

Guide to Computer Forensics and Investigations Sixth Edition

Chapter 16

Ethics for the Expert Witness





Objectives

- Explain how ethics and codes apply to expert witnesses
- Explain how other organizations' codes of ethics apply to expert testimony
- Describe ethical difficulties in expert testimony
- Explain the process of carving data manually



Applying Ethics and Codes to Expert Witnesses (1 of 3)

- **Ethics**

- Rules you internalize and use to measure your performance

- **Codes of professional conduct or responsibility**

- Standards that others apply to you or that you are compelled to adhere to by external forces
 - Such as licensing bodies
- People need ethics to help maintain their balance
 - And self-respect and the respect of their profession



Applying Ethics and Codes to Expert Witnesses (2 of 3)

- Laws governing codes of professional conduct or responsibility
 - Define the lowest level of action or performance required to avoid liability
- Expert witnesses should present unbiased, specialized, and technical evidence to a jury
 - Control your biases, do not allow them to control you
- Expert witnesses testify in more than 80% of trials
 - And in many trials, multiple expert witnesses testify



Applying Ethics and Codes to Expert Witnesses (3 of 3)

- The most important laws applying to attorneys and witnesses are the rules of evidence
- Experts are bound by their personal ethics and the ethics of their professional organizations
- In the United States, there's no state or national licensing body for digital forensics examiners
 - Your sources for ethical standards are your internal values and codes of professional associations you belong to



Forensics Examiners' Roles in Testifying

- Digital forensics examiners have two roles:
 - Fact witness and expert witness
- As an expert witness
 - You can testify even if you weren't present when the event occurred
 - Or didn't handle the data storage device personally
- Criticism: it's possible to find and hire an expert to testify to almost any opinion on any topic
 - Beware of attorneys' opinion shopping



Considerations in Disqualification (1 of 4)

- One of the effects of violating court rules or laws is **disqualification**
- Opposing counsel might attempt to disqualify you
 - Based on any deviations from opinions you've given in previous cases
- Some attorneys contact many experts as a ploy to disqualify them
 - Or prevent opposing counsel from hiring them
- Determine who the parties are to reduce the possibility of a conflict



Considerations in Disqualification (2 of 4)

- Whenever you are aware of a possible disqualification issue
 - Bring it to the attention of the attorney who has retained you
- Factors to disqualify an expert include:
 - Whether the attorney informed the expert that their discussions were confidential
 - Whether the expert reviewed materials marked as confidential or attorney work product
 - Whether the expert was asked to sign a confidentiality agreement



Considerations in Disqualification (3 of 4)

- Factors to disqualify an expert include: (cont'd)
 - Number of discussions held over a period of time
 - The type of documents that were reviewed
 - The type of information conveyed to the expert
 - The amount of time involved in discussions or meetings between the expert and attorney
 - Whether the expert provided the attorney with confidential information
 - Whether the attorney formally retained the expert



Considerations in Disqualification (4 of 4)

- Factors to disqualify an expert include: (cont'd)
 - Whether the expert voiced concerns about being retained
 - Whether the expert was requested to perform services for the attorney
 - Whether the attorney compensated the expert



Traps for Unwary Experts (1 of 3)

- Be cautious about the following potential traps
 - What are some differences between the attorney's motives and the investigator's duty?
 - Is the function of the expert witness in conflict with the investigator's code of professional responsibility?
 - You should anticipate that the opposing counsel will look at your organization memberships and those organizations' codes of professional responsibility
- **Contingency fees** aren't allowed except in certain limited circumstances



Traps for Unwary Experts (2 of 3)

- Avoid obvious ethical errors
 - Don't alter data or present false data
 - Don't report work that was not done
 - Don't ignore available contradictory data
 - Don't do work beyond your expertise or competence
 - Don't allow the attorney who retained you to influence your opinion in an unauthorized way



Traps for Unwary Experts (3 of 3)

- Avoid obvious ethical errors (cont'd)
 - Don't accept an assignment if it cannot be done reasonably in the allowed time
 - Don't reach a conclusion before doing complete research
 - Don't fail to report possible conflicts of interest



Determining Admissibility of Evidence

- Hypothetical questions can give you the factual structure to support and defend your opinion
- Although expert opinions can be presented without stating the underlying factual basis
 - The testimony isn't admissible if the facts on which the opinion is based are inadequate
 - Or there's not enough evidence to allow stating a legitimate opinion



Organizations with Codes of Ethics

- No single source offers a definitive code of ethics for expert witnesses
- You must draw on standards from other organizations to form your own ethical standards
- Many organizations have rules to guide their members in areas such as:
 - Interaction with patients/clients, objectivity, role in society, fees, solicitation, independence, and contractual relationships



International Society of Forensic Computer Examiners (1 of 2)

- ISFCE includes guidelines such as the following:
 - Maintain the utmost objectivity in all forensic examinations and present findings accurately
 - Conduct examinations based on established, validated principles
 - Testify truthfully in all matters before any board, court, or proceeding
 - Avoid any action that would appear to be a conflict of interest



International Society of Forensic Computer Examiners (2 of 2)

- ISFCE includes guidelines such as the following: (cont'd)
 - Never misrepresent training, credentials, or association membership
 - Never reveal any confidential matters or knowledge learned in an examination without an order from a court of competent jurisdiction or the client's express permission



International High Technology Crime Investigation Association

- HTCIA core values include the following requirements related to testifying:
 - The HTCIA values the Truth uncovered within digital information and the effective techniques used to uncover that Truth, so that no one is wrongfully convicted
 - The HTCIA values the Integrity of its members and the evidence they expose through common investigative and digital forensics best practices, including specialized techniques used to gather digital evidence



International Association of Computer Investigative Specialists

- Standards for IACIS members include:
 - Maintain the highest level of objectivity in all forensic examinations and accurately present the facts involved
 - Thoroughly examine and analyze the evidence
 - Conduct examinations based on established, validated principles
 - Render opinions having a basis that is demonstratively reasonable
 - Not withhold any findings that would cause the facts of a case to be misrepresented or distorted



American Bar Association

- Be aware of the basic rules of professional conduct attorneys must follow
- ABA's Model Code of Professional Responsibility (Model Code) and its successor, the Model Rules of Professional Conduct (Model Rules)
 - Are the basis of state licensing bodies' codes
- The ABA has stated that expert witnesses do not owe a duty of loyalty to their clients



American Psychological Association

- For psychologists, the broadly accepted guidelines governing their conduct as experts are:
 - The American Psychological Association's (APA's) Ethical Principles of Psychologists and Code of Conduct
 - Commonly referred to as "Ethics Code"
- These guidelines offer comprehensive regulations
 - With an entire section devoted to forensics activities



Ethical Difficulties in Expert Testimony (1 of 2)

- There are inherent conflicts between the goals of attorneys
 - And the goals of scientists or technicians (experts)
- Attorneys work in an adversarial system and look to sway the judge or jury
- Science requires experts to focus on the evidence without the influence of others' objectives
- *Daubert* and the APA's forensics guidelines
 - Can challenge experts to choose between complete impartiality and responsible advocacy



Ethical Difficulties in Expert Testimony (2 of 2)

- Enforcing any professional organization's ethical guidelines is difficult
 - Principles can be enforced only against members of the organization
- All guidelines rely primarily on internalization of the codes and witnesses' analysis of when and how they will participate in a case
- Available guidelines set only a minimum level of acceptable performance or competence as the standard



Ethical Responsibilities Owed to You (1 of 2)

- Your attorney owes you
 - A fair statement of the case or situation
 - Adequate time to review evidence and prepare your report
 - A reasonable opportunity to examine data, conduct testing, and investigate the matter before rendering an opinion
- Most attorneys, including opposing counsel, are competent, courteous professionals



Ethical Responsibilities Owed to You (2 of 2)

- Some opposing counsel attempt to make discovery depositions physically uncomfortable
 - After noting a problem, you can refuse to continue with the deposition
- As a measure of protection, you might want to have your personal attorney attend the deposition
 - This attorney can't object to questions but is available to advise the attorney who retained you or to advise you during breaks



Standard and Personally Created Forensics Tools

- The tools you use to recover, control, and track evidence are subject to review by opposing parties
 - If the court deems them unreliable, the evidence you recovered with those tools might not be admitted
 - Or might be admitted with a limiting instruction
- If you use standard tools, you simplify the process of validating them
- Personally created tools might have advantages that you can demonstrate to a judge
 - Who determines whether evidence is admissible



An Ethics Exercise

- By following the activities at the end of the chapter, you will be:
 - Performing a cursory exam of a Forensic Image
 - Performing a Detailed Exam of a Forensic Image
 - Performing the Exam
 - Interpreting Attribute 0x80 Data Runs
 - Finding Attribute 0x80 an MFT Record
 - Configuring Data Interpreter Options in WinHex
 - Calculating Data Runs
 - Carving Data Run Clusters Manually



Performing a Cursory Exam of a Forensic Image

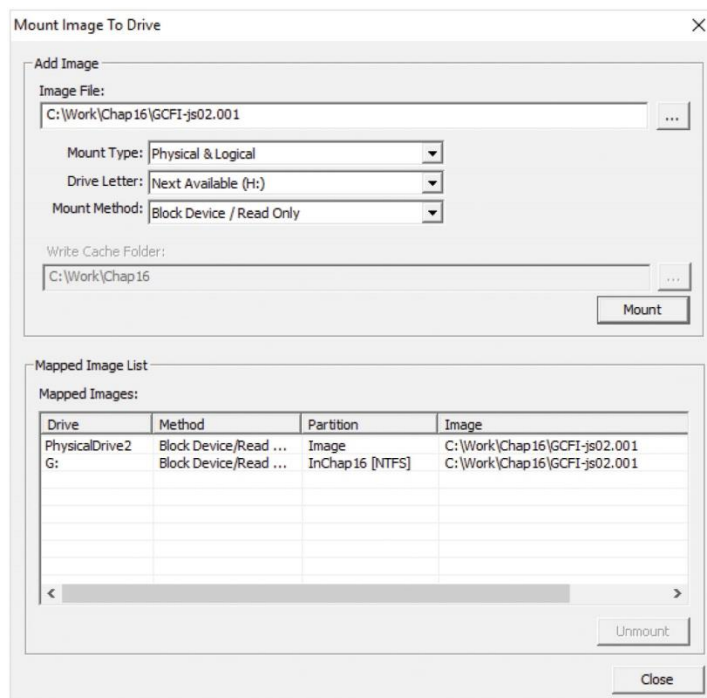


Figure 16-1 The Mount Image To Drive dialog box

Source: AccessData Group, Inc., www.accessdata.com



Performing a Detailed Exam of a Forensic Image

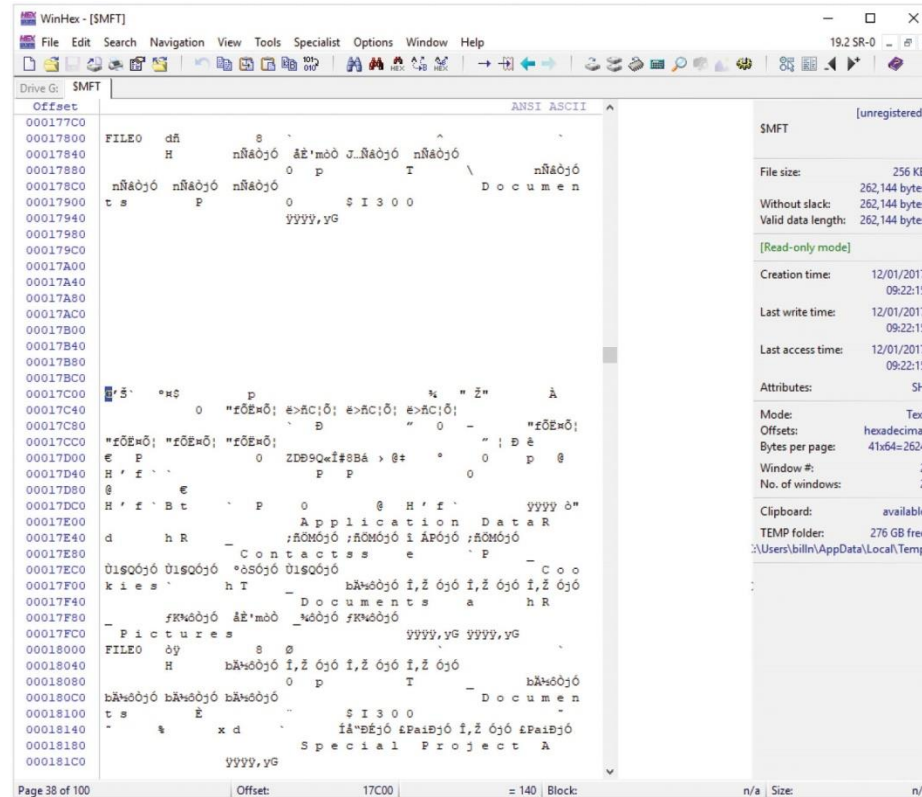


Figure 16-5 Finding a corrupt record in the \$MFT file

Source: X-Ways AG, www.x-ways.net



Performing the Exam

- To maintain the highest possible ethical standards when conducting a forensics examination
 - You should develop a plan and review it before starting your analysis
- Preparing for an Examination
 - Planning stage should cover all possibilities, including giving an opinion of whether data was corrupted intentionally or unintentionally



Interpreting Attribute 0x80 Data Runs

Bytes for the record header from position 0x00 to 0x37

WinHex - [SMFT]

File Edit Search Navigation View Tools Specialist Options Window Help

19.2 SR-0

Drive G: SMFT

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000BC00	46	49	4C	45	30	00	03	00	59	A3	11	00	00	00	00	00
0000BC10	02	00	01	00	38	00	01	00	60	01	00	00	00	04	00	00
0000BC20	00	00	00	00	00	00	00	00	04	00	00	00	2F	00	00	00
0000BC30	04	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00
0000BC40	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00
0000BC50	55	68	39	F0	CE	6A	D3	01	23	5D	40	59	C1	6A	D3	01
0000BC60	72	DF	3E	5C	D0	6A	D3	01	55	68	39	F0	CE	6A	D3	01
0000BC70	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000BC80	00	00	00	00	0C	01	00	00	00	00	00	00	00	00	00	00
0000BC90	00	00	00	00	00	00	00	00	30	00	00	00	78	00	00	00
0000BCA0	00	00	00	00	00	03	00	00	5E	00	00	00	18	00	01	00
0000BCB0	36	00	00	00	00	00	01	00	55	68	39	F0	CE	6A	D3	01
0000BCC0	23	5D	40	59	C1	6A	D3	01	23	5D	40	59	C1	6A	D3	01
0000BCD0	55	68	39	F0	CE	6A	D3	01	00	B0	00	00	00	00	00	00
0000BCE0	21	A1	00	00	00	00	00	00	20	00	00	00	00	00	00	00
0000BCF0	0E	00	4B	00	61	00	79	00	61	00	6B	00	34	00	20	00
0000BD00	28	00	31	00	29	00	2E	00	4A	00	50	00	47	00	00	00
0000BD10	80	00	00	00	48	00	00	00	01	00	00	00	00	00	01	00
0000BD20	00	00	00	00	00	00	00	00	0A	00	00	00	00	00	00	00
0000BD30	40	00	00	00	00	00	00	00	00	B0	00	00	00	00	00	00
0000BD40	21	A1	00	00	00	00	00	00	21	A1	00	00	00	00	00	00
0000BD50	21	0B	B3	00	00	00	00	00	FF	FF	FF	FF	82	79	47	11
0000BD60	FF	FF	FF	FF	12	79	47	11	00	00	00	00	00	00	00	00
0000BD70	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000BD80	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000BD90	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000BDA0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000BDB0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000BDC0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000BDD0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000BDE0	00	00	70	00	00	00	00	00	00	00	00	00	00	00	00	00

Page 98 of 529

Offset: BC37 = 0 Block: BC00 - BC37 Size: 38

Starting position of attribute 0x10

Offset counter displayed in hexadecimal mode

Figure 16-12 Selecting an MFT record header

Source: X-Ways AG, www.x-ways.net



Carving Data Run Clusters Manually

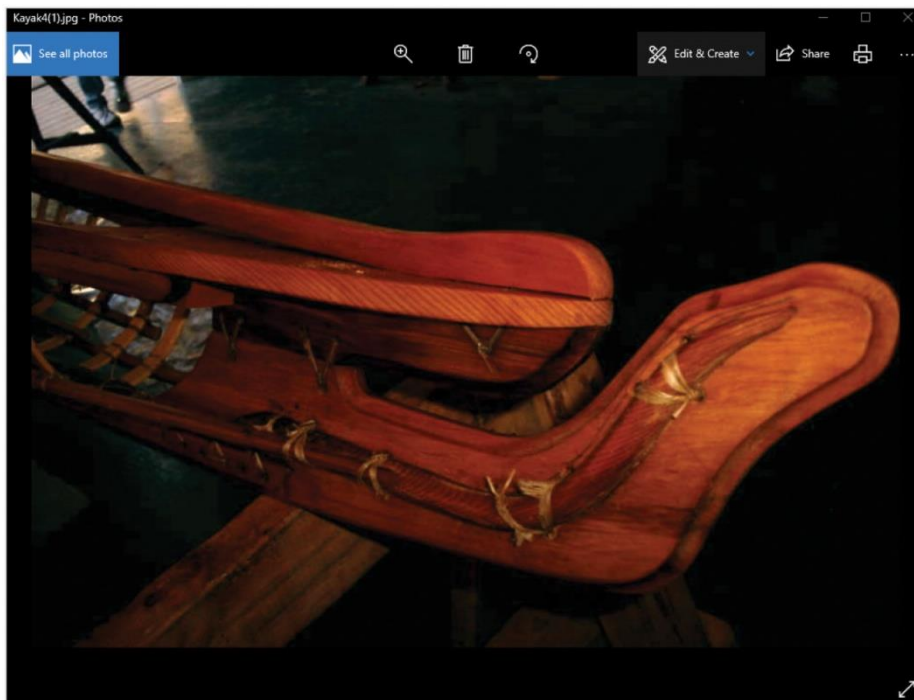


Figure 16-22 The recovered `Kayak4 (1) .jpg` file



Summary (1 of 3)

- Ethics can be defined as rules you internalize and use to measure your performance
- Digital forensics examiners don't have the same formal codes of conduct that professions such as medicine and the law have
- You owe your client a full understanding of the facts relevant to your opinion
- Be aware of attempts to disqualify you as an expert
- Courts use many factors in determining whether to disqualify an expert



Summary (2 of 3)

- Be aware of obvious ethical errors, such as:
 - Ignoring contradictory data
 - Performing work beyond your expertise
 - Allowing attorneys to influence your opinion
 - Reaching a conclusion before completing research
- No single source offers a definitive code of ethics for expert witnesses
- The ISFCE Code of Ethics provides guidelines for its members and the IACIS has a guide for expected behavior of forensics examiners



Summary (3 of 3)

- The inherent conflict between the needs of the justice system and your obligations for professional conduct can create ethical difficulties
- The attorney who has retained you, opposing counsel, and the court owe you ethical responsibilities as an expert witness
- The tools you use to recover, control, and track evidence are subject to review by opposing parties
- After carving data artifacts, analyzing as much of the information as possible is critical