Investigative Reports, Expert Witness and Cyber Regulations

MODULE 20

Contents

Investigative Reports, Expert Witness and Cyber Regulations

19.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Know the importance of forensic reports and expert witness.
- Know the legal aspects in computing and cyber laws in India and abroad.
- Know the basic laws in IT Act of India.
- Categorize the basic offences in IT Act and amendments.
- Prepare a forensics report.

19.2 INTRODUCTION

VIDEO LECTURE

One of the most important considerations that a Forensic investigator needs to make while investigating is how to render and communicate the information gathered to the intended audience. The investigator needs to have a best approach of rendering or reporting the findings in a manner that would be categorical, technically sound and yet easily readable and understandable. A good technical report would facilitate the judicial process. A poor technical

report would hamper the process and at many times induces lots of ambiguities which can lead to the acquittal of the culprit.

As in [5] Digital forensic reports can be produced for investigative purposes, separately from reports designed for litigation or electronic discovery. Oftentimes, E-Investigations reports on facts for internal review and investigation. Who used this laptop and for what purpose? Who hacked the server? Was the hacker based inside our organization or did the attack come from outside the network?

An expert witness is a very powerful source of evidence in court. Reports on data electronically discovered by computer forensics methods are important because they provide strong evidence in court documents and in overall analysis in an active lawsuit or settlement. An expert witness is one who allegedly has specialized knowledge relevant to the matter of interest, which knowledge purportedly helps to either make sense of other evidence, including other testimony, documentary evidence or physical evidence (e.g., a fingerprint). An expert witness may or may not also be a percipient witness, as in a doctor or may or may not have treated the victim of an accident or crime. In a court proceeding, a witness may be called (requested to testify) by either the prosecution or the defense. The side that calls the witness first asks questions, in what is called direct examination. The opposing side then may ask their own questions in what is called cross-examination. In some cases, redirect examination may then be used by the side that called the witness, but usually only to contradict specific testimony from the cross-examination. An expert report is a study written by one or more authorities that states findings and offers opinions.

In law, expert reports are generated by expert witnesses and investigators offering their opinions on points of controversy in a legal case, and are typically sponsored by one side or the other in litigation, in order to support that party's claims. The reports state facts, discuss details, explain reasoning, and justify the experts' conclusions and opinions.

19.3 REPORT PREPARATION

19.3.1 Gathering the data

It is highly important that the investigator has a right approach and proper planning with perspective of the case and the report that he/she is going to furnish after all findings being made. The investigator should have a priori view or idea about what form he is going to use while presenting. The right form of report would enhance the acceptability and adaptability of the audience towards right direction in the case. Documentation should be disciplined and organized. Also,this well prepared approach is essential to successful forensic technical writing. Every aspect should be well written so that it is easily understandable to all. It is advised not to use too many shortcuts or short hands as it can bring you into wrong foot many times while comprehending and can kill lot of efforts.Precise, clear and an explanative approach of writing can avoid lots of confusion to either you or the audience at a later stage. As suggested in [sans] we must be disciplined and the approach involves documenting

everything elaborately as we move forward in the case investigation and findings. Also we need to keep in mind the representation of the data and findings in the final report. Thus, any need for additional forensic data will be revealed before the forensic program is completed.

19.3.2 Analyzing the results

The analysis of the result involves following steps:

a. Assumptive conclusions for lead
b. Expert report and opinion
c. Conclusive opinion
d. Data consistency and labeling
e. Hash records of the findings.

Analyzing the results is probably the most difficult because here we need to have a thorough understanding about the point and opinion that we intend to give and the point or aspects that the audience as well as the case requires. This stage overlaps the gathering data stage in the beginning parts, the initial analysis will guide us further and lead us to newer approach or ideas, thus newer set of findings and details might be required. (i.e. data analysis should begin as the data are collected). During the analysis and data review, conclusions should be drawn because the conclusions are the reason for the report and the basis for the technical report preparation. However, we must be careful while drawing conclusions. A conclusion with very few supportive data can lead to incorrectness. The incorrect conclusions are that they can create a potential for "reasonable" doubt in the courtroom. Therefore, it is best to document the conclusions in this phase (Analyzing the Results), since most of the data has already been gathered. Once the conclusions are drawn, it is advisable to list them in an order of importance with highest important conclusion first and so on.

A report offering a conclusion (an opinion) is referred to as an *expert report*. The investigator from law enforcement agencies is generally trained to merely state the facts in their reports rather giving conclusions. Once the case goes under trial a forensic analyst will be called to provide valuable suggestions. The technical witness or the forensic analyst will provide facts as found in the forensic investigation. The analyst will and can comment on the methodologies of the collection of the evidence. The forensic analyst does not offer conclusions, only the facts. However, an expert witness, (which can be another forensic analyst) can have opinions and conclusions about what was found as evidence. The opinions and conclusions are based on experience and the facts found during the forensic investigation and examination of the data obtained. Forensic analysts are usually requested to give an opinion in court about the evidences and the conclusions that can be drawn from them. In most cases, the forensic analyst's professional opinion about a case is the most useful item in any case.

It is also very important to keep data in a consistent form. i.e the records must be referenced properly with proper labels assigned to every item. Thus, referring these items using labels will always help the reader to be consistent in their understanding.

Finally, we need to create MD5 hashes of the collected data/evidences and record the MD5 hashes as metadata for every file so that they can be cited in the forensic report. Creating MD5

hashes ensures the integrity of the collected data and it generates a good deal of confidence among the readers about the manner in which the investigation is being handled.

19.3.3 Outlining and organizing the report

The report outlines need to be adhered to and the subject lines under each outline have to be addresses with proper entries and supportive write-ups. Many a times the whole case goes under confusion and jeopardy if an un-experienced forensic analyst makes a very mediocre report of the findings. An unclear and improper report can create lot of confusion leading to the loss while claiming conclusions and while performing act reconstruction. In the above two phases we needed to concentrate on what results have to be collected and reported (Gathering data and Analysis phase). In the outline phase we need to concentrate on how the results be presented so that the conclusions can be drawn and believed into. We suggests an initial template of the report and the investigator or experts can modify or adjust this according to their need. The outlines of this template are:

a. Executive Summary: Contains mainly the background of the investigation like, who authorized the forensic investigation, description of why a forensic examination of computer media was necessary, give a listing of what significant findings were found, signature block for the examiner(s) who performed the investigation etc. information of all people involved in the investigation along with important dates of pertinent communications are also included.
b. Objectives: All the tasks of the investigation are outlined as well as a proper list of objectives as decided for the investigation needs to be kept here.
c. Computer Evidence Analyzed: All the evidences collected and interpreted are introduced in this section. Better way is to tabulate the evidences in form of evidence, date of collection, interpretation, expert opinion etc.
d. Relevant Findings: A summary of the findings of value are included in this section. This is the conclusions and opinions of the forensic analyst. This section tries to put the findings on the table for the reader. The reader can get an idea about what are results drawn from the evidences analyzed. It is advised to keep them in an order of increasing importance or relevance for the case.
e. Supporting Details: The findings listed in the relevant findings section is supported in a descriptive and in-depth fashion. The descriptive part suggests and emphasizes on how we reached to the conclusions in the previous section. Illustrations such as tables and figures can be very good in this section.
f. Investigative Leads: Many times because of time constraints the investigator could not proceed for further investigation though he might be having important leads. These leads can be very importantly kept in this section. The court or the client can also permit more investigation in a later stage where we can start moving further spontaneously using the leads mentioned here.
g. Subsections: In cases of computing attacks, the readers may want to know the exact attack that was performed, for this we might require analyzing a binary. So, a section “Binary Analysis” may be appropriate to the investigation. Similarly, based on requirement we can add more sub sections in other sections discussed above.

19.3.4 Writing and Revising a Rough Draft

With a logical template for computer forensic reports, writing the rough draft will be much easier. However, because many technical materials are included in forensic reports, we will be having many versions of the report. Hence, we need to keep on writing a rough report and revising it. Mostly we need many readings and revising the report many times before coming to final version. Lastly, we need to format the report in nice appearance using available editors. Figure 1 describes a template for a forensics report.

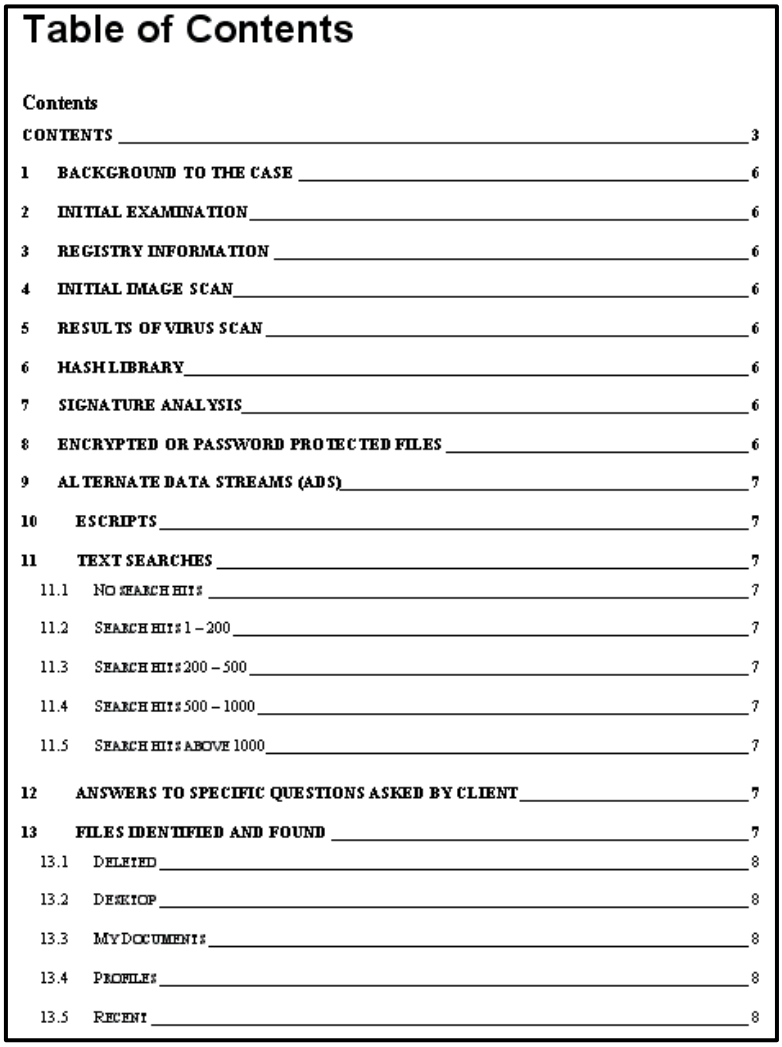

Table of Contents

Contents

Figure 1: A digital forensic Report format[1]

19.4 EXPERT WITNESS

In litigations, experts have become very important. Experts are involved in testimony, consultation and expert opinion. An expert witness, professional witness or judicial expert is a witness, who by virtue of education, training, skill, or experience, is believed to have expertise

[1] Image courtesy: Computer Forensics Report Template - Privacy Resources, computer-forensics.privacyresources.org/forensic-template.htm

and specialized knowledge in a particular subject beyond that of the average person, sufficient that others may officially and legally rely upon the witness's specialized (scientific, technical or other) opinion about an evidence or fact issue within the scope of his expertise, referred to as the expert opinion, as an assistance to the fact-finder. Expert witnesses may also deliver expert evidence about facts from the domain of their expertise. At times, their testimony may be rebutted with a learned treatise, sometimes to the detriment of their reputations.

Typically, experts are relied on for opinions on severity of injury, degree of sanity, cause of failure in a machine or other device, loss of earnings, care costs, and the like. In an intellectual property case and an expert may be shown two music scores, book texts, or circuit boards and asked to ascertain their degree of similarity. In the majority of cases the expert's personal relation to the defendant is considered and irrelevant.

The tribunal itself, or the judge, can in some systems and call upon experts to technically evaluate a certain fact or action, in order to provide the court with a complete knowledge on the fact/action it is judging. The expertise has the legal value of an acquisition of data. The results of these experts are then compared to those by the experts of the parties.

19.4.1 Finding an expert

While finding an expert in an area of investigation we need to be very careful. Lots of people can claim to be experts in the field. It is very vital to look at the experience and expertise of an individual. The affiliation of the individual might be trivial. Apart from ability to retrieve data, a forensic analysis with expert view is more important.

The expert will likely be called to testify in court and to explain what he or she did to the computer and its data. The court will weigh the fact that the expert had a proper training and experience, Least is the affiliation weightage in the minds of the court. The experience of an expert should be specifically in computer forensics, as skill with computers does not necessarily translate to forensic expertise. Proper consulting needs to be done with litigators who have used the expert before or have seen the expert testifying in the court.

19.4.1.1 Testifying v. Consulting

The fact that attorneys use expert witnesses for purpose of testimonies. However, nowadays in cyber cases it is becoming more common to use experts for consultations and not as testifying experts. The non-testifying experts often provide technical as well expert guidance for the attorneys to progress in the line of litigations. There can be many cases where the attorneys/investigators might not have know-how as well as skills to carry out investigation or building the case. Generally, the consulting experts need not be revealed or disclosed since a consultant is not a person having knowledge of any discoverable matter in the case.

19.4.2 What Can (and Can't) an Expert Do?

The primary purpose of testifying experts in a given litigation is to apply scientific or technical expertise to the facts of the case and render relevant opinions that assist the trier of fact in understanding complicated or confusing matters. For instance, a forensic computer scientist

will often testify to a sequence of events that took place on a given computer or network of computers. Without the expert's testimony, the system logs, file system time stamps, and other application metadata that reveal this sequence of events, is extremely difficult to compile and present effectively. Furthermore, the expert's special knowledge allows interpretation of the underlying data that would otherwise be inadmissible. Whereas a forensic computer expert might be able easily to determine a sequence of events that took place on a given computer, it is sometimes much harder to connect those events with a particular individual. What if the computer at issue in a case is accessible by many people? What if the opposing party contends he was not "at the keyboard" when a pertinent event took place? A forensic computer scientist may be able to provide circumstantial evidence regarding the party who appeared to be using the computer. This might be based on the user logged in to the system. It could also be indicated by something like an individual's Web-based email session simultaneously open at the time of other events. Since these events are less tied to the forensic computer scientist's domain of expertise, establishment of the party using aa computer at a given time may need to be established by other means. Bringing in a computer expert for consultation early on can be extremely beneficial. For example, consider the issue of preservation. Every case an attorney is involved with carries with it a duty to preserve potentially relevant evidence. When that evidence is stored on a computer, the method of preservation becomes critical. The first issue an expert can guide you through is to explain the different preservation options available for electronically stored information (ESI). The safest option is generally forensic imaging of the storage media on the relevant computers. Forensic images are bit-for-bit copies of an entire storage medium, including space on the medium that may not currently hold any active files. This differs from simply copying all of the files on a given medium, since the inactive sections of the image may contain portions of previously deleted files, files that are still discoverable. So the first thing your expert can do is save you from falling victim to under-preservation by making an inadequate copy. After the consulting expert has explained the effectiveness of different preservation mechanisms, that expert can then further explain the impact of such preservation on your client's computer systems. For example, large servers may be in near constant use, and require special provisions may need to be made prior to acquiring a forensic image from them. Furthermore, their storage systems may be complicated or very large, which can necessitate a greater time of unavailability. On the other hand, forensic imaging of laptop or desktop computers can often be accomplished in only a few hours, often with little or no interruption to the client's use. These issues are difficult to navigate without a firm grasp of the underlying technology, the specialized knowledge a consulting expert can bring to bear.

19.4.3 Why Use an Expert

An effective attorney knows the facts of the case. That need to grasp the facts of the case is the key reason why an attorney should use an expert. In a trade secret case, the attorney must prove that protected information was unlawfully obtained. How can that be done if the trade secret is a customer list stored in an Excel spreadsheet? An expert can help obtain access to the computing equipment of the opposing party through discovery, and potentially find that the spreadsheet in question was copied to a USB flash drive or burned to a CD-R. Sometimes, the expert can even find that the trade secret spreadsheet was deleted, recover it and provide the time of the deletion.

19.5 LEGAL ASPECTS OF COMPUTING

IT law consists of the law (statutes, regulations, and case law) which governs the digital dissemination of both (digitalized) information and software itself (see history of free and open-source software) and legal aspects of information technology more broadly. IT law covers mainly the digital information (including information security and electronic commerce) aspects and it has been described as "paper laws" for a "paperless environment".

Cyber law or Internet law is a term that encapsulates the legal issues related to use of the Internet. It is less a distinct field of law than intellectual property or contract law, as it is a domain covering many areas of law and regulation. Some leading topics include internet access and usage, privacy, freedom of expression, and jurisdiction.

In various countries, areas of the computing and communication industries are regulated, often strictly by government bodies.

There are laws on censorship versus freedom of expression, rules on public access to government information, and individual access to information held on them by private bodies. There are laws on what data must be retained for law enforcement, and what may not be gathered or retained, for privacy reasons.

In certain circumstances and jurisdictions, computer communications may be used in evidence, and to establish contracts. New methods of tapping and surveillance made possible by computers have wildly differing rules on how they may be used by law enforcement bodies and as evidence in court.

19.5.1 Jurisdiction

Jurisdiction is an aspect of state sovereignty and it refers to judicial, legislative and administrative competence. Although jurisdiction is an aspect of sovereignty, it is not coextensive with it. The laws of a nation may have extraterritorial impact extending the jurisdiction beyond the sovereign and territorial limits of that nation. This is particularly problematic as the medium of the Internet does not explicitly recognize sovereignty and territorial limitations. There is no uniform, international jurisdictional law of universal application, and such questions are generally a matter of conflict of laws, particularly private international law. An example would be where the contents of a web site are legal in one country and illegal in another. In the absence of a uniform jurisdictional code, legal practitioners are generally left with a conflict of law issue.

Another major problem of cyberlaw lies in whether to treat the Internet as if it were physical space (and thus subject to a given jurisdiction's laws) or to act as if the Internet is a world unto itself (and therefore free of such restraints). Those who favor the latter view often feel that government should leave the Internet community to self-regulate. John Perry Barlow, for example, has addressed the governments of the world and stated, "Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We

are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different".

With the internationalism of the Internet, jurisdiction is a much more tricky area than before, and courts in different countries have taken various views on whether they have jurisdiction over items published on the Internet, or business agreements entered into over the Internet. This can cover areas from contract law, trading standards and tax, through rules on unauthorized access, data privacy and spamming to more political areas such as freedom of speech, censorship, libel or sedition.

In practical terms, a user of the Internet is subject to the laws of the state or nation within which he or she goes online. Thus, in the U.S., Jake Baker faced criminal charges for his e-conduct, and numerous users of peer-to-peer file-sharing software were subject to civil lawsuits for copyright infringement. This system runs into conflicts, however, when these suits are international in nature. Simply put, legal conduct in one nation may be decidedly illegal in another. In fact, even different standards concerning the burden of proof in a civil case can cause jurisdictional problems. For example, an American celebrity, claiming to be insulted by an online American magazine, faces a difficult task of winning a lawsuit against that magazine for libel. But if the celebrity has ties, economic or otherwise, to England, he or she can sue for libel in the British court system, where the standard of "libelous speech" is far lower.

19.5.2 Net neutrality

Network neutrality is the principle that all Internet traffic should be treated equally. According to Columbia Law School professor Tim Wu, the best way to explain network neutrality is that a public information network will end up being most useful if all content, sites, and platforms are treated equally. A more detailed proposed definition of technical and service network neutrality suggests that service network neutrality is the adherence to the paradigm that operation of a service at a certain layer is not influenced by any data other than the data interpreted at that layer, and in accordance with the protocol specification for that layer.

19.5.3 Open Internet

The idea of an open Internet is the idea that the full resources of the Internet and means to operate on it are easily accessible to all individuals and companies. This often includes ideas such as net neutrality, open standards, transparency, lack of Internet censorship, and low barriers to entry. The concept of the open Internet is sometimes expressed as an expectation of decentralized technological power, and is seen by some as closely related to open-source software.

Proponents often see net neutrality as an important component of an open Internet, where policies such as equal treatment of data and open web standards allow those on the Internet to easily communicate and conduct business without interference from a third party. A closed Internet refers to the opposite situation, in which established persons, corporations or governments favor certain uses. A closed Internet may have restricted access to necessary web standards, artificially degrade some services, or explicitly filter out content.

As of 2015, India had no laws governing net neutrality and there have been violations of net neutrality principles by some service providers. While the Telecom Regulatory Authority of India (TRAI) guidelines for the Unified Access Service license promote net neutrality, they do not enforce it. The Information Technology Act, 2000 does not prohibit companies from throttling their service in accordance with their business interests. In India, telecom operators and ISPs offering VoIP services have to pay a part of their revenues to the government.

In March 2015, the TRAI released a formal consultation paper on Regulatory Framework for Over-the-top (OTT) services, seeking comments from the public. The consultation paper was criticized for being one sided and having confusing statements. It was condemned by various politicians and internet users. By 24 April 2015, over a million emails had been sent to TRAI demanding net neutrality.

19.5.4 Indian Information Technology Act(IT Act) 2000[6]

An example of information technology law is India's Information Technology Act, 2000, which was substantially amended in 2008. The IT Act, 2000 came into force on 17 October 2000. This Act applies to whole of India, and its provisions also apply to any offense or contravention, committed even outside the territorial jurisdiction of Republic of India, by any person irrespective of his nationality. In order to attract provisions of this Act, such an offence or contravention should involve a computer, computer system, or computer network located in India. The IT Act 2000 provides an extraterritorial applicability to its provisions by virtue of section 1(2) read with section 75. This Act has 90 sections.

India's The Information Technology Act 2000 has tried to assimilate legal principles available in several such laws (relating to information technology) enacted earlier in several other countries, as also various guidelines pertaining to information technology law. The Act gives legal validity to electronic contracts, recognition of electronic signatures. This is a modern legislation which makes acts like hacking, data theft, spreading of virus, identity theft, defamation (sending offensive messages) pornography, child pornography, cyber terrorism, a criminal offence. The Act is supplemented by a number of rules which includes rules for, cyber cafes, electronic service delivery, data security, blocking of websites. It also has rules for observance of due diligence by internet intermediaries (ISP's, network service providers, cyber cafes, etc.). Any person affected by data theft, hacking, spreading of viruses can apply for compensation from Adjudicator appointed under Section 46 as well as file a criminal complaint.

The original Act contained 94 sections, divided in 19 chapters and 4 schedules. The laws apply to the whole of India. Persons of other nationalities can also be indicted under the law, if the crime involves a computer or network located in India.

The Act provides legal framework for electronic governance by giving recognition to electronic records and digital signatures. The formation of Controller of Certifying Authorities was directed by the Act, to regulation issuing of digital signatures. It also defined cybercrimes and

prescribed penalties for them. It also established a Cyber Appellate Tribunal to resolve disputes arising from this new law.

Commission of cybercrime may be divided into three basic groups:

- Individual
- Organization
- Society at Large

The following are the crimes which can be committed against the following groups.

19.5.4.1 Against Individual

- Harassment via Emails
- Cyber Stalking
- Dissemination of obscene material
- Defamation
- Hacking/Cracking
- Indecent Exposure

19.5.4.2 Individual Property

- Computer Vandalism
- Transmitting a Virus
- Network Trespassing
- Unauthorized Control over Computer System
- Hacking/Cracking

19.5.4.3 Against Organization

- Hacking & Cracking
- Possession of unauthorized Information
- Cyber- Terrorism against Government Organization
- Distribution of Pirated Software etc.

19.5.4.4 Against Society at Large

- Pornography
- Polluting the youth through indecent exposure
- Trafficking

The Act also amended various sections of Indian Penal Code, 1860, Indian Evidence Act, 1872, Banker's Book Evidence Act, 1891, and Reserve Bank of India Act, 1934 to make them compliant with new technologies.

19.5.5 Amendments– Indian IT Act (2008)

A major amendment was made in 2008. It introduced the Section 66A which penalized sending of "offensive messages". It also introduced the Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource".

It also introduced penalties for child porn, cyber terrorism and voyeurism. It was passed on 22 December 2008 which any debate in Lok Sabha. The next day it was passed by the Rajya Sabha. It was signed by the President of 5 February 2009. The following are the list of offences and penalties.

Table 1: List of offences and the corresponding penalties

Section	Offence	Description	Penalty
65	Tampering with computer source documents	If a person knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force.	Imprisonment up to three years, or/and with fine up to ₹200,000
66	Hacking with computer system	If a person with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.	Imprisonment up to three years, or/and with fine up to ₹500,000
66B	Receiving stolen computer or communication device	A person receives or retains a computer resource or communication device which is known to be stolen or the person has reason to believe is stolen.	Imprisonment up to three years, or/and with fine up to ₹100,000
66C	Using password of another person	A person fraudulently uses the password, digital signature or	Imprisonment up to three years, or/and with fine up to ₹100,000

		other unique identification of another person.	
66D	Cheating using computer resource	If a person cheats someone using a computer resource or communication.	Imprisonment up to three years, or/and with fine up to ₹100,000
66E	Publishing private images of others	If a person capture, transmits or publishes images of a person's private parts without his/her consent or knowledge.	Imprisonment up to three years, or/and with fine up to ₹200,000
66F	Acts of cyber terrorism	If a person denies access to an authorized personnel to a computer resource, accesses a protected system or introduces contaminant into a system, which the intention of threatening the unity, integrity, sovereignty or security of India, then he commits cyberterrorism.	Imprisonment up to life.
67	Publishing information which is obscene in electronic form.	If a person publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.	Imprisonment up to five years, or/and with fine up to ₹1,000,000
67A	Publishing images containing sexual acts	If a person publishes or transmits images containing a sexually explicit act or conduct.	Imprisonment up to seven years, or/and with fine up to ₹1,000,000
67B	Publishing child porn or predating children online	If a person captures, publishes or transmits images of a child in a sexually explicit act or conduct. If a person induces a child into a	Imprisonment up to five years, or/and with fine up to ₹1,000,000 on first conviction.

		sexual act. A child is defined as anyone under 18.	Imprisonment up to seven years, or/and with fine up to ₹1,000,000on second conviction.
67C	Failure to maintain records	Persons deemed as intermediatory (such as an ISP) must maintain required records for stipulated time. Failure is an offence.	Imprisonment up to three years, or/and with fine.
68	Failure/refusal to comply with orders	The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder. Any person who fails to comply with any such order shall be guilty of an offence.	Imprisonment up to three years, or/and with fine up to ₹200,000
69	Failure/refusal to decrypt data	If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed, must extend all facilities and	Imprisonment up to seven years and possible fine.

		technical assistance to decrypt the information. The subscriber or any person who fails to assist the agency referred is deemed to have committed a crime.	
70	Securing access or attempting to secure access to a protected system	The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system. The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems. If a person who secures access or attempts to secure access to a protected system, then he is committing an offence.	Imprisonment up to ten years, or/and with fine.
71	Misrepresentation	If anyone makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate.	Imprisonment up to three years, or/and with fine up to ₹100,000

19.6 SUMMARY

1. Expert reports are generated by expert witnesses and investigators offering their opinions on points of controversy in a legal case
2. The right form of report would enhance the acceptability and adaptability of the audience towards right direction in the case.
3. A report offering a conclusion (an opinion) is referred to as an expert report. During the analysis and data review, conclusions should be drawn because the conclusions are the reason for the report and the basis for the technical report preparation. However, we must be careful while drawing conclusions.
4. The outlines of a typical expert report can have sections in sequence like; Executive Summary, Objectives, Analysed Computer Evidence, Relevant Findings, Supporting Details, Investigative Leads and other Subsections.
5. We need many reading and revising the report before coming to final version and also we need to format the report in nice appearance using available editors
6. The tribunal itself, or the judge, can in some systems and call upon experts to technically evaluate a certain fact or action, in order to provide the court with a complete knowledge on the fact/action it is judging.
7. An expert witness, professional witness or judicial expert is a witness, who by virtue of education, training, skill, or experience, is believed to have expertise and specialized knowledge in a particular subject beyond that of the average person.
8. Cyber law or Internet law is a term that encapsulates the legal issues related to use of the Internet. In various countries, areas of the computing and communication industries are regulated, often strictly by government bodies.
9. An example of information technology law is India's Information Technology Act, 2000, which was substantially amended in 2008.

19.7 CHECK YOUR PROGRESS

1. Fill in the blanks.

a) An _____ is a very powerful source of evidence in court.
b) A conclusion with very few supportive data can lead to _____.
c) The IT Act, 2000 came into force on _____.
d) _____ contains mainly the background of the investigation.
e) IT Laws has been described as "____" for a "_____".

2. State True or False

a) The IT Act 2000 has 80 sections.
b) The descriptive part of the report suggests and emphasizes on how we reached to the conclusions in the previous section.
c) Without the expert's testimony, the system logs, file system time stamps, and other application metadata that reveal this sequence of events, is difficult to compile and present effectively.

d) An expert witness, professional witness or judicial expert is a witness, who has specialized knowledge in his domain.
e) Network neutrality is the principle that all Internet traffic should have same speed.

19.8 ANSWERS TO CHECK YOUR PROGRESS

1. Fill in the blanks.

a) Expert witness
b) Incorrectness
c) 17 October 2000
d) Executive Summary
e) Paper laws ,paperless environment

2. State True or False

a) False.
b) True.
c) True.
d) True.
e) False.

19.9 FURTHER READINGS

1. Becoming a Forensic Investigator - SANS Institute, https://www.sans.org/reading-room/.../forensics/forensic-investigator-1453.pdf
2. Vivek Sood, Cyber Law Simplified, Tata McGraw-Hill Education, 2008
3. PavanDuggal, Cyberlaw: the Indian perspective, Saakshar Law Publications, 2002
4. Philip J. Candilis, Robert Weinstock, Richard Martinez, Forensic Ethics and the Expert Witness, Springer Science & Business Media, 2007
5. Faust F. Rossi, Eleanor M. Fox, James T. Halverson , Expert Witnesses, American Bar Association.
6. Becoming a Forensic Investigator - SANS Institute, https://www.sans.org/reading-room/.../forensics/forensic-investigator-1453.pdf
7. Computer Forensics Report Template - Privacy Resources, computer-forensics.privacyresources.org/forensic-template.htm.
8. When to Hire a Computer Expert Witness,web.interhack.com/publications/when-to-hire.pdf

19.10 MODEL QUESTIONS

1. Describe the major amendments in the INDIAN IT Act (2008). Describe some offences and the corresponding penalties.
2. Commission of cybercrime may be divided into how many groups? Describe them.
3. What do you mean by net neutrality and open internet?

4. Why the testimonies of the experts are becoming increasingly important these days?
5. Describe the various steps of report preparation in detail.

References, Article Source & Contributors

[1] Expert witness - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Expert_witness

[2] Expert witness, http://einvestigations.com/computer-forensics/expert-witness/

[3] Information Technology Act, 2000 - Wikipedia, https://en.wikipedia.org/wiki/Information_Technology_Act,_2000

[4] Legal aspects of computing - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Legal_aspects_of_computing

[5] Net neutrality - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Net_neutrality

EXPERT PANEL

Dr. Jeetendra Pande, Associate Professor- Computer Science, School of Computer Science & IT, Uttarakhand Open University, Haldwani

Dr. Ajay Prasad, Sr. Associate Professor, University of Petroleum and Energy Studies, Dehradun

Dr. Akashdeep Bharadwaj, Professor, University of Petroleum and Energy Studies, Dehradun

Mr. Sridhar Chandramohan Iyer, Assistant Professor- Universal College of Engineering, Kaman, Vasai, University of Mumbai

Mr. Rishikesh Ojha, Digital Forensics and eDiscovery Expert

Ms. Priyanka Tewari, IT Consultant

Mr. Ketan Joglekar, Assistant Professor, GJ College, Maharastra

Dr. Ashutosh Kumar Bhatt, Associate Professor, Uttarakhand Open University, Haldwani

Dr. Sangram Panigrahi, Assistant Professor, Siksha 'O' Anusandhan, Bhubaneswar

This MOOC has been prepared with the support of