Webology (ISSN: 1735-188X)
Volume 18, Number 5, 2021

# Authentication Of Digital Evidence With Reference To USA And Pakistani Courts

**Mahboob Usman[1] , Dr. Fazli Dayan[2] , Iftikhar Ahmad Khan[3] , Kamran Abdullah[4] , Mian Muhammad Sheraz[5] , Dr. Ghufran Ahmad[6] , Muhammad Haroon Khan[7]**

[1]Department of Law, IIU, Islamabad.

[2]Assistant Professor, Department of Sharaih & Law, Islamia College University, Peshawar.

[3]Assistant Professor Law, Islamia College University, Peshawar.

[4]Lecturer Law, Islamia College University, Peshawar.

[5]Principal/Assistant Professor, Mardan Law College, Mardan.

[6]Assistant Professor, Department of Law, University of Sialkot, Punjab.

[7]Assistant Professor Law, Islamia College University, Peshawar.

## Abstract

The law of evidence prescribes minimum criteria for every type of evidence to make it admissible in judicial proceedings. Inter alia, authenticity of the evidence, if the investigator is unable to establish the link with the case and the evidence then it shall be very difficult for him to prove the fact(s). It further adds more complexities when, the evidence is in digital form which are to be addressed before admitting the evidence in court proceedings. Present article attempts to analyze authenticity of digital evidence on computer, internet and mobile phones in the light of USA courts' decision. Followed by, the authentication challenges which are discussed to discover the issues face by the experts dealing with digital evidence, and finally, finding a way out for Pakistani legislature to improve the authenticity of digital evidence and to provide a proper mechanism while dealing with such delicate type of evidence.

**Keywords:** Authenticity, digital evidence, computer evidence, website evidence

## Introduction

Everywhere in the world, the legislature has prescribed minimum threshold for acceptance of evidence in judicial proceedings. With the prevailing digital devices, the nature of evidence has been changed significantly. Mostly, nowadays, the information is created electronically which is not printed. Hence, the paradigm is being shifted from printed documents to electronic documents. There are certain basic rules of evidence. At least, five important rules (admissible, authenticate, complete, reliable and believable) are very much important in respect of for evidence, which are also applicable to digital evidence, in addition to other related rules. These are some basic rules which relate to "five properties that evidence must have to be useful." (Vacca, 2005, 220) If any of the rule mentioned above is missing in evidence that will weaken the evidence value. In any legal system, "reliability" is very much important in respect of evidence. Rule 702 of Federal Rules of Evidence (FRE), requires that testimony of expert witness and scientific evidence "must be reliable both with respect to the principles and methods used by the expert and application of the principles and methods to the specific facts." Thus, criteria laid down by the USA Courts will be examined in coming pages.

After collecting digital evidence, investigator will make necessary arrangements for presentation in the court for trial of the case. In legal proceedings, in last century, reservations were made regarding proper understanding amongst legal fraternity and legislators for lack of proper understanding to address the problems faced by the LEAs and investigator due to increasing reliance upon digital evidence. (Boddington, 2016, 10) However, by the turn of the century various scholars were uncertain in respect of prevalent error in understanding the factual nature of digital data. The most import issue was the "inefficiency and ineffectiveness of some forensic processes used in its recovery, analysis, and subsequent use in legal proceedings." (Boddington, 2016, 10)

As the criminal may leave many artifacts in hurry, therefore, it is imperative for the investigator to carefully collect the artifacts, as the artifacts has lot of importance in data collection, which are very useful for tracing the suspect, Yet, these are difficult to discover, and if these are found successfully, then they have a lot of significance for investigator to link and trace the culprit.

Many courts in Pakistan have applied the ETO amendments of the QSO to various cases involving computer, internet or mobile phone, without considering that the amendments brought in QSO through ETO are just applicable to ETO not to any other law, in a similar way to traditional documents. Digital evidence, however, is more voluminous, expressive and readily available. Besides, digital evidence is difficult to destroy, easily modified and duplicated. As such, no court, although the courts have allowed in some circumstance to use e-mails, Automated Teller Machine (ATM) transaction, Global Positioning System (GPS), online transactions, computer generated evidence, Call Detail Records (CDR), Closed-circuit television (CCTV) footage, audio and video recording in Pakistan has been dealt with digital evidence quite differently for determinations of authentication of digital devices because of lack of suitable understanding of cyber forensics.

Digital evidence is not like physical traditional evidence, in authentication of digital evidence; it is indispensable to evaluate its trustworthiness. There are various approaches adopted globally, but two approaches for evaluating the authentication of digital evidence is discussed. For

instance, one method is to entirely focus on the computer which generated the evidence and whether the computer was functioning normally. The other method is to examine digital evidence for tampering and other damage. (Casey, 2011, 60) In Arif Hashwani case, (Arif Hashwani v. Sadruddin Hashwani, 2007), the Sindh High Court (SHC) held that record in the shape of audio and video is per se permissible portion of evidence in judicial proceedings, nevertheless, the authenticity of this type of evidence is "subject to proof in case the party against which it can be used disputed and or denied the authenticity and information contained in the said electronic documents."

Like other types of evidence, authenticity and integrity of digital evidence must also be established, which is critical in digital evidence and challenging. In paper-based evidence either the original document was presented in court or original's copy, but in case of electronic documents, somehow, according to Stanfield (2016) it is very difficult for the examiner to establish that which document, presented as evidence, is the actual one "since two electronic documents can be identical." (p.123). The most important part of digital evidence according to Stanfield (2016) is that it is dynamic and changeable which is the most concern issue in authentication of evidence (p. 6). In cyber-crimes cases, investigators use centuries old procedure for authentication of digital evidence. Instead, the investigators should adopt ICT compatible procedures in which all the relevant data or entire hard drive is hashed.

Three aspects of ICT are important for authentication of digital evidence such a people (creator of evidence), process and the technology (what technology was used). Besides, chain of custody also plays an important role. There are also three challenges to authentication of digital evidence such as who is the author of the document, is the computer program reliable and was the record, after its creation, changed, altered, modified, manipulated or damaged? At least following questions may be asked in relation to computer generated evidence:

i. How reliable is the computer equipment used for the purpose which kept the records and produce the print-out?
ii. How reliable is the computer program (including all types of software's used)?
iii. How accurate is the program?
iv. Ratio of error in program?
v. How the data was entered?
vi. Whether the entry of relevant data was made in the usual way or otherwise?
vii. Whether adequate measures were taken (or in place) for assurance of accuracy and safety of electronic data?
viii. What was the storing technique for data? Whether the storage method is generally accepted or not?
ix. When this printout was made, and how it was prepared?
x. Whether the authenticity of the digital data has been challenged, if so, on what basis?
xi. Metadata?

In any case, proponent is under obligation to lay the proper foundation of evidence. Whereas courts prime concern is with the reliability evidence. Whether the evidence is reliable or not? Whereas, in USA, in previous court verdicts was required that authentication must have comprehensive foundation. (United States v. Scholle, 1977) Now the question of familiarity of court, particularly in legislation developed countries, with digital evidence is out of context. Thus, the courts have adopted little bit lower standards in Vela case (United States v. Vela, 1982) where the court treated the computer data similar with other records, but the requirements were increased thereafter.

Initially, in the USA, the courts have applied the FRE to digital evidence, without realizing important difference between both types of evidence. In 2006, new rules were enacted to accommodate ESI. Digital evidence is more often challenged for its genuineness that it can easily be modified. In the USA, the requirement of authentication of digital evidence are governed by the rule 901 of FRE, which says that "to satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is." Several examples have been provided under this rule, but these examples are not exclusive. Only genuine evidence is admissible in court. In USA legal system, authentication of evidence is a prerequisite for admitting any document or data into evidence, (United States v. Vayner, 2014) and the requirement of authentication of digital evidence is not very extraordinary (United States v Gagliardi, 2007). Though, this rule discusses the requirement of authenticating ESI, but it does not provide procedure for authentication of digital evidence. Nonetheless, this rule just provides some examples that how authentication can be completed.

In USA, Rule 901(b) (1) of FRE requires that a proponent of evidence should confirm every evidence presented through testimony in court that the electronic evidence "is what it is claimed to be." However, in digital evidence, this process is little bit different. For instance, the relevant witness (creator of the document) producing evidence before the court shall be the person who has generated the said document or who is under obligation under any law to maintain the digital evidence in its original form. Therefore, a witness involved in the process of authenticating digital evidence should at least "provide factual specificity about the process by which the electronically stored information is created, acquired, maintained, and preserved without alteration or change." Lorraine v. Markel 2007) whereas, failure to provide required testimony in digital evidence may held to be inadmissible. Under Rule 901(b) (3) of FRE, in court proceedings, any expert witness can authenticate digital evidence by comparing it to already collected samplings. Initially, this rule was merely for authentication of digital evidence as this was meant for authenticate of handwriting and signatures, now rule 901(b)(4) of FRE has also been applied to authenticate electronic communications.

Clearly, if it is established that the computer-generated records were changed or modified then the computer-generated records will not be admissible. Besides, for computer-generated records, trustworthiness of computer program that created the records can also be challenged. Moreover, authenticity of digital evidence can be challenged by questioning the author's identity. Metadata is an integral part of electronic documents. When documents are printed then metadata

is invisible. Therefore, it may be ensured by the investigator that the electronic version of documents is available, and if required in future the document can be properly authenticated.

**Authentication of Digital Evidence on Computer**

In court proceedings, showing of the authenticity of digital evidence in crucial, therefore, evidence is not accepted by the courts until or unless same is proved to be authentic to satisfaction of the court that complete and exact copy of electronic data was collected from a specific computer and remained unchanged from its collection by the investigator. Question arises whether the acquired data is the same data as the originally seized media or there is some difference between both of them? Casey discuss its technical perspective and says while running computer every moment the data is changing constantly, therefore, for the investigator or forensic expert to compare the data with original is not always possible. (Casey, 2011, 20) Network traffic is captured in transit, once it is seized, then just copies remain and the original data or devices is not available for comparison purposes. (Casey, 2011, 20-21). This was from technical angle and from legal angle, authentication of evidence is the method for determination whether it is reliable or not.

Whether mere raising possibility of tempering is sufficient to challenge the admissibility of digital evidence or some more evidence is required to strengthen the evidence and merely on the allegation of tempering this will lose weight? In Allen case (United States v. Allen, 1997) authenticity of digital evidence was challenged and the court found that mere "raising the possibility of tampering is insufficient to render evidence inadmissible." Rather, strong piece of evidence is required to prove the authenticity. Furthermore, general allegation of interference with digital evidence is not sufficient, obvious evidence of tampering is required, mere assertions claiming computer records have been altered is not sufficient. (Brown, 37) Whereas in Bonallo case (United States v. Bonallo, 1988), the court held that, the mere fact that computer containing digital data can easily be altered is "plainly insufficient to establish untrustworthiness." Nonetheless, the other collaborative evidence is required and "more comprehensive" foundation for authentication is required by Scholle (United States v. Scholle, 1977), is upright approach for proving the authenticity of digital data.

Although, witnesses are testifying in the courts regarding authenticity of computer-generated evidences is not required special education. Besides, he must not be the person who has programmed the computer himself. Instead, at least, he should have basic information of the related facts to which he testifies in any court. Authentication nature of digital evidence will differ, due to various reasons, such as pages from the Internet and websites; use of an ATM card or other card; social media sites, e-mails, chat rooms, messengers, social mobile application, instant messages.

For authentication of digital evidence, the author and creation date of document are important. Change of computer's clock is quite easy, therefore, it can easily be changed to show that a curtain document was created on such a date and time, suppose an earlier date. Hence, this will make it extra completion for the investigator "to determine who wrote a document and when it was created. However, there are various approaches that forensic analysts can use to authenticate a digital document." (Casey, 2010) The investigator may apply different methods and approaches

including the metadata on computer-generated files and in log files "to determine the provenance of a document." (Casey, 2010) False documents can be detected.

Courts in USA, in 2007, observed that digital evidence is creating unique set of issues. These issues (admissibility problems of e-mail) were discussed by Judge Grimm in Lorraine v. Markel. In many cases, metadata is also be used for establishing the authenticity of digital evidence, as Grimm Judge (USA) noted regarding Rule 34 of the Federal Rule of Civil Procedure which authorities parties to discovery of digital evidence. Party can request the court for production before it in electronic data in its natural format that may include the metadata of the electronically generated document. This shows the author's identity, time and date of the electronic record creation, modification and changes made later on. Actually, it's data about data, which has a lot of significance in respect of authenticity of electronic data. Consequently, metadata is a distinguishing characteristic of all electronic record that may be used for authentication of evidence under rule 901 (b) (4). Grimm Judge recognized this aspect for authentication of ESI which presents many concerns as "technology changes so rapidly that it is often new to many judges".

**Authentication of Websites**

Every organization maintains her website for various purpose including business, education, entertainment and banking. In USA, courts authenticating web pages in digital evidence drive powers from "warrant a reasonable person in determining that the evidence is what it purports to be," through testimony of expert opinion, public records evidence process or system evidence and an official publication is self-authenticating as per Rule 902 FRE. In Lorraine v. Markel case the court suggested some additional factors that should be considered while authenticating web pages. In USA, under Rule 901(b)(1) of FRE, in court matters, witness's testimony with personal knowledge is accepted to authenticate websites, but how much knowledge is required to authenticate? This is to be seen from the court decisions. Dealing with authentication of websites is not an easy task, thus three questions must be answered with respect to websites:

i. What was originally available on the given website?
ii. Whether the testimony of a witness or exhibits accurately reflects it?
iii. If testimony or exhibits reflects it, then whether it is possible to attributed to the website proprietor?
iv. Whether given website was hacked?
v. Whether the website was accessed by unauthorized person?

Thus, a witness who testify before the court should authenticate website data by means of showing that the particular person typed the specified URL, logged into the website, reviewed what was there on website, and whether printouts properly and exactly reflects the data. Some courts in USA, however, authenticate website content on the basis of presentation of printouts containing the URL of website and the date on which the website pages were printed. Duty of the lawyers cannot end here, but as per Nightlight case (Nightlight v. Nitelites Franchise, 2007) lawyers are required to "present evidence from a witness with personal knowledge of the website".

In St. Luke's Cataract case, (St. Luke's Cataract v. Sanderson, 2006), the court rejected affidavits regarding authentication of WebPages where he lacked personal knowledge of the

relevant facts. Similar, view was taken in Wady case. (Wady v. Provident Life, 2002) However, in Jackson (United States v. Jackson, 2000), the court refused to accept the evidence on the ground that the "proponent failed to authenticate exhibits taken from an organization's website." In case of authentication of websites, the same can be done by calling the witness, who could testify before the court that he has seen the material on website and he printed the same as held in Estate of Konell case (Estate of Konell v. Allied Prop, 2014). Whereas, in USA, government department i.e. official Websites are considered as self-authenticating. In many case Pakistani courts upheld refused the bail on the basis of uploading material on Facebook. In Farhan Kamrani case (Farhan Kamrani v. the State, 2018), bail petition of the petitioner was refused on the basis of creating fake Facebook ID of the complaint which was provided through investigation by the FIA on the basis of IP address. In Junaid Arshad case (Junaid Arshad v. the State, 2018) the court likewise rejected bail application of the petitioner on the basis of evidence collected from mobile and IP address.

**Authentication of E-Mail**

Nowadays, everywhere in the world email is being used to correspond and communicate with other entities for personal as well as business purposes. Generally, people believe that the email is secure; however, this is not true, as it can easily by tamper during transmission. Thus, it is a great source of evidence and hence it is being used in evidence for proving or disproving the facts, which is routinely being used in evidence. Email is not as such as known mail which is prevailing since centuries. Therefore, email has some distinctive characteristics which are not prevailing in daily mail, which includes "it's 'contents, substance, internal patterns, or other distinctive characteristics." (Lorraine v. Markel 2007)

In Cyber-world, proving of authorship of e-mail is very complicated (i.e., who is the author of e-mail), therefore other means (circumstantial evidence) is required to authenticate it. For this purpose, different technical means are available which can be used to trace its origins including assistance from ISPs, cellular network companies, and password of the email. Still, identifying the actual person may not be an easy task. In USA, rule 901(b) (4) of the FRE accompanied by rule 901(b) (1) of the FRE is used for authentication of e-mail messages and other electronic records. Further, under rule 902(7), an email can be self-authenticating and courts have admitted e-mails into evidence. (United States v. Safavian, 2006) Although, an e-mail is being used as a common form of communication, but it is unique form of communication as it does not have signature of any person, which was a common feature in hard copy correspondence. In the past, signatures were the best way to authenticate a document, but the signature are removed in email. Therefore, it is necessary to develop a method of digital signature which is accepted as a replacement of handwritten signature. Resultantly, to prove someone was the real author the email, either to call the author or use circumstantial evidence. In Talada case (Talada v. City of Martinez, 2009), the court held that an e-mail is suitably authenticated by the testimony of the source person who sent the email. In 2005, first time in the USA legal history, the courts in International Casings Group case (International Casings Group v. Premium Standard Forms, 2005) accepted email as a document.

Digital data can easily be created, altered, manipulated or forged without apparent detection as it can easily be forged by any lay person having some basic knowledge, especially criminals adopt this technique to conceal their identity. Therefore, admissibility must be considered in the light of these facts. While forwarding an e-mail, it can be edit easily by the sender without leaving any sign of edition making it difficult for the recipient to detect alterations.

Next issue is whether in criminal investigation the forensics expert report can be relied upon to authentic emails or not? Whether e-mails can be authenticated with already authenticated e-mails or not? In Kupper case (Kupper v. State 2004) the court held that e-mails acquired by a qualified computer expert may be used for authentication of emails. Whereas, in Safavian case (United States v. Safavian, 2006) the court held that comparing an e-mail with other e-mails of the accused already collected and authenticated may help in authentication of new e-mails. However, this technique is mainly advantageous in such circumstance where the sender's e-mail address does not have any sign of identification. Meaning thereby, it is not an easy task to prove or establish the authorship of email messages. Similarly, in Lorraine v. Markel case the court held that whatever the offered ESI counsel have to prove its origins and chain of custody of the evidence.

When e-mail evidence is offered in proceedings, lawyers should establish that the information under review of the court is self-authenticating under rule 902 of FRE or at least meets the standards of authentication mentioned in rule 901 of FRE. With regard to any other evidence, lawyer should prove that the collected e-mail is "what it purports to be." Still, testimony of a witness, before the competent court, with his personal knowledge regarding e-mail under consideration is an accepted way for showing e-mail's authenticity.

**Authentication Challenges**

The Pakistani legal system has law and precedents regarding the admissibility and authenticity of conventional evidence. However, courts in Pakistan are working hard to regulate the issues attached to digital evidence. The prevalent of electronic devices has formed unique challenges, both legal and technical, for the courts in Pakistan, that how to properly authentic digital data collected through modern devices and techniques, under the current law of evidence. Although, the basic requirement are the same, however, their applicability to digital devices raise complex issues and challenges.

Any evidence to be admissible in Pakistani legal system, or any of the legal systems of the world, it must meet certain well-established minimum criteria. Before accepting the evidence in court, courts usually examine about any evidence that whether the evidence is authentic, admissible, whether the copy of original electronic data is sufficient or the original device is required. Digital evidence is altogether different from paper-based evidence. Though, this evidence can easily be changed or modified by any person having approach to the said evidence. Nonetheless, approach to the digital evidence does not mean that the relevant data has been changed or modified altogether. However, this raise some serious questions about its authenticity.

FRE are applicable to computerized data as these rules are applicable to the conventional evidence. Yet this raises some distinctive concerns of correctness and genuineness of computerized data. Manual of complex litigation described the accuracy and integrity issues. More specifically,

there are various import challenges attached to the authenticity of digital evidence such as alteration, manipulation and damaged of data relevant data during the whole process. Whether the computer program which generated the record was reliable? What was the identity of the author of digital evidence? What is the reliability and standard of evidence collected from a social media website? Whether the messages have direct nexuses to a particular person? When more than one person has access to the device and "whether the person alleged to have used his PIN, password or clicked the 'I accept' icon was the person who actually carried out the action." (Mason and Seng, 2017, 197) These challenges make complication for dealing digital evidence. Yet, it is undefined that whether an attorney challenging authenticity of digital evidence "can ever raise sufficient doubt about the authenticity of digital data." (Mason and Seng, 2017, 197) All the institutions dealing with digital evidence should manage/discuss the admissibility and authentication issues prior to presentation of evidence before the court that may arise in legal proceedings. If evidence collected from electronic devices is not properly examined and authenticated, then, it will be of no use for the investigator. At all the time, the investigator should maintain proper chain of custody of digital evidence. Otherwise, this will also be challenged making entire exercise doubtful, resultantly, making way for acquittal of the accessed. When, a piece of evidence is disbelieved by the courts, the whole evidence will collapse. To avoid these challenges the investigator should use extra caution while handing the digital evidence at every stage from collection to presentation in the courts.

The legal fraternity and judges alike have some basic understanding of the authenticity of evidence. But, Pakistani law of evidence is meant for tradition records, which does not discuss many aspects of digital data. Applying these conventional rules to electronic evidence presents unique issues. The failure to understand basic requirements of authentication of digital data may resulted in adverse rulings by the courts.

## Conclusion

Credibility of evidence is crucially significant for admissibility of evidence in judicial proceedings. However, examining authenticity of digital evidence is not possible, without proper and thorough examination of the same. Reliability of computer equipment, computer programs, (including all types of software used), accuracy of the program, ratio of error in program, procedure for data entry, adequate measures adopted for accuracy and safety, storing method of data, procedure for print out and metadata are to be examined in all types of computer evidence. Besides, in website related evidence, availability of data on website, information related to website hacking and access to unauthorized persons is also examined. Unfortunately, his exercise is not in practice in the Pakistani system, which needs to be addressed to properly authentic it. Judges in Pakistan are not much familiar with technology, if some basic training is provided to judges, then this will improve the decisions of the courts.

## References

Adams v. Disbennett, 2008 WL 4615623 (Ohio App. 3 Dist., Oct 20, 2008).

American Express Travel Related Services Co. v. Vinhnee (In re Vinhnee) 336 B.R. 437 (B.A.P. 9th Cir. 2005),
Arif Hashwani v. Sadruddin Hashwani, PLD 2007 Karachi, 448.
Boddington, Richard (2016). Practical Digital Forensics. Packet Publishing Ltd.
Brown, Christopher L.T. (2010). Computer Evidence: Collection and Preservation (2nd ed). Course Technology PTR,
Buzz Off Insect Shield, LLC v. S.C. Johnson & Son, Inc., 2009 U.S. Dist. LEXIS 17530 (M.D.N.C. Mar. 6, 2009.
Casey, Eoghan (2010). Handbook of Digital Forensics and Investigation. Elsevier.
Casey, Eoghan (2011). Digital Evidence and Computer Crime (3rd ed). Elsevier.
Estate of Konell v. Allied Prop. & Cas. Ins. Co., 2014 U.S. Dist. LEXIS 10183 (D. Or. Jan. 28, 2014).
Farhan Kamrani v. the State, 2018 YLR 329 (Sindh).
Federal Judicial Centre (2004). Manual for Complex Litigation (4th ed). Federal Judicial Centre.
Federal Rule of Civil Procedure (USA).
Fenje v. Feld, 2003 LEXIS 24387 (N.D. Ill., December 8, 2003).
Imwinkelreid, Edward J. (2018). Evidentiary Foundations (10th ed). Carolina Academic Press.
in Re: Vee Vinhnee, 336 B.R. 437 (B.A.P, 9th Cir, 2005).
International Casings Group Inc. v. Premium Standard Forms, 358 F.Supp.2d 863 (W.D. Mo. 2005).
Junaid Arshad v. the State, 2018 PCr LJ 739 (Lahore).
Kearley v. State, 843 So. 2d 66 (Miss. Ct. App. 2002
Kupper v. State 2004 WL 60768 (Tex. App. Jan. 14, 2004),
Lenzini v. Columbia Foods, 829 S.W.2d 482 (Mo. App. 1992).
Lorraine v. Markel American Insurance Co., 241 F.R.D. 534 (D. Md. 2007).
Mason, Stephan & Seng, Daniel (2017). Electronic Evidence (4th ed). School of Advanced Study.
New York v. Microsoft Corp., 224 F. Supp. 2d 76 (D.D.C. 2002).
Nightlight Sys., Inc. v. Nitelites Franchise Sys., Inc., No. 1:04-CV-2112-CAP, 2007 U.S. Dist. LEXIS 95538, (N.D. Ga. May 11, 2007),
Paralyzed Veterans of America v. McPherson, 2008 WL 4183981 (N.D. Cal. Sept. 9, 2008).
People v. Downin, 828 N.E.2d 341 (Ill. App. Ct., April 29, 2005).
People v. Morrow, 628 N.E.2d 550 (111. App. 1993).
Potamkin Cadillac Corp. v. B.R.I. Coverage Corp., 38 F.3d 627 (2d Cir. 1994).
St. Luke's Cataract & Laser Inst., P.A. v. Sanderson, 2006 WL 1320242 (M.D. Fla. May 12, 2006.
Talada v. City of Martinez, 656 F. Supp. 2d 1147, (N.D. Cal. 2009).
Toytrackerz, LLC v. Koehler, No. 08-2297-GLR, 2009 U.S. Dist. LEXIS 74484, (D. Kan. Aug. 21, 2009);
U.S. Equal Employment Opportunity Commission v. E.I. DuPont De Nemours & Co., 347 F. Supp. 2d 284 (E.D. La. 2004)
United States v Gagliardi, 506 F.3d 140 (2d Cir. 2007).

United States v. Allen, 106 F.3d 695 (6th Cir. 1997).
United States v. Barlow, 568 F.3d 215 (5th Cir. 2009).
United States v. Bonallo, 858 F.2d 1427 (9th Cir. 1988).
United States v. Cameron, 762 F. Supp. 2d 152, (D. Maine 2011);
United States v. Gagliardi, 506 F.3d 140 (2nd Cir, 2007);
United States v. Holmquist, 36 F.3d 154 (1st Cir. 1994)
United States v. Jackson, 208 F.3d 633, 638 (7th Cir. 2000).
United States v. Maldonado-Rivera, 922 F.2d 934 (2d Cir. 1990).
United States v. Moore, 923 F.2d 910 (1st Cir. 1991).
United States v. Safavian, 435 F. Supp. 2d 36 (D.D.C. 2006),
United States v. Scholle, 553 F.2d 1109 (8th Cir. 1977).
United States v. Simpson, 152 F.3d 1241 (10th Cir. 1998);
United States v. Sliker, 751 F.2d 477 (2d Cir. 1948);
United States v. Tank, 200 F.3d 627 (9th Cir. 2000);
United States v. Vayner, 769 F.3d 125 (2d Cir. 2014);
United States v. Vela, 673 F.2d 86 (5th Cir. 1982).
United States v. Whitaker, 127 F.3d 595, (7th Cir. 1997),
United States vs. Simpson, 152 F.3d 1241 (10th Cir. 1998).
Vacca, John R. (2005) Computer Forensics: Computer Crime Scene Investigation (2nd ed). Charles River Media, Inc..
Wady v. Provident Life & Accident Ins. Co. of America, 216 F. Supp. 2d 1060 (C.D. Cal. 2002).
Williams v. Long, 585 F.Supp.2d 679 (D. Md. 2008).