

Postgraduate Diploma in IT Forensics

Week 6 of Module 5: Collecting Digital Evidence & Presentation in Court

Hayson Tse, PhD (HK), Adjunct Lecturer, HKUSPACE

25 April 2019

Contents

1 Prologue	2
1.1 Help	2
1.2 Contact information	2
1.3 Copyright	2
1.4 Disclaimer	3
1.5 Classroom regulations	3
1.6 Important dates	3
1.7 Overview of your work cycle	4
2 Reference	4
3 Daily feeds	5
4 Who guards the guardians	5
4.1 <i>U.S. v Shane Ragland</i>	5
5 Expert Evidence	8
5.1 Digital evidence	8
5.2 Opinion based on four principles	8
5.3 Reports	9
5.4 One example	9
5.5 Degree of certainty	11
5.6 Another example	12
5.7 Code of Practice	14
5.8 Expert reports in mainland	15
5.9 Free tools	15
5.10 Reports by software	15
5.11 The Official EnCE: EnCase Certified Examiner Study Guide	16
5.12 How a judge evaluates the expert evidence	17

6 Disclosure	18
6.1 Disclosure Manual	18
6.2 Guidance Booklet for Experts Disclosure	18
7 Trial	21
7.1 Voir dire	21
7.2 Examination-in-chief	22
7.3 Questions type	23
8 <i>California v. David Alan Westerfield</i>	24
8.1 Introduction from Wikipedia	24
8.2 Testimony of James Watkins	25
9 <i>Florida v. Casey Anthony</i>	30
9.1 Some digital evidence	30
9.2 The story from Wikipedia	30
9.3 The story from Goodison et al.	30
9.4 The timeline	31
9.5 The teams	32
9.6 The videos	32
9.7 Three prosecution computer forensic experts	33
9.8 Detective Sandra Osborne	33
9.9 Detective Sergeant Kevin Stenger	33
9.10 Detective Sandra Osborne, Examination-in-chief	33
9.11 An Interview with Sandra Osborne	37
10 Epilogue	37
10.1 Summary	37

1 Prologue

1.1 Help

- Blue means I am a link; please click me.

1.2 Contact information

- Personal email
 - hayson.tse

1.3 Copyright

This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International Licence.



1.4 Disclaimer

- All materials come from the public domain. There are no government or trade secrets.
- Newspaper clippings may or may not contain the complete sets of allegations in relation to a case.
- A person who has been reported by newspaper clippings as being arrested or charged is presumed innocent until he is convicted or even until his appeal against conviction is dismissed.

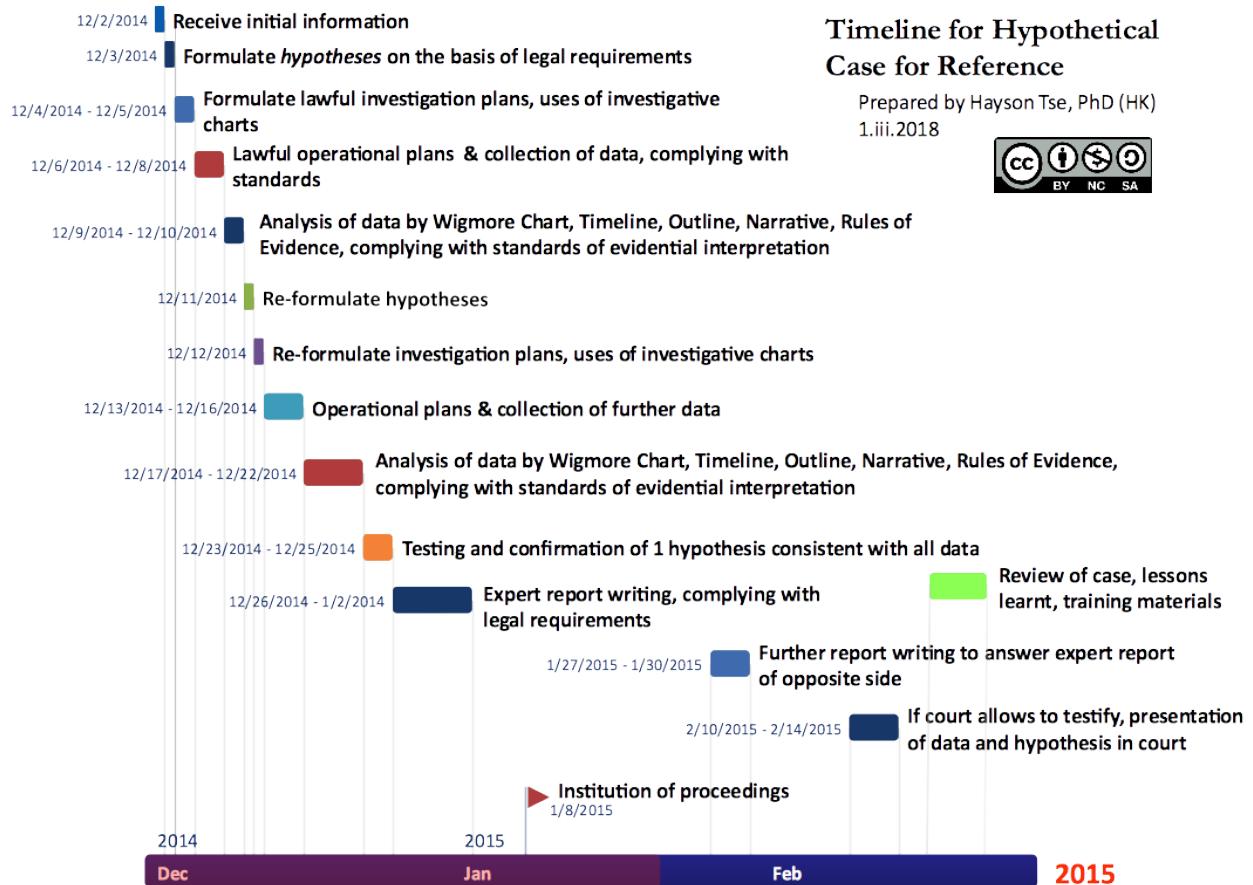
1.5 Classroom regulations

- [HKU SPACE Handbook](#)
- No reservation of seats.
- No eating or drinking.
- Turn off all mobile phones and pagers.
- No smoking at all HKU SPACE learning centres and the University campus.
- *No video / audio recording, unless with the permission of the Programme Director / Manager*
- The Programme Direction / Manager may impose any conditions when granting the permission.
- No unattended personal belongings.

1.6 Important dates

- Assignment: 2 May 2019
- EXAMINATION: 6 June 2019

1.7 Overview of your work cycle



2 Reference

- First appeal: *Au-Yeung Ping Keung v. R* CACC 966/1975
- Second appeal: *Au-Yeung Ping Keung v. R* CACC 528/1976
- Commission of persons with special knowledge to participate in investigation of criminal case in Mainland
 - regulation available [here](#)
 - explanation available [here](#)
- Confirmation of digital evidence with physical evidence, witness statements and confessions
 - examples [here](#)
- Insufficiency of expert report
 - A news report regarding insufficiency of expert evidence in KTCC 4438/2016
 - Another news report regarding insufficiency of expert evidence in KTCC 4438/2016

- Third news report regarding insufficiency of expert evidence in KTCC 4438/2016

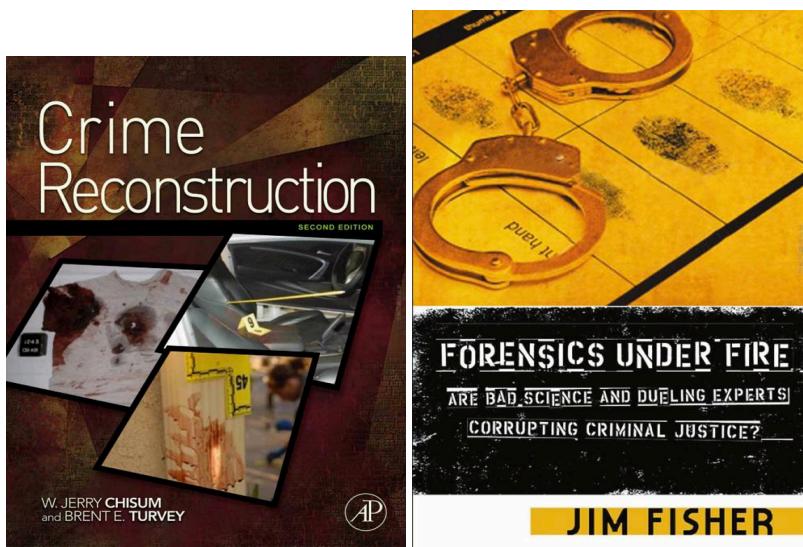
3 Daily feeds

- <https://twitter.com/GCHQ>
- <https://twitter.com/NCSC>
- <https://twitter.com/DIIPolice>
- <https://twitter.com/IDIIAwards>
- <https://twitter.com/EnCase>
- <https://twitter.com/sleuthkit>
- <https://twitter.com/volatility>
- <https://twitter.com/Cisco>
- <https://twitter.com/CTFtime>
- <https://twitter.com/OSINTtechniques>
- <https://twitter.com/sansforensics>
- <https://hitcon.org/>
- <https://www.defcon.org/>

4 Who guards the guardians

4.1 *U.S. v Shane Ragland*

4.1.1 Books



- W. Jerry Chisum and Brent Turvey. Crime Reconstruction. Academic Press, 2011.
- Jim Fisher. Forensics Under Fire: Are Bad Science and Dueling Experts Corrupting Criminal Justice? Rutgers University Press, 2008.

4.1.2 The trial

"In 1994, Trent DiGiuro, football player and honour student, was shot in the head while celebrating his 21st birthday. He was sitting on the front porch of a house he and two teammates shared near campus. His murder was unsolved for six years until Ragland's former girlfriend claimed he had told her in 1995 that he committed the shooting."

- In 2002, Ragland was found guilty and was sentenced to 30 years for the murder.
- Ragland appealed.

4.1.3 The appeal

"In May 2004, at issue before the Supreme Court was a particular sequence during the prosecution's closing argument in which the prosecuting counsel told jurors that the exact location of where the fatal shot had been fired was not determined because Ragland "hadn't seen fit to tell us." The court's decision hinged on whether a comment made by a prosecutor during his closing argument improperly mentioned that Ragland exercised his Fifth Amendment right to not testify. In a 4-3 decision, the court found that prosecutor Mike Malone's closing statement "requires" that Ragland get a new trial."

- Supreme Court decision: *Shane Ragland v. Commonwealth of Kentucky* 191 S.W.3d 569 (2006)

4.1.4 Another ground of appeal

- Another ground of appeal was that Special Agent Kathleen Lundy of the FBI Crime Laboratory, an expert in comparative bullet-lead analysis, had made a false statement.
- Lundy testified that the murder-scene bullet fragments were "analytically indistinguishable" from the bullets in the box seized in the search of Ragland's residence.

4.1.5 The 2 scientific assumptions of the opinion

- Every batch of lead is perfectly consistent in its chemical composition (Comparative bullet-lead analysis (CBLA) experts use the term "homogenous" in this context)
- Every manufacturer's batch of lead has a unique chemical composition, different from all other batches.

4.1.6 Testimony of Kathleen Lundy

"Under oath in court, she knowingly gave false testimony that the Winchester company had melted its own bullet lead until 1996, when in reality Winchester had stopped the practice in 1986. She did so to bolster her conclusion that two bullets had come from the same batch of manufacturing lead and could therefore be linked to the same person."

- Why did she give false testimony? (see question 1 of assignment)

"This is consistent with the specimens within each group originating from the same source of bullet lead at the Winchester Ammunition manufacturing plant. . . . These results are typical of what is expected among bullets originating from the same box of cartridges or other boxes of the same manufacturer, caliber and type packaged on or about the same date." (quoting from her report)

"[W]e have seen that bullets that come from the same source of lead will have the same composition, and bullets from different sources of lead have different composition. . . . And we have studied the production processes within the plants and seen that you will have bullets of the same composition in a given box or other boxes of that same product that are packaged at the same time . . ."

"[Y]ou expect to find bullets of the same composition in a given box or other boxes, but, you know, it's the same type of ammunition that's produced at the same time. That's the – that's where you expect to find compositional similarities. . . . Well, again, that means that from analyzing many boxes of ammunition over the years in many cases in research projects and in many of the cases I've worked there have been multiple boxes with the same packing code, which means they were produced at the same time. And I've seen that you do expect to find the same compositions in these different boxes."

4.1.7 Why she lied?

"I cannot explain why I made the original error . . . nor why, knowing that the testimony was false, I failed to correct it at the time," Lundy wrote in a May 28 internal FBI memo. "I was stressed out by this case and work in general. I had been under a great deal of professional pressure for over a year and had considered resigning. This pressure was increased by new and repeated challenges to the validity of the science associated with bullet-lead comparison analysis. These challenges affected me a great deal, perhaps more than they should have. I also felt that there was ineffective support from the FBI to meet the challenges."

"Lundy claimed that she gave the false testimony under pressure coming from the many recent challenges to her area of expertise – she feared that her testimony might be disallowed and that her field might lose credibility with the courts."

4.1.8 What happened to her

"The federal authorities declined to prosecute her for any wrongdoing; however, the State of Kentucky took a slightly different view. She was charged and pleaded guilty to false swearing in Fayette County District Court. She received a 90-day suspended sentence and a \$250 fine."

4.1.9 What happened to Ragland

- In 2006, the court ruled that in Ragland's retrial, the government could not present lead composition evidence.
- In 2007, the girl friend refused to cooperate.

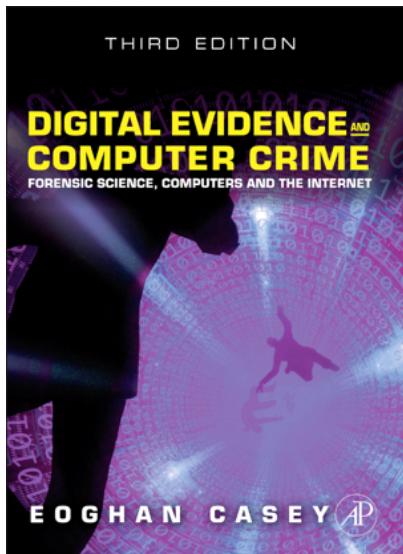
4.1.10 Who killed DiGiuro?

- After negotiation, Ragland pleaded guilty to manslaughter.

5 Expert Evidence

5.1 Digital evidence

- Digital Evidence and Computer Crime Forensic Science, Computers and the Internet
- Eoghan Casey



5.2 Opinion based on four principles

- Balance
- Logic
- Robustness
- Transparency

5.2.1 Balance

"The expert should address at least one pair of propositions usually one based upon the prosecution issue and one based upon an alternative (defence issue). If a reasonable alternative cannot be identified then the expert may address only the

one proposition but will make it clear that he cannot evaluate the strength of the evidence.”

- at least deal with a pair of propositions: for and against
- identify reasonable alternative for propositions

5.2.2 Logic

“The expert will address the probability of the evidence given the proposition and relevant background information and not the probability of the proposition given the evidence and background information.”

“probability of the evidence given the proposition and relevant background information” vs. “the probability of the proposition given the evidence and background information.”

5.2.3 Robustness

“The expert will provide opinion that is capable of scrutiny by other experts and cross-examination. He will base his opinion upon sound knowledge of the evidence type(s)”

- capable of scrutiny by other experts and cross-examination
- opinion on the basis of sound knowledge of the evidence

5.2.4 Transparency

“The expert will be able to demonstrate how he came to his conclusion. He will set out in report the basis of his opinion viz.: Propositions addressed, Test or examination results, The background information he has used in arriving at his conclusion.”

- Propositions addressed
- Test or examination results
- Background information
- Reasoning

5.3 Reports

5.4 One example

- Digital Evidence and Computer Crime Forensic Science, Computers and the Internet
- Sample report structures:
- Introduction

- Evidence Summary
- Examination Summary
- File System Examination
- Forensic Analysis and Findings
- Conclusions

5.4.1 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.”

5.4.2 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.”

5.4.3 Examination Summary

“Provide an overview of the critical findings relating to the investigation. . . . with any recommendations or conclusions in short form. This section is intended for decision makers . . . 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.”

5.4.4 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.”

5.4.5 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."

5.4.6 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."

5.5 Degree of certainty

- Table of Degree of Certainty:-

Certainty Level	Description/Indicators	Commensurate Qualification
C0	Evidence contradicts known facts	Erroneous/incorrect
C1	Evidence is highly questionable	Highly uncertain
C2	Only one source of evidence that is not protected against tampering	Somewhat uncertain
C3	The source(s) of evidence are more difficult to tamper with but there is not enough evidence to support a firm conclusion or there are unexplained inconsistencies in the available evidence	Possible
C4	(a) Evidence is protected against tampering or (b) evidence is not protected against tampering but multiple, independent sources of evidence agree	Probable
C5	Agreement of evidence from multiple, independent sources that are protected against tampering. However, small uncertainties exist (e.g., temporal error and data loss)	Almost certain
C6	The evidence is tamper proof or has a high statistical confidence	Certain

5.6 Another example

5.6.1 Style and format

- Report should contain:-
- Details of qualifications, experience or accreditation
- Relevant to the work performed
- The range and extent of expertise
- Details of any information, e.g. literature, reliance of which opinion is based
- Details of any statements of fact reliance of which opinion is reached
- Clarification of which of the facts are within personal knowledge

5.6.2 Not a scientific paper

- Write for an intelligent lay audience
- Minimize jargon
- Use jargon correctly
- Define jargon and terms
- Define all abbreviations
- Be succinct

5.6.3 Not a scientific paper

- Cite page numbers in the material referenced
- Explain all complicated concepts
- Also explain seemingly simple concept
- Report should include all charts, graphs, quotes, that will be used as exhibits in court

5.6.4 Contents

- Academic and professional qualifications
- A statement of the source of instructions and the purpose of the advice or report
- A chronology of the relevant events

“A statement of the methodology used, in particular what laboratory or other tests (if any) were employed, by whom and under whose supervision”

- Details of the documents or any other evidence upon which any aspects of the advice or report is based;

“A statement setting out the substance of all instructions (whether written or oral). The statement should summarize the facts and instructions given to the expert which are material to the opinions expressed in the report or upon which those opinions are based.”

“Should not express a view in favour of one or other competing sets of facts, unless, because of their particular learning and experience, they perceive one set of facts as being improbable or less probable, in which case they may express that view, and should give reasons;”

- Should express separate opinions on every set of facts in issue (what are facts in issue)
- Begin with name, office address, qualification and experience of the expert
- A statement as to the issues to which the report relates and identify the problem
- Specify the investigations that has been carried out
- Set out details as to the test that has been carried out and any test which appear relevant were not carried out and explain the reason
- Set out the facts as that were established
- Assessment of the facts with explanatory reasons
- State the conclusions on the issues set out in the beginning of the report
- Sign and date the report
- May contain footnote and appendices and any supporting documentation, e.g. plans, photographs, diagrams

5.7 Code of Practice

5.7.1 The Code of Practice for Expert Witnesses Engaged by the Prosecuting Authority

- October 2004
- [Statement by the Director of Public Prosecutions](#)

5.7.2 Application of the Code

- Any expert engaged by prosecution who:-
 - provides a report and/or witness statement as to opinion for use as evidence (testimony)
 - gives opinion evidence (testimony)
 - is the Court appointed expert
- Does not apply:-
 - to a civil servant, a public servant or an employee of a public body

5.7.3 General obligation to court

- primary duty is to the Court and not to the person retaining the expert.
- not an advocate for a party.
- overriding duty to assist the Court impartially

5.7.4 Form of expert report

- qualifications and experience
- purpose of the report
- facts, matters, observations and assumptions on which the opinions in the report is based
- the facts and matters assumed or observed by the expert
- differentiate assumed facts, observed facts, facts asserted upon the basis of experience, facts as the product of the exercise of expert reasoning
- reasons for opinion
- question or issue falls outside expertise
- literature or other materials utilised in support of the opinion
- any Hong Kong, Australian, British, American or European Union , relied upon examinations, tests or other investigations relied upon
- details of the person(s) who carried out those examinations, tests or other investigations
- the expert's reasoning, disclosed in a manner sufficient to enable the tribunal of fact to understand and evaluate his or her conclusions.
- any qualified opinions and such qualifications
- any not concluded opinion and the reasons
- any change of opinion (by supplementary report)

5.7.5 Where the expert is unable to comply with the Code

- Where an expert to whom the Code applies is unable to comply with any of the provisions of the Code, he or she should state that fact in his or her report and provide details of the reason or reasons for non-compliance.

5.7.6 Duty to disclose relevant personal information

- any criminal convictions
- any criminal investigation of which the expert is aware, relating to the expert, which has commenced but has not yet concluded;
- any adverse finding relating to the expert, made by any statutory, disciplinary or professional body or tribunal
- any investigation of which the expert is aware, relating to the expert, by any statutory, disciplinary or professional body or tribunal, which has commenced but has not yet concluded

5.7.7 If no relevant personal information

"I have never been convicted of any criminal offence; nor have I been the subject of an adverse finding by any statutory, disciplinary or professional body or tribunal, nor, so far as I am aware, am I the subject of any investigation by any statutory, disciplinary or professional body or tribunal."

5.8 Expert reports in mainland

5.8.1 Legal requirement

- Serial number (covering page)
- Declaration
- Introduction
- Summary of the case
- Examination process
- Descriptions of analysis
- Forensic opinion
- Conclusion
- Appendix

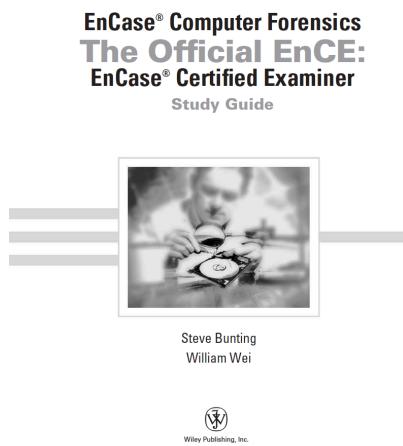
5.9 Free tools

- [Top 20 Free Digital Forensic Investigation Tools for SysAdmins](#)

5.10 Reports by software

- I am not recommending EnCase
- Report by EnCase, as an example

5.11 The Official EnCE: EnCase Certified Examiner Study Guide



Contents at a Glance

<i>Foreword</i>	<i>xiv</i>
<i>About the Authors</i>	<i>xvii</i>
<i>Introduction</i>	<i>xxvi</i>
<i>Assessment Test</i>	<i>xxxiii</i>
Chapter 1 Computer Hardware	1
Chapter 2 File Systems	29
Chapter 3 First Response	77
Chapter 4 Acquiring Digital Evidence	103
Chapter 5 EnCase Concepts	155
Chapter 6 EnCase Environment	183
Chapter 7 Understanding, Searching for, and Bookmarking Data	241
Chapter 8 File Signature Analysis and Hash Analysis	307
Chapter 9 Windows Operating System Artifacts	335
Chapter 10 Advanced EnCase	401
Appendix A Creating Paperless Reports	485
Glossary	499
Index	507

- Appendix A is creating report step by step instructions

5.11.1 George State University

- George State University
- Instructions for preparing report by Encase

We will use the following bookmark folders for a forensics report of this evidence:

1. Introduction
 - a. Author: Report Prepared By
 - b. Client: Report Prepared For
 - c. Case Overview
 - d. Executive Summary: Results
2. Device Folder Structures
3. Examination Findings
 - a. Dry Ice
 - b. Nigeria
 - c. Terrorism, Bombs, and Explosions
4. Forensic Process
 - a. Validation
 - b. Recovery
 - c. Chain of custody
 - d. License statement
 - e. Examiner Qualifications

5.12 How a judge evaluates the expert evidence

- The Code of Practice for Expert Witnesses Engaged by the Prosecuting Authority
- How a judge evaluates
- *Scott v. Bloomsbury Health Authority* [1990] 1 Med LR 214
- *Loveday v. Renton* [1990] 1 Med LR 117
- Reasons given for his opinions.
- Extent of reasons supported by evidence.
- Internal consistency and logic of his evidence.
- Precision and accuracy of thought as demonstrated by his answers.
- Care with which he has considered the subject and presented his evidence.
- How he responds to searching and informed cross-examination.
- How he faces up to and accepts the logic of a proposition put in cross-examination.
- How he is prepared to concede points that are correct.
- Extent to which a witness has conceived an opinion and is reluctant to re-examine it in the light of later evidence.
- Where criticisms have been made on grounds of bias or lack of independence, the witness's demeanor is a factor.
- Inappropriate expertise.
- Outdated expertise.
- Campaigning approach.
- Lack of familiarity with notes.
- Exaggerated inferences from notes.
- Lack of familiarity with literature.
- Disrespect for other experts.
- Late invention.
- Exaggerated expressions of opinion.

6 Disclosure

6.1 Disclosure Manual

- [Crown Prosecution Service Disclosure Manual 26 February 2018](#)
- Chapter 36: Expert Witnesses – Prosecution Disclosure Obligations

“36.2 There is no definitive legal definition of an expert. It is a matter for the court to rule upon in each case. However for the purposes of this guidance, an expert is defined as: “a person whose evidence is intended to be tendered before a court and who has relevant skill or knowledge achieved through research, experience or professional application within a specific field sufficient to entitle them to give evidence of their opinion and upon which the court may require independent, impartial assistance”.”

“36.3 The difference between an expert and other witnesses is that experts are the only witnesses allowed to give opinion evidence. For that reason, an expert witnesses’ competence in their field of expertise may be in issue as well as their credibility. If an expert’s credibility and/or competence is the subject of concern, that information should be considered for disclosure.”

6.2 Guidance Booklet for Experts Disclosure

- [Guidance Booklet for Experts Disclosure: Experts’ Evidence, Case Management and Unused Material May 2010](#)

6.2.1 Aims of disclosure

“The regime for disclosure is set out in the [Criminal Procedure and Investigations Act] and the Code issued under it. This is designed to ensure that there is a fair system for the disclosure of unused material which assists the defence in the timely preparation of its case, does not overburden the parties and enables the court to focus on all the important issues in the trial.”

6.2.2 The meaning of unused material

“During the course of any investigation material is generated. Some of it is used as evidence and other material is not used. The material that is not used as evidence is known as unused material, to which the disclosure regime applies.”

“Unused material is material that is relevant to the investigation but which does not actually form part of the case for the prosecution against the accused. Even though the material may not be used as evidence, it is important that for the purposes of disclosure this material is retained. It is not for you to determine whether

the material generated in the course of an investigation is relevant to the investigation.”

6.2.3 Discharging obligations

“There are three key obligations arising for you, as an expert, as the investigation progresses. Your understanding of these obligations and your delivery of them is the key to you adequately fulfilling your disclosure obligations. The relevant steps are to retain, to record, and to reveal.”

6.2.4 What to retain

“You should retain everything, including physical, written and electronically captured material, until otherwise instructed and the investigator has indicated the appropriate action to take.”

6.2.5 How long to retain

“The period of time for which materials are required to be retained will vary from case to case and will depend on a number of factors. Examples include the nature of the offence; the stage and status of any legal proceedings; whether the case is of special interest. It must also be remembered that the retention requirement may alter as a result of a change of circumstances during the course of the investigation.”

6.2.6 When to record

“The requirement for you to commence making records begins at the time you receive instructions and continues for the whole of the time you are involved.”

6.2.7 What to record

“You should keep records of all the work you have carried out and any findings you make in relation to the investigation. The guidance provided . . . as a minimum . . . :”

“your notes, and those of any assistant, should be signed, dated, attributable to the individual and produced contemporaneously, whenever practicable;”

“the notes should be sufficiently detailed and expressed in such a manner that another expert in your field can follow the nature of the work undertaken, any assumptions made and the inferences you have drawn from the work.”

“verbal and other communications:”

“you should keep your own notes of all meetings you attend;”

“you should keep your own notes of telephone conversations and it is important that points of agreement, or disagreement and agreed actions are recorded;”

“you should ensure that a record of all emails and other electronic transmissions (such as images), sent or received, is kept;”

“you should keep clear notes of any witness accounts or explanations that you have been provided with, or any other information received.”

6.2.8 Report should contain

“details of your qualifications, experience or accreditation relevant to the work performed;”

“the range and extent of your expertise;”

“details of any information upon which you have relied in arriving at your opinion;”

“details of any statements of fact upon which you have relied in reaching your opinion;”

“clarification of which of the facts are within your own knowledge;”

“information relating to who has carried out measurements, examinations, tests etc and if under your supervision”

“your opinion(s) and a justification for these”

“where you have provided qualified opinions details of these qualifications”

“a summary of all your conclusions”

6.2.9 Failure to comply disclosure

- prosecution halted or delayed
- appellate courts finding that a conviction is unsafe
- trial court makes adverse comment about you
- professional embarrassment (action by professional body)

- credibility

7 Trial

7.1 Vior dire

- Trial within a trial

7.1.1 Process

- Specific issues (preliminary questions)
- General issues
- See [HK Law Reform Commision: Report on the Procedure Governing the Admissibility of Confession Statements](#)
- Section 189 of the Evidence Act 1995 (New South Wales):
 - (1) If the determination of a question whether:
 - (a) evidence should be admitted (whether in the exercise of a discretion or not), or
 - (b) evidence can be used against a person, or
 - (c) a witness is competent or compellable,

depends on the court finding that a particular fact exists, the question whether that fact exists is, for the purposes of this section, a preliminary question

“If the determination of a question whether evidence should be admitted (whether in the exercise of a discretion or not); or evidence can be used against a person; or a witness is competent or compellable; depends on the court finding that a particular fact exists, the question whether that fact exists is, . . . , a preliminary question.”

- Specific issue (preliminary questions)
- Prosecution Case
- Defence Case
- Judge’s ruling on specific issue

7.1.2 Specific issue - Prosecution case

- Witnesses for the specific issue

- Examination-in-chief
- Cross-examination
- Re-examination

7.1.3 Specific issue - Defence case

- Witnesses for the specific issue
- Examination-in-chief
- Cross-examination
- Re-examination

7.2 Examination-in-chief

7.2.1 Book

- Steven Lubet, Modern Trial Advocacy and Practice

7.2.2 A persuasive trial story (allegations) consists of:

- Theory of the case (legal and logic); AND
- Theme of the case (moral).

7.2.3 A theory of the case:

- 3-sentence or 4-sentence summary that wraps up all the key elements:-
 - who did what to whom and why did they do it?
 - What was the result?
 - What are the legal and moral reasons that requires a decision in your favour?
 - What is your single most important item of data or information?
 - What is your best response to the other side's case?

7.2.4 Theme of the case:

- A word, phrase, or simple sentence that captures the controlling or dominant emotion and reality of the theory of the case:-

“One central theory that organizes all facts, reasons, arguments and furnishes the basic position from which one determines every action in the trial.” – Mario G. Conte

“coerced to confess”; “hard working mother knocked down by careless driver”

7.2.5 What is examination-in-chief

- A good examination-in-chief is like the director of a film crew

- Although limited by the script, the director can inject his own approach and perspective into the production
- Expert reports and witness statements are the script of the movie. Good script is easily produced into a good movie. Bad script needs good director.

7.2.6 Reasons for planning

“A witness may know only a portion of the entire story, may have poor memory, and even may contradict other witnesses.”

“Witnesses only testify in response to the questions you ask.”

“Requires clear, logically organized presentation.”

“Make the evidence persuasive and able to be remembered.”

“Judge must hear, understand and remember (like you watch a good movie).”

7.2.7 How

“Maintain chronological order.”

“Subdivide direct examination into smaller units.”

“Plan transitions between segments.”

“Elicit facts and details, not conclusions.”

“Select which topics to cover. The selection is based on your theory of the case.”

“Which issues you will pursue? What important themes and facts you will emphasize?”

“Which items of evidence will help the judge to resolve the issue?”

7.3 Questions type

- (so that you know what the lawyer is doing or not doing)
- Leading
- Open-ended
- Close-ended
- Compound

7.3.1 Leading question

- A leading question is one which suggests the desired answer to the witness so that it puts the desired answer in the witness's mouth, or is unclear as to whether the witness or the lawyer is testifying. Leading questions are generally forbidden on examination-in-chief and permitted on cross-examination.
- Leading: Are you going to New Zealand for the Chinese New Year?

7.3.2 Open-ended

- What do you plan to do during the Chinese New Year?
- What was the weather like on Monday?

7.3.3 Close-ended

- A closed question can usually be answered with a Yes or No.
- Are you going to South Africa for the Chinese New Year?

7.3.4 Compound

- Containing two separate inquiries that are not necessarily susceptible of a single answer
- A question that asks for 2 or more items of information at the same time, so that it is impossible to understand the meaning of the answer to the question
- Wasn't the fire engine driving in the left lane and flashing its lights?

8 *California v. David Alan Westerfield*

8.1 Introduction from Wikipedia

"On the Friday evening of February 1, 2002, Danielle's mother Brenda Van Dam and a couple of friends went out to a bar. Her husband Damon Van Dam stayed behind to look after their daughter Danielle and her two brothers. Damon put Danielle to bed around 10:30 p.m., and she fell asleep. Damon and Brenda went to sleep thinking that their daughter was safely sleeping in her room. About an hour later, Damon awoke and noticed that an alarm light was flashing. He found the sliding glass door leading to the back yard open, so he closed it. The next morning, Danielle was missing."

"David Westerfield has been charged with murder with special circumstances, kidnapping, and misdemeanor possession of child pornography. Before the police arrested him, they searched Westerfield's home several times and seized, among other items, thousands of computer-stored and video images of allegedly obscene matter."

"David Alan Westerfield, of San Diego, California, was convicted and sentenced

to death for the kidnapping and murder of seven-year-old Danielle Van Dam in 2002. He was a successful, self-employed engineer who owned a luxury motor home and lived two houses away from Van Dam. A divorced father of two college students, . . .”

“According to the prosecution computer expert, James Watkins, 100,000 images were found, including 8,000 to 10,000 nude images and 80 which could be considered child pornography. The material included brief movie clips found in Westerfield’s office which featured an underage girl being raped by one man while another man restrained her. These clips, including sound of the girl struggling, were played in the courtroom. In all, two sets of movie clips, six animated cartoons, and 13 still images taken from computers, zip disks, or CD-Roms in David Westerfield’s home were shown, each featuring underage girls.”

8.2 Testimony of James Watkins

- Examination-in-chief
- 25 June 2002 (Day 13)
- (Direct examination by Mr Clarke)

Q: Good afternoon, Mr. Watkins.

A: Good afternoon.

Q: Who are you employed by?

A: I’m employed by the San Diego Police Department.

Q: In what role?

A: I’m a computer forensic examiner, and I’m currently assigned to the Regional Computer Forensics Lab.

Q: Let’s start with a computer forensics examiner. What is that?

A: You have to excuse me. I’m getting over a cold right now. A computer forensic examiner or as a computer forensic examiner, my job is to examine computers for any sort of digital evidence, such as computer evidence, floppy disk, hard drives, and extract evidence off of them.

Q: All right. You also used the term I think Regional Computer Forensics Labora-

tory?

A: Yes.

Q: What is that?

A: The Regional Computer Forensics Laboratory or R.C.F.L. is a cooperative effort of all – about thirty-two law enforcement agencies here in Southern California. We have responsibilities for the investigation or the – I'm sorry – the analysis of computer evidence in both San Diego and Imperial Counties both for the state and for the federal agencies.

Q: How long has this laboratory been in existence?

A: Approximately three years now.

Q: Was this the first such laboratory in the United States?

A: Yes, it was.

Q: Could you describe - well, let me ask a different way. What are your duties as a computer forensics examiner as far as the R.C.F.L. is concerned and your work in San Diego and Imperial Counties?

A: Well, my duties are to – the one to go out to the field and seize computers that have been used in crimes or that are evidence in crimes. Also to go out and do what we call imaging. There are certain situations where we can't physically take the computer, where the court won't allow it or it's just impractical. We can go out into the field and make copies of the hard drives there on the scene and take those back to the laboratory with us. The other part is once back at the laboratory is the actual analysis of that evidence.

Q: All right. How long have you been with the R.C.F.L.?

A: Since actually before its inception. About three and a half years.

Q: Now, you have used the term hard drive. Perhaps we can define some of these terms as you use them. What is that?

A: A hard drive is a – it's a little metal case that's about three and a half inches by

about four inches. It's inside the computer, and it's actually the memory where all of the information is stored on the computer.

Q: So if I type a file upon a computer and I decide I want to save this so I can go back to it another day, is that the location that typically I would save such a file?

A: That is one of the locations, yes, sir.

Q: Could you describe for the jury, if you would, the education, training, and experience that you have that has led to your position as a computer forensics examiner.

A: Yes. I've been – I was assigned to the R.C.F.L.. The R.C.F.L.. is all of our examiners including myself are certified by the F.B.I. Laboratory in Washington, D. C. I received approximately eight hundred hours' worth of training just in computer forensics. . . .

A: . . . The training I've received has been from the Federal Bureau Of Investigation, the computer training unit in the F.B.I. Academy at Quantico, Virginia. I've received training from the Computer Analysis and Response Team out of Quantico. I received training from the National White Collar Crime Center, the Search Group up in Sacramento, the International Association of Computer Investigative Specialists. I've also received specific training in different software programs by Guidance Software, Access Data, as well as the program ILook. Again I'm certified by the F.B.I. I'm also certified by the International Association of Computer Investigative Specialists as a Computer Forensic Certified Examiner or C. F. C. E.

Q: I would now like to direct your attention to early february of this year, specifically february 4th, and ask if you were requested to take part in the investigation of the disappearance of Danielle van Dam.

A: Yes, I was.

Q: In particular were you asked to assist in the search of a residence?

A: Yes.

Q: what residence was that?

A: The residence located at 11995 on mountain pass in San Diego.

Q: Was that identified — I'm sorry.

A: In San Diego.

Q: Was that address identified to you as the residence of any particular individual?

A: It was.

Q: Who was that?

A: Mr. David Westerfield.

Q: What was your role to be in that search on that particular date?

A: I was requested to go to the scene and make copies of the hard drives of the computers there.

Q: You've defined what a hard drive is. How do you make a copy of a hard drive?

A: We have portable computers that we take with us. We'll set those up at the scene. We will remove the hard drives from the subject computers, hook those up to our computer, and make what's called a physical image, which is a — just an identical copy of all the data off the subject computer onto our computer.

Q: When you say you bring equipment with you, do you bring your own personal computers? what do you bring?

A: We bring — they are computers that we have built at the R. C. F. L. We call them field imaging kits. They look like an overgrown for want of a better term lunch box. It's totally self-contained, keyboard, monitor, but it's a fully-powered computer, not just like a laptop. With that device we can hook it up to any hard drive and go ahead and make our copy.

Q: You arrived at the residence on february 4th.

A: Yes, sir.

Q: Did you enter the residence?

A: Yes.

Q: What did you do once that happened?

A: I was directed to the — well, when we went in, I talked to sergeant holmes who directed us to the upstairs office.

Q: What did you do?

A: Took a — well, examined the office, saw that there were two computers inside the office area there. We set up a table and set up a couple of computers and then conducted the imaging process.

Q: Do you recall what date it was when you actually arrived at the residence?

A: It was the morning of the 5th.

Q: All right. was this — was it dark out?

A: Yes, it was.

Q: So this was after midnight on the 4th?

A: Yes.

Q: I would like to show you a board of photographs that's been previously marked exhibit 102. And if you would, Mr. Watkins, take a look at those photographs labeled A through J. Do you see those photographs?

A: Yes, I do.

Q: Okay. Do any of those photographs show something that you are familiar with from your entry of the residence on february 5th?

A: The first thing it points out are the computers that are visible in photograph A, G, and H.

Q: Do you recognize them?

A: Yes, I do.

Q: What are they?

A: Those are actually in — you can see in photograph A, you can see computer monitors and just below the desk the monitors are sitting on there are some computers or the central process units or C.P. units of the computers.

9 *Florida v. Casey Anthony*

9.1 Some digital evidence

- [some Digital forensic files](#)
 - Chloroform Searches from Casey Anthony HP Desktop Computer. (Allocated IE History)
 - Chloroform Searches from Casey Anthony HP Desktop Computer (Firefox unallocated space)
 - others

9.2 The story from Wikipedia

“Caylee Marie Anthony was a two-year-old . . . girl who lived . . . with her mother, Marie Anthony, and her maternal grandparents, George and Anthony. On July 15, 2008, she was reported missing to 9-1-1 by Cindy, who said she had not seen Caylee for 31 days and that Casey’s car smelled like a dead body had been inside it. Casey told detectives several falsehoods, including that the child had been kidnapped by a nanny on June 9, and that she had been trying to find her, too frightened to alert the authorities. . . .”.

“On December 11, 2008, Caylee’s skeletal remains were found with a blanket inside a trash bag in a wooded area near the family home. Investigative reports and trial testimony alternated between duct tape being found near the front of the skull and on the mouth of the skull. The medical examiner mentioned duct tape as one reason she ruled the death a homicide, but officially listed it as “death by undetermined means”. . . . The prosecution . . . alleged Casey murdered her daughter to free herself from parental responsibilities by administering chloroform and applying duct tape. The defense . . . countered that the child had drowned accidentally in the family’s swimming pool on June 16, 2008, and that George Anthony disposed of the body.”

9.3 The story from Goodison et al.

- Goodison, Davis and Jackson. [Digital Evidence and the US Criminal Justice System](#)

“. . . Anthony reported her two-year-old daughter, Caylee, missing in 2008. She claimed Caylee was last seen being dropped off with a babysitter, though she did not report the incident to police until over one month later. The State of Florida arrested Anthony on charges of child neglect, false statements, and obstruction. As the police investigation continued, physical evidence from Anthony’s car suggested potential homicide, which led to a grand jury indicting her on murder charges as well. Months after the indictment, Caylee’s remains were found in a wooded area near her home.”

“During trial, the state argued that digital evidence would prove Anthony searched for information on various homicide related issues (methods, techniques, etc.) on the day her daughter was last seen. Most such evidence focused on Internet browser searches. Digital investigators initially used software that later would be found highly inaccurate. Investigators testified that Anthony’s browser searched 84 times for “chloroform,” a chemical that had been found in her car trunk; however, the software designer later discovered serious faults in the program and subsequently testified that the term was only searched for once. This error likely contributed to the reasonable doubt jurors found when they acquitted Anthony of first-degree murder, especially since the correction occurred during trial.”

“Interestingly, further evidence came to light in the years after the trial to suggest more digital evidence mistakes that served to further weaken the case. Investigators used tools that only tapped into Microsoft’s Internet Explorer history. While technicians determined the computer was being used through a password-protected account of Anthony’s, thus strongly suggesting it was Anthony and not other family members using the computer, they missed that Anthony preferred Mozilla’s Firefox browser with their software; as result, investigators did not have information on more than 98 percent of the browser history records at trial, including a search for “foolproof suffocation”.”

9.4 The timeline

- June 16, 2008: 2-year-old Caylee Anthony is last seen alive leaving the home of her grandparents, George and Cindy Anthony, along with her mother, Casey.
- June 18, 2008: Casey Anthony borrows a shovel from Brian Burner, a neighbor of George and Cindy Anthony. Burner says that Anthony returned it an hour later.
- June 19, 2008: Casey Anthony goes with boyfriend Tony Lazzaro to help him look for an apartment.
- June 20, 2008: Casey Anthony is captured in various photos partying at Fusion nightclub and participating in a “hard body contest.”
- June 23, 2008: Casey Anthony and her boyfriend, Lazzaro, break into a shed at the Anthony family home to borrow her father’s gas cans to fill her car, which had run empty.
- June 24, 2008: Casey Anthony gets into a fight with George Anthony about the gas and

- she storms out of the home. She tells her father that Caylee is with the baby sitter, Zanny.
- June 25, 2008: Cell phone records show Casey Anthony was in the area of her parents' home.
 - June 28, 2008: Casey Anthony's car is towed from the parking lot of a check cashing store after a supervisor calls to report it abandoned.
 - June 30, 2008: Casey Anthony is captured in surveillance videos shopping at JC Penney and Target. July 1, 2008: Surveillance video shows Casey Anthony back in JC Penney buying more clothes.
 - July 10, 2008: Casey Anthony is recorded in surveillance video at Target.
 - July 12, 2008: Casey Anthony is seen in surveillance video at Winn-Dixie
 - July 15, 2008: Casey Anthony is recorded in Blockbuster Video, Bank of America and Winn-Dixie surveillance videos.
 - July 15, 2008: George and Cindy Anthony pick up Casey's car from a tow yard. George Anthony observes a strong odor emanating from the vehicle. Later, back at the Anthony family home, Casey tells her mother and brother, Lee Anthony, that she hasn't seen Caylee in a month and that a baby sitter named Zanaida Fernandez Gonzalez (Zanny) kidnapped her.
 - July 15-16, 2008: Casey Anthony takes police to the last place she says she saw Caylee. It turns out to be a vacant apartment. Authorities also take her to Universal Studios where she said she worked, but supervisors there say she hasn't worked there in more than two years.
 - July 16, 2008: Casey Anthony is arrested on charges of child neglect, making false official statements and obstructing a criminal investigation.
 - Aug. 21, 2008: Casey Anthony is released on \$500,000 bail and is ordered to wear an ankle monitoring bracelet while on house arrest awaiting trial.
 - Aug. 29, 2008: Casey Anthony is arrested on charges related to check fraud and theft for using a friend's checkbook without permission, allegations unrelated to Caylee.

9.5 The teams

- Prosecution:
 - Linda Drane Burdick, Frank George, Jeff Ashton
- Defence:
 - Jose Baez, J. Cheney Mason, Dorothy Clay Sims, Ann Finnell

9.6 The videos

- ["Crime and Punishment: Caylee the Untold Story"](#) (2 hours)
- CBS: ["Casey Anthony: Judgment Day"](#) (43 minutes)
- Dateline NBC: ["The Defence of Casey Anthony"](#) (43 minutes)

["Casey Anthony Trial: In a new book, defense attorney Jose Baez makes the case for his client's innocence"](#)

- Book: Presumed Guilty – Casey Anthony: The Inside Story (written by Jose Baez)

"He calls the media a "monster," the police "careless," and the prosecution "scheming, ruthless."'" ([news here](#))

- [Anthony spoke 10 years later](#)
- [Trial judge's theory of how the baby died 9 years later](#)
- [Casey Anthony Juror Speaks Out: 'Needed Something More Solid' for Conviction](#)
- [Casey Anthony Juror: 'Sick to Our Stomachs' Over Not Guilty Verdict](#)

— graphical images of the videos removed —

9.7 Three prosecution computer forensic experts

- Detective Sandra Osborne
- Detective Sergeant Kevin Stenger
- Mr John Bradley

9.8 Detective Sandra Osborne

- She explained the cell phone evidence and how she acquired the evidence by Cellebrite. She examined two computers used by Casey Anthony Osborne and found some internet searches performed by someone using the computer.

9.9 Detective Sergeant Kevin Stenger

- He also performed his own analysis of the two computers and discovered some internet searches potentially relevant to the murder case.
- Mr John Bradley
 - Mr Bradley is the author of Cacheback. Some forensic examiners used it to reconstruct internet browsing history. According to the testimony, Bradley was brought into this case because Detective Sergeant Stenger decided to use Cacheback to reconstruct the Firefox web browsing history from a computer system used by defendant Casey Anthony.
 - read [this paper](#), section 1.1 Answering the Right Questions about Mr Bradley' answers in court

9.10 Detective Sandra Osborne, Examination-in-chief

Q: "Please tell the members of the jury how you are employed."

A: "I'm employed as a computer examiner for the Orange County Sheriff's Office."

Q: "And how long have you worked for the Orange County Sheriff?"

A: I'm finishing up 21 years, this year.

Q: "What assignments have you had with that agency?"

A: I started out in patrol, from there I went into investigations, and crime scene investigations, from there I've been into sex crimes, child abuse, I did a short stint with homicide, and now I'm in computer crimes.

Q: "What sort of training and background do you have that qualifies for the position that you now hold at the Orange County Sheriff?"

A: I have a college business degree through Columbia College, I have over 700 hours of computer examiner forensic training specifically, and I hold two computer forensic examiner certifications.

Q: "What is involved in the certification process?"

A: The two certifications that I hold, the first one is through the 39 International Association of Computer Investigation [*sic*: Investigative] Specialists. For short we call that IASIS [spoken phonetically: EYE-AY-SIS]. The certification process for IASIS, the certification for IASIS involves a lengthy process, the first of which I attended a two week certification class, which involved a classroom setting. From there, once you successfully complete the two week class, I moved on to the peer review phase of the process, where I completed, successfully, a series of practical exam problems. From there, once that was successfully completed, I moved on to the 100 question practical knowledge exam, which I successfully completed.

Q: "What is it that they are asking you to do in the certification programs, specifically? I understand that you receive classroom instruction, and you take proficiency tests, but what is it that you are doing, that they are testing you on?"

A: What the testing is, especially through the peer review phase of the IASIS certification, what they're asking you to do is demonstrate proficiency with the computer forensic exam. They're asking that you, if you know the basics of computers, and basics of what an exam is for, where to locate things on a computer, how to report and document those findings accurately.

Q: "Do you also have a practical experience in this area, aside from the certifications that you hold?"

A: Yes, I do.

Q: "Explain that to us."

A: Practical, meaning on the job experience?

Q: "Absolutely."

A: Yes ma'am. In the last four years of my computer forensics experience with the Orange County Sheriff's Office, I've conducted several hundred exams over all kinds of digital evidence from, from anything from computers, to cell phones, to PDAs, iPhones, anything that contains, any electronic device that might contain a digital file.

Q: "Have you testified as an expert witness in court?"

A: I have.

Q: "Did that occur in Orange County, Florida?"

A: Yes.

Q: "And were you permitted to give opinions and explain issues that were surrounding computer forensics?"

A: Yes, I was.

Linda Drain BURDICK: "Your honor, at this point I would tender the witness for voir dire, or as an expert if there is no voir dire."

Jose Baez: "No objections."

THE COURT: "There being no objections, the witness will be accepted as an expert witness in the area of forensic computer analysis."

Q: "Do you have a title such as Detective? I want to make sure I'm going to call you the right name, Detective Osborne?"

A: Detective is fine.

Q: Detective Osbourne, as a result of your position, in the forensics unit with the Orange County Sheriff's office, did you receive several items of evidence in connection with the investigation into the disappearance of Caylee Marie Anthony?"

A: I did.

Q: Did the first item that was provided to you consist of a cell phone, purported to belong to Casey Marie Anthony?

A: Yes.

Q: I'll have you take a look at that and tell me if you recognize the exterior of that package as something that you've had contact with in the past?

A: I do.

Q: And how do you recognize it?

A: The label that's affixed to the front up here is filled out in my handwriting. And, I also resealed the evidence package once I was finished examining the item. When I resealed it back, those are my initials and that's the date that I sealed the package.

Q: "Did you indicate on the label, on the exterior, what is contained inside?"

A: "Yes, I did."

Q: "And what item did you place inside that package and ultimately seal?"

A: "This is a Nokia cell phone."

Q: "Your honor, I would seek to introduce HQ for identification into evidence."

Court: "What says the defense?"

Defence: "No objections."

Court: "It will be received in evidence as ..." (inaudible)

A: "Are there, and please correct me if I use the wrong terminology, are there forensic applications that can be utilized to retrieve information and data from a cell phone, such as the one that you received as belonging to Ms. Anthony."

A: "Yes, there are."

Q: "What, what processes are available?"

A: "The process I use most often, and the one that I used in this investigation, is a hardware tool called CELLEBRITE."

Q: "Is that one that is recognized as premier in the field? Able to give reliable data to an examiner, such as yourself?"

A: "It is."

9.11 An Interview with Sandra Osborne

- [Exclusive: An Interview with Sandra Osborne: Part I](#) in 2011
- [Exclusive: An Interview with Sandra Osborne Part II \(UnCut\)](#) in 2011

10 Epilogue

10.1 Summary

- An expert in *Shane Ragland*
- Expert report contents
- How a judge evaluates the expert evidence
- Disclosure
- Examination-in-chief of experts