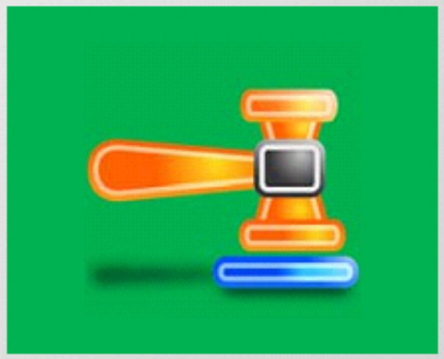
Forensics Report Writing and Presentation

Module 14

Designed by Cyber Crime Investigators. Presented by Professionals.



Module Objectives

After successfully completing this module, you will be able to:

1. Understand the importance of forensic investigation reports
2. Understand the important aspects of a good report
3. Summarize the contents of a forensics investigation report template
4. Classify the investigation reports and review the guidelines for writing a report
5. Define an expert witness and describe the roles of an expert witness
6. Differentiate Technical Witness Vs. Expert Witness
7. Understand Daubert and Fyre Standards
8. describe how to testify in a court and discuss the general ethics while testifying

Writing Investigation Reports

Forensics Investigation Reports

- An investigation report provides detailed information on the **complete forensics investigation process**

- It includes **scope of investigation**, **tools used** to acquire and analyze data, **evidence gathered**, **details of investigator**, etc.

- The report **presents a scientific testimony** about a case with relevant evidence and facts to support an argument in civil and criminal proceedings

Important Aspects of a Good Report

- It should accurately define the details of an incident
- It should convey all necessary information in a concise manner
- It should be technically sound and understandable to the target audience
- It should be unambiguous and not open to confusion
- It should be structured in a logical manner so that information can be easily located
- It should be created in a timely manner
- It should be able to withstand legal inspection
- It should contain results that can be completely reproducible by a third party
- It should try to answer questions raised during a judicial trial
- It should provide valid conclusions, opinions, and recommendations supported by figures and facts
- It should adhere to local laws to be admissible in court

Forensics Investigation Report Template

In general, a forensics investigation report template contains:

1. **Executive summary**
   - Case number
   - Names and Social Security Numbers of authors, investigators, and examiners
   - Purpose of investigation
   - Significant findings
   - Signature analysis
2. **Investigation objectives**
3. **Details of the incident**
   - Date and time the incident allegedly occurred
   - Date and time the incident was reported to the agency's personnel
   - Details of the person or persons reporting the incident
4. **Investigation process**
   - Date and time the investigation was assigned
   - Allotted investigators
   - Nature of claim and information provided to the investigators
5. **Evidence information**
   - Location of the evidence
   - List of the collected evidence
   - Tools involved in collecting the evidence
   - Preservation of the evidence
6. **Evaluation and analysis Process**
   - Initial evaluation of the evidence
   - Investigative techniques
   - Analysis of the computer evidence (Tools involved)
7. **Relevant findings**
8. **Supporting Files**
   - Attachments and appendices
   - Full path of the important files
   - Expert reviews and opinion
9. **Other supporting details**
   - Attacker's methodology
   - User's applications and Internet activity
   - Recommendations

Report Classification

01

Verbal Formal Report

A structured verbal report delivered under oath to a board of directors/managers/ panel of jury

02

Written Informal Report

An informal or preliminary report in written form

03

Written Formal Report

A written report sworn under oath, such as an affidavit or declaration

04

Verbal Informal Report

A verbal report that is less structured than a formal report and is delivered in person, usually in an attorney's office or police station

Guidelines for Writing a Report

C|HFI Computer Hacking Forensic Investigator

1. **Document each step** carried out in the **investigation process** immediately, and in a clear and concise manner. This saves time and promotes accuracy.

2. Know the **objectives of your examination** before you begin with analysis. This results in generating a more focused report.

3. **Organize your report** in such a manner that it gets **progressively complex**. This allows high-level executives to grab its essence by just reading the initial pages of the report.

4. Create and use a **standard report template** with all essentials elements to save time

5. **Use unique identifier** or reference tag for each person, thing, and place mentioned repeatedly in your report. This eliminates ambiguity or confusion

Guidelines for Writing a Report (Cont'd)

6. **Write your reports** considering the **technical capability** and **knowledge of your audience**. Also, get the report proofread by others to get to know the ease of understandability, and quality in terms of grammar and other errors

7. Use attachments or appendices to maintain flow of your report. They provide further details of any **terminology**, **findings**, or **recommendations** cited in the report. Also, add references to the appendices in the report

8. **Record MD5 hashes** in the report for all evidence recovered (hard disk, USB, specific file, etc.) during acquisition, verification of image, and at the end of the examination. This shows that you are handling the data in appropriate manner and it is admissible in a court of law

9. **Include metadata** (file location, file path, file size, time/date stamps, author, etc.) for every file named in your report. This eliminates confusion and increases customer confidence

Guidelines for Writing a Report (Cont'd)

- Write opinions that are based on knowledge and experience
- Create a logical structure from beginning to end
- Maintain consistent font and spacing throughout the report
- Use bullet or number lists where applicable to make the information more readable
- Try to avoid hypothetical questions
- Use theoretical questions to guide and support opinions based on factual evidence
- Avoid using repetitive and vague language
- Group associated ideas and sentences into paragraphs and later into sections
- Do not use slang words, specialist language (which is not understood by the average person), and colloquial terms (which creates the effect of conversation)
- If any abbreviations or acronyms are used, define and explain them in detail
- After completing the report, check the grammar, vocabulary, punctuation, and spelling
- Always use active voice when writing a report so that the communication appears direct and straightforward
- Write the report in a concise manner so that it is easily understandable and interesting to any audience
- Never include any clues in the report
- Avoid mentioning too many details and personal observations in the report

Expert Witness Testimony

Who is an Expert Witness?

- An expert witness is a witness, who by virtue of his/her education, profession, or experience, is **believed to have special knowledge** on the subject, beyond that of the average person, and sufficient to the extent that others **legally depend upon his/her opinion**
- The opinion of an expert witness, authorized by a court, has **legal status and can be accepted as evidence** in a court of law

Roles of an Expert Witness

C|HFI Computer Hacking Forensic Investigator

1. **Evaluates** the evidence
2. Helps the attorney to get to the **truth**
3. **Testifies** in court
4. Assists the court in understanding **intricate technical evidence**
5. **Assists** plaintiff's or defendant's lawyers to establish facts, assess merits, help in the preparation of a case, and aid in making the **initial decision** of whether to start a litigation
6. Truthfully, and objectively express his or her expert opinion, without regard to any others' **views** or **influence**
7. **Conducts investigations** on behalf of the court and reports the findings back to the court
8. **Participates** in court-appointed expert witness conferences to **study any intriguing incident**
9. **Educates** the public and the court

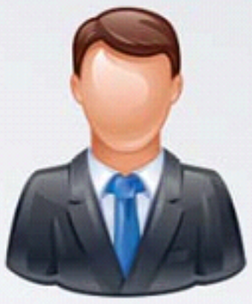
Technical Witness Vs. Expert Witness

A **technical witness** is an individual who:

- Does the actual **fieldwork**
- **Submits** only the results of his findings
- Does not offer a **view in court and conclusion**
- Provides facts found in **investigation**
- Prepares **testimony**

An **expert witness** is an individual who:

- Has absolute **field knowledge**
- Offers a **view** in court
- Offers opinions based on **observations**
- Works for the **attorney**



Daubert Standard

The Daubert Standard is a **legal precedent** set in 1993 by the Supreme Court of the United States regarding the admissibility of expert witnesses' testimony during **federal legal proceedings**

In order to reject the **presentation of unqualified evidence** to the jury, the Daubert motion takes place **before or during trial**

Trial judges make a decision as to whether the evidence is both **relevant and reliable**

Expert's evidence can be decided based on the **facts of the case**

The expert should derive his or her **conclusions using scientific method** in order to consider the evidence reliable

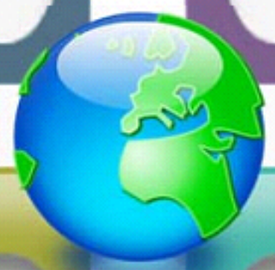
Frye Standard

1

Frye Standard is a **legal precedent** regarding the admissibility of **scientific examinations** or experiments in **legal cases**

2

To meet the Frye Standard, scientific evidence submitted in the court should be accepted as an important part of the **associated scientific community**



3

It can be applied to **procedures, principles, and analysis** presented in the court case, but it is not an appropriate test for **voice identification evidence**

4

According to this standard, supporters of a particular **scientific issue** should come up with a number of experts to speak about the science behind the **issue in question**

What Makes a Good Expert Witness?

Good experts can talk to the jurors in a way that shows they have **confidence** in their case and are sincere, without seeming like an advocate

Experts need to change the **complicated material** into **understandable material**, so as to make it comprehensible for the lay audience

Expert witnesses should observe the jurors to determine their level of interest, and notice when any juror is **sleeping** or **uninterested**

Avoid **overextended** opinions

Develop **repetition into details** and descriptions for the jury

Expert witnesses should enhance their credibility by **adhering** to a formal **dress code**

Importance of Curriculum Vitae

01

- Curriculum Vitae (CV) shows the **capability of an expert witness**

02

- **It is essential to update** the CV regularly

- The following things must be kept in mind while preparing a CV:
  - Certifications/credentials/accomplishments
  - Recent work as an expert witness or testimony log
  - Expertise
  - List of books written, if any
  - Any training undergone
  - Referrals and contacts
  - List basic and advanced skills

Professional Code of Conduct for an Expert Witness

- Do not record **conversations** or telephone calls
- Learn about all other people involved and **basic points in dispute**
- Define **analysis procedures**
- Do not agree to **testify on subject matters** for which you are not an expert or in which you do not believe
- Do not keep **secrets** from the **client's legal team**
- Never **exaggerate** or fudge details, stick with the **facts in evidence**
- Do not be **intimidated by the process**
- Do not write, fax, email, or **communicate** in any other way, unless **explicitly instructed** to do so
- Do not conduct **research and analysis** on the device you have not been asked to do, and respect the **guidelines** imposed by the client's legal team
- Do not ever permit **compensation** to be tied to the outcome of the **litigation**
- Do not let the client's legal team form **opinions**; if they insist, **resign** from the case
- Never **compromise** on **integrity** for any reason

Preparing for a Testimony

- When **evidence is technical** in nature, and consequently difficult for the **layman** to comprehend, an expert is required to explain its nature and what it means to the case

Points to bear in mind while preparing a testimony:

- Go through the **documentation thoroughly**
- Establish early **communication** with the attorney
- Determine the basic facts of the case before beginning with the **examination of evidence and documentation**

- Substantiate the findings with **documentation**, and by **collaborating** with other computer forensic professionals

Testifying in the Court

- **Familiarize** the witness to the **usual procedures** that are followed during a trial
- The attorney introduces the expert witness with **high regards**
- The opposing counsel may try to **discredit the expert witness**
- The attorney would lead the expert witness through the **evidence**
- Later, it is followed by a cross-examination by the **opposing counsel**

General Order of Trial Proceedings

C|HFI Computer Hacking Forensic Investigator

1. Motion in beginning

- Objections to particular testimonies are framed in the form of lists
- Allows judge to examine whether certain evidence should be admitted in the absence of the jury

4. Rebuttal session

- Cross-examination by both plaintiff and defendant

2. Opening statement

- Offers an outline of the case

5. Jury orders

- Proposed by the counsel
- Approved and read by the judge to the jury

3. Plaintiff and defendant

- The attorney and the opposing counsel present the case

6. Closing arguments

- Statements that organize the evidence and the law

General Ethics While Testifying

Ethics to be followed while **presenting a testimony**, as an **expert witness**, to any court or an attorney:

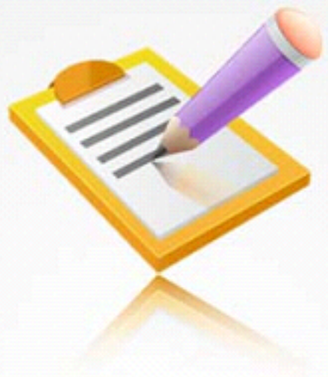
- Be professional, polite, and sincere in presenting a testimony
- Maintain a steady body language, a balanced stance, and do not reveal any nervousness
- Be enthusiastic
- Keep the jury interested in what you are saying
- It is important to maintain visual control in the courtroom
- Show an open physical and psychological attitude to the jurors
- Be aware and prepare for the possible rebuttal questions, especially from the opposing counsel
- Always pay tribute to the jury
- Avoid leanings
- Develop self-confidence and create personal space for winning professional style in the courtroom

Importance of Graphics in a Testimony

1. Use clear and easily **understandable graphics**
2. Make **graphical demonstrations** such as charts to illustrate and elucidate your findings
3. Make sure the graphics are **seen by the jury**
4. **Face the jury** while exhibiting these graphics
5. Make a habit of using **charts** and **tables** for courtroom testimony

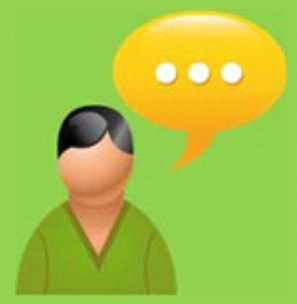
Helping your Attorney

Prepare a list of important questions



- Enable the attorney to get the **expert's testimony** into the trial
- Practice presenting your **testimony** for **direct examination**
- Help the attorney to **review and improve** on how he or she wants to try the case

- Develop a script and work with the attorney to get the **perfect language**
  - **Communicate the message** to the jury



Avoiding Testimony Issues

1. Offer **clear opinions**
2. Outline your **boundaries** of knowledge and ethics
3. Create a **case outline** and summary for the attorney, which does the following
   - Enables reviewing of the **case plan**
   - Offers a clear overview of **the level of knowledge** used in the case
4. Make efforts to **coordinate your testimony with other experts**, who are retained by your attorney for the same case
5. Meet with the paralegal to **communicate necessary information** to your attorney
   - Paralegal is a person with **special training** in either a specific or general area of law

Testifying during Direct Examination

- **Direct examination** refers to the process of the **witness** being **questioned by** the **attorney** who called the latter to the stand
- The attorney asks questions for the purpose of eliciting facts about the case

Some ways to enhance your credibility as a witness:

- Be on time or slightly early for court
- Dress professionally
- Do not appear to be nervous
- Maintain a proper posture
- Remain calm and do not get angry
- When applicable, answer with a "yes" or "no"
- Don't volunteer to provide extra information
- Avoid making absolutes in your statements
- Don't discuss the case with anyone but the attorney
- Consider the question carefully before you answer
- Speak clearly and confidently
- If the judge or attorney begins to speak, stop talking
- Avoid memorizing answers
- Remain impartial and speak facts

Testifying during Cross-Examination

- Cross-examination is the process of **providing the opposing side** in a trial the **opportunity to question a witness**
- It is the job of the **cross-examining attorney** to discredit the opposing side's witness. In this attempt, they may use psychological techniques

Be prepared for and ready to avoid such cross-examination tactics as:

- Rapid-fire questions with no time to answer between questions
- Leading questions ("Isn't it true that what you saw was …?")
- Repeating your words with a twist that changes their meaning
- Pretending to be friendly, then turning against you suddenly
- Feigning bewilderment, outrage, or shock at what you have said
- Prolonged silence designed to cause discomfort in hope that you'll reveal more

The most important thing to remember when subjected to such tactics is "not to take the attorney's tactics personally as he or she is just doing his or her job". Likewise, you should be doing your job by stating the facts without getting flustered

Testifying during Cross-Examination: Best Practices

1. **Do not offer guesses** when asked about something irrelevant to the case
2. **Use your own words** and phrases when answering the opposing counsel
3. **Speak slowly** as the best offense to problematic questions is to be patient with your answers
4. Turn towards the jury slowly while **giving your response**. This allows you to maintain control over the opposing counsel

Deposition

- Deposition is the process of **questioning witnesses prior to a trial**, and it is used in the pretrial stages of both civil and criminal cases
- The **attorney** arranges a location for the deposition

Deposition differs from a trial as:

- Both **attorneys** are present
- No **jury** or **judge** present
- Opposing **counsel** asks questions

Purpose of a deposition:

- Enables opposing **counsel** to preview your **testimony** at trial

Guidelines to Testify at a Deposition

C|HFI Computer Hacking Forensic Investigator

01 Convey a calm, relaxed, confident, and **professional appearance** during a deposition

02 Do not get influenced by the **opposing counsel's tone**, expression, or tactics

03 Use the **opposing counsel's name** while responding to him/her and reply confidently

04 Maintain **eye contact** with the opposing counsel

05 Keep your hands on the table, which makes you **appear more open and friendly**

06 Use facts when **describing your opinion**

07 **Avoid conversation** with opponents and their attorney **after** the **deposition**

Dealing with Media

1. Avoid contact with **media** during a case
2. Do not give **opinions** about the trial to media; simply **refer** to the **attorney**
3. Avoid **conversing** with the **media** because:
   - It is **unpredictable** what the journalists might publish
   - The **comments** might influence the case
   - It can create a record that could be used **against** you while you present future **testimonies**
4. Record your interviews, if any, with the media

Module Summary

- An investigation report provides detailed information on the complete forensics investigation process
- Reports are classified into: written formal report, written informal report, verbal formal report, and verbal informal report
- An expert witness is a witness, who by virtue of education, profession, or experience, is believed to have special knowledge of his/her subject beyond that of the average person, sufficient that others legally depend upon his/her opinion
- Direct examination refers to the process of a witness being questioned by the attorney who called him or her to the stand
- Cross-examination is the process of providing the opposing side in a trial the opportunity to question a witness
- Deposition is the process of questioning witnesses prior to a trial, and it is used in the pretrial stages of both civil and criminal cases