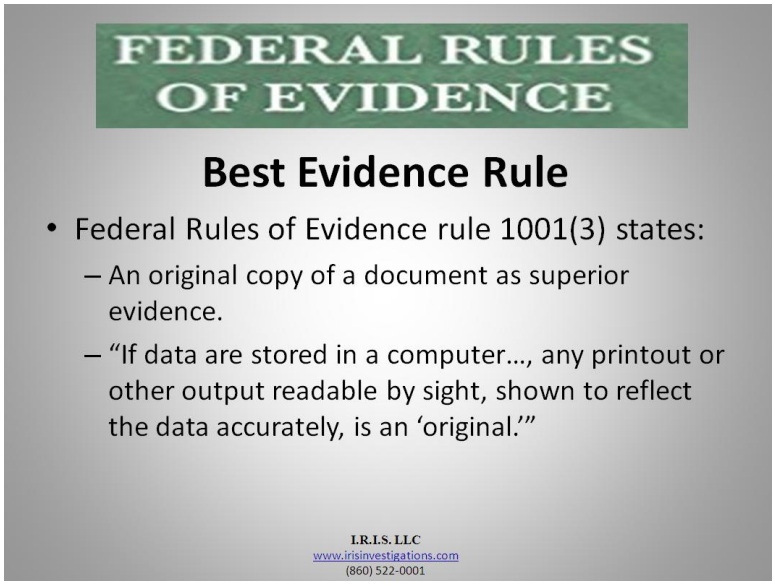
RULES OF EVIDENCE – LEGAL STANDARDS

Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial.

The use of digital evidence has increased in the past few decades as courts have allowed the use of e-mails, digital photographs, ATM transaction logs, word processing documents, instant message histories, files saved from accounting programs, spreadsheets, internet browser histories, databases, the contents of computer memory, computer backups, computer printouts, Global Positioning System tracks, logs from a hotel's electronic door locks and digital video or audio files.

Before accepting digital evidence, a court will determine if the evidence is relevant, whether it is authentic, if it is hearsay and whether a copy is acceptable or the original is required. Many courts in the United States have applied the Federal Rules of Evidence to digital evidence in a similar way to traditional documents.

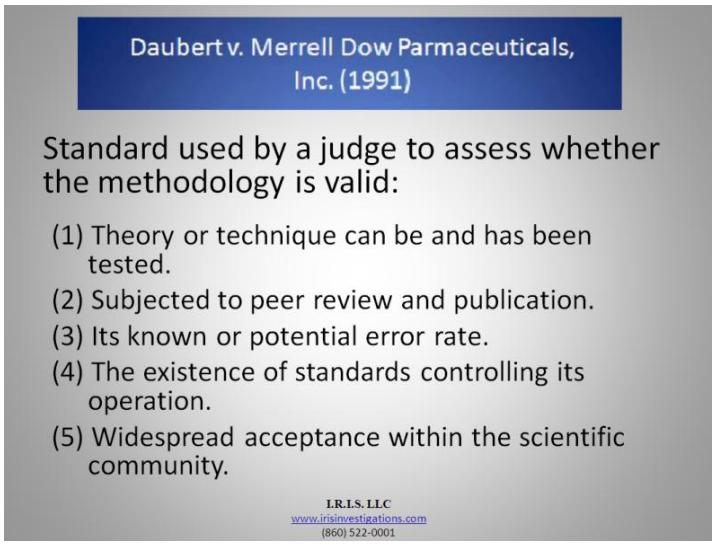
In addition, digital evidence tends to be more voluminous, more difficult to destroy, easily modified, easily duplicated, potentially more expressive and more readily available. As such, some courts have sometimes treated digital evidence differently for purposes of authentication, hearsay, the best evidence rule and privilege.



Background

In 1975, the Federal Rules of Evidence went into effect. Up to this point, Frye v. United States (1923) remains the yardstick and is widely accepted and followed by the courts. That the legislative history of the Federal Rules never addressed Frye v. United States (1923) or the issue of admittance of scientific evidence or use of expert witnesses, kept the 1923 opinion at the forefront in the making of judicial decisions.

This finally changed in 1993 when the U.S. Supreme Court decided the first of the Daubert Trilogy. In Daubert v. Merrell Dow Pharmaceuticals, Inc., the Court ruled that scientific expert testimony should be admitted based on the following:



Judge is Gatekeeper
"The judge must ensure that any and all scientific testimony or evidence admitted is not only relevant, but reliable."

Relevance and Reliability
The trial judge must ensure that the expert's testimony is "relevant to the task at hand" and rests "on a reliable foundation."

Scientific Knowledge
The Rule's requirement that the testimony "assist the trier of fact to understand the evidence or to determine a fact in issue" goes primarily to relevance by demanding a valid scientific connection to the pertinent inquiry as a precondition to admissibility.

Relevancy Concerns
The Court defined "scientific methodology" as the process of formulating hypotheses and then conducting experiments to prove or falsify the hypothesis, and provided a non-dispositive, nonexclusive, "flexible" test for establishing its "validity."

1. Ordinarily, a key question to be answered in determining whether a theory or technique is scientific knowledge that will assist the trier of fact will be whether it can be (and has been) tested.

2. Another pertinent consideration is whether the theory or technique has been subjected to peer review and publication.

3. Additionally, in the case of a particular scientific technique, the court ordinarily should consider the known or potential rate of error.

4. Finally, "general acceptance" can yet have a bearing on the inquiry.

Digital Evidence Admissibility

Legal Guidance	*Subject*
Federal Rules of Evidence 104(a)	Preliminary Questions; relationship between judge and jury
Federal Rules of Evidence 104(b)	
Federal Rules of Evidence 401	Relevance
Federal Rules of Evidence 402	
Federal Rules of Evidence 901	Authenticity; including examples of how to authenticate
Federal Rules of Evidence 902	Self-Authentication; including examples
Federal Rules of Evidence 801	Hearsay; including exceptions to the hearsay
Federal Rules of Evidence 803	
Federal Rules of Evidence 804	
Federal Rules of Evidence 807	
Federal Rules of Evidence 1001 through 1008	Original Writing Rule; also known as the "Best Evidence Rule." Includes use of accurate duplicates.
Federal Rules of Evidence 403	Balance of Probative Value with Unfair Prejudice

Reliability Concerns

A common attack on digital evidence is that digital media can be easily altered. However, in 2002 a U.S. Court ruled that "the fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness." (U.S. v. Bonallo, 858 F.2d 1427 - 1988 - Court of Appeals, 9th).

The American Law Reports lists a number of ways to establish the comprehensive foundation.

1. The reliability of the computer equipment.
2. The manner in which the basic data was initially entered.
3. The measures taken to ensure the accuracy of the data as entered.
4. The method of storing the data and the precautions taken to prevent its loss.
5. The reliability of the computer programs used to process the data.
6. The measures taken to verify the accuracy of the program.

Authentication Concerns

Federal Rules of Evidence 902 shows 12 non-exclusive methods that can be used for 'self-authentication' of digital evidence.

1. Domestic public documents that are sealed and signed.
2. Domestic public documents that are not sealed but are signed and certified.
3. Foreign public documents.
4. Certified copies of public records.
5. Official publications.
6. Newspapers and periodicals.
7. Trade inscriptions and the like.
8. Acknowledged documents.
9. Commercial paper and related documents.
10. Presumptions under a federal statute.
11. Certified domestic records of a regularly conducted activity.
12. Certified foreign records of a regularly conducted activity.

Forensic Commercial Software

As a result a breed of commercial software technology solutions designed to preserve digital evidence in its original form and to authenticate it for admissibility in disputes and in court were developed.

Digital Forensic Discipline

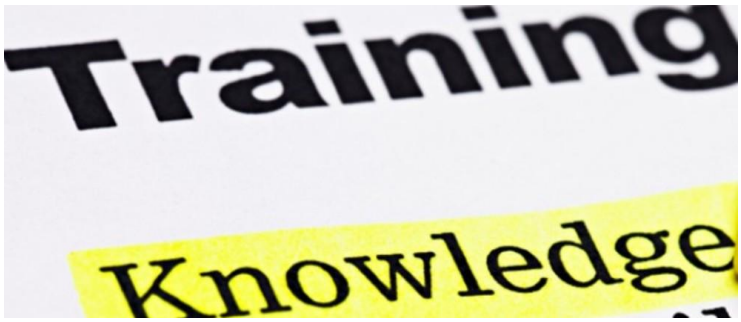
The American Academy of Forensic Sciences (AAFS) identifies digital forensics as a forensic science and the processes of all forensic sciences are fundamentally the same:

"Detection, Preservation, Collection, Examination, Analysis and Reporting"

Each phase in the process must be performed in such a manner so as to preserve the integrity of the evidence and assure its admissibility.

Qualifying Experts

Rule 702 of the Federal Rules of Evidence (FRE) provides guidance to courts about qualifying expert testimony and places the particular burden of ensuring that scientific testimony is both relevant and reliable on judges. Thus, the Daubert test and Rule 702, plus a number of additional laws, apply to digital evidence as well as other types of scientific evidence.



Minimum Professional Standards

Electronic discovery is slowly catching on attorneys are learning to use it to their clients' advantage. Within a few years, there will be no escaping electronic discovery as litigators, rule makers and courts address the hard fact that the vast majority of contemporary information is created, manipulated, transmitted or stored as electronic data.

Legal professionals do not need to be able to convert decimals into hexadecimals or understand hash values, but must have a basic knowledge of how data is stored on electronic media so that they can ask questions that will identify all sources of relevant information, develop viable discovery plans and protect our clients.

Education Recommendations

Studies have shown that defense attorneys, particularly in criminal trials, rarely raise a challenge based upon Daubert grounds of reliability (i.e., authentic and dependable), accuracy (i.e., correct and free from mistakes), and veracity (i.e., truthfulness).

The Lorraine v. Markel Am. opinion specifically states that the burden of ensuring that digital evidence is what it purports to be depends largely on objections by opposing counsel. Thus, it is the responsibility of legal professionals to be sufficiently knowledgeable to object competently to faulty evidence. Laying proper foundation qualifying the expert witness, as well as directing a competent line of questioning, rely heavily on the computer literacy of the lawyers involved.

Basic Computer Literacy

This includes an understanding of computers. This knowledge will enable lawyers to establish proper foundation and a proper line of questioning.

Understanding of the Digital Forensics Process

This includes basic knowledge of how easily digital evidence can be altered and what it means to have a proper chain of evidence, including storage and control. In addition, there should be sufficient knowledge of how evidence is collected on a computer hard drive (and on a network), how a hard drive is appropriately duplicated for forensic purposes, and then searched by forensic tools.

Knowledge of the Federal Rules of Evidence, and How They Apply to Electronic Evidence

The Federal Rules of Evidence are integral to understanding the process for admitting digital evidence. Lorraine v. Markel Am. Insurance Co. provides a framework for applying these rules to digital evidence. Fed. R. Evid. 901 and 902 specifically deal with authentication of digital evidence, including examples of how to do so. It also provides a basis for questioning whether the digital chain of evidence was reliable, and not broken, during the investigatory process.

Survey of Case Law

A thorough survey of other cases will provide an even more comprehensive understanding of the state of the practice regarding digital evidence as well as the understanding that the burden of ensuring digital evidence admissibility rests largely on objections to such evidence by opposing counsel.

MOBILE DEVICES

Riley v. California, No. 13-132

This decision highlighted the differences between digital and physical evidence in that a warrant is now required to examine the contents of a cell phone, unlike physical papers which may be on a person. The difference was drawn due to the considerably larger storage potential of a portable electronic device which can contain information on lifestyle, associates and activities which may be outside of the investigation's scope.

Digital Evidence Tool Box
For more information see the section on Mobile Devices

NON DIGITAL RELATED EVIDENCE

Real Time Tracking - Ping
Recent decisions by some courts have made it possible for government agencies to obtain real time tracking information using an individual's cellular phone or other cellular device. Obtaining real time geo-location of a cell phone via the emergency 911 (E911) system in many cases requires either a warrant or permission from the cellular carrier.

Historical Call Detail Records
Additionally, the government and courts continue to maintain the position that obtaining historical call detail records for an individual does not require probable cause or a warrant since the person holding the cell phone is voluntarily providing their location data to a third party, namely the cellular service provider.

Cell Site Accuracy
Properly applied and interpreted cell phone location evidence can be helpful in many cases. The issue is the overstatement of the accuracy of the phone's location.

For instance, if the phone is using a cell site in a particular town where an incident occurred and the person who was in possession of the phone claims to have been in a different town, it is a simple presentation to dispute the person's claim.

Historical Cell Site Analysis

Evidence involves identifying the location of relevant cell phones within mapped RF areas, relative to geographically-fixed cell site, and at fixed points in time.

This analysis begins with reviewing CDRs, cell site locations and cell sector orientation to identify relevant voice call or SMS (text) message connections in relation to crime scenes or any other relevant locations, along with relevant patterns of movement in connection with these locations.

Relevant voice call or text connections are then overlaid on mapping software depicting relevant cell site and sectors along with locations relevant to the case.

FED. R. EVID. 702

Historical cell site analysis evidence may be presented through a witness who is qualified "as an expert by knowledge, skill, experience, training or education" if the witness' testimony will be offered in the form of an opinion or otherwise and such testimony is based on sufficient facts or data and is the product of reliable principles and methods that the witness has reliably applied to the facts of the case.

In addition to Rule 702, expert testimony on historical cell site analysis, non-expert summary testimony involving historical cell site analysis may be offered where such testimony is limited to presentation of summary maps, charts or other demonstrative summary exhibits based on evidence admitted at trial without offering any expert opinions.

Cell Provider Experts

Cell provider employee experts should be eligible to qualify as a Rule 702 expert, subject to their degree of training and experience in this field. An engineer or cellular network technician familiar with the cell provider's network and CDRs should qualify as a Rule 702 expert.

Cell Provider Records Custodians

Cell provider records custodians, however, may lack the requisite training and experience to testify as Rule 702 experts. Some cell provider records custodians may have sufficient training and experience to testify about cell site locations and cell site sectors, particularly where such information is recorded in the CDRs or other business records that the records custodian produces at trial.

Non-Expert

Limited, non-expert summary testimony regarding cell site locations and cell phone transmissions recorded in the CDRs should be admissible because most, if not all, jurors, judges and attorneys have cell phones, have observed cell phone towers, know that the quality of their cell phone call reception depends, at least in part, on their proximity to cell sites.

Methods

Additionally, plotting tower locations in relation to crime scenes on accurate, readily-available computer mapping software can be accomplished easily through the input of the longitude and latitude of cell sites identified in a cell provider's business records. This input results in a graphic summary of the geographical location of cell sites on a map that can be easily verified, along with any other CDR data admitted into evidence.

Consideration should be give to restricting testimony by a non-expert summary witness to mapped crime scenes and cell site locations, along with corresponding CDR information admitted into evidence—such as dates, times, connecting telephone numbers and incoming/outgoing communications.

Any additional testimony further explaining details about cellular communications, such as cell sectors, number and direction of cell site sectors for each cell site and depictions of the directional orientation and reach of cell site sectors on a map arguably may require that the testifying witness be qualified as a Rule 702 expert.

FED. R. EVID. 802, 803(6)

Rule 803(6) of the Federal Rules of Evidence governs the admissibility of a cell provider's CDRs and cell site data/maps through a cell provider's records custodian or other qualified witness. These records qualify as business records and should be admitted into evidence as an exception to the hearsay rule.

CDRs and cell site data/maps also may be introduced into evidence through certification of a records custodian or other qualified witness pursuant to Federal Rule of Evidence 902(11) without violating the Confrontation Clause.

Digital Evidence Tool Box

For more information see the sections on Call Detail & Cell Site Analysis and Location Data

INTERNET AND SOCIAL MEDIA

Rule of Evidence 901(a)

Federal Rule of Evidence 901(a) and its corresponding state laws require laying a foundation of "evidence sufficient to support a finding that the matter in question is what its proponent claims." Federal Rule of Evidence Rule 901(b) provides an illustrative list of methods by which evidence can be authenticated.

Rule 901(b)(1)
Federal Rule of Evidence Rule 901(b)(1) allows for authentication through testimony from a witness with knowledge that a matter is what it is claimed to be. The person who created the evidence can testify to authenticate it. The authenticating witness must provide "factual specificity about the process by which the electronically stored information is created, acquired, maintained and preserved without alteration or change, or the process by which it is produced if the result of a system or process that does so."

Rule 901(b)(4)
Federal Rule of Evidence Rule 901(b)(4) provides that circumstantial evidence, including "appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances," can help to authenticate evidence.

Digital Evidence Tool Box
For more information see the section on Internet & Social Media Evidence

E-DISCOVERY

New E-Discovery Federal Rules of Civil Procedure Amendments went into effect December 1, 2015. The changes should have a significant impact on the scope, speed and specificity of discovery obligations. Below is a summary of some of the changes.

Rule 26(b)
Rule 26(b) has been reorganized to place new emphasis on relevance and proportionality of discovery. The new rule changes the scope standard from "any relevant subject matter involved in the action" and information "reasonably calculated to lead to the discovery of admissible evidence," to information "relevant to any party's claim or defense and proportional to the needs of the case."

The proportionality factors include:

- the importance of the issues at stake in the action;
- the amount in controversy;
- the parties' relative access to relevant information;
- the parties' resources;
- the importance of the discovery in resolving the issues; and
- whether the burden or expense of the proposed discovery outweighs its likely benefit.

These changes stress the parties' obligation to consider proportionality when propounding and responding to discovery and to focus on discovery of relevant information.

Rules 30 and 31
Additional depositions are permitted with leave of court in Rules 30 and 31, but the court can consider proportionality factors from 26(b).

Rules 33
Rule 33 still limits interrogatories to 25, and additional interrogatories are permitted only to the extent consistent with the relevance and proportionality concepts in Rules 26(b)(1) and (2).

Rules 16
Rule 16 will reduce delays at the beginning of litigation by limiting the time to issue the scheduling order to the earlier of either 90 days (not 120 days) after service or 60 days (not 90 days) after any defendant has appeared. Also, the scheduling order may include Federal Rule of Evidence 502 agreements, which further the Courts' encouragement of non-waiver and claw-back agreements.

Rules 34
Rule 34 adds a requirement that a response to a document request must state with specificity the grounds for objecting to the request, banning the previous practice of "boilerplate" objections.

Rules 37 Changes - The Preservation or Loss of Electronically-Stored Information

- Rule 37(e) adopts a common law principle that a duty to preserve arises when litigation is "reasonably anticipated."
- Consequences for failing to preserve data are also better defined in the new Rules.
- Rule 37(e)(1) provides that the court, "upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice."

Under the new Rule, more serious sanctions for loss of ESI are only appropriate where the court finds a party intended to deprive the other party's use of the ESI in litigation. Only upon a finding of intent can the court impose sanctions of an adverse inference jury instruction, dismissal of the action or default judgment.

For more information on mobile devices, digital forensics and digital evidence, call now and speak with a certified expert. IRIS LLC is available 24 hours in emergency cases.