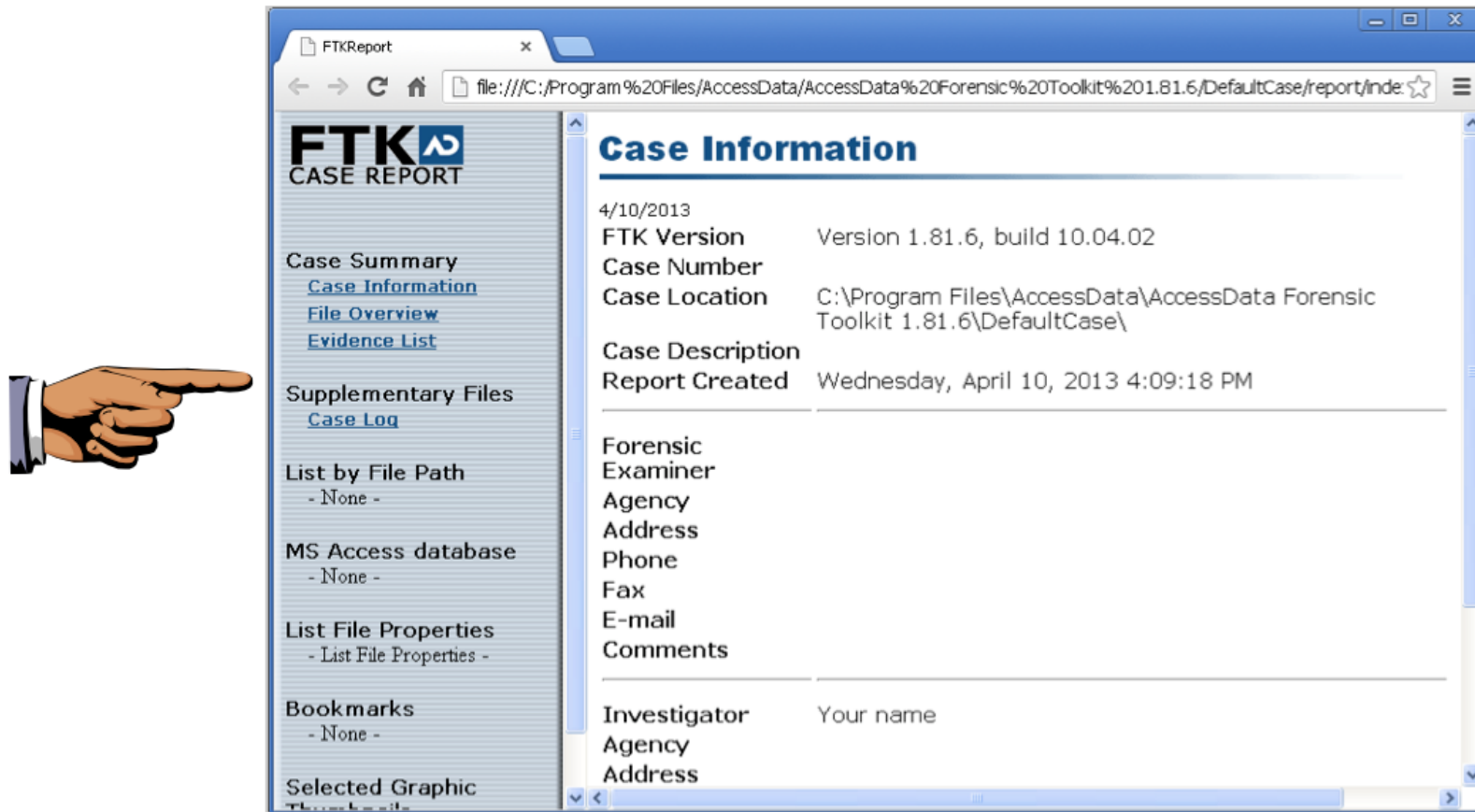
Generating Report Findings with Forensics Software Tools

- Forensics tools generate reports when performing analysis
- Report formats
 - Plaintext
 - Word processor
 - HTML format

Using FTK to Generate Reports

- Create a new case
- Add evidence to the case
- Analyze evidence with FTK
 - Look for image files
 - Locate encrypted files
 - Search for specific keywords
 - Indexed search
 - Live search
- Create bookmarks
- Generate a report from your bookmarks

Using FTK to Generate Reports



Using Autopsy to Generate Reports

- Open the case in Autopsy.
- Navigate to Tools and then to Generate Report.
- Select Results - HTML. Click on Next and then All Results.
- This produces an HTML report that will open in the default browser

Using Autopsy to Generate Reports

Digital Forensics and Incident Response,
Gerard Johansen (2nd, 2020) (p.g 315)

Report Navigation

- Case Summary
- ★ Data Source Usage (1)
- ★ Download Source (2044)
- EXIF Metadata (20)
- Encryption Suspected (13)
- Extension Mismatch Detected (46)
- ✎ Installed Programs (114)
- 🔍 Keyword Hits (3068)
- 🖨 Operating System Information (4)
- ★ Operating System User Account (9)
- 📄 Recent Documents (24)
- ★ Tagged Files (0)
- ★ Tagged Images (0)
- ★ Tagged Results (0)
- 🔌 USB Device Attached (16)
- 🔴 Web Bookmarks (25)
- ★ Web Cache (2038)

Autopsy Forensic Report

HTML Report Generated on 2019/09/23 17:51:51

Case:	Potential Data Leak Investigation
Case Number:	Incident-2019-0145
Number of Images:	1
Notes:	Suspected data leak from laptop
Examiner:	Gerard Johansen

Image Information:

JSmith_LT_0976.e01	
Timezone:	UTC
Path:	D:\Suspect_Images\JSmith_LT_0976\JSmith_LT_0976.e01
Path:	D:\Suspect_Images\JSmith_LT_0976\JSmith_LT_0976.e02
Path:	D:\Suspect_Images\JSmith_LT_0976\JSmith_LT_0976.e03
Path:	D:\Suspect_Images\JSmith_LT_0976\JSmith_LT_0976.e04

Types of Witness

- Two key types of Witness:
- Technical Witness
 - Only testify on facts experienced, offer no opinions
- Expert Witness
 - A third party whose testimony can be accepted in a criminal or civil case
 - Expert witnesses in digital forensics cases must be qualified to serve as an expert witness
 - Permitted to issue their opinions or draw conclusions on matters that fall under their umbrella of expertise

Key points

- All U.S. district courts and many state courts require expert witnesses to submit written reports
- Attorneys use deposition banks to research expert witnesses' previous testimony
- Reports should answer the questions you were retained to answer
- A well-defined report structure contributes to readers' ability to understand the information you're communicating

Summary

1. Different Types of witnesses
2. Different Types of Reports
3. The Importance of Reports and Structure
4. Guidelines for Writing Reports
5. Report Layout and Presentation
6. Generating Report Findings with Forensic Software Tools



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Any Questions?

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk