**Digital Evidence :**

“Digital evidence” is any documentation that satisﬁes the requirements of “evidence” in a proceeding, but that exists in electronic digital form. Digital evidence may rest in microscopic spots on spinning platters, magnetized to greater or lesser degrees in a somewhat nonvolatile scheme, but regardless, unintelligible except through multiple layers of abstraction and ﬁle system protocols. In other cases, digital evidence may be charges held in volatile storage, which dissipate within seconds of a loss of power to the system. Digital evidence may be no more tangible, nor permanent, than pulses of photons, radio frequency waves, or diﬀerential levels of voltage on copper wires.

Naturally, digital evidence poses challenges for investigators seeking to preserve it and attorneys seeking to admit it in court. In order for evidence to be admissible in United States federal courts, digital evidence must adhere to the same standards as other types of evidence: it must be deemed relevant to the case and authentic. “The standard for authenticating computer records is the same as for authenticating other records ...,” wrote the U.S. Department of Justice (DoJ) in 2009. “Importantly, courts have rejected arguments that electronic evidence is inherently unreliable because of its potential for manipulation. As with paper documents, the mere possibility of alteration is not suﬃcient to exclude electronic evidence. Absent speciﬁc evidence of alteration, such possibilities go only to the evidence’s weight, not admissibility.

Examples of “digital evidence” include:

• Emails and IM sessions

• Invoices and records of payment received

• Routinely kept access logs

• /var/log/messages

**Network-Based Digital Evidence**:

“Network-based digital evidence” is digital evidence that is produced as a result of communications over a network. The primary and secondary storage media of computers (e.g., the RAM and hard drives) tend to be fruitful fodder for forensic analysis. Due to data remanence, persistent storage can retain forensically recoverable and relevant evidence for hours, days, even years beyond ﬁle deletion and storage reuse. In contrast, network-based digital evidence can be extremely volatile. Packets ﬂit across the wire in milliseconds, vanish from switches in the blink of an eye. Web sites change depending on from where they’re viewed and when.

The requirements for admissibility of network-based digital evidence are murky. Often, the source that generated the evidence is not obtainable or cannot be identiﬁed. When the evidence is a recording of a chat log, blog posting, or email, the identity of the parties in the conversation (and therefore the authors of the statements) may be diﬃcult to prove. When the evidence is a web site, the litigant may need to provide supporting evidence to demonstrate that the image presented in court is what actually existed at the time and location that it was supposedly viewed. For example, “[s]everal cases have considered what foundation is necessary to authenticate the contents and appearance of a website at a particular time. Print-outs of web pages, even those bearing the URL and date stamp, are not self-authenticating.... Thus, courts typically require the testimony of a person with knowledge of the website’s appearance to authenticate images of that website.”14 There is little case precedent on the admissibility of network packet captures. Depending on the method of capture and the details of the case, packet captures of network traﬃc may be treated as recordings of events, similar to a taped conversation.

**Examples of “network-based digital evidence” can include:**

• Emails and IM sessions

• Browser activity, including web-based email

• Routinely kept packet logs

• /var/log/messages