

Bootleg CCE Slides

By Doug White, PHD, CCE, CISSP



Slides

- These slides are additional material provided by Secure Technology.
- Slides are available at whitehatresearch.com



Case Writing Strategy

- Case Writing Style
 - Cases need to make your point as quickly as possible (note this is not defined).
 - I recommend a Summation followed by the details.
 - The website (KCStoolbelt) has other examples that are more law enforcement oriented.



Case Writing Strategy

- Key sections
 - Summation – This contains solid statements which
 - Answer direct questions – Did this person send email X?
 - Provide Major evidence – 6,478 known child porn images
 - Conclusions drawn directly from evidence
 - Table of Contents
 - Key sections



Case Writing Strategy

- Key Sections, cont.
 - Analysis
 - Contains grim details of all findings.
 - Don't hesitate to include anything and everything relevant.
 - This would include filenames, dates, times, hashes, screenshots
 - This section may also include details of techniques if they are **directly** related to the case.



Case Writing Strategy

- Key Sections, cont.
 - Appendix A: Glossary – This should contain definitions of two things.
 - Anything you think your average 12 year old doesn't understand
 - Any complex explanations you need to provide – say like how a hash works. Simplify these down to something you completely are comfortable with and that can be understood by anyone.



Case Writing Strategy

- Key Sections, cont.
 - Appendix B - ? – These are explanations of techniques beyond the glossary.
 - Hashes
 - Disk Formatting
 - Undeletes
 - Anything that is relevant that you used.
 - DON'T CUT AND PASTE. Use your own descriptions.



Case Writing Strategy

- Key Sections, cont.
 - Appendix: Supplemental
 - Company policies on
 - Sterile Media
 - Evidence Storage and Chain of Custody
 - Software Licensing Policy
 - Privacy Policy
 - Evidence Return Policy (what happens after the trial).
 - Evidence/Case Number Policy
 - Appendix: Supplemental
 - CV of examiners on case. Include your CCE #
 - Include any other Daubert Credentials



Case Writing Strategy

- Appendix Supplemental
 - Logs from case
 - Chain of Custody Document
 - Consent to Image
 - Listing of all files
 - Consent to Image
 - Consent to Analyze



Case Writing Tactics

- <http://cisweb.rwu.edu/dwhite/rwclasses/cjs528/Files/philstips.pdf>
- Phil Harrold, A CCE and longtime Examiner of CCEs wrote this set of tips.



Case Writing Tactics

- Section recommendation
 - S == Summation; A == Analysis; P == Appendix; L == Log; O == Policy
- Describe any and all media and include a picture of that media (A)
- Color, size, labels, serial number, any other descriptive (A)
- Establish that a physical Chain of Custody was established (L, A, S, P, O)



Case Writing Tactics

- Who gave it to you (A)
- Receipt for the media (L, P)
- That it was securely stored (L, P, O)
- Provenance
 - How did you get it (L, A)
 - Was it in a computer (L, A)
 - Did you remove it (L, A)



Case Writing Tactics

- Provenance (cont.)
 - How was it delivered
 - Hand delivery (receipts tracking L, A)
 - Mail Shipping (tracking, L, A)
- How was the media protected (L, A, O)
 - Use of Antistatic bags
- Document write protection and validation of write protection (L, A, O)
- Validate the write protection of machines (L, O)



Case Writing Tactics

- Hash original media (L, A)
- Target media was wiped and formatted (L, A, O)
- Image using write blocking (L, A, O)
- Hash image (L, A)
- Perform examination on image (L)
- Note all volume attributes (A)
 - Name of volume
 - Date of format
 - OS/Filesystem



Case Writing Tactics

- Note all partitions on Media (A)
- Analyze media partition by partition and file by file (A)
- Note all active and deleted files on the media (A)
- Note path or location of files on media (A)
- Indicate if the file was deleted or not viewable for some reason (A)



Case Writing Tactics

- Recover any documents and note content (A)
- Recover and Note Passwords (A, P (method))
- Analyze document metadata (A, P (method))
- Analyze internet activity (A, P (methods))
 - Browsing history
 - Temp internet files
 - Uploads and downloads
 - Cookies
 - Webpage source



Case Writing Tactics

- Note any unusual software (A, P) – Profiling
 - E.g. SSH clients, FTP clients, CISCO VPNs etc.
- Analyze peer to peer of any other connections (A, P)
- Trace ownership of websites or domains found (A, P)
- Note any software used (A)
- Note any attempts to conceal or destroy information (A)
 - Include notes about shredders, encryption, et. al.



Case Writing Tactics

- Examine Slack/Unallocated space (A)
- Use Data Carving on Slack and unallocated (A, P)
- Document all procedures and steps (P, L)
- Draw conclusions about any files that appear relevant (S)
- Draw conclusions about any files that appear related (S)



Case Writing Tactics

- PROOFREAD
- SPELLCHECK
- GRAMMARCHECK
- Level Check?



Case Writing Implementation

- Policies and Guidelines
 - Checklists
- Log
- Analysis
 - Glossary
 - Appendices
- Summation
- Review and Editing



Case Presentation

- Web enabled
- Traditional
- Things to AVOID
 - *Weird fonts, Weirder Fonts, Weirdest Fonts*
 - Weird paper, formats, etc.



Notes about techniques

- If you do something no one else does be prepared to explain it in intimate detail
 - Example – Instead of MD5 hash you use a Panama Hash
 - This is a good thing to fully document in an appendix.



Notes about Images

- You often receive images made by someone else.
- Two big formats that are used are:
 - Dd – old Unix format from the dd command.
 - Most versatile and my recommendation
 - ENN (E01) – Encase format. Originally only encase supported by Access data uses this as well as do others. Lawsuits tried to prevent use.



Dealing with Images

- Document receipt
- Document condition and add numbers.
- Document handling in the log
- Hash the image and compare to provided hashes
- Duplicate the image and hash the duplicate.
- Note the hash matches in your log notes.
- Always work from the copy. If you need another copy, make one.



FTK

- Using FTK to build a case demonstration.

C Six months ago, Danny Hampton, a teenager at Evergreen High School contacted a music store in Denver, CO regarding the sale of a guitar which was claimed to have belonged to T-Bone McKee. The music store was already aware of the theft of two guitars from Mr. McKee named Esmeralda and Gwendolyn. The music store asked the caller for his telephone number and he hung up. The music store then called the police.

Police went to Mr. Hampton's parent's home in Evergreen and asked the parents about the guitars and were told that their son played the guitar but would never steal anything. When the police asked if they might examine Mr. Hampton's computer, the father consented to the examination in writing. The computer appeared to have no operating system installed and upon investigation it was found the hard drive was missing. D. Hampton then denied anything and said that the hard drive had gone bad months ago and he didn't want to tell his dad.

While looking around, the officer saw a USB key beside the trash bin in the back of the house and was told he could take that for examination by D. Hampton's dad.

You have been retained by the Evergreen Police Department to examine the image of the USB key. The objective is to develop evidence that Mr. Danny Hampton had any knowledge of the two stolen guitars and to develop any other evidence which may prove valuable.

The guitar pictures which were provided by Mr. McKee are as follows:



Both of these are currently listed as stolen by Mr. McKee.



For Hampton

- Take the next 2 hours and prep your analysis
- Then we discuss
- Then you should write your summation.

Case II

Karen Vandergriff

Karen Vandergriff works for her uncle Ned, at his bakery (which is a giant bakery that supplies bread to most of Southern Michigan). Karen, who also goes by the name Kim, brought a USB key to an attorney on the day after her Uncle's death from cancer. She claimed she found it in his desk and looked at it on her computer and found that it had a will on the disk. She claimed she had not looked at the file and brought it to the attorney since it might be important. She and the family live in Ypsilanti, MI.

Attorney Konroy stated in his report "This contains a will but it has a funny feeling to it and Karen Vandergriff was acting strangely when she brought it to me, nervous, that kind of thing."

A week after the death (4-Mar-08), the nephew, Kyle Rollins, contacted YPD with a complaint and indicated that the accounting records of the company showed large numbers of withdrawals for "MISC" in amounts of 500, 1000, 5000 over the past several years. These were approved by Ms. Vandergriff. When she was asked about this by a detective, she acted very strange and said she thought she needed an attorney. Investigators received a warrant for her apartment and found that she was not present and could not be contacted. The officer heard her cell phone ringing inside the apartment when the number was dialed and determined she might be in danger so forced the door open. She was not there and her clothes, belongings, and other material were gone. Currently, her whereabouts are unknown.

You have been retained to work on this case. So far the evidence consists of a single image of a USB key (the one she surrendered). Examine the evidence and see if any information which might assist in the investigation can be obtained. The image was provided to you personally by Officer Molo, the detective in charge.



For Vandergriffe

- Develop the case.