

# Forensics Report Writing and Presentation

## Module 14






## Computer Hacking Forensic Investigator v9

### Module 14: Forensics Report Writing and Presentation

Exam 312-49



# 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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

An investigative report contains all the findings of a forensic investigation that are presented in a written form. It contains only facts, and there is no room for any personal opinions of a forensic investigator. This module provides guidelines for an investigator to implement the best practices in the investigations and prepare an effective report. The module will familiarize you with the topics mentioned in the slide.









Investigative reports are the records of actions performed during the investigation process starting from obtaining the first incident report till the derived conclusions. The report should provide every minute detail of the performed actions, reasons behind the actions, and the results. As a result, the non-technical people involved in the case can easily understand the case details and prosecute the perpetrator. Investigators should be capable of writing these reports in a clear and easy to understand language.



# 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 

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

A forensic investigation report is a statement of allegations and conclusions drawn from the computer forensics investigation. It contains all the findings of the investigator in written form, thereby making it a concise, precise, accurate, and organized report. It represents all the aspects of an investigation, which is unbiased, organized, and understandable.

The investigators report and present their findings in a technically sound, disciplined, and easily understandable manner for legal proceedings after cross-examination. It can present the facts to communicate the expert's opinion.

### Goals of an investigative report:


Investigative report writing involves a well-structured documentation that should be truthful, timely, and understandable to the target audience.

Before creating any investigative report, an investigator has to follow certain objectives. The reports should provide every detail about the incident without compromising on the conciseness, avoiding jargons, and should be factual. In a report, an investigator should cover the incident in detail that should be legally admissible. The report should meet its purpose without any ambiguity and be properly formatted, thereby making it easy for the readers to understand.

The report should enclose all the supporting documents like tables and graphs and multiple references to support it while deriving conclusions. The results should be clear and trouble-free so that it can be reproducible by the third party as well.



## 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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The main objective of a cybercrime investigation is to identify the evidence and facts. It should also give a detailed account of the incidents by emphasizing the discrepancies in the statements of the witnesses. It should be a well-written document that focuses on the circumstances of the incident, statements of the witnesses, photographs of the crime scene, reference materials leading to the evidence, schematic drawings of the computer system, and the network forensic analysis report. The conclusions of the investigative report should be subject to the facts and not the opinions of the investigators. An investigator should draft the documentation keeping in view that the defense team will also scrutinize it.

Aspects of a good investigative report are:

- It should provide a detailed explanation of the approach to the problem. The examination procedures, materials or equipments used, analytical or statistical techniques implemented, and data collection of sources are few subsections that should be included in the report to make the reader understand the investigation process.
- The data collection process is a critical factor from the examiner's point of view, so it is important to present data in a well-organized manner. While preparing the lab report, it is better to record all the data and observations in a laboratory notebook. All the data presented in tabular forms should be labeled properly.
- It is advisable to include all calculations and algorithms done during the investigation in a summarized form. The algorithms denoted in the report should be coined with some




specific names, such as Message Digest 5 (MD5) hash. Additionally, the report should contain a brief description of the standard tools used in the investigation and their cited sources.

- It should provide a statement of uncertainty and error analysis during the observation. It is necessary to provide the limitations of knowledge to protect the integrity during a computer investigation. E.g., if an investigator retrieves a time stamp from a computer file, then one should state explicitly in the report that a time stamp can be reset easily. Hence, one should not rely solely on the results.
- It should explain all the results in a logical order, using subheadings, tables, and figures, to address the purpose of the report and enhance the presentation. The results should be presented in such a way that any reader, irrespective of his/her knowledge of the case, can understand the whole investigation process from the report.
- For further improvement of the report, the results and conclusions should be discussed. All the findings and their significances should be established in light of overall examination in the discussion section. The questions on how the case developed, what were the problems faced, and how the solutions were approached should also be answered.
- It should enlist all the references in alphabetical order for providing sufficient details to track down the information used in drafting the report. It should follow a standard writing style for references including books, journal articles, leaflets, websites, and other materials mentioned in the report.
- Any extra materials used in the report should be included as appendix in the table of contents. It contains charts, diagrams, graphs, transcripts, and copies of materials with proper description of each particular. They should be mentioned in their order of occurrence in the text of the report. Some portions of the appendices may be optional or important.
- Although its optional, a report can end up with an acknowledgment section. It is not a dedication but a gesture of thanking people in general who helped during the research. For example, the people who contributed in analysis and proofreading of the report can be mentioned in this section.



# Forensics Investigation Report Template



In general, a forensics investigation report template contains:

<ol style="list-style-type: none"><li><b>Executive summary</b><ul style="list-style-type: none"><li>Case number</li><li>Names and Social Security Numbers of authors, investigators, and examiners</li><li>Purpose of investigation</li><li>Significant findings</li><li>Signature analysis</li></ul></li><li><b>Investigation objectives</b></li><li><b>Details of the incident</b><ul style="list-style-type: none"><li>Date and time the incident allegedly occurred</li><li>Date and time the incident was reported to the agency's personnel</li><li>Details of the person or persons reporting the incident</li></ul></li><li><b>Investigation process</b><ul style="list-style-type: none"><li>Date and time the investigation was assigned</li><li>Allotted investigators</li><li>Nature of claim and information provided to the investigators</li></ul></li></ol>	<ol style="list-style-type: none"><li><b>Evidence information</b><ul style="list-style-type: none"><li>Location of the evidence</li><li>List of the collected evidence</li><li>Tools involved in collecting the evidence</li><li>Preservation of the evidence</li></ul></li><li><b>Evaluation and analysis Process</b><ul style="list-style-type: none"><li>Initial evaluation of the evidence</li><li>Investigative techniques</li><li>Analysis of the computer evidence (Tools involved)</li></ul></li><li><b>Relevant findings</b></li><li><b>Supporting Files</b><ul style="list-style-type: none"><li>Attachments and appendices</li><li>Full path of the important files</li><li>Expert reviews and opinion</li></ul></li><li><b>Other supporting details</b><ul style="list-style-type: none"><li>Attacker's methodology</li><li>User's applications and Internet activity</li><li>Recommendations</li></ul></li></ol>
---	---

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


An Investigative Report Template is a set of pre-defined styles allowing investigators to add different sections of a report like case number, names and social security numbers of the authors, objectives of the investigation, details of the incident, executive summary, remit of investigation, investigation process, list of findings, and tools used, etc.

Every investigative report starts with a unique case number, followed by names as well as social security number (SSN) of the authors, investigators, and the examiners involved in the investigation. The report covers all the details of the incident that are updated with the day to day progress in the investigative process with data and time of the allocated investigators. It includes every detail of the evidence like location, list of the collected evidence, tools used in the investigation, and the process of extracting and preserving the evidence.

It should also record the evaluation and analysis procedure starting from the initial evaluation of the evidence to the techniques used in the investigation, including the analysis of electronic/digital evidences with the relevant files, supporting documents like attachments and appendices, and path of the files. The report also includes reviews by experts with supporting details on attacker's intension, appliances used, internet activity, and the 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



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Report writing should begin with the identification of audience and objective of a particular report. The investigative report should be presented in such a manner that a person with less technical knowledge is also able to understand the findings and proceedings of the case.

Reports can be categorized as:

- Verbal
- Written

Further division of the previous categories includes:

- Formal
- Informal

The investigators should produce a formal verbal report for the board of directors, managers, or jury. It should be organized within the time frame. Attorneys should create a guide - called as the examination plan – to aid investigators in preparing the document containing expected questions and relevant answers of the investigation. An examiner can propose changes through this report such as asking for clarification or definition to the attorney for any misused expression or term. Irrelevant things should be avoided in the testimony.

Generally, the informal verbal report does not have a proper structure compared to a formal report, and investigators submit it to the attorney's office. This preliminary report should not



be mishandled or released in any case. It also mentions the areas that need investigation, such as incomplete tests, interrogations, document production, and depositions.

A formal written report is a document sworn under oath alike an affidavit or declaration. Hence, it is essential to pay attention to word usage, grammar, spelling, and details while drafting such formal reports. Mostly, first person voice and natural language style is preferred in such reports due to its formal nature like an affidavit while issuing a warrant or an evidence for a grand jury hearing. Therefore, it demands extra attention while documenting the details.

On the other hand, an informal written report precedes the main event of a particular case. They are not suitable to be produced in court, because it contains sensitive information that can be used by the opposing counsel. The information can be a written request for admissions of fact, deposition, or questions and answers written under oath.

It is, hence, advisable to include the contents of an informal written report in an informal verbal report and the essentials such as the subject system, tools used, and findings should be summarized in it. If the produced informal written report is destroyed then it is considered as destruction or concealing of evidence, which in legal terms is known as spoliation.



## Guidelines for Writing a Report



- 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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


In a computer forensic investigative report, investigators should record each step of the process immediately in a perfect manner to avoid any shorthand and shortcut errors avoided or else it may lead to redundancy and failure in comprehending the proceedings. Such reports help the investigators to communicate the process in a crisp manner at any point of time. It clearly depicts the main idea or objective of examination before starting the analysis, as it may improve the quality of the report and delivers the incident as required by the client.

The reports should be organized to increase the readability allowing high level executives to grab essence of the conclusions. The tables are used in the report to save space and time along with the table of contents with an intension to include the logical approach as well as make it easy the user understand the report agenda.

A report should follow a standardized template across the report to makes it scalable, and create a repetitive standard, thereby saving time and effort. Unique identifiers should be used in addressing the repetitive nouns in the report as well as eliminate the ambiguity and confusion. For example, if the investigative report is about the analysis of a PC used by John, the investigator can use capital letters to refer the belongings, e.g., "During the investigation, investigators found that the JOHN-PC was misconfigured."



## 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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

The reports should be drafted in consideration with the technical standards of the end-users or the target audience. The investigator should proofread and peer-review the report to check for the quality levels, consistency, and grammatical errors. Lengthy information or files are included as attachments and appendices to maintain the flow and style of the report.


Safety measures should be ensured for the digital evidences by creating and recording MD5 hashes, be it entire hard disk or a particular file. These evidences can ensure the data integrity standards and win the confidence of the audience. Each and every minute details of the recorded metadata should be tabulated to avoid the chances of ambiguity, like file creation date, last accessed, last edited, file location, file path, Hash value, etc.

Item	JOHN PC
File name	Case File
File path	C:\Users\John\Desktop\Casestudy
File size	9,982,720 bytes
Created	Tuesday, March 8, 2016, 10:05:45 AM
MD5 Checksum	D1C0DECDFD590AD899122D9958C9F9833

TABLE 14.1: Sample Report Draft



**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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Other Guidelines for Writing a Report

Following are the guidelines for writing a report:

- Write the opinions that are based on knowledge and experience.
- Proper flow must be maintained from beginning to the end of the report.
- Try to avoid hypothetical questions because they change the facts that are relevant to your opinion.
- Apply theoretical questions to guide and support your opinion, which should be based on the factual evidence only.
- Avoid writing repetitive and vague language in the report.
- The report should be written in a simple format so that it can be easily passed from one person to another.
- Lay out the ideas in a logical order.
- Group the associated ideas and sentences into paragraphs and later into sections.
- It should not contain any slang words, technical language, and colloquial terms.
- All the abbreviations or acronyms should be defined and explained in detail.
- After completing the report, check the grammar, vocabulary, punctuation, and spelling of the report.



- Always use the active voice narration in the report to make the communication direct and straightforward.
- Write the report in a concise manner making it understandable and interesting to read by any type of reader.
- Write everything with proper validation.
- Never mention any clues in the report.
- Avoid using too many informative details and personal observations in the report.







Expert witnesses refer to the persons recognized by the court of law as trustworthy for taking an opinion or verify a process by virtue of their education, skills, expertise, knowledge, and experience in a specific field. In this case, expert witnesses are the technically sound persons, who understand the working, process of attacks, investigative methods and the results obtained. These expert witnesses are basically non-biased and verify the technical aspects of the case on the request of the attorney or a prosecutor and present their views accordingly. Investigators must first submit their report to an expert for verification and make changes if any and also get their approval before submission in the court of law.






# 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



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

The term “expert witness”, coined in the 1780s, refers to an individual who has gained vast knowledge about a subject, surpassing an average person by virtue of education, profession, or experience.

The prosecutors or the client pay the expert witness to present their opinion based on the evidence collected in the investigation, and when required they should support their opinion at court during the hearings. At times, the Court can also appoint expert witnesses to authenticate the facts and witnesses during any complex case proceedings. Accident and death cases often need the help of an expert witness to verify the severity of injuries and mode of death. An expert witness is often consulted when the juries or attorneys fail to understand the facts, which eventually help the judiciary to come to a decision.

Expert witnesses, usually, cross-examine witnesses and evidence as numerous factors can influence the witnesses. The opinion of an expert witness, authorized by a court, has legal status and the court of law also accepts it as evidence. However, the expert witnesses should also comply with certain laws and can be liable for prosecution, if found giving false and misleading opinions.





An expert witness plays an important role in an under trial case with an objective of helping the court.

An expert witness is a person who can:

- Investigate a particular case related to a particular field
- Evaluate the evidence and present it before the court of law.
- Testify the matter related to the subject in court.
- Assist the plaintiff's or defendant's lawyers to establish and measure the facts, understand the complicated issues regarding evidence, and help in the preparation of a case.
- Aid the attorney to find the truth.
- Be honest and reliable in expressing his or her opinion effectively, without being influenced by any third party.
- Conduct investigations on behalf of the court and report the findings back to the court.
- Participate in court as an appointed expert witness to study any intriguing incident.
- Educate the jury, court, and the individuals related to the case about the findings.



Depending on the need, an expert witness plays either the role of a consulting expert, court's expert, or a testifying expert. They are:

- **Consulting Expert:** To offer technical explanations for a complex situation during court trials.
- **Court's Expert:** To advise the court on technical issues that the court fails to comprehend.
- **Testifying Expert:** To present testimony whenever required during the trial.



## 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**



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

There are two important witness testimonies that can play a pivotal role when cases go to trial, i.e., from a technical witness or an expert witness.


Technical witnesses' testimony may only provide facts found during the investigation to showcase an incident or a crime. He/she explains what exactly the evidence leads to in the process of acquisition; however, they cannot draw conclusions or offer opinion. They only conduct the fieldwork and submit the findings or facts of the investigation.


On the other hand, expert witnesses can give opinions based on their observation and experiences. They can also perform a deductive analysis with facts found during an investigation. Since computer forensics is a comparatively new field and does not follow any standards of practice, the expert witnesses must provide a clear opinion to the jury who may not be fully aware of the latest developments in the field of computer forensics.

A forensic investigator, who serves as an expert witness, can provide an opinion based on the evidences that can turn into a helping factor for litigation purposes.




# 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**



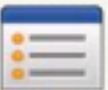
In order to reject the **presentation of unqualified evidence** to the jury, the Daubert motion takes place **before or during trial**



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**



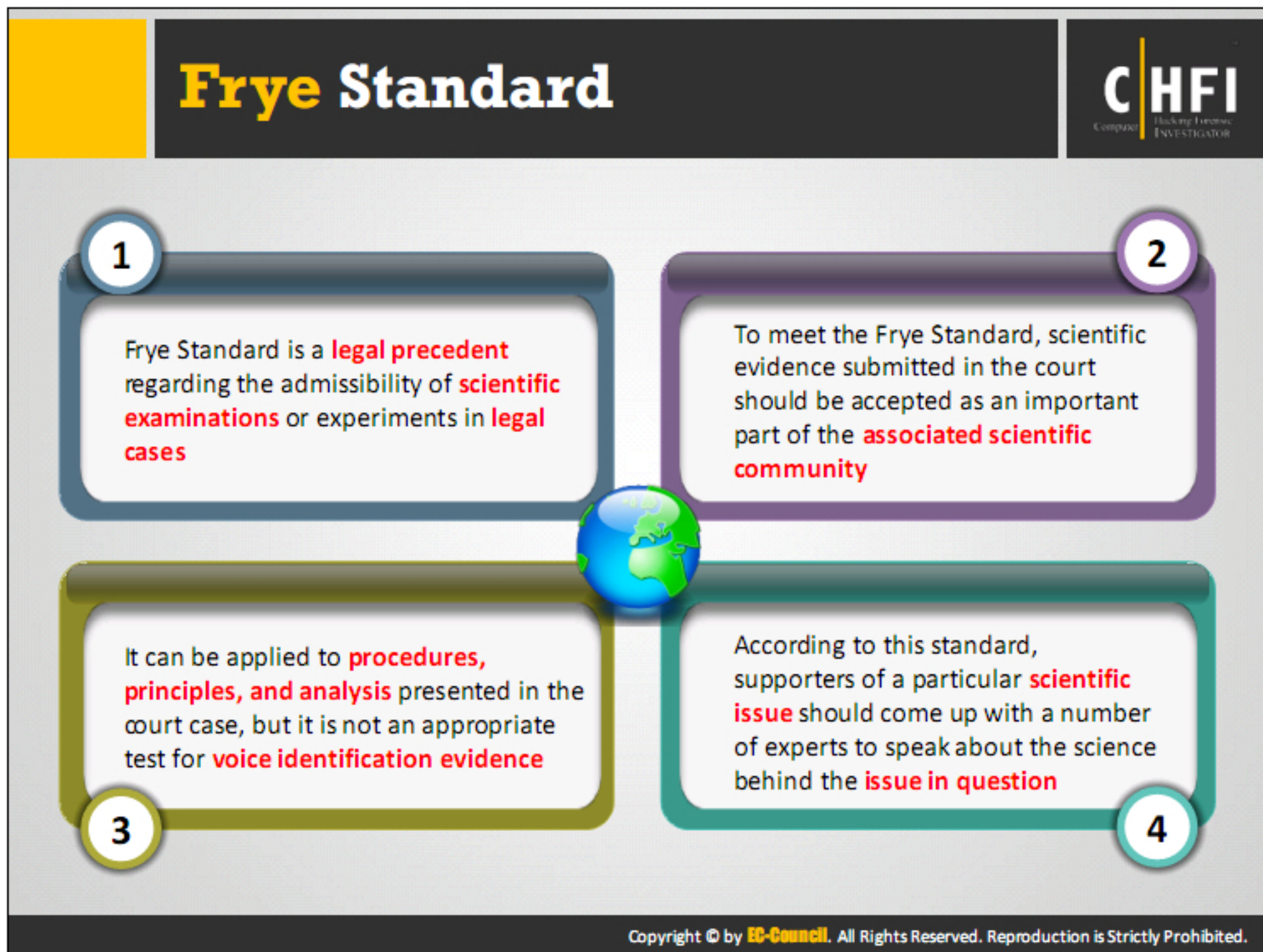
The expert should derive his or her **conclusions using scientific method** in order to consider the evidence reliable

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

The Daubert Standard, a legal act established in 1993 by the Supreme Court of the United States, explains about the rule of evidence regarding the admissibility of the expert witnesses' testimony during the federal legal proceedings. Under this act, the plaintiff or defendant can raise a motion to exclude the unqualified evidence at a jury trial.

In Daubert Standard Act, the Supreme Court passed a rule for federal trial judges to act as “gatekeepers” of scientific evidence. The trial judges should analyze the proffered expert witnesses to decide whether their testimony is both “relevant” and “reliable”. The relevance of a testimony decides whether the expert's evidence applies to the facts of the case or not. The counsel can opt for Daubert motion before or during the trial to stop the presentation of ineffectual evidence to the jury. The expert's testimony should be based on the evidence and facts of the case. An expert witness uses the scientific method of investigation to describe that the evidence is reliable and relevant to the case.





The Frye Standard is a legal act related to the admissibility of scientific examinations or experiments in legal cases. According to this act, any kind of expert opinion based on scientific techniques is admissible, if the technique involved is acceptable by the relevant scientific community. It applies to procedures, principles, and analysis presented in the court cases. Under this act, the supporters of a particular scientific issue should provide a number of experts to speak about the issue in question.

In Daubert 509 U.S. 579 (1994), the Supreme Court conveyed that this act under the Federal Rules of Evidence for accepting expert evidence in federal courts is old-fashioned. However, some states still adhere to the Frye Standard.



## 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**

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


Good expert witnesses must always speak the truth and talk directly to-the-point. They should talk to the jury with full confidence and sincerity in their case, instead of representing like a lawyer only. Experts should change the complicated material into an understandable document to make the general audience understand it easily. A good expert witness should always be well-prepared to answer the opposition's challenges before entering the court room. He/she should be a good observer during jury trials to identify the level of interest among the jury members. Mostly, computer forensic experts should have non-verbal characteristics, i.e.:

- Self-confidence
- Politeness
- Sincerity
- Preparedness
- Awareness
- Relaxed excellence

Forensic experts must never overextend or exaggerate their opinions, as it would mislead the jury members having less knowledge in computers. The experts should develop repetition in their details and descriptions for the jury.



# 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



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

A curriculum vita (CV) of an expert witness is helpful in qualifying his/her testimony by acknowledging his/her previous professional experiences. Keeping an updated CV helps to confirm his/her eligibility along with skills and credentials as an expert witness to assist his/her testimony in the court.

Guidelines for preparing an expert witness's Curriculum Vitae:

- Specify the certifications received, credentials acquired, and any other accomplishments. These will increase the credibility of the expert witness before the jury.
- A testimony log of an expert witness contains all the previous testimonies and results of the case. Enlist all the recent works of the expert witness in the CV.
- Mention the field of expertise and include the books written, if any.
- Specify any professional training received in the resume.
- Give the names of important and high ranking people as referrals in the CV to increase their credibility.
- List the basic and advanced skills of the expert witness.



## 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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.




# 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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

When employed as a technical or expert witness in a computer forensic litigation, he/she must prepare the testimony methodically and carefully. The expert witness must establish the communication before the case goes to trial. While drafting the testimony, the witness must acquire absolute knowledge on all the general concepts related to the case before beginning with evidence processing and examining.

It is important to bear in mind that while working on a case as an expert witness, the investigator is not working for the client but the attorney. Therefore, if he identifies any negative findings, he should immediately communicate with the attorney about the findings and not to the client. Therefore, the expert witness must substantiate his/her findings with proper documentation or cooperate with other computer forensics professionals associated with the attorney while preparing for the testimony.

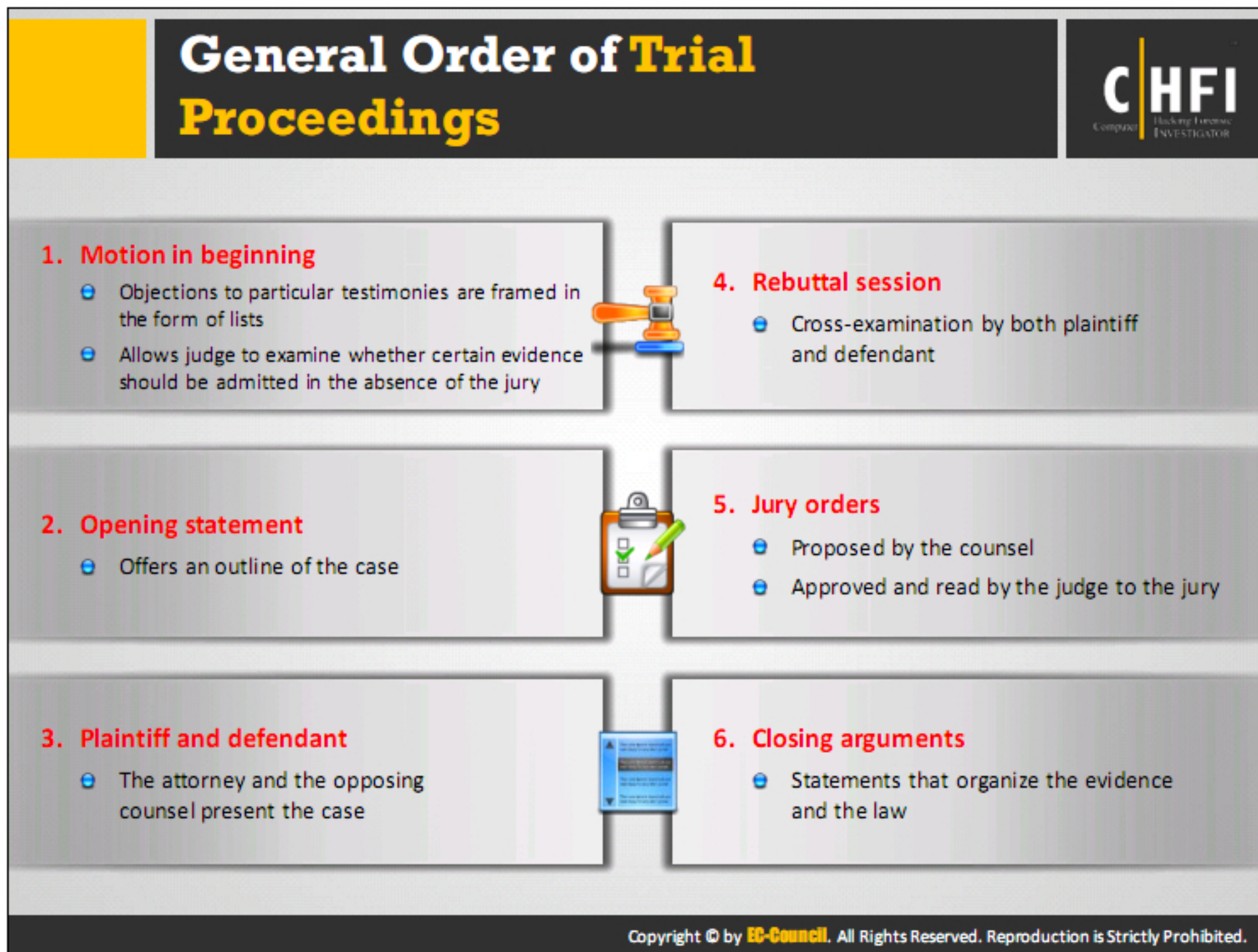




An expert witness must keep certain factors in mind while testifying in the court. He/she should gather sufficient information about the usual procedures during a trial, and must never query his attorney in this regard. Before the expert witness testifies in the court, the attorney will first introduce him/her to the court with high regards and narrate his credentials and accomplishments to establish his/her credibility with the jury. However, the opposing counsel at times would try to damage the reputation of the expert witness by revealing his/her earlier failures as an expert witness, if any.

The attorney then leads the expert witness through the evidence and will explain his role concerning the evidence in an understandable way to the jury, audience, and the opposing counsel followed by cross-examination with the opposing counsel. The opposing counsel will later question the expert witness regarding his description of the evidence and the methods he/she followed while collecting and analyzing the evidence.





The standard order of trial proceedings include:

▪ **Motion in Limine (Motion in Beginning):**

This is a handwritten list of objections to a certain testimony. It is a special hearing on the acceptability of evidence or restriction of evidence. It is usually done a day or two before the beginning of the trial proceedings. This allows the judge to determine if the evidence should be allowed without the jury's presence.

▪ **Opening Statement:**

An opening statement is important because it offers an outline of the case.

▪ **Plaintiff and Defendant:**

A plaintiff is a person who initiates the lawsuit, claiming for damages; whereas the defendant is the person who is answerable to the plaintiff's complaints or claims. The attorney and the opposing counsel presents the case, explains what, when, where, and how it happened.

▪ **Rebuttal Session:**

The rebuttal session is the cross-examination of the expert witness by both the plaintiff and the defendant.



- **Jury Orders:**

The judge educates the jury about the law points related to the case. They can be presented either before or after the closing statements. These are intended to assist the jury with the application of certain specific laws to the details involved in the case, which is then read and approved by the jury.

- **Closing Arguments:**

After the presentation of all the evidence, both the plaintiff and defendant have the chance to present the summarized closing statements of the case. The attorney and the opposing counsel can suggest solutions for the case but must leave the verdict to be decided by the jury.



## General Ethics While Testifying



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

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


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

There are certain ethics that the expert witness has to follow while presenting testimony to any court or an attorney. They are as follows:

- Be professional, polite, and sincere to any attorney or the court.
- Show an open physical and psychological attitude to the jurors.
- Maintain a steady body expression (that is, with a balanced stance and without revealing any nervousness).
- Be aware of the possible rebuttal questions, especially from the opposing counsel and be ready with the necessary preparations for such questions.
- Always be enthusiastic while giving testimony.
- Always pay a compliment to the jury.
- Keep the jury interested in the testimony, and do not sound monotonous and dull.
- Avoid leaning, develop self-confidence and create personal space with a winning professional style in the courtroom.
- Maintaining visual control is important in the courtroom.
- Show an interest in explaining procedures, listening, and communicating objectivity.



## 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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

The expert witness must make graphical demonstrations such as tables, charts, and pie diagrams that will illustrate and elucidate the findings. It will also make the presentation interesting.

An expert witness must make use of a pointer to stress the specific areas that will enhance the testimony. It is another good practice to make smaller photocopies of demonstrations for each juror, thus enabling them to see the demonstrations clearly.

The expert witness should also explain both the hardware and software mechanisms to the jury by using diagrammatic representations and relating evidence to the case.






Before presenting the testimony, the expert witness must have a clear picture about the jury. The expert witness should make it a habit of using examples that are relevant to the descriptions in the testimony.

It is the duty of the expert witness to make a list of crucial questions, which will help the attorney to understand the testimony during the trial. It will also help in reviewing or making any corrections to improve the presentation of the testimony and avoid possible problems during the trial proceedings.

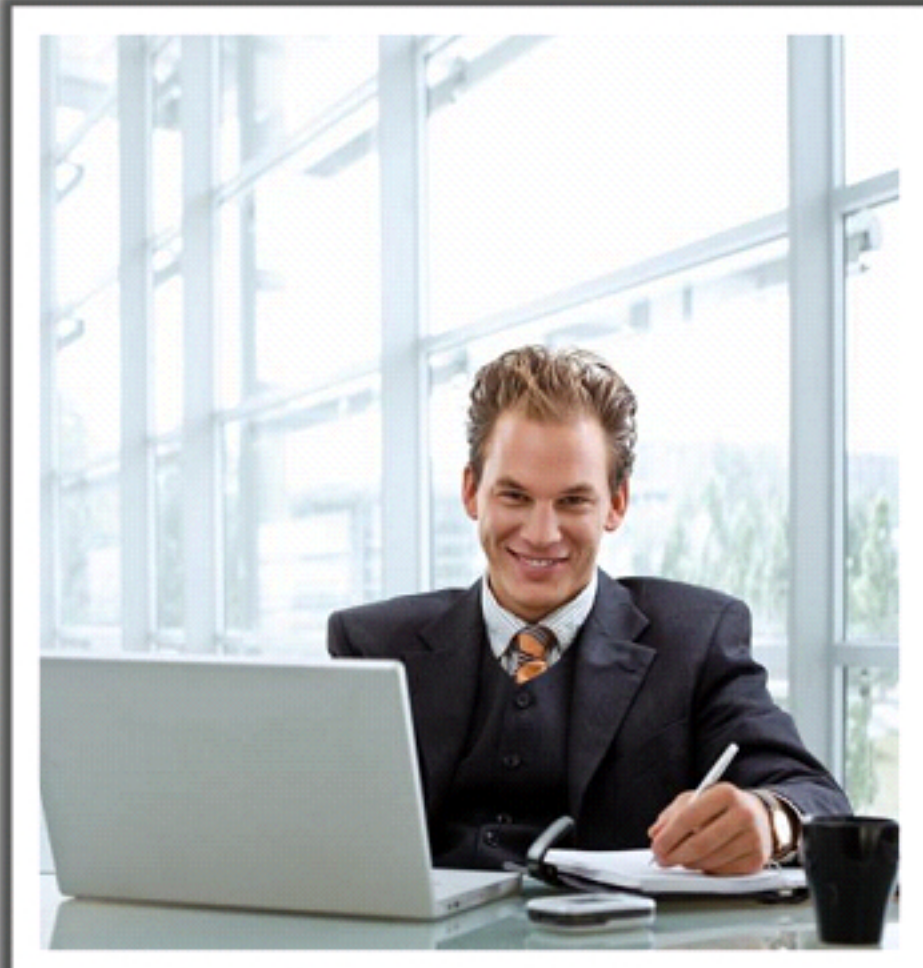
In case of first-time appearance in a trial, an expert witness should prepare a draft testimony and work with the attorney to acquire the right language that will effectively communicate the message to the jury. After the testimony is over, the attorney will again call the expert witness to evaluate his work and update the testimony in his curriculum vitae or record him/her as a rebuttal witness.



# 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



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

The expert witness employed by an attorney must be a neutral witness. He must clearly state his opinion and outline his boundaries of knowledge and ethics, if required. He must use graphics for the validation of any issues in business lawsuits to enhance the testimony.

While preparing a summarized case outline for the attorney, he should make sure that the document is understandable to the attorney. Therefore, the expert witness must acquire a clear picture of how to present the evidence in support of his attorney in the court.


He/she must recheck and synchronize his testimony with other experts. The attorney should also be spared some time to ensure that he is aware of all the facts in the expert's testimony or opinion.

The expert witness must meet the paralegal to acquire a general idea about the court of law and co-work with his attorney to guide him/her about all the technical terms used in his testimony.

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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


Direct examination constitutes an important part of the testimony at a trial, as it offers a clear overview of all the findings. Cross-examination may not be that crucial, even though the opposing counsel may attempt to discredit the expert witness. As a result of which, most of the cases never make it to the court. Under these circumstances, the expert witness must provide direct testimony when he/she testifies on behalf of the attorney who has employed him/her.

The expert witness must provide a lucid overview of all of the case findings. While giving testimony, he/she must affirm her background, qualifications, and credentials to state his/her importance in the present case. She must design a systematic and easy-to-follow plan for explaining her evidence collection methods. The expert witness must find the point of balance between technical language and amateur language for explaining the complex matters. The expert witness's speech should match up to the educational level of the jury.

The expert witness must provide answers when questioned by the opposing counsel, and thus, the testimony should be prepared accordingly in association with his attorney. The attorney guides the expert regarding the precise wording and language that are used while presenting the testimony. It is not wise to provide information to an opposing counsel voluntarily. If the opposing counsel asks something irrelevant to the case, an expert witness should not offer guesses. The expert witness must always use his/her words and phrases while answering the questions by the opposing counsel. The strategy for a successful direct examination is to continue presenting oneself to the jury, even if the opposing counsel attempts to discredit. Speak slowly, as it is the best tactic against problematic questions. Turn towards the jury slowly while giving your response; this allows you to maintain control over the opposing counsel.



## 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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

The expert witness must face the rebuttal session from the opposing counsel after presenting evidence and establishing credentials. The opposing counsel can ask questions about the presented evidence and testimony in a process known as cross-examination.

The expert witness must never offer any guesses but simply deny of knowing anything irrelevant to the case. Avoid using words having additional meanings as they can prove as an advantage to the opposing counsel.

Although the judge disapproves interruptions, the opposing counsel uses general strategies to stop an expert witness from answering questions during cross-examination for which he/she should be ready to face. Certain questions may have contradictory answers, so the expert witness must be aware of it.

The best offense as well as defense against upsetting questions is to be calm and patient with answering them. The expert witness must turn towards the jury while giving answers. Even if the opposing counsel makes the expert witness turn away from the jury, he must take his time while answering the question by turning toward the jury. This will enable him to maintain control over the opposing attorney.

Apart from the above, an expert witness should practice the following:


- Keep vigorous conduct and use energetic speech.
- Avoid feeling stressed and losing control.
- State background and qualifications.



- Balance the language.
- Practice testifying.
- Be fair.
- Avoid ambiguity.



## 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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

The lesser and slower a witness speaks, the more the opposing counsel control over a sneaky cross-examination. When a cross-examiner tries to confuse the witness, the opponent (cross-examiner) faces trouble while trying to avoid word to word answers by the witness, who adheres to the facts.

In case a cross-examiner asks for a YES/NO question during a trial, the best way to deal with it show your inability to answer in an incomplete manner, as a result of which he/she can be saved from a tuff situation. For instance, the witness can say that “I can understand that you are asking for a ‘yes or no’ answer in this situation, and I could answer you in that way, but by doing so the answer would be an incomplete answer, and I don’t want to mislead you or the court.”

It is better to answer the questions during a trial in own way or style.



**Deposition**

**CHFI**  
Computer Hacking Forensic Investigator

- 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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

A deposition is a question and answer session in which both the attorney and the opposing counsel are present and are involved in the cross-examination of a witness. Generally, the opposing counsel asks questions while deposing and a reporter records the testimony taken under oath, which is admissible at trial.

Even though under an informal atmosphere, an expert witness must maintain professionalism during a trial. Usually, the attorney informs the expert witness that the opposing counsel wishes to take a deposition, and the attorney's office is the best location for conducting the deposition.

The purpose of a deposition is to identify the facts and acquire evidence of the investigation. It is a golden chance for the opposing counsel to ask questions to the expert witness to learn about the evidence and to cross-examine. It will help the expert witness to substantiate the testimony and focus on the facts and issues as well as help the attorney to evaluate the case for trial.

### Deposition vs. Trial



A deposition is different from testifying at trial, as there is no jury or judge during the session. The opposing counsel asks questions in the presence of the attorney.

In general, the procedural rules during examination are direct examination, cross-examination, and redirect examination. These rules are different during a deposition, however the opposing counsel asks question and allows cross-examination of the expert witness for few important questions.



## Guidelines to Testify at a Deposition



- 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** 

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

There are certain guidelines that should be followed to testify during the deposition. The expert witness should consider that his/her deposition is under oath, and the court can use the testimony to charge the accused during a trial, hence the testimony should be error-free. An expert witness must be aware of all the facts in the case and should convey a calm, relaxed, and professional appearance during the deposition.

The expert witness must review her documentation and organize it in chronological order. The expert witness must never forget to review her curriculum vitae before going for a deposition. If asked, he/she must explain to the opposing counsel about his/her educational background and other qualifications.

The expert witness should understand every point before giving replies to the questions. On being unable to understand, he/she should immediately ask the opposing counsel to repeat the question or describe it in another way to clearly understand it before answering. The expert should have knowledge on leading or repetitive questions.



# 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



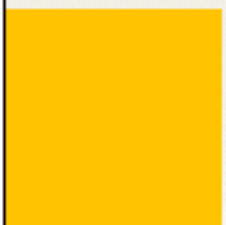
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Media reporters are the people who look for scandalous or controversial quotes. Therefore, the expert witness must avoid any communication with the media when a case is on trial. The expert witness must refer them to his/her attorney, if asked for information.


The expert witness may need to consult the attorney about what to tell the reporters, if required. The expert witness must always record interviews with the reporters, as it can be vital if the reporters misquote the expert witness in the news.

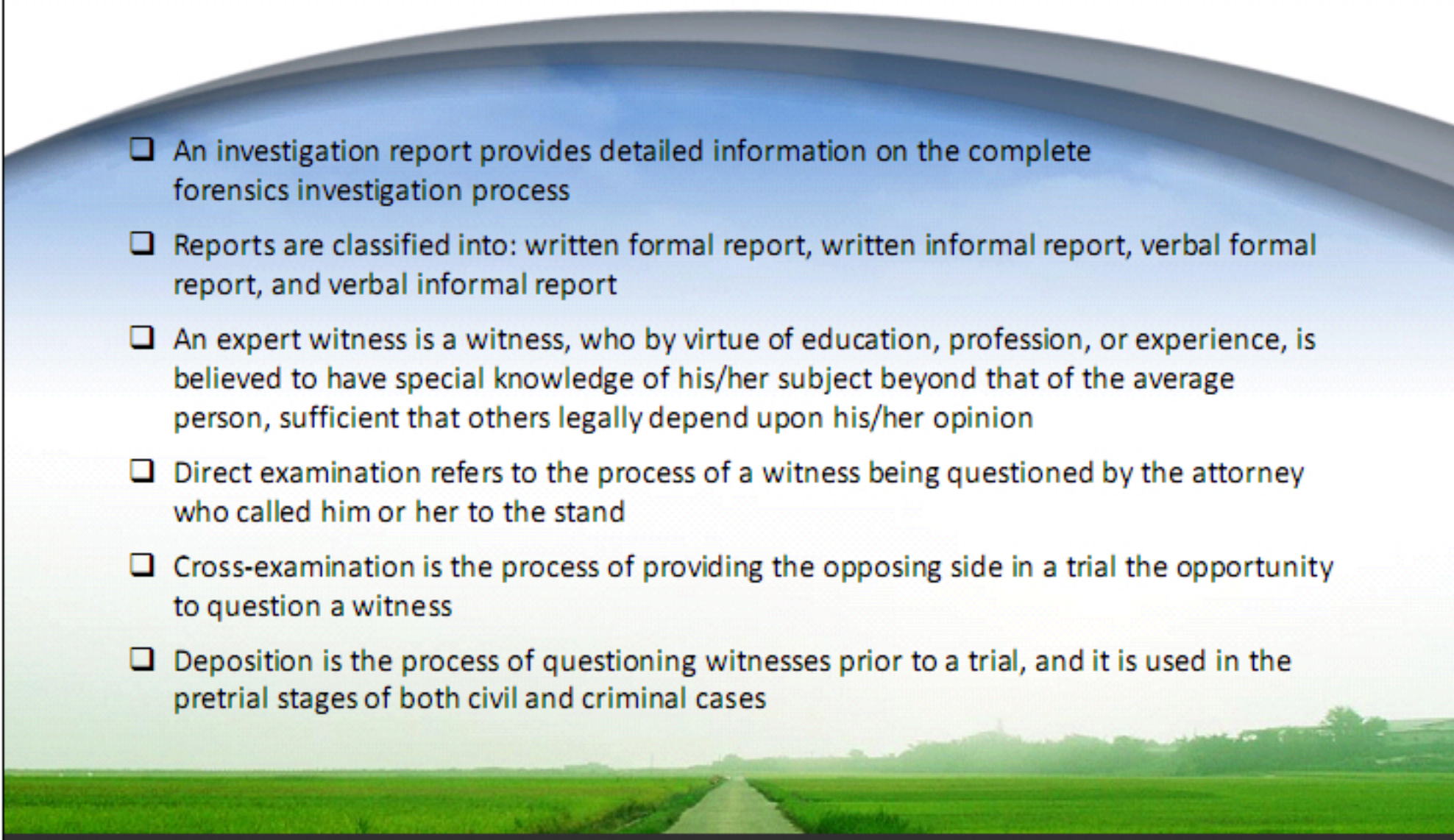
Using the phrase “no comment” could attract more attention than avoiding reporters. The expert witness must be careful about disclosing information to the reporters. The expert witness should refrain from answering anything to the reporters if he/she is not confident about. The simple reason behind this act is to avoid circulate any wrong information that can harm the case. The comments also create a record that can be used against the expert witness during future testimonies.





# 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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

This module discusses the process of reporting an evidence analysis in the court of law, selection, behavior and job roles of expert witnesses, guidelines for writing reports, standards used to choose expert witnesses, and the process of testifying during examination.