**Admissibility of Evidence**

The concept of admissibility is a simple one. Courts need to determine whether evidence is “**safe**” to put before a jury and will help provide a solid foundation for making a decision in the case. **In practice**, admissibility is a set of legal tests carried out by a judge to assess an item of evidence. This assessment process can become complicated, particularly when the evidence was not handled properly or has traits that make it **less reliable or more prejudicial**.

Some jurisdictions have rules relating to admissibility that are formal and sometimes inflexible, while other jurisdictions give judges more discretion.

**Example: Admissibility**

In 2007, a case in Maryland dealt with the admissibility of digital evidence specifically and provided general guidelines for reaching a decision.

[I]t can be expected that electronic evidence will constitute much, if not most, of the evidence used in future motions practice or at trial, [and] counsel should know how to get it right on the first try **[Lorraine v. Markel Am. Ins. Co., 2007 WL 1300739 (D. Md., May 4, 2007) ].**

**In this legal case**, both parties offered copies of e-mail messages that could not be authenticated properly. The magistrate judge would not admit the e-mail messages, noting that unauthenticated e-mails are a form of computer-generated evidence that pose evidential issues. The magistrate outlined five issues that must be considered when assessing whether digital evidence will be admitted:

1. Relevance

2. Authenticity

3. Not hearsay or admissible hearsay

4. Best evidence

5. Not unduly prejudicial

Although some of these issues may not be applicable in certain instances, each must be considered. Other issues that may prevent digital evidence from being admitted by courts are improper handling and illegal search and seizure. Although courts have been somewhat lenient in the past on improper handling of digital evidence, more challenges are being raised relating to evidence handling procedures as more judges and attorneys become familiar with digital evidence. Courts are much less forgiving of illegal search and seizure of evidence.

**Hearsay**

Why do we have a hearsay rule? The answer is based largely on common sense.

As the history of jury trials developed, decision makers and, at some point, juries received evidence for which there was no indicia of credibility. John told Bill, who told Sally, who testified. The version of the facts Sally provided differed from John’s original recollection of an event, but without John, how could anyone be sure Sally’s recitation of the facts was accurate?

The advice to Lawyers is to ready, in a legal case, is to object any time a witness (or a document) is introduced to the court if that witness says anything that implies hearsay, or if the document relates only to hearsay.

**Relevance**

Relevant evidence is “evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.”

Essentially this means that lawyers must answer the following questions. What is the nature of the problem? Is there documentation relevant to the resolution of the case? Who are the players in the drama? How did each person that emails mention come to know the facts, i.e., have they lived the facts or were they told the facts?

This of course is not part of the job of the digital forensics analyst, but the analyst, in presenting evidence, must give cognisance to how the case will be prosecuted and thus must consider relevance.

The analyst’s primary focus must be on the evidence that is needed to prove the claim or the defence of the claim.

**Prejudice**

Prejudice can be defined by asking the question, “Does the danger of unfair prejudice substantially outweigh the probative value of the evidence?”. The evidence may be excluded if it confuses the issues, misleads the jury, causes undue delay, or wastes court time.

The best examples of prejudicial evidence are graphic photographs of a murder scene or a particularly gory accident case. The issue at hand might be whether the prosecution has proven beyond a reasonable doubt that the defendant committed the crime. The photograph may induce the jurors to become transfixed by the emotion they feel about the victim’s plight, thus creating a foregone conclusion on the ultimate issue. In the accident case, the gory photographs may not speak to the ultimate issue of design defect in a products liability action. In either case, the admission of the photographs could create a dangerous predisposition unrelated to the ultimate issues to be determined. At some point, even though the photographs are relevant, the prejudice could prove overwhelming and leave such an indelible impression that the jury could be irrevocably biased.

**Authenticity**

The rules concerning the authenticity of evidence basically boils down to “Objection, Your Honor, this document has no indicia of authenticity and reliability.”

Authenticity, in the law of evidence, is the process by which documentary evidence and physical evidence (hence the need to take photos of hard disks etc) is proven to be genuine and not a forgery. Generally authenticity can be shown in one of two ways (a) a witness can testify using the chain of custody (the route through which evidence passed from the time of discovery to the time of trial. (b) the evidence can be authenticated through the testimony of an Expert Witness who examined the evidence (in this case the expert witness is the digital forensic examiner).

**Best Evidence**

An issue created by digital documents is whether **a paper copy of the original digital version** satisfies the best evidence rule when the digital document contains metadata. ... As for email, metadata will tell you who was blind-copied or when it was read, while the paper printout will not reveal such nuggets.

The job of the digital forensic analyst is to present the information (all of it) and it is up to the court to determine whether the evidence is admissible. Knowledgeable Digital Forensics investigators can save court time, by pointing out to the legal team where evidence can or cannot be substantiated under the admissibility of evidence.