Checklist on the Admissibility of Electronic Evidence

Mary Novacheck, Bowman and Brooke LLP

Skip Durocher, Dorsey & Whitney LLP

TABLE OF CONTENTS

Checklist on the Admissibility of Electronic Evidence

Employing Rules of Civil Procedure during the discovery period that assist with admissibility of ESI at trial.

The Rules of Evidence do not separately address admissibility of electronic evidence or electronically stored information ("ESI"). The challenge is applying the rules to computerized data the same as other forms of evidence given it can be easily altered.

The core is examining trustworthiness of the evidence. Address issues with the admissibility of ESI during pretrial discovery. You risk exclusion if you recognize those issues for the first time after discovery closes.

- ✓ Minn. R. Civ. P. 16.03(c). Seek stipulations regarding the authenticity of documents as well as seeking advance rulings on the admissibility of evidence.

- ✓ Minn. R. Civ. P. 16.03(d). Seek stipulations/orders to "avoid unnecessary proof" and "cumulative evidence."

- ✓ Minn. R. Civ. P. 16.03(l). Consider the need for adopting special procedures for managing potentially difficult actions that may involve "unusual proof problems" (cloud data? snapchat? temporary data?)

- ✓ Minn. R. Civ. P. 26.01. Parties must disclose a description of "all" ESI the party may use to support its claims or defenses within sixty days of the original date when an answer is due. (These disclosures are your first opportunity to begin planning your attack on or support of admissibility of ESI disclosed at trial.)

- ✓ Minn. R. Civ. P. 26.02(b). Scope of discovery includes "the existence, description, nature, custody, condition and location" of "documents." (Consider the need to develop admissibility when showing "good cause" for conducting discovery.)

- ✓ Minn. R. Civ. P. 36.01: Request for Admission. Request to admit the "genuineness" of ESI. (Also, move to determine the sufficiency of the answers or objections if clean admissions are not obtained.)

- ✓ Minnesota has not adopted Fed. R. Evid. 902(11) and 902(12) regarding the certification of domestic and foreign records of a regularly conducted activity.

The 5 Steps to Admissibility of ESI

- ✓ *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007)
- ✓ Then Chief United States Magistrate Judge Paul W. Judge Grimm outlined 5 factors for determining whether ESI is admissible into evidence:

1. Relevance (*id*. at 540);
2. Balancing Probative Value Against the Danger of Unfair Prejudice (*id*. at 583);
3. Authenticity (*id*. at 541);
4. Hearsay (*id*. at 562);
5. The Original Writing Rule (*id*. at 576).

Checklist on the Admissibility of Electronic Evidence

Steps 1 and 2: Show the relevance of the ESI under Minn. R. Evid. / Fed. R. Evid. 401 and that the probative value of the ESI is not substantially outweighed by the danger of unfair prejudice or otherwise inadmissible under Minn. R. Evid. / Fed. R. Evid. 403.

- ✓ *In re Welfare of D.L.W.*, No. A11-1238, 2012 WL 171412 (Minn. Ct. App. Jan. 23, 2012):
  - Defendant's **Facebook** posts offered to support first and second-degree assault charges
  - D.L.W. and B.P. were acquaintances since junior high
  - D.L.W. accused B.P. of not paying for marijuana and they exchanged threats on Facebook
  - The Court stated that the relevance standard is "very low," and found that because the Facebook posts contradicted D.L.W.'s statements to police, they were relevant and not prejudicial

- ✓ *Farkarlun v. Hanning,* 855 F.Supp.2d 906 (D. Minn. 2012):
  - Civil rights action alleging police misconduct
  - Plaintiff sought to introduce e-mail from police blog to show police were aware of rape allegations
  - Held: Blog *not* relevant because:
    - No evidence police officers read blog
    - No probative evidence on police knowledge of rape allegations
    - Nothing offered that was accurately reproduced

- ✓ Consider whether the evidence will unfairly prejudice the party against whom it is offered, confuse or mislead the jury, unduly delay the trial of the case, or interject collateral matters into the case. Fed. R. Evid. 403 is generally used sparingly, and courts will err on side of admitting the evidence, along with precautions like contemporaneous instructions to the jury followed by additional admonitions in the charge. WEINSTEIN § 403.02[2][c].

- ✓ A court is most likely to invoke Minn. R. Evid. / Fed. R. Evid. 403 to exclude otherwise relevant electronic evidence where such evidence:

  (1) "Contain[s] offensive or highly derogatory language that may provoke an emotional response."

  - Trial court properly excluded an e-mail from a Microsoft employee under Fed. R. Evid. 403 that contained a "highly derogatory and offensive description of . . . [another company's] type director." *Monotype Corp. PLC v. Int'l Typeface Corp.*, 43 F. 3d 443, 450 (9th Cir. 1994).

  (2) Consists of computer animations or simulations where "there is a substantial risk that the jury may mistake them for the actual events [at issue] in the litigation."

  - Question of whether the animation accurately demonstrates the scene of the accident, and whether the probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations undue delay, waste of time, or needless presentation of evidence. *Friend v. Time Mfg. Co.*, No. 03-343-TUC-CKJ, 2006 WL 2135807, at *7 (D. Ariz. July 28, 2006).

(3) Consists "of summaries of voluminous electronic writings, recordings or photographs under Rule 1006." Minn. R. Evid. / Fed. R. Evid. 1006 is an especially important tool for electronically stored evidence because the production of ESI is particularly voluminous in civil cases, and courts can be expected to allow the use of summaries provided the procedural requirements of the rule are met.

- Summary evidence is subject to the balancing test under Fed. R. Evid. 403 that weighs the probative value of evidence against its prejudicial effect. WEINSTEIN § 1006.08[3].

(4) Or is potentially unreliable or inaccurate.

- The court expressed extreme skepticism regarding the reliability and accuracy of information posted on the Internet, referring to it variously as "voodoo information." *St Clair v. Johnny's Oyster & Shrimp Inc.*, 76 F. Supp. 2d 733, 775 (S.D. Tex. 1999).
    - The case doesn't refer explicitly to Fed. R. Evid. 403, but the possibility of unfair prejudice associated with the admissibility of unreliable or inaccurate information, as well as confusion of the jury, makes Fed. R. Evid. 403 likely to be applied for exclusion of this evidence

Step 3: Employ Minn. R. Evid. / Fed. R. Evid. 901(a), 902 to authenticate the ESI.

✓ Is the evidence what it purports to be? A non-exhaustive illustrative list of authentication methods:

- Minn. R. Evid. / Fed. R. Evid. 901(b)(1). Testimony of a witness with knowledge.
- Minn. R. Evid. / Fed. R. Evid. 901(b)(3). Comparison by trier or expert witness.
- Minn. R. Evid. / Fed. R. Evid. 901(b)(4). Distinctive characteristics and the like.
- Minn. R. Evid. / Fed. R. Evid. 901(b)(9). Process or system.
- Minn. R. Evid. / Fed. R. Evid. 902. Self-Authentication.

✓ Witnesses with Knowledge:

In the Matter of the Welfare of S.A.M., 570 N.W.2d 162 (Minn. Ct. App. 1997):

- No witness observed events depicted on video
- Video technician, Bus driver and Police sergeant testified as to video system, consistency of contents with events and chain of custody
- Held: Authenticated under 901(B)(1)

State v. Haines, No. A07-1743, 2008 WL 5333357 (Minn. Ct. App. Dec. 23, 2008):

- The State offered 3 cell phone photos of victim's text messages in support of felony domestic assault and terroristic threat charges

- Held: To authenticate, proponent did not have to eliminate "all possibility of tampering or substitution"
  - Must show "it is reasonably probable" it did not occur

- Evidence offered in support of authenticity:
  - exhibit showing profile of telephone number and name of sender on victim's phone
  - victim's personal testimony - text messages were "how he would speak to me"
  - testimony of the officer who took photographs of each message that he observed on her phone

✓ Either direct or circumstantial evidence is permitted. The contents, substance, internal patterns or other distinctive characteristics, taken in conjunction with the totality of the circumstances, may be sufficient for authentication.

- The Minnesota Supreme Court recognized relevant circumstantial evidence as bearing on authentication. *State v. Johnson*, 228 N.W. 926, 927 (Minn. 1930).

- *State v. Bohlman*, No. A05-207, 2006 WL 915765 (Minn. Ct. App. Apr. 11, 2006):

  - State offered the e-mails sent to the minor in support of the claim of criminal sexual conduct

  - The minor testified that the e-mails contained Bohlman's name and e-mail address and that the minor frequently sent and received e-mails from Bohlman at that e-mail address

  - Held: Minor's testimony authenticated the e-mails

✓ When considering paperless records "the focus is not on the circumstances of the creation of the record, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally created." *In re Vee Vinhnee*, 336 B.R. 437, 444 (B.A.P. 9th Cir. 2005).

- This case sets forth stringent foundational requirements for Fed. R. Evid. 901(b)(9) using an 11-part test developed by Professor Imwinkelreid for evidence about a process or system of keeping accurate results in an electronic system.

✓ For items susceptible to alteration, substitution or change of condition, the greater the need to negate such possibilities. ESI can exist in multiple locations with varying degrees of access and can be readily altered. To demonstrate a chain of custody

showing under Fed. R. Evid. 901, a party should include a description of the evidence, unique identifier of the evidence, name who has controlled the evidence, and the date and times of the handoffs of the evidence. *United States v. Howard-Arias,* 679 F.2d 363, 366 (4th Cir. 1982).

- ✓ A piece of paper or ESI, without any indication of its creator, source, or custodian, may not be authenticated under Minn. R. Evid. / Fed. R. Evid. 901. Once a prima facie showing of authenticity is shown, the evidence goes to the jury, which will determine its authenticity. *State v. Garcia*, 7 A.3d 355 (Conn. 2010).

- ✓ Some courts have found that a party producing ESI during discovery implicitly admits its authenticity and are barred from later objecting to its admission by opposing party on authentication grounds. *Sprinkle v. Lowe's Home Centers, Inc.*, No. 04-CV-4116-JPG, 2006 WL 2038580, at *2 (S.D. Ill. July 19, 2006); *Indianapolis Minority Contractors Ass'n, Inc. v. Wiley*, No. IP 94-1175-C-T/G, 1998 WL 1988826, at *6 (S.D. Ind. May 13, 1998).

Authenticating specific types of data through your forensic collection.

- ✓ Involves the location, examination, identification, collection, preservation, and analysis of computer systems and electronically stored evidence.

    - It may often include retaining an outside e-discovery vendor or certified forensic examiner to collect the relevant ESI. They will have established procedures, maintain comprehensive documentation, and be prepared to testify as to the methodology and defensibility of the process.

    - Forensically sound procedures are defined as those "used for acquiring electronic information in a manner that ensures it is 'as originally discovered' and is reliable enough to be admitted into evidence." Novacheck et al., *IT Technologies and How to Preserve ESI Cost Effectively*, 40 William Mitchell L. Rev. 486, 493 (2014).

    - Computer forensics for ESI "combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law." *Id.*

- ✓ Metadata shows time, date, and identity of the creator of an electronic record, as well as describing the history, tracking, or management of an electronic document. It includes all of the contextual, processing, and uses information needed to identify and certify the scope, authenticity, and integrity of active or archival electronic information or records.

- ✓ "Hash values" or "hash marks" assign a unique identifier assigned to a file or group of files to guarantee the authenticity of an original data set. It is an electronic "Bates stamp" that assists when creating the "final" or "legally operative" version of an electronic record with distinctive characteristics.

    - Encryption and digital signatures can provide a basis for trust. A digital signature uses a secret key to enable a party to use its secret key to indicate that it has "signed" an electronic document. Through this, a

person signing an electronic document has viewed and approved the document.

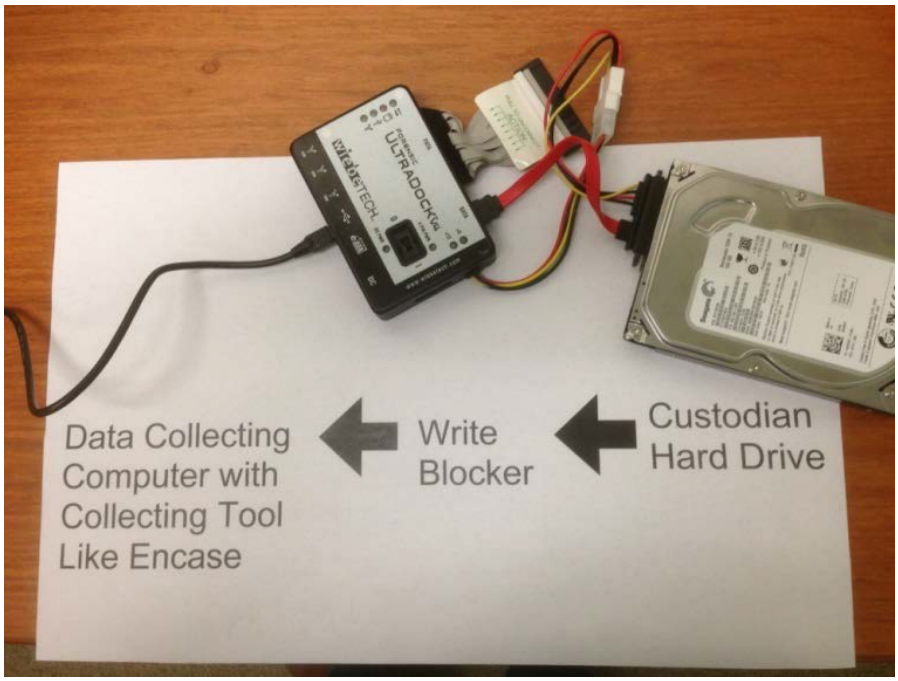
- Note: prepare for challenges to falsity of the value/appearance of such digital signatures.

Vendor testimony can help authenticate the collection method of documents stored on a hard drive:

Q: Ms. Vendor, what steps did you take when you collected this document from the hard drive of witness X?[3]

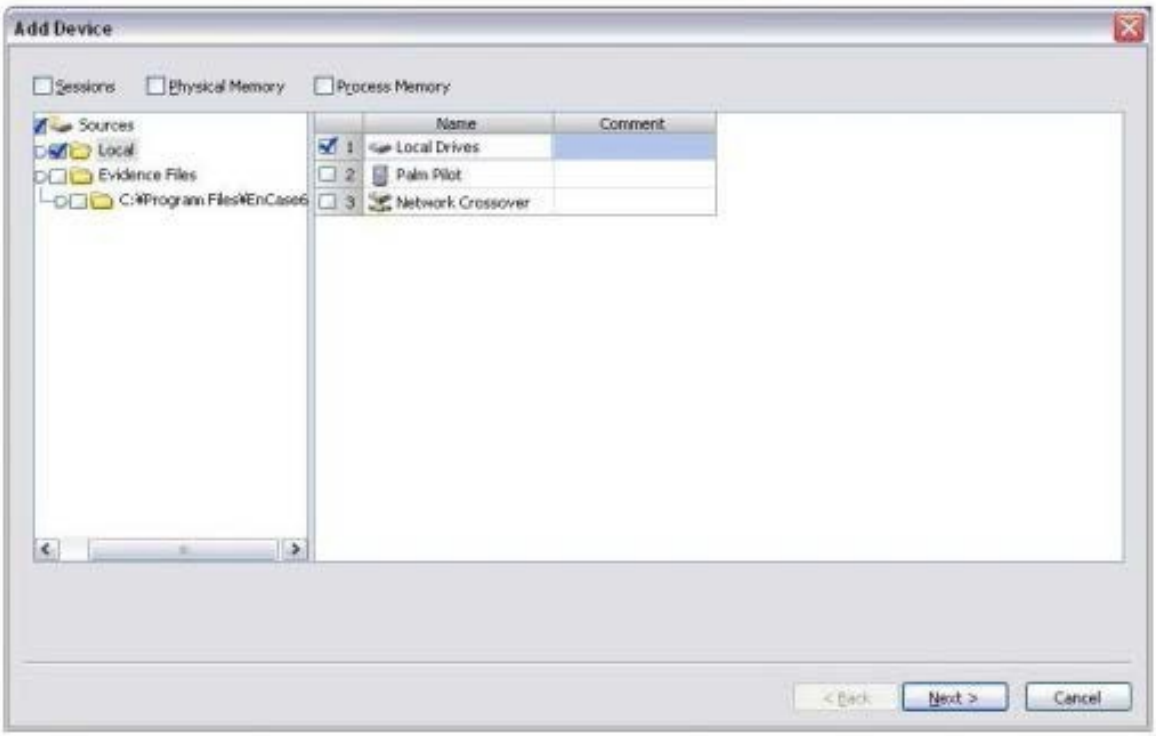
A: Step 1. I created a checklist to log and account for all actions that I took in the hard drive preservation and collection process.

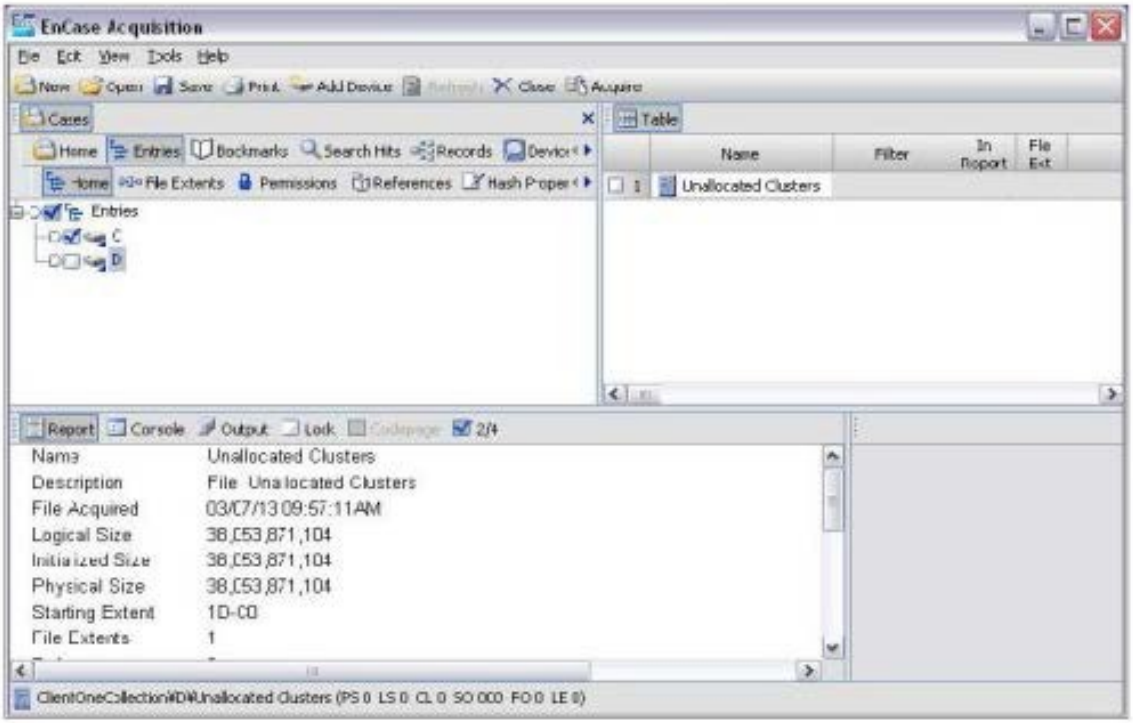
Step 2. I extracted the custodian's hard drive from his computer and plugged it into a write blocker to prevent data alteration during the preservation/ collection process.



Step 3. I connected the write blocker to the computer with a forensically sound data-collecting tool, EnCase, and then add the hard drive to EnCase. This was a targeted collection, so I burrowed down into the custodian drive and selected the file within the folder titled "x." (If a full collection is required: I selected the device and clicked "Acquire" to begin the process.")

[3] All images in this presentation are from Novacheck et al., *IT Technologies and How to Preserve ESI Cost Effectively*, 40 William Mitchell L. Rev. 486 (2014).





Step 4. I then defined the location and properties of the output similar to below, and placed the output in a password protected hard drive. The output data was an E01 forensic image, which is a secure way of storing the data, and with the Acquisition MD5 selected, the file will be automatically verified once the process completes to ensure integrity.

Step 5. When the verification process was complete, I safely unplugged the hard drive with the collected data from the collecting computer and made sure it was physically secure and safe. I unplugged the write blocker from the collecting computer, unhooked the custodian hard drive, and put the hard drive back in his/her computer. I completed the chain of custody process and made sure all the requirements in the checklist were met.

[NOTE: a vendor can similarly authenticate data stored in other locations, such as a shared drive, on an external media device, on a server, in the cloud, etc.]

Website authentication:

(1) What was actually on the website?

- Use a webmaster or someone who has personally managed the website to aid in authenticating the website's content. *St. Luke's Cataract & Laser Inst., P.A. v. Sanderson*, No. 8:06-CV-223-T-MSS, 2006 WL 1320242, at *1-2 (M.D. Fla. May 12, 2006).

- Analyzing admissibility of the content of a website. *Telewizja Polska USA, Inc. v. Echostar Satellite Corp*., No. 02 C 3293, 2004 WL 2367740 (N.D. Ill. Oct. 15, 2004).

(2) *Does the exhibit or testimony accurately reflect what was on the website?*

- Reasonable to presume that material on a website was placed there by the owner of the site. If issues of trustworthiness remain, look at the totality of circumstances, such as:
    - The length of time data was posted on site, whether others report seeing it, whether it remains for the court to verify, whether data is of the type ordinarily posted on that website or websites of similar entities, whether the owner of the site has published the same data elsewhere, whether others have published the same data, and whether data has been republications by others who identify the source of the data as the website in question.
    - Sufficient for witness with knowledge to attest to the fact that the witness logged onto the site and to describe what he or she saw. *Van Westrienen v. Americontinental Collection Corp.,* 94 F. Supp.2d 1087, 1109 (D. Or. 2000).

(3) *If so, is it attributable to the owner of the site?*

- Website postings were not properly authenticated because the proponent needed to show that the website posting were actually posted by a particular group, and not the proponent herself. *United States v. Jackson*, 208 F.3d 633, 638 (7th Cir. 2000).
- A proponent might search the computer of the purported author for Internet history and stored documents, or seek authenticating information from the commercial host of the e-mail, cell phone messaging, or social networking account. *Griffin v. State*, 19 A.3d 415 (Md. 2011).

(4) Is a printout of the website sufficient?

- *State v. Jackson*, 770 N.W.2d 470 (Minn. 2009)
    - State offered printed webpage from social networking site depicting photo of defendant wearing gang colors
    - Defendant objected: it could be “photoshopped"
    - Trial Court admitted, Supreme Court expressed concern as to the lack of testimony that the image accurately depicts issue and a lack of testimony from employee of website with personal knowledge of website content

- Courts consider "distinctive characteristics" of website in determining whether a document is sufficiently authenticated, i.e. printouts of webpages were authenticated when printouts included web addresses and dates. *Premier Nutrition, Inc. v. Organic Food Bar, Inc.,* No. SACV-06-0827 AG (RNBx), 208 WL. 1913163, at *6 (C.D. Cal. Mar. 27, 2008).

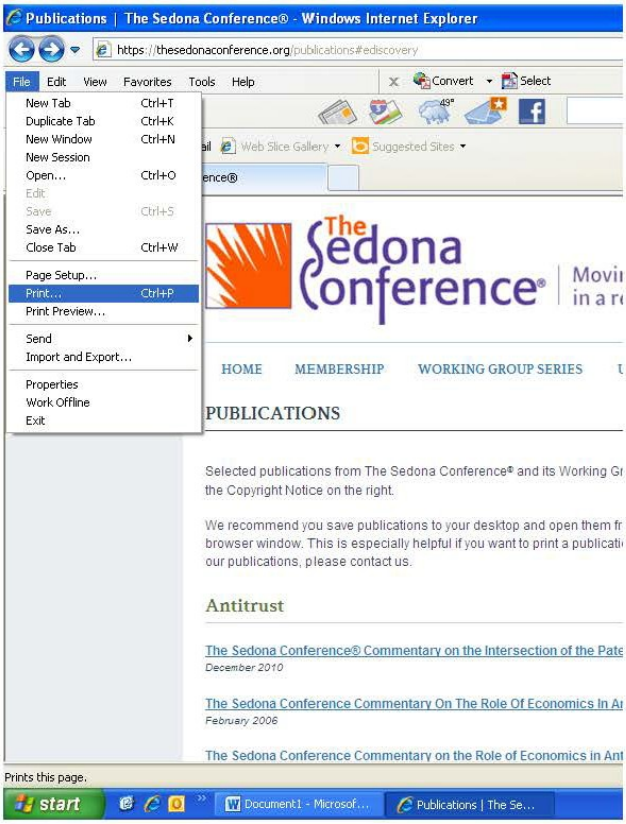
- The court examined the evidence and held that although the printouts had a URL address, a date stamp, and the attorney submitted a declaration stating the printouts were true and correct, the copies were not properly authenticated under Fed. R. Evid. 901 because the attorney failed to submit a declaration by the person who personally conducted the search, or by the company stating that the computer printouts are a true and correct copy of the information from its website. *Whealen v. Hartford Life & Acc. Ins. Co*., No. CV06-4948PSG (PLAX), 2007 WL 1891175, at *1 (C.D. Cal. June 28, 2007) *aff'd*, 332 F. App'x 443 (9th Cir. 2009).

- Analyzing admissibility of printouts of computerized records. Evidence describing a process or system used to produce a result is useful in authenticating electronic evidence stored in or generated by computers. *United States v. Meienberg,* 263 F.3d 1177, 1180 (10th Cir. 2001).

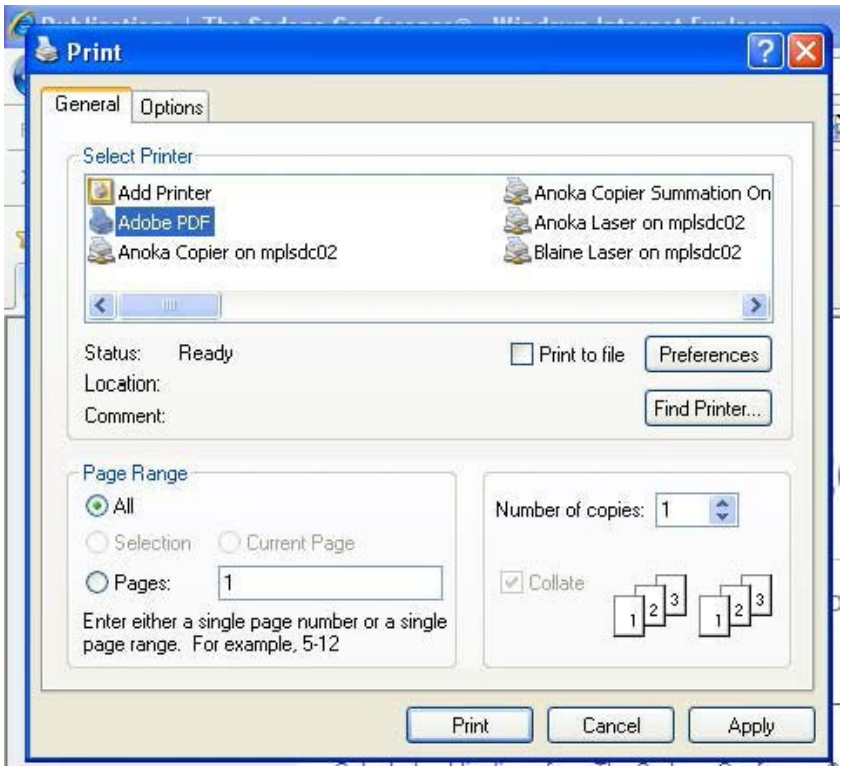
(5) Use testimony of technology vendor/expert to authenticate website through evidence of forensic collection methods:

Q: Ms. Vendor, describe the steps you took to collect the website in question.

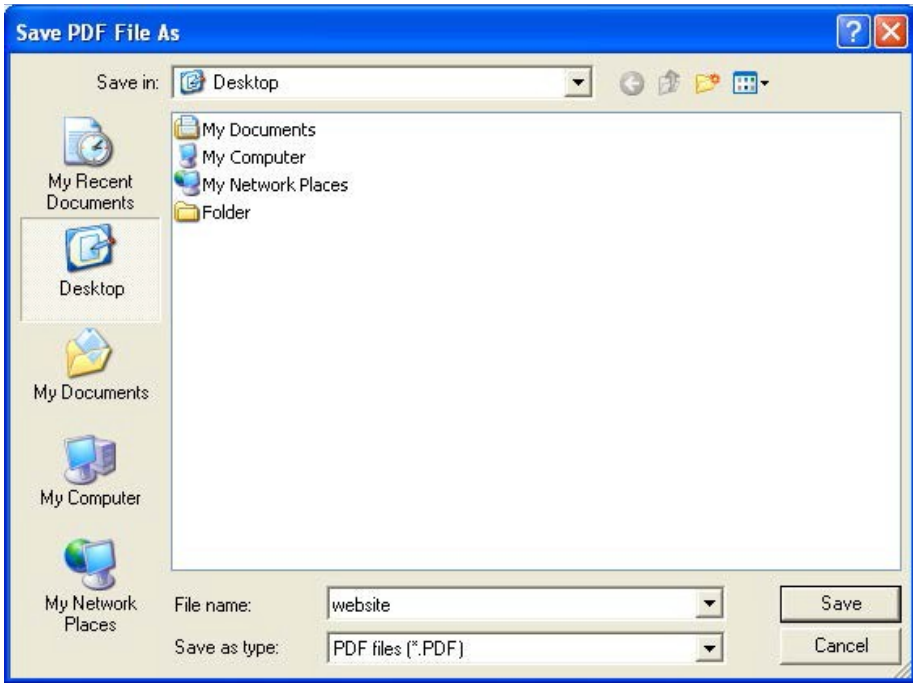
A: Step 1. I went to the desired web page and chose *File* > *Print* in the application. The Print dialog box opened:



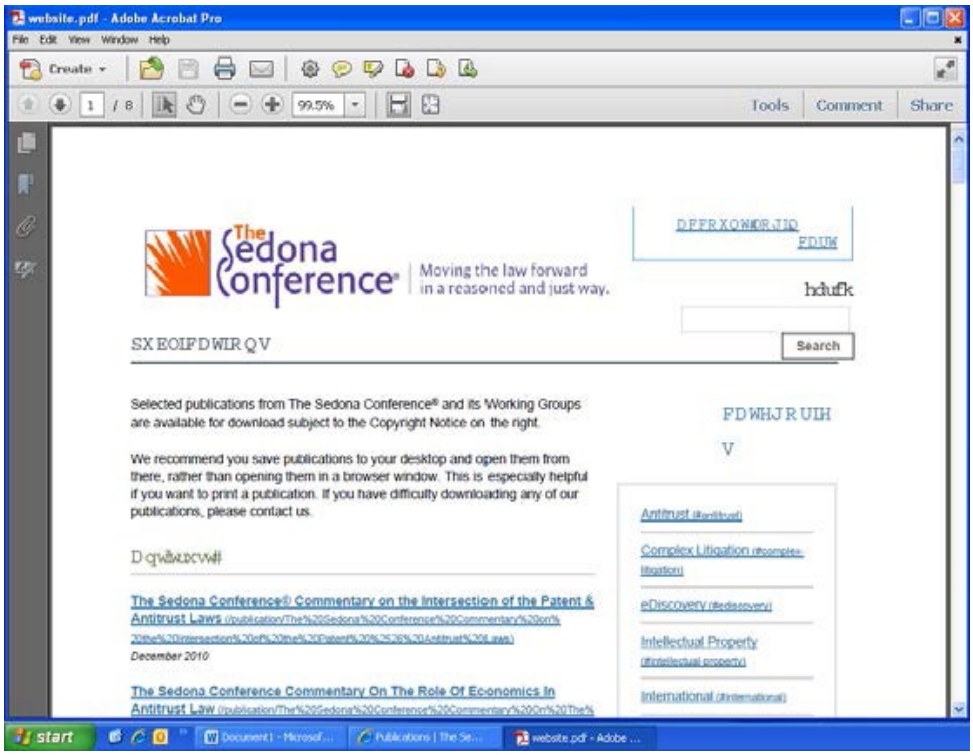
Step 2. Then under the *Print* menu, I chose *ADOBE PDF* as the printer selection. I clicked *Print*.



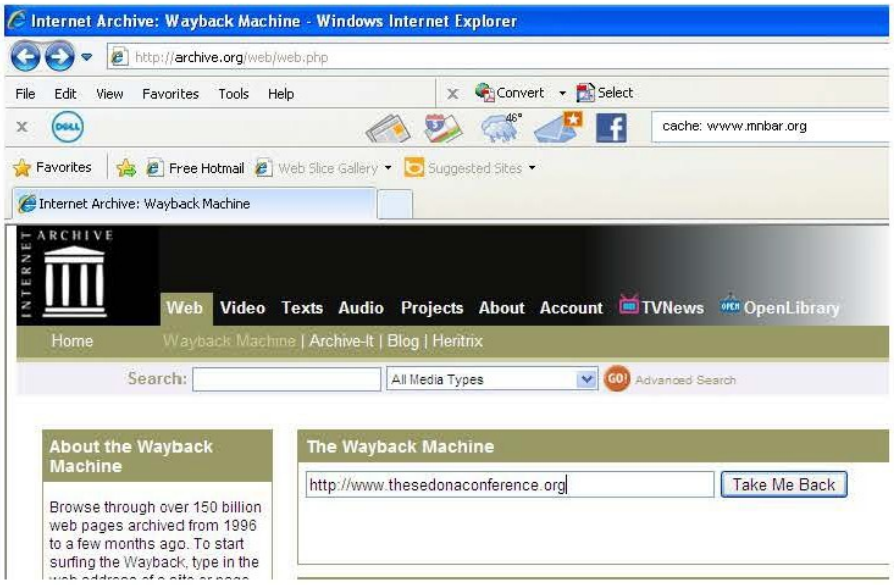
Step 3. When the standard *Save* dialog box opened, I typed a name for the file. Next, I selected the location that I wanted to save the file in (for example, the desktop). Then I clicked *Save* or *OK*.



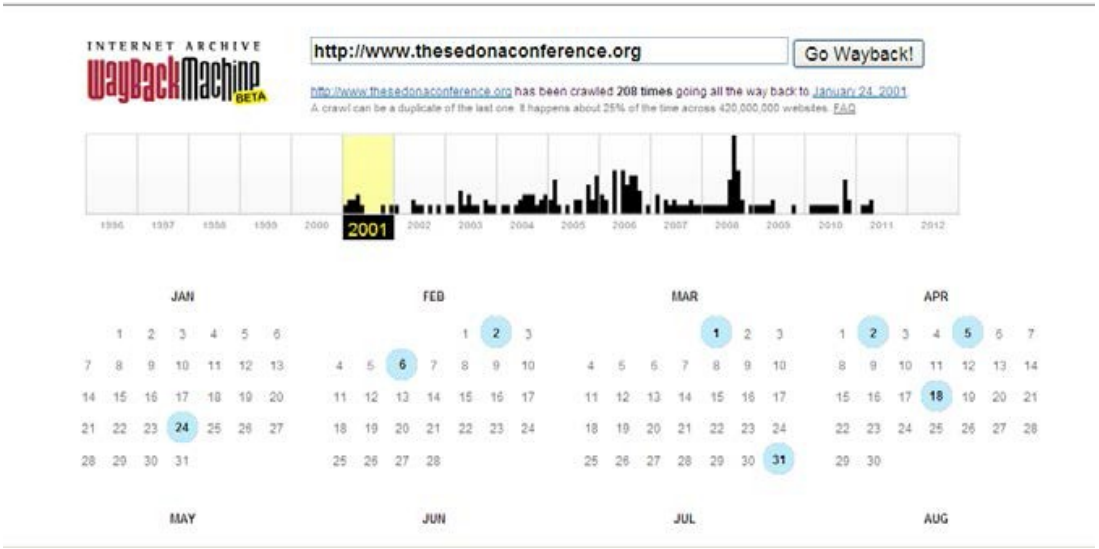
Step 4. A newly created PDF file appeared. I saved the file to my desktop:



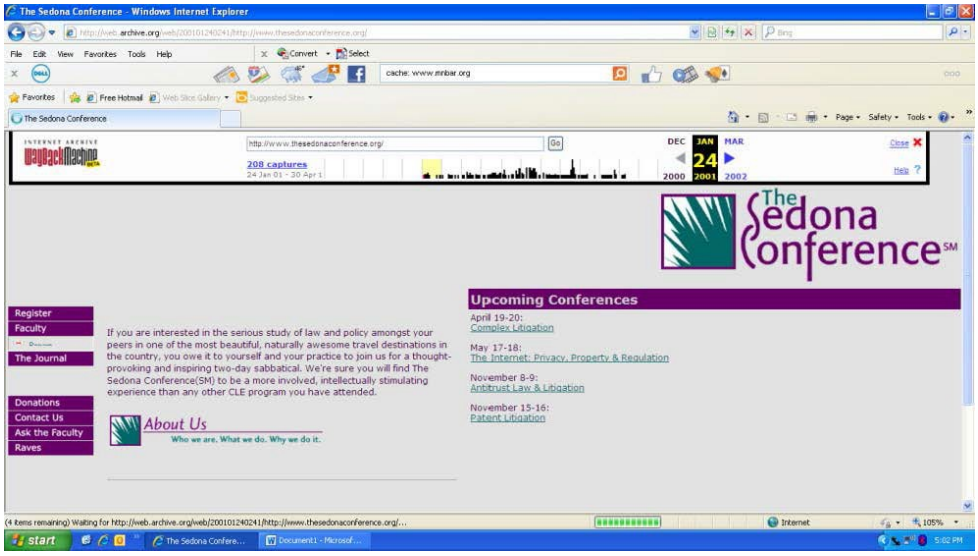
Step 5. (If collecting a prior version of the website) I used the *Wayback Machine*, at http://archive.org/web/web.php. Then I entered the desired web page into the search box under the Wayback Machine. Then I clicked *Take Me Back*.



Step 6. The Wayback Machine pulled up a calendar listing the available dates that contained an archive of the web page.



Step 7. I clicked on the desired date, and the past web page appeared. Here, I clicked January 24, 2001.



E-mail authentication:

- E-mails satisfy authentication requirements when they bear distinctive characteristics, including actual e-mail address containing name of the person connected to the address, signatures within e-mails linking e-mails to alleged sender, discussions in the e-mails of personal and professional matters known to be associated with senders. *United States v. Safavian,* 435 F. Supp. 2d 36 (D.D.C. 2006).

- Lower standard of authentication than other data types.

- Inadequate foundation to support plaintiff's claims that author of e-mail was CFO because e-mails were "unsolicited, contained only publicly available, self-serving information and contained no substantive or unique information that supported authenticity." *Jimena v. UBS AG Bank, Inc.,* 1:07-CV-00367-OWW, 2011 WL 2551413 (E.D. Cal. June 27, 2011).

    - General information with no unique information to support authenticity isn't admissible.

Text messages: similar process of authentication to e-mails.

- Defendant sent texts threatening the recipient. The recipient testified to personal nature of messages and showed aligned with defendant's knowledge of recipient's family. *United States v. Teran*, 496 F. App'x 287, 292 (4th Cir. 2012).

- Text messages made on SkyTel pagers properly authenticated by distinctive characteristics including auto signatures, nicknames used, recognized phrases in signature lines, and other personal information confirming identity of sender and by defendant's admissions that the parties regularly communicated that way. *United States v. Kilpatrick*, No. 10-20403, 2012 WL 3236727, at *4 (E.D. Mich. Aug. 7, 2012).

- At least one court has stated that "more than mere confirmation that the number or address belonged to the particular person" is needed to authenticate SMS evidence, and that circumstantial evidence "which tends to corroborate the identity of the sender" is required. *Pennsylvania v. Koch*, 39 A.3d 996, 1005 (Pa. 2011)(stating that detective's description of how text messages were transcribed was not sufficient to establish the identity of the sender, which was essential for admissibility).

- The court held that transcriptions of text messages did not violate the best evidence rule because the proponent satisfied Fed. R. Evid. 1004(a), which provides that an original is not required when "all originals are lost or destroyed, and not by the proponent acting in bad faith. . ." *State v. Espiritu*, 176 P.3d 885, 892-93 (Haw. 2008).

Using the testimony of a technology expert on forensic collection to authenticate the text message:

Q: Ms. Vendor, what steps did you take when you preserved and collected text message data from witness X's iPhone?

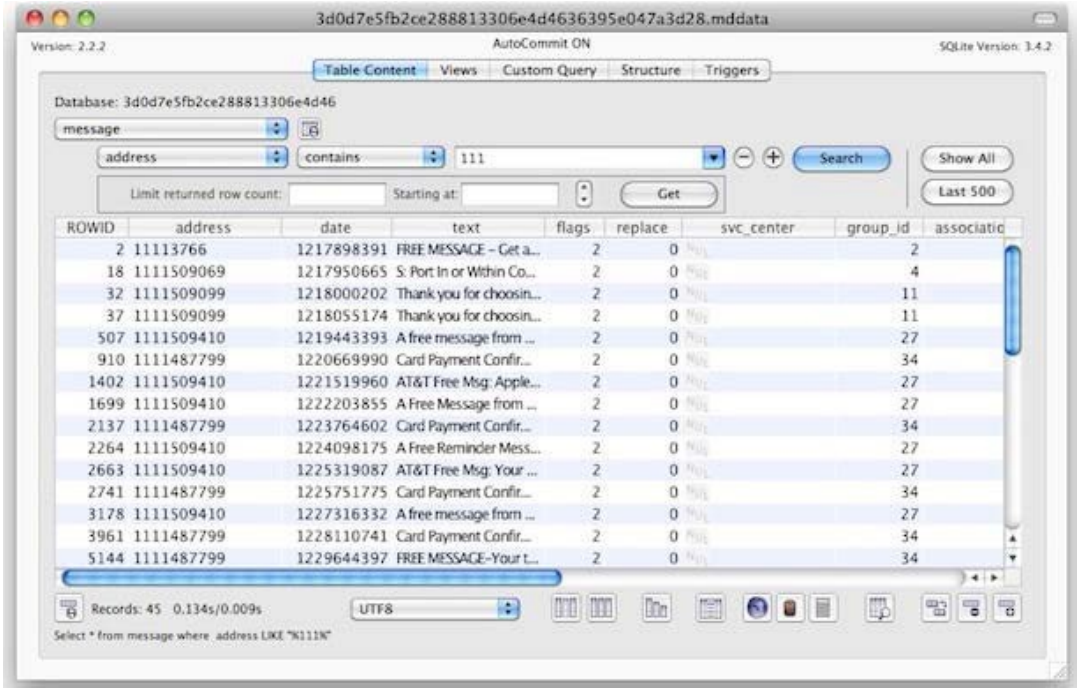
A: Step 1. I created a backup of the phone, which ensures that the process does not affect or alter active data. The SMS/text messages are backed up when the phone is backed up and stored within the standard iPhone backup location.

The standard iPhone backup location located at: ~/Library/Application Support/MobileSync/Backup/. When backed up to the computer, SMS/text messages can found at the following locations:

- Mac iPhone backup file: %APPDATA%\Apple Computer \MobileSync\Backup\
- Windows XP: C:\Documents and Settings\[your username] \Application Data\
- Windows Vista: %APPDATA% = C:\Users\[your username]
- \AppData\Roaming Windows 7: C:\Users\user\AppData\Roaming\Apple Computer \MobileSync\Backup

The messages are stored in randomly generated hexadecimal filenames such as: 7182649a9879a8798c798e98794798f9279877c98 7984. This file is a small database called SQLite and can be read by any application that reads a SQLite database. There are plenty of SQLite and free applications online for Windows and Mac. For example, MesaSQLite for Mac OS X.

Step 2. Next I downloaded a SQLite application and open the SMS/ text file. It looked like this:



Step 3. I queried the information just like any other database. For example, the text number, the date of the text, or the keywords of the text message can be queried. The text messages can also be dragged to a text editor like notepad or textpad.

Step 4. After a review of the file and confirmation that the text message could be viewed, I closed out the application and copied the SMS/text file to an encrypted hard drive with a password for storage.

Online chats: similar process of authentication to e-mails and text messages.

- Evidence that individual used the screen name in question when participating in chat room conversations;
- Evidence that when a meeting with the person using the screen name was arranged, the individual showed up;
- Evidence that the person using the screen name identified himself as the person in the chat conversation;
- Evidence that the individual had in his possession information given to the person using the screen name; and
- Evidence from the hard drive of the individual's computer.
- Authentication of online chats through testimony of a person in the chat that could testify the chats were fairly reproduced through direct personal knowledge. *United States v. Barlow,* 568 F.3d 215, 220 (5th Cir. 2009).
- A printout of online chat is admissible as a duplicate to satisfy the best evidence rule under Fed. R. Evid. 1003. *United States v. Nobrega,* 1:10-CR-00186-JAW, 2011 WL 2116991 (D. Me. May 23, 2011).
- Transcripts of instant message chats copied from defendant's electronic communications and pasted in word processing files were properly authenticated by law enforcement agent and an informant. The court noted that a reasonable juror could find the exhibits did represent those conversations, notwithstanding that the e-mails and online chats were editable. *United States v. Gagliardi,* 506 F.3d 140, 151 (2d Cir. 2007).
- Ample circumstantial evidence existed to authenticate printouts of the content of chat room discussions between the defendant and an undercover detective, including use of the e-mail name of the defendant, presence of defendant's correct address in messages, and notes seized at the defendant's home containing the address, e-mail address and telephone number given by the undercover officer. *United States v. Simpson,* 152 F.3d 1241, 1249 (10th Cir. 1998).
- Analyzing admissibility of exhibits reflecting chat room conversations. *United States v. Tank,* 200 F.3d 627, 630 (9th Cir. 2000).

Social Network Chats: authenticated in same way as chat room evidence.

- He or she knows the user name on the social networking site of the person in question;
- Printouts of conversation appear to be accurate records of his or her electronic conversation with the person; and

- Portion of contents of communications are known only to the person or a group of people of whom the person in question is one.

- E-mail communication sent on a social network and bearing a person's name is insufficient to authenticate the communication as having been authored or sent by that person.

    - Must have confirming circumstances sufficient to permit the inference that the purported sender was in fact the author.

Voicemail:

- Identification of a voice, whether firsthand or through mechanical or electronic transmission or recording, by opinion based upon hearing the voice at any time under circumstances connecting it with the alleged speaker. *State v. Williams*, 136 Wn. App. 486, 500 nt.7 (2007).

- Steps taken to authenticate a voicemail include the proponent demonstrating (1) the operator's competency, (2) the fidelity of the recording equipment, (3) the absence of material alteration, and (4) the identification of relevant sounds or voices. *United States v. Hare*, 150 F.3d 419, 424 (5th Cir. 1998) *overruled on other grounds by United States v. Doggett*, 230 F.3d 160 (5th Cir. 2000) (citing *United States v. Buchanan*, 70 F.3d 818, 827 (5th Cir. 1995)).

- The court has broad discretion to admit a recording in the absence of these requirements if it is convinced that the recording reproduces the auditory experience. *United States v. Buchanan*, 70 F.3d 818, 827 (5th Cir. 1995), *as amended* (Feb. 22, 1996).

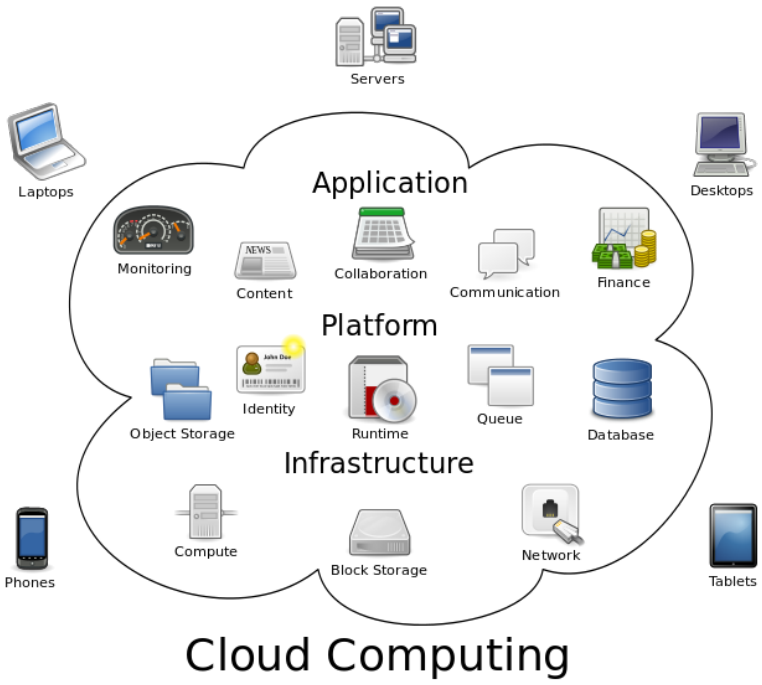
- Seven foundational elements for admission of a tape recording that have the potential to apply to ESI. *Furlev Sales & Associates, Inc. v. N. Am. Auto. Warehouse, Inc.*, 325 N.W.2d 20, 28 n.9 (Minn. 1982).

- To authenticate the voicemail message, may need a witness who overheard the person leaving the message and can say the message being offered into evidence is the same message, or use chain of custody.

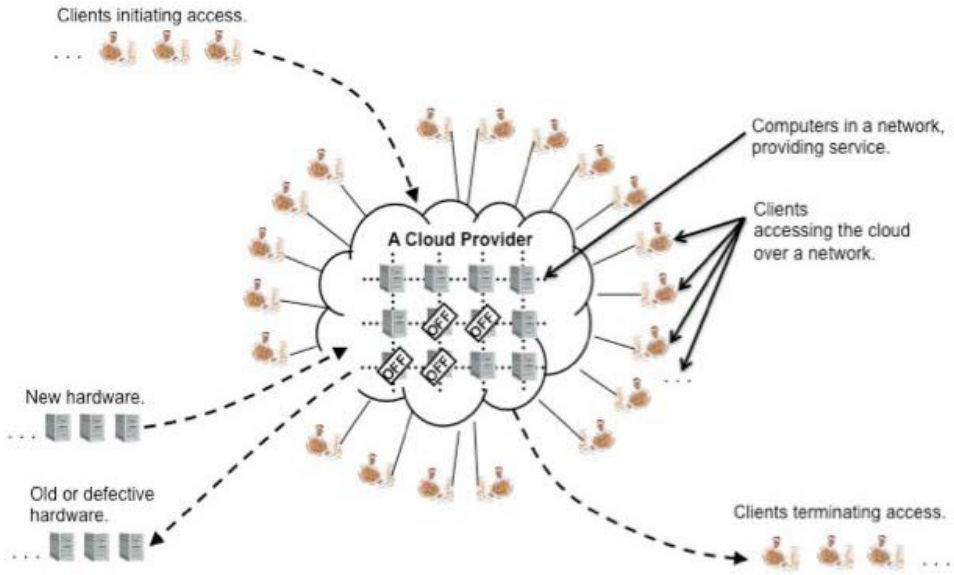
- Voicemail attached to e-mail poses difficulties because audio attachment content cannot be searched or found by text-based keyword searches. There may be a large investment in live human efforts to listen to and transcribe audio messages to pull out relevant information.

Cloud Data: Understand what it is – another storage location.

- Defined as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."



- Essential characteristics of cloud computing include: (1) on demand self-service, (2) broad network access), (3) resource pooling, (4) rapid elasticity, and (5) measured service.



- There are no universally accepted standards that cloud computing providers must follow in storing and maintaining information.

- Consider the location of the data and whether the party has possession, custody or control of the data as defined under Fed. R. Civ. Pro. 34.

    - Courts generally hold that electronically stored information stored with a provider is within control of the party because a party cannot evade e-discovery obligations by shipping its data to a third party. *Flagg v. City of Detroit*, No. 05-74253, 2008 WL 787061, at *2 (E.D. Mich. Mar. 20, 2008) (focusing upon whether the information stored with non-party service provider SkyTel was in the city's "control.").

- With customer to cloud service providers, one should be aware of data privacy issues arising with cloud storage, privacy, hybrid storage, preservation, and collection considerations.

- Use evidence of forensic collection methods employed, including testimony of a technology vendor/expert, if necessary, to authenticate ESI housed in the "cloud."

Step 4: Prepare for challenges to the ESI as hearsay and whether it falls within hearsay exceptions/exclusions.

✓ Is ESI offered to prove the truth of the matter?

✓ Is it hearsay as defined under Minn. R. Evid. / Fed. R. Evid. 801?

State v. Mohamed, No. A11-1993, 2012 WL 3641006 (Minn. Ct. App. Aug. 27, 2012)

- The state offered testimony about text messages exchanged between accuser and her roommate in support of claim that cab driver committed criminal sexual misconduct

- Also offered copies of cellphone bills to show text exchanges occurred

- Mixed decision:

  "My cabbie is attacking me" was *not* hearsay because it was consistent with the accuser's testimony and it went to her credibility

  "I'm in the cab. He touched me and he will not let me out" *was* hearsay because it was offered to prove the truth of matter asserted

✓ Does it fit under any of the many exceptions or exclusions to hearsay under Minn. R. Evid. / Fed. R. Evid. 803, 804 and 807?

- ✓ Courts have held that e-mails may constitute business records.
    - E-mail records of sales made when e-mails kept in normal course of company's business and created at or near time of matters referred to in e-mails and affidavit of D's records custodian established authenticity. *DirecTV, Inc. v. Murray,* 307 F. Supp. 2d 764, 772-73 (D.S.C. 2004).
    - But not all business e-mails fall into business records exception. A court may find an e-mail lacks indicia that e-mail was a business record. Not an extremely broad rule.
- ✓ Testimony of a witness qualified to explain the record keeping system of the organization will be able to confirm that the requirements of records of a regularly conducted activity (Fed. R. Evid. 803(6)) have been met. *United States v. Kassimu*, 188 F. App'x 264, 265 (5th Cir. 2006)

Step 5: Is the ESI an original or duplicate under original writing rule? If not, is it admissible as secondary evidence to prove the content under Minn. R. Evid. / Fed. R. Evid. 1001-1008?

- ✓ Computer generated records fall within the definition of a writing.
- ✓ For ESI "original" means any printout – or other output readable by sight – if it accurately reflects the information. Minn. R. Evid. 1001(3) / Fed. R. Evid. 1001(d).
- ✓ *State v. Brown*, 739 N.W.2d 716 (Minn. 2007):
    - The State offered a digital copy of an apartment complex surveillance video to show the time and conduct of murder defendants
    - The original was created and stored on VCR tape
    - A digital copy was created to preserve the video and use it at trial
        - Testimony of building caretaker described the system
        - Testimony of police officer with expertise in forensic video processing described the copying process
    - Held: "Digital copies may qualify as duplicates of the original", it was admissible
- ✓ Secondary evidence may be used to prove the contents of electronically stored evidence (a) when the originals or duplicates have been lost or destroyed, absent any bad faith by their proponent; (b) if the originals or duplicates are not obtainable by the judicial process; (c) if the originals or duplicates are in the possession, custody or control of an adverse party who is on notice by the pleadings or otherwise that their contents would be the subject of proof at trial or hearing and who does not bring them; or (d) the documents are "collateral" to the litigation, meaning that they do not closely relate to a controlling issue in the litigation. Minn. R. Evid. 1004(1)-(4) / Fed. R. Evid. 1004(a)-(d).

- ✓ The court found that the cut-and-paste documents were not admissible at trial because the document does not accurately represent the entire conversations, noting there were numerous examples of missing data, time sequences that did not make sense, and editorial information that creates a doubt to trustworthiness of the document. *United States v. Jackson*, 488 F. Supp. 2d 866, 871 (D. Neb. 2007). The document also failed the original writing rule because the document is not an accurate original or duplicate under Fed. R. Evid. 1001(d), 1002, 1003, and 1004. *Id*. at 871.