# Table of Contents

1.0 Introduction ........................................................................................................................................ 1

2.0 Types of Evidence .................................................................................................................................. 1

3.0 Impacts on the Audit Profession ........................................................................................................... 2

4.0 Differences between Paper and Electronic Evidence ............................................................................... 4
   4.1 Shortfall of Electronic Evidence .......................................................................................................... 4
   4.2 Value of Electronic Evidence ............................................................................................................. 5
   4.3 Other Differences ................................................................................................................................ 5

5.0 Control over Electronic Evidence ........................................................................................................ 7

6.0 Gathering Electronic Evidence ............................................................................................................. 8
   6.1 Sources of Electronic Evidence .......................................................................................................... 9
   6.2 Phases of Electronic Evidence Gathering ............................................................................................ 10
   6.3 Considerations while Gathering Electronic Evidence .......................................................................... 11

7.0 Implication on Audit Clients ............................................................................................................... 12

8.0 Conclusion ............................................................................................................................................ 14

Annotated Bibliography ................................................................................................................................ 15
1.0 Introduction
As the digital age advances, businesses today are vigorously moving towards electronic transactions and fully utilizing the power of the internet. This technological progression has greatly impacted the audit profession. In order to verify the relevant audit evidence, typically, auditors are required to browse through thousands of electronic records and documents, in addition to the familiar original, physically signed paper documents. As the audit evidence turns virtual and increases significantly in volume, what is the impact on the profession? How should the profession proceed to collect and control this new form of evidence? And lastly, what should their clients be aware of?

2.0 Types of Evidence
The Uniform Electronic Evidence Act defines “electronic record” in paragraph 1(b) as

"data that is recorded or stored on any medium in or by a computer system or other similar device, that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout or other output of that data, other than a printout referred to in Sub-section 4(2)." ¹

This implies that “the Federal Rules of civil Procedures for discovery in litigation” is not only limited to emails, word processing documents, and spreadsheets. ² Other items that can be requested includes “information databases, operating systems, applications programs, ‘computer-generated models’, electronic and voice mail messages and records, and other information or ‘instructions residing the computer memory’. "³

In an audit engagement, the uses of electronic records as audit evidence are now very common. As the audits become digital, the clients become more reliant on computers. The Canadian Institute of Chartered Accountants (CICA) defined electronic audit evidence as: “any information created, transmitted, processed, recorded and/or maintained electronically that the auditor relies on to support the content of the audit report.” ⁴ In a typical engagement, auditors would not go as far as looking through all client backup files, obtain employee email and phone records, recover deleted items, or hire experts to determine the authentication of electronic documents; they do, however, now have many different forms

of electronic records to go through. From the client, auditors may obtain calculations on balance sheet figures performed on spreadsheets, letters and invoices presented in word processing documents, journal entries and transactions that were entered into computer software, confirmation of payments completed through electronic fund transfer, as well as general ledgers and the financial statements which were generated from computers. Auditors would also obtain third party confirmations (from banks, lawyers, etc.) in electronic formats, through emails, or voice messages.

In fact, large number of paper evidence obtained in today’s audit engagements are originally generated from computers. Hardcopies and printouts generated by the computers are susceptible to the same type of manipulation risks as electronic evidence (while the information was still on the computers); thus, these types of paper records would also be considered as electronic evidence. Other original paper records (such as paper cheques, signed confirmation letters, etc.) can become electronic records after they have been scanned into the computer.

3.0 Impacts on the Audit Profession

The auditors must obtain sufficient appropriate evidence to conclude and support their audit opinion. With the use and reliance on computers and other electronic devices, there is an increase in acceptance of evidence in electronic form. This has significant impact on the audit profession as the audit evidence being relied on is becoming digital.

Many jurisdictions, including the Canadian federal government and most of Canada’s provinces, “[passed] e-commerce legislation and amended their evidence act to recognize electronic documents.”

Electronic evidence started appearing in courts since the late 1950s, and there were cases where emails were admitted as evidence beginning in 1996. The 2006 amendments to the Federal Rules of Civil

---


Procedures also made electronic records discoverable.\textsuperscript{10} Documents and records in electronic format are also being considered as audit evidence and some guidance were provided in the Generally Accepted Auditing Standards (GAAS) as well as the Canadian Auditing Standards (CAS).

As electronic evidence becomes more acceptable and common, the major impact of collecting electronic audit evidence is the “change in subject of audits”, as manual operations and internal controls becomes automated and applied by the information systems (IS).\textsuperscript{11} The automation would make auditors gain evidence over operating effectiveness of internal controls and the overall IS before they can determine reliance over all the documents generated by the client’s computer systems. Another impact on auditors is the pressure to “offer fuller services” as companies, with help from financial software, can now generate financial/non-financial public reports whenever they desire.\textsuperscript{12} This creates pressure on the auditors: although they are not responsible for these reports (such as quarterly statements), they are responsible for ensuring effectiveness of internal controls which would have prevented these non-audited reports from being completely inaccurate or unreliable. Auditors may need to perform more thorough work during the year end audit, or adopt the “continuous auditing” method instead of “backward inspection by testing the accuracy of the reported figures.”\textsuperscript{13}

The audit procedures around electronic evidence has a different focus as a research performed by the CICA found that auditors tend to use a combined approach to decrease risk when the client’s financial information is “created, transmitted, processed, recorded and/or maintained electronically.” Auditors would want to first ensure that internal controls are operating effectively and adequately prior to performing substantive tests, otherwise, “it may be impossible to sufficiently mitigate detection risk to reduce the audit risk to an acceptably low level.”\textsuperscript{14} The use of the combined approach is because the


“reliability of electronic information depends on the reliability of the IS and supporting technologies;”¹⁵ the use of substantive testing alone would not be able to provide sufficient and appropriate audit evidence.

The above factors lead to an increase in the need to understand the clients’ businesses and industries because it will help the auditors properly access the relevant risks and the appropriateness of internal controls and its IS. Client knowledge also helps with determining the relevance and reliability of the electronic evidence collected when reviewing the various “documents, records, and data”. The auditors should understand the “flow of transactions and related control activities” in order to determine the validity and reliability of electronic evidence and access the risk of manipulation.¹⁶

There is also the need for auditors to have some essential computer knowledge since they will have to effectively audit the internal controls over client’s IS. Over the past few years, the amount of electronic records received by the auditors has significantly increased; furthermore, with the adoption of digital audits, all evidence collected are electronic. Auditors need to receive and access electronic records, analyze and document these records, and appropriately store these records as evidence in the audit files. Although it is not necessary to become experts in the technical field, it is critical to have some computer knowledge in today’s audit engagements.

4.0 Differences between Paper and Electronic Evidence

There are more differences between the paper and the electronic evidences than just their form. They both have different intrinsic values and it is hard to determine which dominates over the other.

4.1 Shortfall of Electronic Evidence

The major difference when dealing with electronic records is that “there is no concept of an ‘original’ digital object”,¹⁷ and there is no difference between an “original” electronic record and a “copy” of that record.¹⁸

This difference create a more difficult environment for auditors (and lawyers) as, traditionally, they are “used to [deal with an original document] or an authenticated copy of the original of a document.”¹⁹

---


²⁰ Study
performed by members from the CICA indicated that the use of electronic records increases risks in "authentication, integrity, authorization and nonrepudiation of the information," which are the main "elements" that determines the reliability of audit evidence.20

Unlike paper files/records, electronic transactions can be altered or deleted without a trace, and digital documents can be easily manipulated without being detected. Even the output of the document itself can appear differently on various hardware and software. The “fragility of storage media, ease of alteration or corruption of stored data, complexity of computer systems” all contribute to the decrease in reliability and credibility of the electronic files to be used as audit evidence and more likely to be challenged during litigation.21

4.2 Value of Electronic Evidence

On the other hand, electronic evidence often includes additional information that cannot be found on paper records such as “how, when, and why people record information in electronic form.”22

In addition to the actual information shown on the file, electronic records contain information, or metadata, on whom created/modified the file and exactly what time that occurred. The electronic file would hold information on the person whom is authorized to have access to the documents and those who have ability to modify versus strictly viewing the document. There may also include information on whether the file was directly created or a result of another file/database (such as calculation or lists). Distribution documents (such as emails) in their electronic formats would also show the distribution list and time of circulation.

All these additional information can be used as audit evidence since they are part of the electronic records. A paper records, however, only contains information that is physically shown on the document.

4.3 Other Differences

Depending on the nature, timing, and extent of the audit, some other features of the electronic evidence can be beneficial to the auditor in one engagements while creates challenges in another.

Electronic records tend to come in large quantities because they can be generated very quickly and accurately duplicated. This becomes problematic and time consuming when auditors need to go through all these records to select the most appropriate items as audit evidence and/or determine the most appropriate method to select a representative sample for testing. This large quantity of information will increase detection risk in an audit, as the percentage of total data being tested decreases. However, large quantities also means auditors can review (and maintain copies of) progress of certain documents/reports, since people often keep several draft versions throughout different stages of completion to minimize loss of data in the event of technical failures. People are more willing to pass around electronic version of draft reports or informal documents rather than the actual carbon copies of the documents as paper versions appears to be more formal. These informal documents can either act as audit evidence or be used for audit planning.

The extensive use of email creates opportunities for auditors to obtain large amount of timely electronic information. Emails provide digital evidence on the occurrence of communication/agreements between two parties and visual proof of the context of conversation. People tend to be more casual and careless in email conversations\textsuperscript{23} which may provide the auditors with unexpected information or insight to the client corporation. Conversely, with the large number of emails send per day (it was estimated that average of 247 billion emails per sent per day in 2009\textsuperscript{24}), it can get very time consuming or complex to browse through and locate the one email with the desired information.

Electronic evidence is also harder to destroy because simply deleting the file on the computer is not enough. With appropriate forensic tools, experts can now recover deleted files (as long as they are not completely written over).\textsuperscript{25} In addition, backup copies of the file may exist in other locations, as most technical reliant companies are performing file backups regularly and storing them offsite.\textsuperscript{26} This feature of the electronic evidence comes in handy during forensic audit or litigation; however, this may also create a problem for confidential documents that are meant to be destroyed. As clients sometimes will provide the auditors with confidential documents that must be destroyed after use or after issuance of audit report, procedures must be taken to ensure that these electronic evidences are properly destroyed.


Storage and organization of electronic evidence is very different from paper records. Electronic evidence takes up a lot less physical storage space than boxes of paper files, and it is much faster to find and pull up than logically ordered paper file cabinets. However, electronic evidence requires multiple duplications for backups and to be stored offside because of the "fragility of computer-based data and its dependence on the technology infrastructure." Electronic evidence also needs additional protection than the usual required for paper records: "fire, flood, humidity, temperature extremes, and other environmental issues, such as physical security"; electronic evidence also require "electrical current reliability and stability for equipment, network access controls, and user authentication management." As the Canadian Standard on Quality Control indicated, retention period for engagement documents should be kept for at least five years, the audit firms must ensure that proper technology used and backups created to maintain electronic evidence from audit engagements for at least that amount of time.

5.0 Control over Electronic Evidence

Currently, under the Canadian law, there is still uncertainty regarding "the conditions of admissibility of electronic documents" and "cyber transactions." Thus the best way to "mitigate the legal risks" concerning admissibility is to "implement and maintain reliable information system and use appropriate technologies that will establish the data's authenticity and integrity." A reliable IS requires the controls around the electronic evidence to be operating effectively and adequately.

When collecting electronic evidence, auditors must remain skeptical and consider the possibility of digital evidence to be manipulated without a trail. There should be restriction on access of electronic records to authorized client members and records should be protected physically (restriction of access to computer stations) and electronically (through strong passwords). Auditors need to determine the existence of system logs, its record of "successful and failed access attempts", regularity in reviews on the logs, and proper maintenance on the "continuity of the logs". Same access restriction should be present in the auditor's firm to prevent unauthorized access to the electronic evidence during and after the engagement.


Proper controls should be in place during transfer of electronic evidence since the evidence may be altered during the transfer. The evidence should only be transferred through authorized devices, such as password protected USB keys or encrypted emails, this would reduce the risk of unauthorized access or alteration in the case of interception. The evidence should successfully reach the intended person (the auditor requesting the information) and controls on copy/sharing of the confidential records should be specified.\textsuperscript{31} To prevent manipulation of third party evidence during transmission, auditors need to obtain the evidence directly from the third party or, at least, ensure the copy received from the client includes “read-only” restrictions imposed by the third party.\textsuperscript{32} Since electronic files contain metadata, the auditors should check to ensure the appropriate personnel created the file at an appropriate time and that there were no indication of modifications to the digital file.

The storage of electronic evidence also requires controls. Logs should be kept to ensure proper audit trails of evidence are present. The logs must be “accurate” so that there is no alteration of entries, it must be “complete” so there are no missing/deleted entries, and it must be “compact” so there is no unauthorized addition of entries. The evidence should also be stored in an encrypted format so that it would be protected in the event of unauthorized accesses.\textsuperscript{33} Auditors should also ensure that their clients implement proper disaster recovery plan, and backup tapes are created regularly and sufficiently to satisfy the clients’ predetermined recovery point objectives (amount of acceptable data loss).

### 6.0 Gathering Electronic Evidence

Once it is determined that the client’s internal controls are operating effectively, the auditors can gain some comfort over the reliability and appropriateness of the electronic evidence. The auditors now need to properly gather the evidence to reach an audit opinion. While the computer advanced as Gordon Moore predicted in the Moore’s Law (“the number of transistors on a chip” have been doubling every two years for the past 40 years\textsuperscript{34}), the progress of electronic evidence collection technologies is falling far behind. However, in the recent years, many tools have been developed to facilitate electronic evidence collection, and is expected that there will be more to come.


6.1 Sources of Electronic Evidence

Majority of electronic evidence gathered by auditors (in a regular audit) are obtained directly from the clients, with some obtained from third parties, and others created by auditors themselves while running through data on their software and/or recalculating certain figures on the computer. During more serious situations, such as forensic auditing or electronic discovery for litigation, digital evidence collection will be more thorough and obtained using forensic tools from various computers and devices.

Electronic evidence can be collected from a wide range of devices, with the most common being laptop and desktop hard drives which stores the user’s documents and emails. Portable media, such as CD-ROMs and USBs, are some people’s preferred method of storing and transferring electronic records; and backup tapes contains all important company documents from the past.\(^{35}\) Email, in addition to hard drive of the user’s computer, can be found “on email servers, on ISP servers (a court order is required to access these) and in company backup tapes.”\(^{36}\)

Some electronic evidence can be obtained easily by a staff accountant through direct access of client’s database, while others require special forensic tools and the help of experts. With assistance from new computer forensic tools, such as SmartCarving, it is now possible to recover all or “partial images” of deleted records (as long as the hard drive is not completely overwritten).\(^{37}\) “Fragile” evidences should only be proceeded with experts because these evidence can be unintentionally “tainted” by simply looking through the data (i.e. the modification date will be changes to the current date). Types of “fragile evidence” includes transient data (which will “be lost at shutdown”), fragile data (which can be manipulated very easily), and temporarily accessible data (which “can only be accessed at certain times”).\(^{38}\) Even CAS (and GAAS) specifically stated that electronic evidence should be collected throughout the auditing period to deal with temporarily accessible data and lack of backup files.\(^{39}\)

During a forensic audit, one of the more common places to collect electronic evidence is from the person-in-question’s computer hard drive. Proper care must be taken to “[ensure] that the original is in the best state possible for presentation in a court of law.” This can be done by duplicating the original hard drive.


and all of its contents. This allows the performance of various audit techniques on the data of the duplicated drive without concern over modifying the original data. It is also a good idea to create more than one copy of the original hard drive, such that different test approaches can be performed on the “original” data. The auditors or information technology (IT) personnel must ensure, however, that the hard drive copy is “a perfect reproduction of the original”, otherwise its reliability will be challenged in court.  

Auditors should consider gathering evidence in areas where least expected, since tracks for most common areas will be carefully covered. For example, “internal fraudsters” would use phones that would not be traced to them specifically, such as “the phone on a company fax machine”, thus insightful electronic evidence may be obtained from the phone logs of these machines.  

Many printers and photocopiers can include hard drives and memory capabilities; since almost half of the IT staff surveyed (in a study performed by Albert Marcella) were not aware of the hard drives in these machines and more than half of the IT staffs does not consider those machines as risks, these machines may provide critical digital evidence. Access logs to certain rooms can provide evidence because not many employees are aware that security cards, used to enter rooms, may “[leave] a record of who uses the card and when”. Finally, “people tend to be more careless about what they store on” Blackberries because they consider Blackberries to be personal devices. However, if an employee’s Blackberry is in sync wirelessly with company’s “Outlook Exchange server”, then “everything on [that employee’s] Blackberry [is] also on the server”. Because the server would be the client’s property, search can be performed without consent of the employees.

6.2 Phases of Electronic Evidence Gathering

When gathering electronic evidence, it is important to document “where [the evidence] came from, when it was gathered or how it was passed along” to the auditor in case of re-performance or litigation.

The auditor first need to identify all relevant information and ensure that the “original metadata associated with the file remains preserved.” The identification phase helps the auditor plan out where the evidences are located and the relevance of evidence to the objective (audit or litigation).

---

After identification, there is the need to preserve the electronic evidences to prevent them from unintentional modification or deletion. The evidence content should be "exported from the repository in a legally-defensible manner".45

Finally, the evidence must be collected in such a way that there is no data loss/alteration. There are many tools that can be used for "capturing digital files" and most of the tools will return accurate results for a decent collection "as long as the collection criteria [are] carefully considered".46 For example, specific electronic evidence can be found and extracted from the database through appropriate keyword searches.

Proper care on the electronic evidence is required even after collected, this is because in the event of litigation (or quality control review), the digital evidence must be "authentic". This requires that "the content of the data that a party relies upon has not changed from the moment it was created to the moment it is submitted as evidence." There must be evidence showing that the electronic data was "from the purported source". Finally, "the technical and organizational evidence demonstrates the integrity of the data is trustworthy, and is therefore considered to be reliable."47

After completing collection of electronic evidence, there may be the need to remove "irrelevant and duplicated or near duplicate material."48 Auditors should maintain sufficient audit evidence but not too much so that it will be overwhelming to analyze all the evidence and time consuming for the reviewer to go through.

6.3 Considerations while Gathering Electronic Evidence

During audit evidence gathering, there are several criteria the auditors should keep in mind.

First, despite the effectiveness of controls, the difficulty of alteration (without being detected) of an electronic evidence should be determined and valued higher with higher level of difficulty. Like paper evidence, higher credibility is awarded to those with "independence of the source of the data and the auditor's ability to verify the evidence" such as "read-only" third party documents. The evidence must be

46 Ibid
complete as it contains appropriate metadata and contains “all essential terms and details of the transaction”. Sign of approval, such as electronic signature, would also enhance the completeness and validity of digital evidence. It is also critical that evidence is “easy for an auditor to use” which will imply simplicity of “evaluation and understanding”. It was established that “evidence that can be easily understood and consistently interpreted by different individuals performing the same task is generally the most competent.”

Some evidence collected may originally be paper documents but subsequently converted into electronic evidence through scanning to facilitate record keeping of a digital audit. Use of scanners may “weaken traditional sources of audit evidence” because fraudulent confirmations can be created by scanning in third party’s logo or manipulation performed on the actual scanned in document. Thus auditors should always obtain the original third party documents themselves, verify the authenticity of the documents, and personally scanning them into the audit files.

Other electronic evidence may be collected in the form of paper, such as hardcopy listings or printouts generated from computers. With new sophisticated tools, auditors must maintain skepticism throughout an audit because a scanner and printer can create very convincing paper evidence. Auditors should be cautious of disguised electronic evidence, since the printout version of evidence still contains the same intrinsic values (such as the metadata) and risks as its digital version, however, such information is not shown on the printout itself.

7.0 Implication on Audit Clients
As electronic evidence has drastic impacts on the audit profession, some aspects should be communicated/recommended to the audit clients as they will be affected and even disadvantaged if proper procedures are not taken.


Adequate and effective internal controls should be in place around all electronic records as indicated in the earlier sections: documents should be properly approved and stored, access to files should be restricted to authorized personnel, access logs should be reviewed regularly to detect unauthorized access (or attempts of access), etc. Effective internal controls along with timely review can help detect and prevent fraudulent activities (such as manipulation/deletion of transactions in an attempt to hide wrong doings) within the client organization. Controls around access of electronic records will avoid leakage of private, confidential, and sensitive information since large amount of digital records can be stored in very tiny portable storages.

Organization/management of all records, electronic and physical, is critical in an organization because while physical records still "dominate many workplaces", the electronic records "are a major focus of requests for information" during discovery activities for "regulatory audits and litigation". According to the 2006 amendments to the Federal Rules of Civil Procedure, with reasonable explanation, all "possible sources of electronic records, even their hard-to-access back-up tapes or other disaster recovery systems" may be searched during a litigation-related discovery. Since digital records often come in large quantities, organizations must ensure that the records are organized appropriately and named/described accordingly to facilitate extraction of records during searches. Otherwise, unnecessary resources can be wasted and the client is subject to penalties when the appropriate evidence cannot be found on a timely manner. Appropriate backup tapes should be kept offsite to prevent situations where required electronic evidence cannot be provided due to system failure in one area.

The client should communicate to its employees that appropriate conducts should apply to emails sent during work because employee emails sent through work computers or servers are discoverable. Since emails tend to be informal, any inappropriate content discovered can damage the client’s reputation. Duplicating or redundant electronic records should be deleted to prevent overwhelming evidence searches and inefficient use of storage space (and additional duplications during backup copies).

Like the audit firm, the clients should train/hire employees with sufficient knowledge to handle electronic records. The clients have equal responsibilities to ensure that its electronic records are reliable and free from manipulations. The client must have appropriate IT resources to maintain its IS, guarantee strong controls and effective storage.


8.0 Conclusion

As companies around the world become more reliant on computers and other similar devices, the quantity and impact of electronic records will continue to increase. For auditors, this implies greater significance in electronic audit evidence. They can take advantage of the additional properties in the electronic evidence (the metadata) but should also be aware of the added risks (of undetectable manipulation in data). There will be a shift in audit approach to concentrate more on the internal controls and apply more due care in gathering and preserving the electronic evidence.

The audit client should also be aware and prepared for the shift towards electronic records by having proper internal controls, good management on all records, proper communication to employees, and sufficient resources to maintain the electronic records.

It requires combined efforts between the auditors and their clients to ensure there are sufficient appropriate audit evidence (electronic and physical) to conclude on the audit opinion.
### Annotated Bibliography

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/ website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greene, Tim</td>
<td>Forensic tool will advance data recovery</td>
<td>Network World</td>
<td>Vol. 27, No. 9</td>
<td>2010</td>
<td>21 (1 page)</td>
<td>May 28, 2010</td>
<td>ABI Inform</td>
</tr>
</tbody>
</table>

**Annotation**

- New computer forensic tools, SmartCarving, able to recover 10-15% more digital into than “conventional forensic tools miss”
- Can recover even after deletion, as long as the hard drive is not overwritten
  - This include deleted emails
- Improved form for investigators to get electronic evidence to be used in legal cases
- Traditionally, tools look for a “known header and footer for a file and gathers all the related data blocks in between.” If the data are fragmented then the traditional tool crash when they hit a fragment of a different format that might be sandwiched between pieces of the file being sought.
- SmartCarving “[draw] together data blocks from a single image that are arranged consecutively on a drive and linking them to other groups of data blocks based on whether they seem to blend using criteria such as pixel density and dimensions of the image.”
  - Can now “recover partial images”
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
</table>

**Annotation**

- “make little sense to base an investigation of potential latent data, residing on a photocopier, if it could be proven that the machine itself lacked basic security features that might render any potential evidence”
- Almost half of IT staff surveyed were not aware that printers and photocopiers include hard drives, more than half does not consider those as risk
- Auditors/investigators should consider “any device capable of storing data as a potential source of electronic evidence” which include input/output equipments
  - Determine if the client should have control over these devices

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/ website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mason, Stephen</td>
<td>Electronic evidence and the meaning of &quot;original&quot;</td>
<td>Amicus Curiae</td>
<td>Iss 79 Autumn</td>
<td>2009</td>
<td>26 – 28</td>
<td>May 31, 2010</td>
<td>Google Scholar</td>
</tr>
</tbody>
</table>

**Annotation**
- Traditionally lawyers are “used to dealing with an original document, or an authenticated copy of the original of a document”. However, “there is no concept of an ‘original’ digital object”
- When determine how “authentic” the electronic item is, the following should be followed:
  - The content of the data that a party relies upon has not changed from the moment it was created to the moment it is submitted as evidence
  - The data can be proven to be from the purported source
  - The technical and organizational evidence demonstrates the integrity of the data is trustworthy, and is therefore considered to be reliable.”

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/ website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
</table>

**Annotation**
- “Email, word processing documents, spreadsheets, potentially test messages and even voice mail are all subject to the Federal Rules of Civil Procedures for discovery in litigation”
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/ website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gensler, Steven</td>
<td>Some Thoughts on the Lawyer's Evolving Duties in Discovery</td>
<td>Northern Kentucky Law Review</td>
<td>Vol. 36, No. 4</td>
<td>May 2009</td>
<td>48 pages</td>
<td>June 7, 2010</td>
<td>Social Science Research Network</td>
</tr>
</tbody>
</table>

**Annotation**

- 2006 amendments to Federal Rules of Civil Procedure
  - Electronic records are discoverable
  - With reasonable explanation and “good cause”, can search all "possible sources of electronic records, even their hard-to-access back-up tapes or other disaster recovery systems" → need to apply for this
Annotation

- Case from 1996 admitted email as evidence for fraudulent activity
- Electronic evidence (EE) – “any information created or stored in digital form whenever a computer is used to accomplish a task"
  - Items include: “information databases, operating systems, applications programs, ‘computer-generated models’, electronic and voice mail messages and records, and other information or ‘instructions residing the computer memory’”
- Electronic evidence is playing a more critical role in criminal and civil litigations.
- Difference between EE and paper trail:
  - EE comes in large quantities and can be generated very quickly
    - i.e. very large number of people use emails and the number is growing → at least 20 mil in U.S. in 1994
  - Paper evidence may not exist
    - District court: “[c]omputers have become so commonplace that most court battles now involve discovery of computer-stored information.”
  - EE is hard to destroy
    - “hitting the delete button does not destroy the computer records”
    - Experts are able to get electronic files after deletion
  - There are “fundamental and meaningful” differences between electronic form email and its print out
    - Electronic version includes “distribution lists, directories, and acknowledgements of receipts”
    - Court: “essential transmittal information relevant to a fuller understanding of the context and import of an electronic communication will simply vanish”
  - EE “often contains informal material that do not exist in paper form”
    - EE contains “how, when, and why people record information in electronic form”
    - People “routinely…send draft, informal, or ‘uncensored’ messages they would never ‘put in writing’”
  - EE is “easy to manipulate” and easy to “exchange electronic information”

http://heinonline.org/HOL/Page?handle=hein.journals/jstl4&div=10&g_sent=1#180
Yung, Chin
Electronic Evidence: Disclosure, Discovery and Admissibility
Singapore Journal of Legal Studies
July 2008
219 - 223
June 9, 2010
ABI Inform


Annotation
- Computers and electronics simplified paper document evidence: “copies are now readily accepted (though not in all jurisdictions) because of the accuracy of digital copiers in reproducing paper originals”
- Difficult to “[establish] a sound evidential foundation” for EE because of “fragility of storage media, ease of alteration or corruption of stored data, complexity of computer systems”
  - No difference between “original” and “copy” for EE
- Once EE is accepted, it may be overly relied on
- Very complex to “authenticate” EE
  - Output will can be different depending on hardware and software used
  - “Digital enhancements or editing or changes in metadata that need to be explained to prove the reliability (or integrity) of the output”
  - Mason: “where the authenticity of a digital object is in (sic) issue, the range of considerations to be taken into account will differ, according to the nature of the evidence to be authenticated and where evidence is to be found”
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/ website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
</table>

**Annotation**
- Electronic data impacts audit in 2 ways:
  - “change in subject of audits” → manual operations and internal controls are automated and done by information systems
  - Pressure to “offer fuller services” → company, with help of financial software, can generate financial/non-financial public reports weekly
- Auditors now need to adopt “continuous auditing” instead of “backward inspection by testing the accuracy of the reported figures”
- This report propose a continuous auditing model: the agent-based continuous audit model (ABCAM) → use a multi-agent system
  - The system use “mobile agents to help human auditors to perform auditing work that is tedious, trivial, or complicated.”
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeVries, Delwyn D.</td>
<td>The Risks of “Paperless” Bank Checks</td>
<td>The Journal of Corporate Accounting &amp; Finance</td>
<td>Vol. 16, Iss. 4</td>
<td>May/June 2005</td>
<td>49 – 55</td>
<td>June 9, 2010</td>
<td>ABI Inform</td>
</tr>
</tbody>
</table>

**Annotation**

- Banks starting to use Check Clearing for the 21st Century Act (Check 21) → send digital image (both sides) of cleared check to issuer
  - “All parties must accept substitute checks, and neither financial institutions nor the disbursing party can require return of the original check.”
- Easier to fabricate fake checks since it’s all digital
- Auditors can no longer go through the returned cleared paper checks
  - Must evaluate “validity, completeness, and integrity” of the digital checks when performing substantive test
- In 1997, the American Institute of Certified Public Accountants (AICPA) notes the impact of EE
  - EE “includes information that is transmitted, processed, stored on, or accessed by electronic means such as computers, scanners, and files on magnetic media.”
- Comparison of paper and electronic evidence
  - Difficulty of alteration
    - “Evidence that can be easily altered without detection has low credibility and little value to an auditor.”
    - Paper: auditor can easily detect alteration; can determine if check is genuine (material, signature, etc)
    - EE: hard to determine if the check is something company use regularly; may be manipulated in bank’s or client’s system
    - Recommend: obtain “all paid checks in a read-only format” from the bank
  - Prima Facie Credibility
    - “A primary consideration is the independence of the source of the data and the auditor’s ability to verify the evidence.”
    - Paper: checked processed by 3rd party (the bank) is “typically…and high degree of credibility.”
    - EE: auditor would obtain the check images from client’s system
    - Recommend: “read-only restricted files” with “digital signature that the bank reconciler or auditor would examine”
- Completeness of Documents
  - “The validity of a transaction can be verified from documents or records containing all essential terms and details of the transaction”
- Paper: paid checks can be differentiated from unprocessed checks because they will have endorsements/indicators
- EE: may require transaction codes and cross-referencing (to other files) in order to understand; may not be retained as long as paper
- Recommend: more frequent testing for "transactions such as rejects, confirmations, and other transitory items"; also need to examine and trace codes and cross-reference
  - Evidence of Approvals
    - "Approval of transactions that is integrated into evidence enhances the completeness of that evidence"
    - Paper: visual inspection
    - EE: must first determine what is the evidence of approval, for example "use of sign-off approval codes, digital signatures, and cross-references to authorized individuals or positions."
    - When testing for approval, it is also an efficient way of "evaluating control compliance across all transactions"; 2 separate testing required for paper
    - Recommend: reliance depend on good controls over "code changes and security access privileges to change the information"
  - Ease of use and clarity
    - "Evidence that is easy for an auditor to use leads to ease to evaluation and understanding. Evidence that can be easily understood and consistently interpreted by different individuals performing the same task is generally the most competent"
    - Paper: can evaluate "without special tools or expert analysis"
    - EE: must "interpret in the context of the business’s information system and the presence or lack of system controls"; require data extraction

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/ website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nearon, Bruce</td>
<td>Foundation in Audit and Digital Evidence</td>
<td>The CPA Journal</td>
<td>Vol. 75, Iss. 1</td>
<td>Jan. 2005</td>
<td>32 – 34</td>
<td>June 9, 2010</td>
<td>ABI Inform</td>
</tr>
</tbody>
</table>

**Annotation**
- Assurance over EE of transactions require understanding and testing of IT controls around those transactions
- Foundation for audit: competence, independence and due care
• “Most auditors still approach digital records as if they have the same intrinsic qualities as physical records:
  o Hardcopy listing and printouts are generated from computers (and thus could have been manipulated in the computer) and should be treated as EE
• Auditors must be skeptical since digital transactions are a lot easier to alter/delete without a trail
  o Need to corroborate and test controls around the applications
  o Management or independent review of controls
  o Back-ups?
  o Strong passwords

**Annotation**

- Procedures need to be taken to prevent EE from being “destroyed, corrupted or becoming unavailable for forensic investigation.”
- EE need to be properly stored, security need to take place to ensure that the data are not deleted or manipulated
- Forensic-imaging software can obtain "residual data" including "deleted files, fragments of deleted files and other data that still exist on the electronic media’s recording surface."
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/ website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
</table>

**Annotation**

- Businesses are moving toward electronic transactions and internet
- 1998 Vision Project of AICPA noted that “technological advances are significant forces affecting the accounting profession”
- Audit is affected by continuous auditing in many ways:
  - Increase knowledge of client business/industry → determine relevance and reliability of EE (“documents, records, and data”) and effectiveness of controls
  - Understand “flow of transactions and related control activities” for valid and reliable of EE and determine risk of manipulation
  - Need to utilize “control-risk-oriented audit plan” focusing specifically on internal controls → its “adequacy and effectiveness”; there is less emphasis on substantive testing of digital “documents and transactions”
  - Auditors need to utilize computer software tools (such as Continuous Audit Tools and Techniques) to “assess risk, evaluate internal controls” and perform electronic procedures “including extracting data, downloading information for analytical review, footing ledgers, counting records, selecting samples for tests of controls and substantive tests, identifying exceptions and unusual transactions, and performing confirmations.”
- Auditors can perform control test with substantive test to gain comfort over client’s electronic system to “[produce] reliable and credible financial information”
- Need evidence regarding “(1) how are data electronically gathered; (2) how, from where, and from whom are the data originated; (3) what authentication techniques are used; (4) what networks are used to originate and transmit the data; and (5) how are the data processed”
### Annotation

- "Full forensic analysis of the computer" required to obtain EE because unlike physical evidence they can be deleted without a trace and no clear sign of forced entry (unauthorized access)
- EE may be “tainted” unintentionally by individuals looking at the data trying to figure out what happened
- Types of “fragile evidence”
  - Transient data – data “will be lost at shutdown”
  - Fragile data – stored on hard disk “but can easily be altered”
  - Temporarily accessible data – stored on disk but “can only be accessed at certain times”
- Connecting removable devices (i.e. USB) to computer with fragile evidence is “not advised as this will change the system state”. The “best method of extracting data” is through network connection.

### Annotation

- In paperless accounting, degree of EE increased significantly
- Dependence on EE affect audit risk level because substantive testing may not sufficiently reduce detection risk
  - Additional tests required to “reduce overall audit risk”
  - Hard to spot EE manipulation/alteration → must determine simplicity of alteration
- Need to inspect the “electronic transaction audit trail that identifies the date, time, original terminal and originating user of each transaction”
- Auditors may be required to conduct testing throughout the year due to existence of EE that exist “only at certain point of time and backup files may not exist”

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
</table>

---

26
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/ website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
</table>

**Annotation**

- Evidence used in legal dispute must guarantees of “trustworthiness”
  - Data collected must be a “faithful representation of the events”
  - The collection must “guarantee completeness and authenticity”
  - No unauthorized undetectable deletion of data
  - What “authenticity of audit trails”
- Transmission of data
  - Authorized devices for transfer
  - Confidentiality of transfer
  - Message can’t be manipulated
  - Unique message
  - Received by appropriate person
- Storage
  - Entry contain the “subject (i.e. device and collector) that appends the entry to the audit trail”
  - Audit trail cannot be modified → “accuracy”, “completeness”, and “compactness”
  - Confidentiality – “not stored in clear-text”
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/ website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Annotation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Sarbanes-Oxley Act in 2002 include “retention of electronic documents”</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Public accounting firms must be able to conduct “enterprise-wide discovery efforts” to recover “computer-based evidence” if required by the Public Company Accounting Oversight Board</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Tools such as Enterprise Response, Auditing and Discovery (ERAD) are able to cover “a wide variety of computer incidents ranging from unauthorized deletion of critical data, network intrusions, and internal theft of intellectual property.”</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sommer, Peter</td>
<td>Emerging Problems in Digital Evidence</td>
<td></td>
<td>2004</td>
<td>8 pages</td>
<td></td>
<td>June 10, 2010</td>
<td>Google Scholar</td>
</tr>
<tr>
<td><strong>Annotation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● EE have been used in courts since late 1950s</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Progress were only made in small part of EE: disk and network forensics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Disk: “making an exact copy of a hard-disk” in order to “[reconstruct] past activity” concentrating on hidden and deleted data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Network: “reliably capturing activity on a network” and match against potential computers in order to “reconstruct activities an actions”
- The court require “reliability and admissibility” to use evidence (including EE)
- Current problems:
  - Tracking activities on the internet by law enforcements (with warrant) often cannot state their methods in court otherwise criminals will take preventative actions. However, without indication of method, the other party may argue that these are critical information
  - Too much data. Ex. In 2004, over 1 TB of data seized from 6 UK citizens in addition to thousands of CD-ROMs

In a litigation, when using EE, it is critical to know “where [the evidence] came from, when it was gathered or how it was passed along to arrive in front of you”

Major phases of e-discovery:
- Identification
  - Determine relevance of information and “flag them for litigation” and categorize the information
  - Need information about the flagged data
  - Must ensure that the “original metadata associated with the file remains preserved”
- Preservation
  - After identification, need to prevent the EE from unintentional modification/deletion
  - Need to comply with “pending litigation” and the content “exported from the repository in a legally-defensible manner”
  - Defensible means “deterministic (repeatable and testable results), transparent (well-understood and articulated) and trusted (non-repudiation of the end results)
- Collection
  - There are many tool used for “capturing digital files” and most tools will return accurate results for a decent collection “as long as the collection criteria is carefully considered and proper software “switches” are used”
  - Very costly, but thorough if perform collection personally on client site
- Less costly if client IT is to perform collection or if collect remotely
  - Processing
  - Review
- Metadata ("the data about the data") include information such as "the date the file was created and added to the repository, the person responsible, modification date, and the logical file location" may become critical evidence during litigation/discovery
- Auditor/accountants need to understand company's e-discovery practices and ensure it is "consistent and defensible in court"

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
</table>

**Annotation**

- Importance of EE
  - Large quantity
  - Durable – possible to recover after deletion
  - New types of "objective documentary evidence" – metadata containing information such as date of creation, modification, viewed and by whom
  - "the casual nature of emails makes them a rich source of revealing evidence"

- To go through the large quantity
  - Prioritize source/types; determine method of collection and review of EE
  - Secure the data – perform backup, stop routine deletion of data

- There are different forms/location of data
  - Laptop and desktop hard drives – store documents and emails
  - Portable media – CD-ROMs, USB, etc
  - Back-up tapes
  - Live database – stock, sales, accounting, etc

- Different methodology of collection required for the different types of media

- Before review by investigator, need to remove "irrelevant and duplicate or near duplicate material" (focus on particular file type or data range, etc)

- Depending on the size of the remaining, more relevant, data, additional organization and reduction may be required to end with a reasonable size of data for review
Mike Duren and Chet Hosmer

**Can Digital Evidence Endure the Test of Time?**

2002

7 pages

June 11, 2010

Google Scholar


**Annotation**

- Must maintain digital integrity ("the property whereby digital data has not been altered in an unauthorized manner since the time it was created, transmitted, or stored by an authorized source")
- With application of "cryptographic hashes and digital signature technology" for the EE, the "who" and "what" can be obtained
- However, the system clock that track time when file was created, modified, and access are "unreliable and completely untrustworthy". Even after development of the TimeStampToken, the question of reliability still remains. The Internet Engineering Task Force (IETF) defined an entity called Time Stamp Authority (TAS) and "simply stated that the entity must be trusted."
- Now there are many technical approaches to "[create] traceable time" with different levels of automation
- Toot Time Authority (RTA) is a Trusted Third Party (TTP) that attests validity of time for a Secure Time Module (STM). RTA ensures that the clocks are traceable to the Coordinated Universal Time, but it not necessarily complete the “traceability requirement” back to a clear reference.
Additional Sources

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
</table>

Annotation

- Research report
- Electronic audit evidence – “any information created, transmitted, processed, recorded and/or maintained electronically that the auditor relies on to support the content of the audit report.”
- Evidences includes “accounting records, especially source documents, journals and general ledgers, supporting documents and any other data or information in electronic form useful for the audit.”
- Raise risk: “authentication, integrity, authorization and nonrepudiation of the information” – these are “elements” for assessing reliability
- The Study Group: “reliability of electronic information depends on the reliability of the IS and supporting technologies”
  - Look at the IS’s “controls and technology”
  - Research found that auditors tend to use a combined approach to decrease risk when information is “created, transmitted, processed, recorded and/or maintained electronically”
  - If internal controls is “deficient”, it may be hard to obtain sufficient appropriate audit evidence from substantive testing and “it may be impossible to sufficiently mitigate detection risk to reduce the audit risk to an acceptably low level”
- Should look at electronic signature and ensure “authentication, integrity, authorization and nonrepudiation”
- “federal government and most Canadian provinces have passed e-commerce legislation and amended their evidence act to recognize electronic documents”
  - Under Canadian law there is still uncertainty regarding “the conditions of admissibility of electronic documents and signatures” and “cyber transactions”
  - For electronic documents, must “[prove] its authenticity and integrity by providing evidence capable of supporting a finding that the document is indeed what it purports to be”
  - Best way to “mitigate the legal risks” concerning admissibility is to “implement and maintain reliable information system and use appropriate technologies that will establish the data’s authenticity and integrity”
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paul Caster, and Dino Verardo</td>
<td>Technology Changes the Form and Competence of Audit Evidence</td>
<td>The CPA Journal</td>
<td>Vol. 77, Iss. 1</td>
<td>2007</td>
<td>68 - 70</td>
<td>July 10, 2010</td>
<td>ABI Inform</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Annotation**

- Scanners may "weaken traditional sources of audit evidence" because fraudulent confirmations can be made by scanning 3rd party’s logo
- Printers can also create fraudulent documents
- Emails need to be checked for validation. In the past, with paper mail, auditors can check postmark for city mailed from. Cannot do this for emails.
- Companies often keep electronic version of returned/cleared cheques, instead of the actual one from the bank, this is subject to manipulation
  - Auditors should select sample of cheques and inquire the person that signed the cheque to ensure validity
- Electronic signatures now accepted by law, “contracts and agreements with these signatures legally binding”
  - Auditors should select a sample and contact the signer
- Auditors should test controls along with traditional audit procedures
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
</table>

**Annotation**

- It is critical to have good record management system in an organization
- “Trustworthy and accessible records are authoritative sources of evidence and information that support and sustain the credibility and accountability of any organization”
- The trustworthiness of electronic records are being challenged
- Critical part of an organization’s information strategy is to incorporate “corporate filing structure and explicit records retention and disposal schedules.”
- Trustworthiness – “an information system’s accountability and its ability to produce reliable and authentic records and information”
  - Per South Carolina Trustworthy Information Systems Handbook, 2007
- Trusted records must show integrity, reliability, and authenticity
  - Record integrity – “the completeness of the record” which depends on “their content, context and structure”
  - Record reliability – “the content can be trusted as a full and accurate representation of the transactions, activities or facts to which it attests and can be depended upon in the course of subsequent transactions or activities”
  - Record authenticity – “a record is what it purports to be and has been created by the organization with which it is identified”
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
</table>

**Annotation**
- EE can be found “in sources other than a hard drive”
- Employee emails can be located in several places: “user’s hard drive, on e-mail servers, on ISP servers (a court order is required to access these) and in company backup tapes”
- Recover items from “backup tapes could be time-consuming and expensive”
- Phone logs can be type of EE – “office line and cellphone”
- “internal fraudsters” would use phone that would not be traced to them such as “the phone on a company fax machine”
- Security cards, used to enter rooms, may “[leave] a record of who uses the card and when”
- Data from Blackberry: “People tend to be more careless about what they store on them”
  - If Blackberry is in sync wirelessly with company’s “Outlook Exchange server”, then “everything on [employee's] Blackberry was also on the server” → don’t need to get employee’s Blackberry
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/ website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
</table>

**Annotation**

- Need to know where the EE is located
- Must preserve the EE
- Try to reduce handling the original data
  - Minimize change of altering the data
  - Should duplicate the original data and examine the copy
    - "ensures that the original is in the best state possible for presentation in a court of law"
    - Can work on the copy using different techniques
    - Permit multiple experts to work on the data at the same time
    - Must ensure that the copy is "a perfect reproduction of the original", otherwise may not be reliable
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/ website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
</table>

**Annotation**

- “During regulatory audits and litigation-related discovery activities, electronic records are a major focus of requests for information.”
- Must manage records, electronic and physical, appropriately
- Physical records still “dominate many workplaces”
- Long-term retention of records require “implementing full scale integrated electronic content management/electronic records management (ECM/ERM) systems” and “universally accepted long-term solutions or standards for preserving electronic records.
- Electronic records are “both tracked and stored within the [ECM/ERM] software system” while paper records are only tracked. In order to retrieve records quickly, regardless of the record format, software must be used to integrate the two.
- Example: emails are filed “by keyboard data entry into logical directories within a central ECM/ERM computer-based repository” but paper records are manually filed into “hard copy folders, filing cabinets, or records storage centers.”
- Different “preservation and disaster protection issues”
  - Paper
    - Usually not duplicated
    - Protect from: “fire, flood, humidity, temperature extremes, and other environmental issues, such as physical security.”
    - Need large physical storage space, need to be tracked for retrieval
  - Digital
    - Usually duplicated and store copy (copies) offsite because of “fragility of computer-based data and its dependence on the technology infrastructure”
    - Protect from: same as paper, plus “electrical current reliability and stability for equipment, network access controls, and user authentication management”