Guide to Computer Forensics and Investigations Sixth Edition

Chapter 15

Expert Testimony in Digital Investigations

Objectives

- Explain guidelines for giving testimony as a fact witness or an expert witness
- Describe guidelines for testifying in court
- Explain guidelines for testifying in depositions and hearings
- Describe procedures for preparing forensics evidence for testimony

Preparing for Testimony (1 of 4)

- **Fact witness**
  - Provides facts found in investigation
  - Explain what evidence is and how it was obtained
  - Does not offer conclusions, only facts
- **Expert witness**
  - Has opinions based on observations
  - Opinions are formed from experience and deductive reasoning
  - Opinions make the witness an expert

Preparing for Testimony (2 of 4)

- For either types of testimony:
  - Establish communication early with attorney
  - Learn about the victim, the complainant, opposing experts or fact witnesses, and the opposing attorney
  - Learn the basic points of dispute
  - Keep notes in rough draft form and record only facts
    - Keep opinions to a minimum

Preparing for Testimony (3 of 4)

- Confirm your findings with documentation
  - Corroborate them with other peers
- Digital forensics is only now developing a peer review process
- Check opposing experts to find strengths and weaknesses
  - Internet
  - Curriculum vitae
  - Deposition banks

Preparing for Testimony (4 of 4)

- When preparing your testimony consider the following questions:
  - What is the client's overall theory of the case?
  - What is my story of the case?
  - What can I say with confidence?
  - How does my opinion fit into the theory of the case?
  - What is the scope of the case? Have I gone too far?
  - Have I identified the client's needs for how my testimony fits into the overall theory of the case?

Documenting and Preparing Evidence (1 of 3)

- Document your steps
  - To prove them repeatable
- Validate your tools and verify evidence with hash algorithms to ensure integrity
- Do not use a formal checklist
  - Do not include checklist in final report
  - Opposing attorneys can challenge them
- Collect evidence and document employed tools
- Maintain chain of custody

Documenting and Preparing Evidence (2 of 3)

- Collect the right amount of information
  - Collect only what was asked for
- Note the date and time of your forensic workstation when starting your analysis
- Keep only successful output
  - Do not keep previous runs
- Search for keywords using well-defined parameters

Documenting and Preparing Evidence (3 of 3)

- Keep your notes simple
- List only relevant evidence on your report
- Define any procedures you use to conduct your analysis as scientific
  - And conforming to your profession's standards
  - List any textbooks, technical books, articles by recognized experts, and procedures from authoritative organizations that you relied on or referenced during examination

Reviewing Your Role as a Consulting Expert or an Expert Witness

- Do not record conversations or telephone calls
- Federal information requirements
  - Other cases in which you have testified as an expert witness in the last four years
  - Ten years of any published writings
  - Previous compensations for testifying
- Evaluate the court's expert
- Brief your attorney on your findings and opinion of the court's expert

Creating and Maintaining Your CV

- **Curriculum vitae (CV)**
  - Lists your education, training, and professional experience
  - Used to qualify your testimony
- Show you continuously enhance your skills
  - List any training, teaching, and experience
- Detail specific accomplishments
- List basic and advanced skills
- Include a testimony log

Preparing Technical Definitions (1 of 2)

- Prepare definitions of technical concepts
- Use your own words and language
- Examples of definitions to prepare ahead of time:
  - Digital forensics or computer forensics
  - Hashing algorithms
  - Image files and bit-stream copies
  - File slack and unallocated space
  - File timestamps
  - Computer log files

Preparing Technical Definitions (2 of 2)

- Examples of definitions to prepare ahead of time (cont'd)
  - Folder or directory
  - Hardware
  - Software
  - Operating system

Preparing to Deal with the News Media

- Some legal actions generate interest from the news media
- Reasons to avoid contact with news media
  - Your comments could harm the case and create a record that can be used against you
  - You have no control over the context of the information a journalist publishes
  - You can't rely on a journalist's promises of confidentiality

Testifying in Court

- Procedures during a trial
  - Your attorney presents you as a competent expert
  - Opposing attorney might attempt to discredit you
  - Your attorney guides you through your testimony
  - Opposing attorney cross-examines you
  - Your attorney might have an opportunity for redirect examination of material addressed in cross-examination
- You could be called later as a rebuttal witness

Understanding the Trial Process

- Typical order of trial
  - Motion in limine
  - Impaneling the jury
  - Opening statements
  - Plaintiff
  - Defense
  - Rebuttal
  - Closing arguments
  - Jury instructions

Providing Qualifications for Your Testimony

- Demonstrates you are an expert witness
  - This qualification is called **voir dire**
- Attorney asks the court to accept you as an expert on digital forensics
- Opposing attorney might try to disqualify you
  - Depends on your CV and experience

General Guidelines on Testifying (1 of 9)

- Be professional and polite
- Be conscious of the jury, judge, and attorneys
- If asked something you cannot answer, say:
  - That is beyond the scope of my expertise
  - I was not asked to investigate that
- Avoid overstating opinions
- Guidelines on delivery and presentation:
  - Always acknowledge the jury and direct your testimony to them

General Guidelines on Testifying (2 of 9)

- Guidelines on delivery and presentation: (cont'd)
  - Movement
    - Turn towards the questioner when asked
    - Turn back to the jury when answering
  - Place microphone six to eight inches from you
  - Use simple, direct language to help the jury understand you
  - Avoid humor
  - Build repetition into your explanations

General Guidelines on Testifying (3 of 9)

- Guidelines on delivery and presentation: (cont'd)
  - Use chronological order to describe events
  - If you're using technical terms, identify and define these terms for the jury
  - Cite the source of the evidence the opinion is based on
  - Make sure the chair's height is comfortable, and turn the chair so that it faces the jury

General Guidelines on Testifying (4 of 9)

- Guidelines on delivery and presentation: (cont'd)
  - Dress in a manner that conforms to the community's dress code
  - Don't memorize your testimony
  - For direct examination
    - State your opinions
    - Identify evidence to support your opinion
    - Explain the method used to arrive to that opinion
    - Restate your opinion

General Guidelines on Testifying (5 of 9)

- Prepare your testimony with the attorney who hired you
  - How is data (or evidence) stored on a hard drive?
  - What is an image or a bit-stream copy of a drive?
  - How is deleted data recovered from a drive?
  - What are Windows temporary files, and how do they relate to data or evidence?
  - What are system or network log files?

General Guidelines on Testifying (6 of 9)

- Using graphics during testimony
  - Graphical exhibits illustrate and clarify your findings
  - Your exhibits must be clear and easy to understand
  - Graphics should be big, bold, and simple
  - The goal of using graphics is to provide information the jury needs to know
  - Review all graphics with your attorney before trial
  - Make sure the jury can see your graphics, and face the jury during your presentation

General Guidelines on Testifying (7 of 9)

- Avoiding testimony problems
  - Recognize when conflict-of-interest issues apply to your case
    - **Conflicting out**: an attempt by opposing attorneys to prevent you from serving on an important case
  - Avoid agreeing to review a case unless you're under contract with that person
  - Avoid conversations with opposing attorneys
  - You should receive payment before testifying

General Guidelines on Testifying (8 of 9)

- Avoiding testimony problems (cont'd)
  - Don't talk to anyone during court recess
    - If a juror approaches you, decline to talk with him or her and promptly report the contact to the attorney who retained you
  - Make sure you conduct any conferences with your attorney in a private setting

General Guidelines on Testifying (9 of 9)

- Understanding prosecutorial misconduct
  - If you have found exculpatory evidence, you have an obligation to ensure that the evidence isn't concealed
  - Initially, you should report the evidence to the prosecutor handling the case
    - Be sure you document the communication
  - If this information isn't disclosed to the defense attorney in a reasonable time
    - You can report it to the prosecutor's supervisor or the judge

Testifying During Direct Examination (1 of 2)

- Techniques
  - Work with your attorney to get the right language
  - Be wary of your inclination to be helpful
  - Review the examination plan your attorney has prepared
  - Provide a clear overview of your findings
  - Use a systematic easy-to-follow plan for describing your methods
  - Practice testifying
  - Use your own words when answering questions

Testifying During Direct Examination (2 of 2)

- Techniques (cont'd)
  - Make sure you know the following terms before giving testimony:
    - Independent recollection
    - Customary practice
    - Documentation of the case
  - Present your background and qualifications
  - Avoid vagueness
  - When you're using graphics in a presentation, make sure the jury understands your explanations

Testifying During Cross-Examination (1 of 4)

- Recommendations and practices
  - Use your own words
  - Keep in mind that certain words have additional meanings
  - Be aware of leading questions
  - Never guess when you do not have an answer

Testifying During Cross-Examination (2 of 4)

- Recommendations and practices (cont'd)
  - Be prepared for challenging, pre-constructed questions
    - Did you use more than one tool?
  - Rapid-fire questions
  - Sometimes opposing attorneys declare that you aren't answering the questions
  - Keep eye contact with the jury
  - Sometimes opposing attorneys ask several questions inside one question

Testifying During Cross-Examination (3 of 4)

- Recommendations and practices (cont'd)
  - Attorneys make speeches and phrase them as questions
  - Attorneys might put words in your mouth
  - Be patient
  - Most jurisdictions now allow the judge and jurors to ask questions
  - Avoid feeling stressed and losing control
  - Never have unrealistically high self-expectations when testifying; everyone makes mistakes

Testifying During Cross-Examination (4 of 4)

- Avoid:
  - Being argumentative when being badgered by the opposing attorney
  - Having poor listening skills or using defensive body language
  - Being too talkative or talking too fast
  - Being too technical for the jury to understand
  - Acting surprised and unprepared to respond when presented with unknown or new information

Preparing for a Deposition or Hearing

- **Deposition** differs from trial testimony
  - There is no jury or judge
- Opposing attorney previews your testimony at trial
- **Discovery deposition**
  - Part of the discovery process for a trial
- **Testimony preservation deposition**
  - Requested by your client
  - Preserve your testimony in case of schedule conflicts or health problems

Guidelines for Testifying at Depositions (1 of 4)

- Some recommendations
  - Stay calm, relaxed, and confident
  - Maintain a professional demeanor
  - Use name of attorneys when answering
  - Keep eye contact with attorneys
  - Be assertive in your responses
  - Be professional and polite
  - Use facts when describing your opinion
  - Being deposed in a discovery deposition is an unnatural process

Guidelines for Testifying at Depositions (2 of 4)

- If you prepared a written report, the opposing attorney might attempt to use it against you
- If your attorney objects to a question from the opposing attorney
  - Pause and think of what direction your attorney might want you to go in your answer
- Be prepared at the end of a deposition to spell any specialized or technical words you used

Guidelines for Testifying at Depositions (3 of 4)

- Recognizing deposition problems
  - Discuss any problem before the deposition
    - Identify any negative aspect
  - Be prepared to defend yourself
  - Avoid
    - Omitting information
    - Having the attorney box you into a corner
    - Contradictions
  - Be professional and polite when giving opinions about opposite experts

Guidelines for Testifying at Depositions (4 of 4)

- Recognizing deposition problems (cont'd)
  - To respond to difficult questions that could jeopardize your client's case
    - Pause before answering
  - Keep in mind that you can correct any minor errors you make during your examination
  - Discovery deposition testimony often doesn't make it to the jury
    - It might be presented to the jury, usually as part of an attempt to discredit the witness

Guidelines for Testifying at Hearings

- Testifying at a hearing is generally comparable to testifying at a trial
- A hearing can be before an administrative agency or a legislative body or in a court
- Often administrative or legislative hearings are related to events that resulted in litigation
- A judicial hearing is held in court to determine the admissibility of certain evidence before trial
  - No jury is present

Preparing Forensics Evidence for Testimony (1 of 3)

- Use Autopsy for Windows to extract e-mail in a forensic image
  - See Figures 15-1 and 15-2

Preparing Forensics Evidence for Testimony (2 of 3)

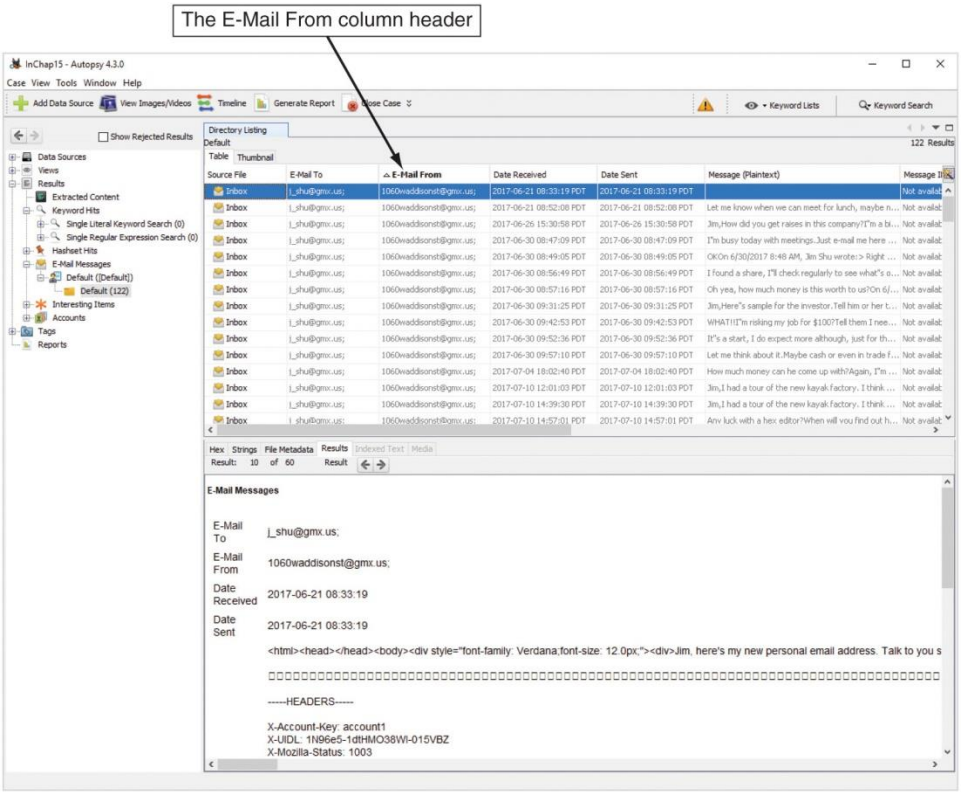

Figure 15-1 E-mails sorted by sender

Source: *www.sleuthkit.org*

Preparing Forensics Evidence for Testimony (3 of 3)

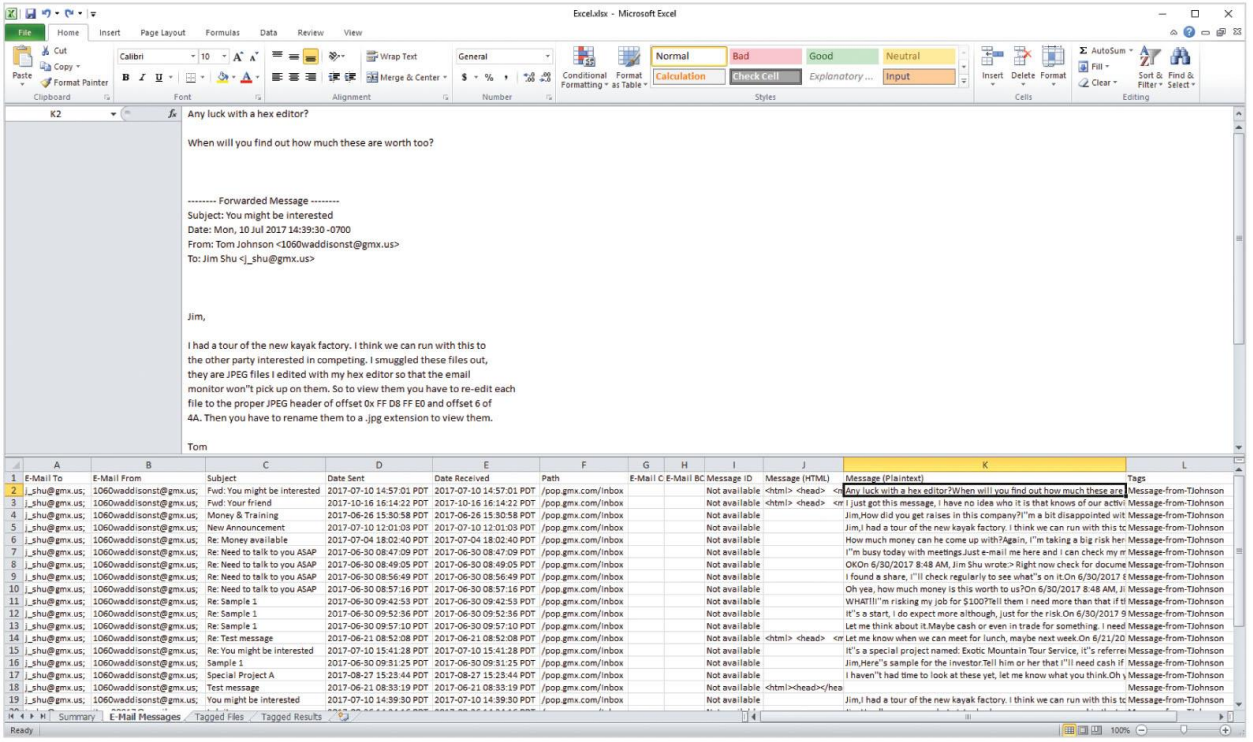

Figure 15-2 The Excel spreadsheet of Jim Shu's e-mails

Preparing a Defense of Your Evidence-Collection Methods

- To prepare for testimony
  - You should prepare answers for questions on what steps you took to extract e-mail metadata and messages
- You might also be asked to explain specific features of the computer, OS, and applications (such as Outlook)
  - And explain how these applications and digital forensics tools work

Summary (1 of 3)

- When cases go to trial, you as the forensics expert play one of two roles: a fact witness or an expert witness
- If you're called as a fact or expert witness in a digital forensics case, you need to prepare for your testimony thoroughly
- When you're called to testify in court, your attorney examines you on your qualifications to establish your competency as an expert or a fact witness

Summary (2 of 3)

- Make sure you're prepared for questions opposing counsel might use to discredit you, confuse you, or throw you off the track
- Know whether you're being called as a fact witness or expert witness (or both) and whether you're being retained as a consulting expert or expert witness
- Deposition differs from a trial because there's no jury or judge

Summary (3 of 3)

- Depositions usually fall into two categories: discovery depositions and testimony preservation depositions
- Guidelines for testifying at depositions and hearings are much the same as guidelines for courtroom testimony
- Make sure you prepare answers for questions on what steps you took to collect and analyze evidence and questions on what tools you used and how they work