

ARKFELD'S

ELECTRONIC DISCOVERY AND EVIDENCE

Volume 1, Issue 2 April, 2005

E-DISCOVERY ARTICLE

Checklist for Interviewing, Selecting and Utilizing a Digital Forensics Expert

By
Larry Leibrock

Larry R. Leibrock, Ph.D., is the Chief Technology Officer for eforensics LLC (www.eforensics.com), a company that specializes in digital forensics and enterprise forensics discovery. Dr. Leibrock can be reached at leibrock@eforensics.com

Perspective

Increasingly, legal professionals are confronted with a wide range of litigation which involves discovery of information contained in digital data stored in electronic devices. These devices typically include; personal computers, servers, networks, portable digital assistant devices and digital storage media. As modern economies make more pervasive use of these devices, it is a reasonable proposition that the effective use of this digital data will be influential for successful legal out-

comes.

Background

Both individual litigators and corporate counsel have become aware of organizational data retention policies and associated repositories of digital information utilized in computerized office administration systems, including email and electronic messaging, and information technology systems which support core business functions such as human resources, finance, logistics and production functions. These are complex, technology-based systems that have a vast array of data forms, types and storage structures. The proper forensics recovery of these data forms is a technically complex and artful set of procedures conducted by qualified digital forensics experts. Most corporations and law firms have limited digital forensics resources and generally need to rely on outside forensics experts for these specialized services. Given this situation, the following is a framework for finding and properly utilizing the proper forensics expert for your legal needs.



RECENT NEWS STORIES

EDD RULES: THE GREAT DEBATE.

"SHOULD THE FEDERAL RULES OF CIVIL PROCEDURE DISTINGUISH BETWEEN TRADITIONAL DISCOVERY AND E-DISCOVERY? "WHEN A FLORIDA COURT ASKED DEFENDANT MORGAN STANLEY TO PRODUCE DISCOVERY DOCUMENTS . . . "

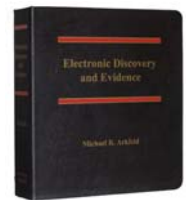
http://arkfeld.blogs.com/ede/2005/04/edd_rules_the_g.html

THE COST OF COMPLIANCE CAN ONLY GO UP

"THE GLOBAL MARKET FOR COMPLIANCE INFORMATION MANAGEMENT WILL GROW AT 22% A YEAR THROUGH 2009 AND PASS THE \$20 BILLION MARK THAT YEAR . . . "

http://arkfeld.blogs.com/ede/2005/03/compliance_it_t.html

SPECIAL POINTS OF INTEREST:



Do You Need to Know About Electronic Discovery to Protect Your Clients?

Find the answers to your questions in the *Electronic Discovery and Evidence (2004-2005 ed.)* treatise by Michael R. Arkfeld, Esq.

INSIDE THIS ISSUE:

ELECTRONIC DISCOVERY AND EVIDENCE TREATISE 2

EDE PRACTICE TIPS 2

BILLION DOLLAR E-MAIL DESTRUCTION CASE 3

ZUBULAKE VERDICT IS IN—\$29 MILLION 3

INADVERTENT DISCLOSURE OF EMAIL 3

UPCOMING EVENTS 4

EDE TRAINING 4

ELECTRONIC DISCOVERY AND EVIDENCE

Michael Arkfeld's *Electronic Discovery and Evidence* is the comprehensive resource for discovering and admitting electronic evidence. The book addresses every aspect of this process including electronic information storage, outside expert assistance, the inherent benefits of electronic formats, as well as the laws and procedures for admitting evidence in your case.

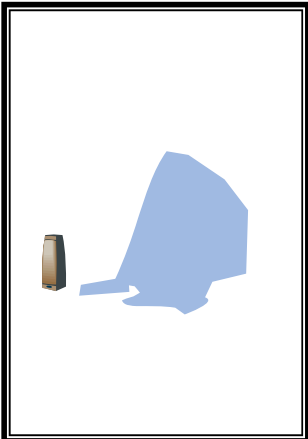
Reviewers have labeled the book as "an extraordinarily useful, practical, accessible guide" and "magnificent resource." "solid digital discovery reference resource" full of detail and repetition," "essential new book" "comprehensive" "practical" "potential" "timely"

EDE PRACTICE

Outside Counsel Preparation Obligations

The Courts have imposed "new" obligations upon outside counsel to ensure the proper handling of electronic information. This is responsible for

With proper preparation, general counsel would



BILLION DOLLAR E-MAIL DESTRUCTION CASE

[Coleman \(Parent\) Holdings, Inc. vs. Morgan Stanley, Inc. \(Florida March, 2005\).](#)

On March 1st, 2005 the Honorable Elizabeth T. Maass, Circuit Court Judge, for the State of Florida, issued an adverse instruction in the case of *Coleman (Parent) Holdings, Inc. vs. Morgan Stanley, Inc.* (March, 2005). Coleman sued Morgan Stanley & Co.,

Inc. for fraud in connection with Coleman's sale of its stock in Coleman, Inc., to Sunbeam Corporation in return for Sunbeam stock. Coleman had sought access to Morgan Stanley's internal files, including e-mails, since the case was filed. However, Morgan Stanley continued to overwrite e-mail for over 12 months after being notified to stop and failed to locate tapes containing additional e-mail. As a result Morgan Stanley was

required to search backup tapes and provide a certification of completeness. The Court granted a Motion to issue an Adverse Interference instruction, a conclusive finding of facts re the failure to disclose e-mail and shifted the burden of proof to the defendants on whether or not their was fraud in Morgan Stanley's advice to Coleman.

For the complete opinion visit www.edecenter.com.



ZUBULAKE VERDICT IS IN—\$29 MILLION

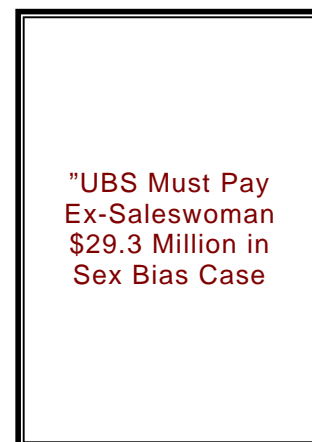
["UBS Must Pay Ex-Saleswoman \\$29.3 Mln in Sex Bias Case . . . UBS AG, Europe's largest bank, must pay \\$29.3 million in damages for discriminating against Laura Zubulake, a former saleswoman who sued the firm for sex bias."](#)

For the complete text of this story as well as the full transcript of the Zubulake

decisions visit the **Electronic Discovery and Evidence Center** located at www.edecenter.com.

This brings to an end, at least at the trial level, the infamous Zubulake case where the Honorable Shira A. Scheindlin wrote five decisions primarily involving electronic discovery issues in this wrongful ter-

mination lawsuit.



INADVERTENT DISCLOSURE OF EMAIL

Premiere Digital Access, Inc. v. Central Telephone Co., 360 F.Supp.2d 1168, 1175(D. Nev. 2005)

After producing 1,280 pages of documents under Rule 26, defendant discovered they had inadvertently disclosed a 5 page string of email between defendant's employees containing a forwarded thread authored by in-house counsel. The e-mail

thread that was authored by in-house counsel contained advice regarding how to terminate a former customer. After filing a motion for a protective order, the Court found that the e-mail was protected under both state and federal law. The Court the e-mail was protected so long as: "(1) legal advice of any kind was sought; (2) the

advice was from a professional legal adviser in his capacity as such; (3) the communications was relating to that purpose; (4) the communication was made in confidence; and (5) the communication was by the client." The Court further held that only the client could waive the attorney-client privilege pursuant to Nevada law.



CONT. FROM PAGE 1—CHECKLIST FOR INTERVIEWING . .

Questions for Your Particular Case

1. Does your case deal with individuals or groups of people who make use of computers, networks, electronic messages, cell phones or paging devices? Can information derived from these devices be useful to your litigation?
2. Have you considered obtaining a list of these devices in use by the person(s) of interest? Do you have indications that these devices are or are not available for your discovery?
3. Have you planned and prepared written discovery requests related to these devices and their information? Do the familiar tools of interrogatories, requests for certain types of production, preservation notices, and depositions plans been properly coordinated among the parties in force? Do these interrogatories encompass digital devices and digital information?
4. Have you considered the utility of focusing on the electronically native form of requested documents and emails rather than the typical printed document? It is important to note that the native digital form production makes use of meta-data (data about data), is more useful and available for computer searching using key terms and enables the use of more advanced "social group" analysis and email forensics analysis. The use of scanned paper documents in the typical "tiffed" scanned form, sharply limits forensics analysis and utility of these types of materials.
5. To what extent do you feel that certain electronic documents have been archived, "deleted," removed or altered? If this is indicated, you should promptly consider preservation action because as time progresses, digital data becomes increasingly difficult to fully recover.

If these aforementioned issues point to the potential utility and critical importance of discovery of digital data, the use of a qualified digital expert should be considered.

Locating the Forensics Expert Candidates

1. Recognize that digital forensics is an emerging profession. The relative professional competencies, knowledge, skills and experiences are quite varied among different forensics examiners. In the US, there is no single de-facto certifying entity responsible for assuring the competency of a particular digital forensics examiner. Therefore, legal professionals should understand that locating the right forensics examiner is time-consuming but necessary in order to make use of the right forensics examiner in your particular case.
2. The legal professional should recognize that digital forensics is not simply recovery of data. On the contrary, digital forensics is much more complex set of investigative processes. Digital forensics is normally construed as the coordinated and proper conduct of these processes:
 - a. Planning and implementing a protocol for the production and forensics examination of the digital devices.
 - b. Digital device identification, characterization and photography.
 - c. Notions as to type, serial identification and physical anomalies.
 - d. Data acquisition and verification from a particular digital device.
 - e. Documentation of the chain of custody activities involving the device and data stored on the device.
 - f. Forensic recovery of files, meta-data, deleted files or fragments.
 - g. Application of key search terms to the forensic dataset.
 - h. Preparation of an understandable and legally sufficient expert report.
 - i. Depositional and testimonial services as necessary.
 - j. Certified return or destruction of digital materials, when so ordered.

In certain case matters, the forensics expert can also provide technical insights and advice about digital devices of potential interest, as well as possible sources of more forensics discovery and the ability to help in constructing additional discovery requests and depositions questions to support your litigation efforts. An experienced forensics examiner can also help discuss the efficacy of statistical sampling and testing of certain digital archival data in various situations. Sampling can be an effective risk management and cost control technique.

3. You should consider asking other legal colleagues about their experiences with digital forensics examiners in past legal activities. You should also consider asking your colleagues about opposing forensics experts in past matters involving their casework. Do not fail to contact the local "techno-lawyer" and ask for potential referrals for names of forensics examiners.

a

- a4. I recommend preparing a list of requirements for the type of litigation and the potential type of digital systems (personal computers, servers, networks, etc). Have your legal staff contact about 5 to 7 potential candidates. Your staff should request that these potential candidates to send three items:

CONT. FROM PAGE 4—CHECKLIST FOR INTERVIEWING . .

- a. Current and full CV.
 - b. A set of at least 3 professional references.
 - c. A sample engagement agreement or letter.
5. You or your staff should carefully examine the CV. Does the CV clearly disclose the candidates' educational background? Does the CV contain a listing of technical forensics skills, qualifications and certifications? Professional, certification-level training should be specific and help you gain assurance that the candidate examiner has a mastery of the scientific theories, procedures and techniques to produce reliable investigative results and expert conclusions.
6. Carefully review the past cases and the types of litigation which the examiner has identified in the CV. Are there discernable patterns, plaintiff versus defendant, civil or criminal, and certain bias in terms of law firms? Is there a specialty focus on certain types of litigation, i.e., intellectual property, child pornography, misuse of information technology?
7. The candidates' references should be contacted and questioned about the candidates' skills in these areas:
- a. Ability to work in accord with the litigation schedule.
 - b. Ability to effectively communicate in non-technical jargon with the legal team.
 - c. The overall quality of the forensics investigation and report.
 - d. The relative quality of any deposition and testimony.
 - e. Finally you should consider making enquiries about both the perceived value and costs with the particular forensics engagement.
8. Based on this information and these insights, you should then consider setting up interviews with the top forensic examiner candidates. I recommend these to be, at least 1 hour and conducted at your offices.
9. Each of the candidates should be asked to bring to the interview these items:
- a. The current CV with case histories.,
 - b. A sample of completed forensics report.,
 - c. A depositions record which involves the expert providing testimony about a forensics matter.,
 - d. A written description or illustrative example of the digital forensics protocol that specifies the planned set of procedures the examiner will utilize in the case involving the type of devices involved in your litigation. This may consist of: computers, workstations, servers, networks, electronic message repositories, closed circuit television, fax machines, voicemail, cell phones or paging devices.

Interviewing the Forensics Expert Candidates

1. Consider disclosing some particulars about the case to the extent necessary to determine that the expert is not conflicted in terms of past work, associations, business or personal relationships.
2. Gain assurance that the offered CV is factual and correct. Make sure the candidate understands the requirements of factual representation of education, skills, knowledge and experience in this documentation.
3. Ensure that you are satisfied that the candidate has the necessary education, training and experience commensurate with the planned digital forensics examination and expert testimony that you envision the expert will required.
4. Discuss some particulars about the types and expected number of devices involved in your litigation, e.g. computers, mission-critical servers, networks, electronic messages (email stored in mail repositories, digital images contained in closed circuit televisions, cell phones or paging devices). You should closely question and receive positive indications that the candidate understands the overarching principles, proper uses, and potential limitations of the necessary forensics hardware and software, as well as the methods and procedures as applied to the forensics tasks in the particular matter.
5. Question the forensics examiner about his/her knowledge of precise procedures and systems to duplicate, authenticate, recover, handle, preserve and examine digital evidence.
6. Review the sample forensics examiner report. It should be clear, substantive and offer a set of explicit expert opinions. Look at attached exhibits and graphics. These should be professional in appearance, illustrative of the opinions and technically correct. You should question the examiner about the utility and experiences of demonstrative exhibits in any recent forensics engagements.
7. Look at the sample deposition. Was the testimony successful in both form and substance? How did the candidate handle opposing questions? How did the examiner defend the expert report and the factual basis for the findings and opinions presented at deposition? Review how the examiner followed counsel's instructions, dealt with objections and effective use of recesses. Test the candidate with certain "interrogation" style questions and observe responses.

CONT. FROM PAGE 5—CHECKLIST FOR INTERVIEWING . .

8. Assess the written description of the digital forensics protocol and support set of procedures. Is the description logical and clear in tone? Does the document represent an understandable and objective methodology as to forensics duplication, recovery, preservation and examination of digital evidence? Are there explicit phases for protocols and technical references contained in the protocol descriptions?
9. Ask the examiner about completion of any professional competency or proficiency tests. What constituted the competency or proficiency test and who administered? Were certificates provided to those examiners who passed these types of tests, or were these tests, in fact, simple training attendance certificates?
10. Inquire as to the extent of continuing forensics training and proficiency training and tests over the past few years. What was the training, what was the topical matter?
11. In the form of an adversarial question, ask for disclosure about any personal history or adverse employment, as well as any administrative or legal investigation or any convictions involved with any ongoing, completed or contemplated proceedings. Ask about uses of controlled substances and request the examiner make an agreement to take random drug tests with supporting polygraph tests as necessary. Carefully assess the candidate's reactions to stress and the candidate's ability to truthfully respond to difficult and intensive sets of this type of questions.
12. Review the business terms contained in the sample engagement agreement or letter. Ask about time and cost estimates and the availability to commit to the necessary work schedule.
13. Resolve, to your satisfaction, the overarching question - Does the particular forensics examiner have the education, relevant skills, experiences, qualifications and character to conduct a proper forensics investigation and deliver meaningful reports and effective testimony that deals with the particular digital devices and media in your litigation?
14. Finally, subjectively assess the overall appearance, professional demeanor and potential perceptions of the candidate forensics examiner in the context of an independent expert witness in courtroom settings.

Retention of the Forensics Examiner

After you have selected the forensics examiner, ensure that the engagement documentation specifies these details; retainer, billing matters, scope of work, timetables and the role of the independent expert. Ensure that certain items such as times to commence work, proposed schedule for forensics examinations, and delivery of the expert work product, interim and final reports are clearly established. Notices about presence of contraband, confidentiality, protection of information and opposing discovery issues should be clearly framed. Given the complexity of your litigation, you may want to consider periodic status updates and schedule review meetings as the forensics investigative work progresses.

The value proposition for your digital forensics examiner

The selection and engagement of a qualified forensics examiner should help you accomplish your litigation plan and support your legal work. Conceptually, the professional forensics examiner should support these objectives:

- Offer your litigation team additional tools and insights about digital data in your litigation plan.
- Increase your capacity to effectively deal with digital data as a form of discovery and evidence.
- Help frame the potential efficacy of several advanced forensics procedures including statistical sampling, recovery of encrypted data, social networks, data hiding discovery, and analysis of graphics imagery.
- Establish a capacity for successfully interpreting both the users and uses of digital data related to your matter.
- Development of expert testimony, supporting facts and demonstrative exhibits necessary to support the theories in your case.
- Help defend or assert claims involving the potential of discovery abuse or spoliation involving computer data.

Many attorneys recognize the potential stakes and how critical digital forensics may be to future success in many types of litigation. The effective engagement of competent digital forensics resources to support these needs is essential to successful practice in these litigation matters.



LAW PARTNER PUBLISHING,
LLC

9602 North 35th Place
Phoenix, Arizona 85028

Phone: (602)993-1937
Fax: (866) 617-0736

E-mail: newsletter@lawpartnerpublishing.com

WE ARE ON THE WEB!

WWW.LAWPARTNERPUBLISHING.COM

**GUIDING YOUR ELECTRONIC
DISCOVERY AND EVIDENCE DECISIONS**

Editor's Corner

Recently, several attorneys have challenged the fact that the changeover to discovering electronic data is not a significant change from discovering paper evidence. Even after citing to the numerous decisions where a court has imposed harsh sanctions for spoliation, they remained unconvinced.

Many attribute this "head in the sand" mentality to the difficulties of "change." Unfortunately, much fear and pain will be felt before many practitioners and their clients embrace this digital "change" that is affecting all of us. In the words of W. Edwards Deming "It is not necessary to change. Survival is not mandatory."

- Michael R. Arkfeld

As a publisher of legal technology books, Law Partner Publishing, LLC is committed to providing the most innovative and flexible reference and educational materials available today.

Whether you are an attorney, legal assistant, law student, service bureau vender or an instructor, this site is the place to find legal solutions to today's technology challenges, ranging from traditional textbooks to CLE programs, and companion websites.

RESOURCES

Consulting Services

Arkfeld and Associates is available to provide consultation re the retention, discovery, production or admissibility of electronic evidence. Visit [Arkfeld and Associates](http://www.arkfeldandassociates.com) site at www.arkfeldandassociates.com.

E-Discovery Training

To bring a CLE approved *Electronic Discovery and Evidence* training session to your firm or organization contact seminars@edecenter.com or visit www.edecenter.com.

**Electronic Discovery and Evidence
treatise**

To read the reviews and to order a copy of the acclaimed 2004-2005 edition of the *Electronic Discovery and Evidence* treatise visit Law Partner Publishing, LLC. (www.lawpartnerpublishing.com).

Upcoming EDE Sessions

May 23, 2005 MER Conference – Chicago, Ill.

June 13, 2005 LegalTech – Los Angeles, CA.

June 18, 2005 State Bar of Arizona Annual Conference—Tucson, AZ

Companion Technology Sites

Electronic Discovery and Evidence Center (www.edecenter.com)

The Electronic Discovery and Evidence Blog (<http://arkfeld.blogs.com/ede/>).

The Digital Practice of Law (www.arkfeld.com)

The Digital Practice of Law Blog (<http://arkfeld.blogs.com/dpl/>)

