Chapter 2

Legal view of digital evidence

Before developing a model or a theory, it is important to understand the requirements of the domain in which the model or the theory is going to be used. The ultimate purpose of digital forensic analysis is to assist in finding and convicting perpetrators of crime. So, it is important to understand the requirements imposed on the forensic analysis by the legal process. This is the purpose of this chapter.

2.1 Legal concepts

For the benefit of readers unfamiliar with legal theory, this section introduces fundamental legal concepts explaining how disputes are resolved in courts and how evidence is used in this process.

2.1.1 The nature of disputes resolved in courts

Disputes, which are resolved in courts, involve two parties. One party, called *plaintiff* or *prosecutor*, contends that certain events in the past happened, and that under the applicable law they make the other party, called *defendant* or *accused*, obligated to perform some act — e.g. go to prison. The defendant disputes one or more of the factual contentions of the accusing party. If the disputed events constitute violation of substantive law by the accused, the dispute is *criminal*. Otherwise, the dispute is *civil*.

Facts to be proved

To resolve a dispute, the court must first establish necessary facts and then apply the law to the facts to make a decision. Facts that need proof include:

- *facts in issue*, facts on which the disputing parties disagree;
- *circumstantial facts*, whose existence can be used to prove or disprove facts in issue;
- facts that must be proved in order for appropriate law to be applied or for evidence to be admitted into court proceedings.

2.1.2 The nature of legal proof

In court proceedings, facts are proved to the finder of fact[1] by demonstrating evidence of the fact. The proof in court differs from mathematical proof in two important ways:

1. No inference procedure is prescribed for the finder of fact by the law. In [2], the term evidence is defined as "any matter of fact, the effect, tendency, or design of which is to produce a persuasion in the mind of existence or non-existence of some other matter of fact". Thus, the finder of fact is expected to use common sense. An advantage of this arrangement is that all sorts of evidence can be considered by the court. A disadvantage is that the way evidence is *presented* has impact on the inferences made from that evidence.

[1] The finder of fact is either the jury or the judge, depending on the type of the trial.

2. Court is limited in time and resources when resolving a dispute. As a result, court can accept a highly probable, but not necessarily correct, hypothesis to be true[2]. It means that each of the disputing parties adopts a strategy aimed at discovery and interpretation of evidence to prove its own position, disprove the other party's position, or both. Neither party is interested in the discovery of the full truth.

2.1.3 Standards of proof

The degree of certainty that must be achieved by the finder of fact in order to accept the truth of a fact is termed the *standard of proof.* The two major standards are the *criminal standard* and the *civil standard.* Criminal standard is generally used in criminal proceedings, and civil standard is generally used in civil proceedings.

According to the criminal standard, the finder of fact must be persuaded "beyond reasonable doubt" to accept the truth of a fact.

According to the civil standard, the fact is considered to be true if the evidence for the fact outweighs evidence against the fact.

2.1.4 Presumptions of fact

In legal proof the conclusion about truth or falsity of a fact is almost never final. After a fact is proved, it is *presumed* true. If new evidence is discovered which clearly disproves a previously proved fact, the finder of fact must change its opinion about that fact.

For most facts nothing is presumed about them until they are proved. Some facts, however, are presumed true from the start of court proceedings. The law defines which facts are to be presumed true. For example, in criminal disputes

[2] In science, the process of determining correctness or falsity of a theory can go on indefinitely

the accused is presumed innocent until the prosecutor proves otherwise.

2.1.5 Burden of proof

When a fact is being proved, one of the disputing parties carries the *burden of proof*. That party is responsible for persuading the finder of fact into believing that the fact is true. Which party carries the burden of proof depends on the type of dispute and on the legislation applied in the case. In general, the party that proclaims existence of a fact carries the burden of proving it.

2.1.6 Characteristics of evidence

Two main characteristics of evidence are relevance and weight. The term *relevance* refers to the relationship between evidence and the fact being proved. A piece of evidence is relevant when it makes the fact in question more or less probable. If the evidence does not change probability of the fact, the evidence is irrelevant. The *weight* of evidence is the measure of how much the evidence changes the probability of the fact.

The relevance and weight of a piece of evidence are determined by the court on the basis of general knowledge.

Admissibility of evidence

In countries with common law tradition each piece of evidence must pass admissibility test before it can be used in court.

The admissibility test is specified by the law. The admissibility of a piece of evidence depends on the type of dispute and on how the evidence is related to the fact being proved. In general, a piece of evidence is inadmissible if has no relevance to the fact being proved. However, a relevant and weighty item of evidence may be excluded because it violates some formal rule.

Evidential integrity

The weight of a piece of evidence depends on how probable the evidence is if the fact is true and on how less probable it is if the fact is false. A piece of evidence that is equally likely to originate from tampering as from existence of the fact being proved, has no weight in proving the fact.

To preserve the weight of evidence, the possibility of tampering with it must be minimised. This is called preserving *evidential integrity.* Evidential integrity is preserved by handling and examining evidence in ways that do not change it. All handling and examination must be performed or witnessed by individuals to whom the finder of fact trusts to be objective and competent to do so.

Proving evidence integrity is usually a part of admissibility test. To prove that no tampering occurred, the history of each piece of evidence is recorded from the moment it is seized to the moment it is presented in court. This record is called the *chain of custody.*

2.1.7 Classes of evidence

Legal evidence can be classified in several ways. In jurisprudence, evidence is classified according to what type of fact it proves, what form it takes, and what law governs its use. The major classes of legal evidence defined in [2] are as follows.

- *Circumstantial evidence* is any evidence that proves not a fact in issue, but some other (circumstantial) fact, which can be used by the finder of fact to infer existence or non-existence of a fact in issue.

- *Direct evidence* is a first hand evidence of a fact. It is usually a testimony of a participant of the disputed events, who perceived the fact with one of the five senses.

- *Hearsay.* The rule against hearsay says that any assertion of fact other than one made by a person while giving oral evidence in the court proceedings is inadmissible as evidence of any fact asserted. Thus, any out of court statements including photographs, video tapes, and digital information produced and stored by a computer are hearsay and cannot be used as evidence. There are, however, multiple exceptions to the hearsay rule, which allow admission of hearsay coming from sufficiently reliable sources. In particular, data recorded by a machine in the normal course of operation is usually admissible as evidence of the recorded events if there was no human intervention in the recording process.
- *Documentary evidence* is admissible hearsay in form of documents, photographs, tapes, etc. presented to the court as evidence of contents.
- *Real evidence* refers to items of evidence which are presented for examination by the senses of the finder of fact (e.g. knife covered in blood).
- *Testimonial evidence* is any oral or written statement made on oath or affirmation for the purpose of legal proceedings.
- *Expert evidence* is a special form of testimonial evidence, in which an expert gives evidence of his opinion. Expert evidence is required when the matters in question are outside of the competence of the finder of fact. When expert is called to give evidence, it must be established that he or she is competent to do so.

The evidence is also classified according to the function it performs in the trial. It is customary to identify

- *Inculpatory evidence* that proves the guilt of a party,
- *Exculpatory evidence* that proves the innocence of a party,
- Evidence that proves or disproves integrity of a piece of evidence.

2.2 Forensic science and evidence

The term *forensic science* refers to "the application of scientific techniques to legal investigations" [29]. There are two main reasons for use of science in court.

1. A scientific fact may be a fact in issue. This happens, for example, when a new drug is claimed to be dangerous.

2. Science can be used at investigation stage to obtain objective, *circumstantial* evidence which is based on logic and scientific theory rather than on common sense. This application of science takes form of specialised techniques such as DNA profiling, or blood group analysis.

In either case, forensic analysis is likely to be outside of the competence of the finder of fact. Thus, forensic evidence is a special case of expert evidence.

2.2.1 Requirements to scientific evidence

When scientific evidence is given, it is possible that a qualified expert may have based his findings on a novel scientific theory that lacks sufficient experimental support to draw reliable conclusions.

The United States has a body of legislation specifically addressing this problem. The article 702 of the federal rules of evidence requires from the trial judge to establish with respect to any scientific testimony submitted to a federal court in the U.S. whether the reasoning or methodology underlying the testimony is scientifically valid.

The U.S. Supreme Court in the Daubert vs. Merrill Dow Pharmaceuticals, Inc. case [30] specified a number of non-mandatory, non-exclusive criteria for determining scientific validity of the reasoning underlying the expert testimony. In Supreme Court's opinion, the key question to answer is

- whether the theory or technique employed by the expert can be (and has been) tested.

In addition, the judge should consider

- the known or potential rate of error associated with the theory or technique, and
- the existence and maintenance of standards controlling the technique's operation.

Finally, the judge may consider

- whether the theory or technique have been subjected to peer review and publication, and
- whether the theory or technique enjoys widespread acceptance,

because "a *known* technique that has been able to attract only minimal support within the community, may properly be viewed with skepticism [30]."

In 1999, the U.S. Supreme Court ruled on Kumho Tire Co. vs. Carmichael case [52] that the Daubert criteria *may* be used by the trial judge when admitting any expert testimony.

Although not all countries with the common law tradition have analogues of Daubert criteria, the law generally requires that the expert findings must be based on a well established knowledge or theory.

2.3 Digital evidence

Digital evidence is defined by [81] as "any information of probative value that is either stored or transmitted in a digital form". It includes files stored on computer hard drive, digital video, digital audio, network packets transmitted over local area network, etc.

Depending on what facts the digital evidence is supposed to prove, it can fall into different classes of evidence.

- Digital images or software presented in court to prove the fact of *possession* are real evidence.

- E-mail messages presented as proof of their content are documentary evidence.
- Log files, file time stamps, all sorts of system information used to reconstruct sequence of events are circumstantial evidence.
- Digital documents notarised using digital signature may fall into testimony category[3].

The use of digital information in legal disputes is complicated by a number of technical problems, which reduce weight of computer based evidence or even make it irrelevant. The following subsections introduce each of the problems.

2.3.1 Anonymity of digital information

Digital information generated, stored, and transmitted between computing devices does not bear any physical imprints connecting it to the individual who caused its generation. Unless the information is a recording from external sensors capable of perceiving individualising characteristics (e.g. speech recording, video, or photographs) or was generated using some secret known to a single person (e.g. digital signature) there is nothing *intrinsic* linking digits to a person.

2.3.2 Context of digital information

Digital information is a sequence of digits encoding some knowledge. The encoding, and hence the meaning of digits is determined by the context in which the information is produced and used. Before inferences can be made, the context determining the meaning of information must be clarified.

[3] provided the law of the country permits use of digitally signed documents as a substitute to paper based documents

If the information is produced for use by the third party devices or computer programs, it must follow some documented format. The format prescribes how the information is to be interpreted.

If the information is produced for internal use by some device or computer program, there is usually no publicly available description of how to interpret it. If this is the case, the investigator must understand the internal operation of the device or program to interpret the information.

2.3.3 Automated interpretation of digital information

Manual interpretation of the digital information can be extremely labor consuming (consider manual reconstruction of a picture stored in a file) or even impossible – how would one manually interpret recorded speech? The use of automated tools for interpreting digital information is unavoidable. A precondition for use of any such tool is the assurance that the tool gives correct interpretation of the information.

2.3.4 Danger of damaged information

Like many other types of evidential material, digital information stored on magnetic and optical media can be damaged by a variety of causes. Dampness, strong magnetic fields, ultraviolet radiation, and incompetent use of storage devices and examination tools are some of the possibilities. But unlike other types of evidential material, digital information is highly sensitive to minor changes. A single bit change may cause dramatic change in its interpretation. At the same time, minor changes may be very hard to detect in a large quantity of digital information, particularly if the damaged information has valid interpretation. To minimise the impact of this problem, typical storage devices use checksumming and similar means allowing them to reasonably reliably detect accidental information damage.

2.4 Summary

This chapter reviewed major legal concepts and terms surrounding the use of digital information in litigation. The notions of legal dispute, proof, and evidence have been introduced. Classes and properties of evidence have been reviewed, as well as specific requirements to expert evidence. A definition of digital evidence has been given, and difficulties associated with its use in litigation have been discussed.

Note that from legal point of view digital evidence is not very different from other forms of evidence. Like any other form of evidence, it has to be relevant to the dispute, and it has to pass admissibility test[4]. The latter usually includes demonstration of evidence integrity (i.e. proving that the evidence has not been tampered with).

Note also that advanced analysis of digital evidence, such as event reconstruction, often requires specialist knowledge and, therefore, falls into the category of expert evidence. As expert evidence, it may have to pass Daubert criteria or similar admissibility test that verifies that its analysis methodology is scientifically valid. Thus, passing admissibility test for expert evidence, is an important requirement for event reconstruction in digital investigations.

Finally, note that admissibility of the event reconstruction *methodology* is different from admissibility of the *information* used in the event reconstruction process. Since the focus of this dissertation is on the methodology, the admissibility of the information is basically ignored. More precisely, the rest of this dissertation assumes that any information used in the event reconstruction process has already been proved admissible.

[4] in countries with common law tradition