Computer Forensic
Evidence Collection and Management

Chapter 14

Court Preparation, Presentations and Testimony

Chapter Objective

- Identify testimony requirements for electronic evidence presentations
- Learn how to be effective in technical courtroom presentations
- Understand why examiners and investigators must be technically proficient
- Learn the various legal terms associated with forensic testimony
- Become familiar with direct examination and cross-examination processes

Introduction

- Forensic investigators and examiners can be expected to provide expert testimony to civil and criminal litigation.
- Electronic evidence might be used in both civil and criminal litigation.
- Computer forensic experts could provide supporting evidence to prosecute criminal cases relating to all categories of serious crimes.
- The forensic team must know how the various state and federal laws apply to the case and evidence.
- Forensic examiners must know how all the computers and electronic devices work.
- Documentation will be required to support all allegations presented.

Computer and Electronic Evidence

- Forensics, as it relates to computers and data, is the collection and preservation of data to investigate or establish facts for any type of legal purpose.
- Computer and electronic forensics is an emerging specialty that has no defined criteria.
- With the speed at which the computer industry changes, it is often a struggle for the legal profession to keep up with all the new laws established to convict criminals or business insiders who use technology as a weapon.
- While the tools or times used to lay the groundwork for the discovery phase may vary, the methodology remains the same.
- Electronic evidence might be used to persecute criminal cases relating to drug trafficking, murder, kidnapping, terrorism, and another endless list.
- Most attorneys have little knowledge about computers and will need guidance as a case develops.
- The majority of work is often discovering how to look at the information and display it so that it makes sense to laymen.
- During the discovery phase, being a forensic computer specialist can be compared to being a private investigator, only the subject matter is mainly dealing with computers and electronic data.

Computer and Electronic Evidence (Cont.)

When Is Forensic Evidence Relevant?

- The legal team is interested in determining what evidence can possibly be recovered that might have some influence on the case.
- The process involved to investigate a computer an be exceptionally time intensive. Because it is initially uncertain what evidence a computer contains, it is essential to quality a particular compute before investing additional resources.

Technical Expert Testimony

- Either technical or expert witnesses might provide testimony.
- The technical witness presents evidence, explains it, and describes how it was obtained. Only facts are offered, not conclusions.
- The expert witness, however, can present opinion and presentations.
- A computer forensics examiner who servers as an expert witness provides an opinion that contributes to the legal process.
- The different capacities in which the expert technical witness may serve in the legal system include:
  - Consulting expert – A consultant or advisor to legal team.
  - Court's expert – A consultant or advisor to a court
  - Testifying expert – The role that most technologists think of when asked to serve as an expert witness.
  - Expert as witness to fact. Here an expert is asked to testify as a "normal" nonexpert witness to something personally witnessed.

The Financial Forensic Expert

- The financial forensic expert is concerned with fact-finding and interpretation of business documents and records.
- The financial expert also looks at matters related to how an organization reports its performance, controls activities and transactions, protects its resources from theft and misuse.
- There is a different between a financial forensic expert and a traditional certified public accountant (CPA) or auditor.
- In gathering facts and evidence, a forensic accountant is more experienced in activities that involve:
  - Knowing where to look
  - Identifying the types of evidence
  - Describing how to extract the evidence
  - Knowing what constitutes relevant and valid support
- The forensic accountant is more experienced at interpreting facts and evidence, as well as presenting findings in a manner that is meaningful and can be used to support the civil, criminal , administrative, and political processes

Forensic Accounting Testimony

- Recent court cases have involved crimes involving financial wrongdoing.
- Forensic accounting and investigation requires a background and expertise that encompasses the following areas:
- Generally accepted accounting principles (GAAPs) and generally accepted auditing standards (GAASs)
  - Accounting and auditing malpractice
  - Securitizations analysis and fraud
  - Financial consulting
  - Forensic actuarial services
  - Expert witness testimony
  - Securities fraud
  - Business fraud
  - Business valuations
  - Actuarial services and testimony

Forensic Accounting Testimony (Cont.)

- A forensic accountant is often retained to analyze, interpret, summarize, and present complex financial and business related issues in a manner that is both understandable and properly supported.
- A forensic accountant is often involved in the following:
  - Investigation and analyzing financial evidence
  - Developing computerized applications to assist in the analysis and presentation of financial evidence
  - Communication finding in the form of reports, exhibits, and collections of documents
  - Assisting in legal proceedings, including testifying in court as an expert witness
  - Preparing visual aids to support trial evidence
- In order to properly perform these services, a forensic account must be familiar with legal concepts and procedure.
- The Association of Certified Fraud Examiners (ACFE) recognized the following areas as qualified professional experience:
  - Accounting and auditing
  - Criminology
  - Fraud investigation
  - Loss prevention
  - Law – fraud related
  - Sociology – fraud related.
- Most financial specialists will probably not possess sufficient skill in computer forensics, which means that an additional expert must be added to the team.

Court Appearances

- This is the venue where all the investigations, examination, and long hours researching an incident pay off.
- All litigants must be aware of their actions and activities when in a public area.
- Before a trial starts, walk into the courtroom and become familiar with the location of the witness char and the path to get there.
- It is essential to dress professionally.
- The court must hear your testimony. It is important to remember that witnesses are not talking to the attorneys; rather they are talking to the jurors.
- Witness must have a copy of the investigative report on the stand and should not be afraid to refer to it.
- The witness must answer all questions clearly and avid nodding as an answer.
- Witness must listen very carefully to every questions asked, and make sure the question is understood before responding.
- Attorneys may try to make witnesses lose their cool.
- Witnesses can make a mistake and respond incorrectly to questions.
- Witnesses must avoid looking at their counselors when answering questions.

Court Appearances (Cont.)

Preparing for Testimony

- Now it is the time to start to thoroughly prepare for the task of presenting the computer forensic evidence to the court. .
- Expert witnesses work with attorneys and not defendants and plaintiffs.
- Before testifying in court, be prepared to provide definitions of electronic and computer terms. An overview of electronic and computer forensics can be provided.
- Witnesses must substantiate finding with documentation and collaboration from supporting sources. In the analysis and report-generating phase of the investigation, develop and maintain a standard method of processing documentation in expectation of testifying.
- Witnesses must be aware of a practice called conflicting out. A good rule is to avoid conversation with opposing attorneys.
- Testimony will lose credibility if the witnesses cannot certify the findings .
- It is also essential that documentation show how the evidence was preserved.
- An important note – do not create a formal checklist of investigative or examination procedures or integrate a checklist into the final report.
- The opposing attorneys will attempt to discredit evidence based on contamination and gaps in custody.

Testifying in Court

- Before appearing in court, be sure to become familiar with the procedures followed during a trial or legal process.
- A document that will be helpful in this process is called *curriculum vitae* (CV).
- A testimony log should be maintained in the CV that records expert testimony provided.
- During the qualification phase, called *voir dire*, the witness's expert qualifications are demonstrated.
- What does all this say to the novice forensic investigator or examiner? It appears a priory is to embark on a compressive training program and become associated with a forensic laboratory.
- Working with a mentor is an excellent method of accumulating forensic experience.

Presenting Evidence

- A technique employed is to tell the court what evidence is going to be presented, present the evidence, and then tell what evidence was presented.
- Expert witnesses must keep the audience in mind. Particularly the jury and sometimes the court.
- When preparing the forensic testimony, consider the following items that could enhance the quality of the presentation:
  - Provide the scope of the case
  - Describe the forensic overview and components of the case
  - Identify the most powerful elements of evidence
  - Tick the forensic evidence to the devices and media
  - State how the evidence support the conclusions
  - Support the allegations of the legal team

- Now comes the had part! The expert witness must be ready to explain MD5. Sha-1, and CRC.
- If disk imaging has been performed, and explanation f the process will be required. As will the tools that were utilized in the process.

Presenting Evidence (Cont.)

- The witness should prepare to answer the following questions:
- How id data or evidence stored on the media in question?
  - What is a bit-stream image or digital copy?
  - How is deleted data recovered fro the media in questions?
  - What is the importance of temporary file and where are they located?
  - What data is contained on system, Interne, e-mail, or network log files?
- It is important to be an impartial expert witness and not be an advocate.
- It is also essential to coordinate forensic testimony with other experts that might be testifying in the trial.

Direct Examination Testifying

- Direct examination is the most important part of testimony at a trial.
- There are several direct testimony techniques that are effective. These include the following:
  - State background and qualifications to testify as a computer forensic expert
  - Provide a clear overview of the examination findings
  - Describe evidence collection methods and processes
  - Describe speech at the juror's education level
  - Preparation is the key to a successful testimony
  - Use the case documentation from the actual written records created during the examinations of evidence
  - Provide testimony concerning facts that are known about a case without being prompted
  - Know the customary practice that has occurred in similar cases
  - When questioned, provide the answers needed to bring attention to the actual findings and opinions that are part of the investigation
  - Remember to engage the jury, making sure to project your voice. If the jury cannot hear the testimony ,the effort is fruitless.
- The user of graphics, such as PowerPoint slides and flipcharts, can enhance the expert testimony.
- Graphics must not be "busy".
- A final note on direct testimony; do not volunteer information or be overly friendly (or hostile) to the opposing attorney.

Cross-Examination Testifying

- In law, cross-examination is the interrogation of a witness called by one's opponent.
- It is preceded by direct examination and may be followed by a redirect.
- When answering questions from the opposing attorney: witnesses should rephrase the anwser using their own words.
- Sample questions the opposing attorney might ask are as follows:
  - How many tools were used to verify the evidence?
  - What tools were used?
  - What are the know problem sand weak features of these tools?
  - Are the tools reliable?
  - Are the tools consistent in producing results?
  - Is the witness a consultant?
  - Are compute forensic manual being reviewed?
  - Is the witness a member of the cyber-forensic organization?
- Questions might be posed to require conflicting answers.
- In summary, maintain a vigorous demeanor and use energetic speech to make the jury listen to the testimony.

The Deposition

- A deposition is a formal meeting where an individual is questioned in which only the opposing attorneys, opposing parties, defendant, and plaintiff are present.
- A deposition differs from a trial because a judge and a jury do not participate.
- The two types of depositions include discovery and testimony preservation.
- The discovery deposition is part of the discovery process.
- The testimony preservation deposition is usually requested to preserve testimony because of heath issue or schedule conflicts.
- There are several rules to follow during the deposition. These include the following:
  - Act professionally
  - Use facts when describing an opinion
  - Understand these episode is a discovery function
  - Avoid making mistakes or providing incorrect information.
- The witness should take time in answering questions, ensuring that answers are correct and understood.