Development and Delivery of Coursework: The Legal/Regulatory/Policy Environment of Cyberforensics

John W. Bagby
Professor of Information Sciences and Technology
College of Information Sciences and Technology
Co-director Institute for Information Policy
The Pennsylvania State University
301C IST Bldg.; University Park PA 16802
814.863.0520 (ofc); 814.865.6426 (fax)
jbagby@ist.psu.edu

John C. Ruhnka
Professor of Law and Ethics
Academic Director of the Bard Center for Entrepreneurship
Graduate School of Business Administration
University of Colorado at Denver and Health Sciences Center
1250 14th St., Suite 242; Denver, CO 80217-3364
303-556-5842 (ofc); 303-556-5904 (fax)
john.ruhnka@cudenver.edu

ABSTRACT

This paper describes a cyber-forensics course that integrates important public policy and legal issues as well as relevant forensic techniques. Cyber-forensics refers to the amalgam of multi-disciplinary activities involved in the identification, gathering, handling, custody, use and security of electronic files and records, involving expertise from the forensic domain, and which produces evidence useful in the proof of facts for both commercial and legal activities. The legal and regulatory environment in which electronic discovery takes place is of critical importance to cyber-forensics experts because the legal process imposes both constraints and opportunities for the effective use of evidence gathered through cyber-forensic techniques. This paper discusses different pedagogies that can be used (including project teams, research and writing assignments, student presentations, case analyses, class activities and participation and examinations), evaluation methods, problem-based learning approaches and critical thinking analysis. A survey and evaluation is provided of the growing body of applicable print and online materials that can be utilized. Target populations for such a course includes students with majors,

minors or supporting elective coursework in law, information sciences, information technology, computer science, computer engineering, financial fraud, security and information assurance, forensic aspects of cyber security, privacy, and electronic commerce.

Keywords: Cyberforensics; Electronic Data Discovery; Electronic Records Management; Pre-Trial Discovery; Admissibility of Electronic Evidence; Information Assurance, Security and Risk Analysis

1. INTRODUCTION

In this paper, we describe our development over several years and current delivery of an upper-division, undergraduate course in the legal, regulatory and public policy aspects of cyberforensics.[1] This course integrates the legal and public policy aspects of "electronic discovery"[2] with various forensic techniques that can be applied to computers, telecommunications and network activities. Information and communication technologies (ICT) are in constant change as new hardware and software technologies are designed, developed and deployed, often in secrecy. This rapid technological evolution necessarily relegates law and public policy to playing catch-up at times. Fortunately, the common law creates policy from precedents developed in real disputes so it is well suited to an ex post approach to policy-making. The cyberforensics law course discussed in this article is an amalgam of multi-disciplinary activities in evidence detection, gathering, handling, custody, security and use. Therefore, cyber-forensics necessarily involves expertise from all the domains that produce and use evidence useful in the proof of facts in various contexts of investigation, defensive-measures, regulatory tribunals and civil or criminal litigation.

The legal, regulatory and policy perspectives of electronic discovery is of critical importance to cyber-forensics experts because the legal process presents the primary opportunities for the effective use of evidence gathered through cyberforensic techniques and it also imposes most of the ultimate constraints on the use of such evidence. The cyberforensics course discussed here supplies critical institutional context to the practice of cyberforensics by non-lawyers. There are three broad categories of legal, regulatory and policy

[1] The authors acknowledge significant teaching assistance of Ms. Erica Culler, PhD Candidate, College of Education, The Pennsylvania State University. Ms. Culler assisted in various key course development activities as well as in the spring 2006 semester pilot delivery of the cyberforensics law course. These activities included the assembly of literature and course materials, syllabus design, rubric development (e.e., quizzes, examinations, student presentations, various deliverables, student evaluations), grading, course assignment management and management of deliverables.

[2] A provisional definition of electronic discovery is the ability to require opposing parties in legal proceedings and governmental investigations to provide electronic files and other data which are potentially relevant to issues in dispute.

restrictions discussed in this article that constrain the practice of cyberforensics: intrusion controls, electronic data discovery (EDD) opportunities, and evidence admissibility standards. These three broad subjects provide the primary content of the cyberforensics law course. First, there are *intrusion controls* derived from constitutional, statutory and regulatory sources as well as Week precedents that limit the compulsory identification and disclosure of electronic information which is protected as privileged or confidential.[3] Second, pre-trial EDD discovery practices govern the identification and disclosure of electronic data once litigation becomes reasonably likely or a complaint is filed. Third, there are constraints from the law of evidence on the *admissibility* of information for regulatory hearings, investigations or civil or criminal trials.

2. JUSTIFICATION FOR COURSEWORK IN CYBERFORENSIC LAW

Many recent high visibility cases clearly demonstrate the critical importance of cyber-forensics in many types of investigations, counter-measure enablement, dispute resolution, and safeguarding of confidential and proprietary information. Despite the considerable deregulation efforts of the 1980s, the tort reform pressures of the 1990s and attendant litigation reforms of the modern era, the volume of litigation continues to grow. Electronic data discovery and cyber-forensics are increasingly key factors in the proof of facts in such cases because today the majority of evidence useful to making such proofs is electronic. Consider how "smoking gun email" messages have often been pivotal in front-page civil and criminal trials involving financial fraud, sexual harassment or misconduct, antitrust violations, obstruction of justice and insider trading. Cyberforensics may involve electronic communications of various types, including email, file attachments of various types, instant messaging, blogs, rss-style aggregation, handheld devices, Internet clickstream, search history, various telephony records and the metadata associated with any of the above electronic records. With the accumulation of nearly fifteen years of Week reflecting the evolution of EDD and cyber-forensic practices, this course demonstrates the application of legal and policy mandates and constraints to particular cyber-forensics practices while establishing models for future trends.

What is the appropriate role of legal knowledge for non-lawyers practicing a profession such as cyber-forensics? The hallmark of professional status for nearly all professions is consensus formation about quality of work standards and ethical practices. Few professions can achieve that status without the conversion of "best practices" by practitioner interest groups and applicable regulatory bodies into conduct expectations that are consistent with or surpass

[3] This includes numerous steps in the process such as search, collection, archival, transmittal and use of electronic information.

the minimum expectations of society as embodied in the requirements of law and policy. As the impact of a profession's activities more closely impact the legal process (such as accountants and the Sarbanes Oxley Act), the legal knowledge component of this profession becomes increasingly relevant. Applied to cyberforensics practice, a professional's advice and work product in electronic data discovery is increasingly critical in high-stakes regulatory investigations, law enforcement, and litigation, and ignorance of relevant law would constitute gross malpractice.

Consider the analogies with other forensic disciplines, such as reliability and certification of DNA testing labs for use as criminal evidence. Such experiences from other forensics disciplines strongly reinforces the expectation that cyber-forensic professionals will self-regulate, certify competencies and procedures. Eventually, cyberforensics may become a licensed profession requiring testing and certification of technical competency, screening of moral character, and even government regulation if professional self-regulatory organizations (SRO's) fail to satisfy applicable demands for accuracy, quality, relevance and objectivity. Litigation and associated legal activities are presently the primary forum for cyber-forensic services and accordingly legal requirements provide the primary guidelines cyberforensic practices.

2.1 Links Between Cyberforensics Law and Related Disciplines

Cyberforensics has enjoyed a significant upsurge in public awareness. Even when adjusted for the "CSI effect" from popular television and movie glamorization of the forensic sciences generally, there are growing of student target populations that may be attracted to cyberforensics as a primary specialization or for whom cyberforensics law exposure would provide valuable knowledge for related fields. For example, cyberforensics law can attract students with majors, minors or supporting elective coursework in information sciences, information technology, computer science, computer engineering, electronic commerce, financial fraud, information security, information assurance, security risk analysis, forensic aspects of cyber security, privacy, and electronic government. Most of these specialties are best served by formal coursework requirements in cyberforensic law.

Consider the role of cyberforensics law in the growing family of curricula involving electronic commerce, information assurance, intelligence and risk analysis. Such curricula reflect the compelling need for the safeguarding and authorized use of both electronic intangibles as well as physical assets. Information assurance requires skills in information systems, databases, networks, human-computer interaction, and the supporting hardware and software information (IT) challenges to maintain their security. Information assurance is a combination of physical security issues (tangible asset protections, personnel screening and monitoring) with integration of electronic systems protection. Information assurance provides the foundation for trust

needed to expand safety and public acceptability of electric commerce and web-based services. Information assurance regularly includes internal audit, forensic accounting and compliance activities. These increasingly require cooperation among information assurance professionals who must work closely with computer and network forensic experts on any investigation project. Also consider how national security activities, criminal investigations and competitive intelligence practices are constrained by cyberforensics law. Such curricula focus on strategic and tactical intelligence collection, analysis, and decision-making utilizing techniques from fields such as decision analysis, statistical analysis, data-mining, information fusion and knowledge management. Cyberforensics contributes an important dimension to these curricula by enabling the exploration of incident analysis, management effectiveness, performance metrics and evaluation of risks, tactics and operations.

2.2 Cyberforensics Law Component in Various Professions

To justify resource investment in cyberforensics law curricula, strong links must be made with the emerging information assurance, security and risk analysis and intelligence professions. Cyberforensics law holds promise as an integral part of security and technology-related positions such as: cryptoanalysis, systems certifier, security specialist, security engineer, information security professional, information security analyst, information security manager, senior systems manager, systems administrator, information systems security officer and chief security officer (CSO). In business domains there are positions benefited by cyberforensics law such as policy analyst, risk/regulatory analyst, business process analyst, program and management analyst, business intelligence analyst, financial fraud analyst, economic crime analyst, financial management analyst, senior financial analyst, finance manager, controller, auditor, tax and compliance manager or senior administrator. Additional positions more directly related to forensic crime investigation or civil litigation support may include crime scene specialist, crime analyst, forensic specialist, counter-terrorism analyst or officer, money-laundering investigator and counter-intelligence threat analyst. Positions that more closely relate to national intelligence that would benefit from cyberforensics law knowledge include intelligence engineer, specialist, analyst or officer, intelligence research specialist, intelligence consultant, criminal intelligence analyst, cyber intelligence analyst and intelligence analysis supervisor.

This demand is being met with development of many new or revised programs at leading universities. Both bachelors and masters level programs in information assurance are currently housed at various programs of computer science, information sciences and technology and in information systems in schools of business. A sample listing of these programs includes: Carnegie

Mellon University, Dakota State University, East Stroudsburg University of Pennsylvania, George Mason University, Georgia Tech University, Idaho State University, Iowa State University, James Madison University, Johns Hopkins University, Kennesaw State University, the Naval Postgraduate School, Northeastern University, Norwich University, The Pennsylvania State University, Purdue University, Stevens Institute of Technology, Towson State University, University of Dallas, the University of Maryland, the University of Nebraska at Omaha, the University of North Carolina at Charlotte, the University of Pittsburgh, the University of Texas at San Antonio and Walsh College.[4] This is a growing list of programs with needs for curricula in information assurance and cyberforensic law and shows promise of further growth.

3. BASIC COURSE STRUCTURE: CYBERFORENSICS LAW

This course is designed as an elective in the Information Assurance Track and the Security and Risk Analysis major in the College of Information Sciences and Technology at the Pennsylvania State University. The official course title is the "Legal, Regulatory, Policy Environment of Cyberforensics," is abbreviated as "Cyberforensics Law," the course is numbered: IST 453. This article is organized consistent with the structure and content of existing literature by addressing the role of law in bachelor's education, describing information responsive to typical range of course proposal requirements, offering sample syllabi, providing bibliographic and appendix compendium of references to known literature and educational materials, discussing the pedagogy of law for teaching undergraduates and concludes with some depth in the deployment of innovative pedagogies.[5] The course catalog description appears as follows:

IST 453 - Legal, Regulatory, Policy Environment of Cyber Forensics

Course Description - Legal, regulatory and public policy environment of computer and network forensics that constrain investigatory and monitoring activities in computer and network environments.

[4] *See generally* Chu, Chao-Hsien, *Security and Information Analysis - White Paper*, unpublished manuscript, September 27, 2005 (College of Information Sciences and Technology, Pennsylvania State University).

[5] *See e.g.,* Ferrera, Gerald R., Stephen D. Lichtenstein & Margo E.K. Reder, *Developing and Implementing a Cyberlaw Course*, 17 J.Leg.Stud.Ed. 201 (Summer/Fall 1999); Hamilton, Lynda Skelton, *Teaching Insurance Law to Undergraduates: A Natural Course for Ethical Instruction*, 8 J.Leg.Stud.Ed. 145 (Fall 1989/Spring 1990); Prentice, Robert A., *Designing and Delivering a Course Entitled "Legal Regulation and Liability of Accountants,"* 13 J.Leg.Stud.Ed. 45 (Winter/Spring 1995).

The instructional, educational, and course objectives are designed, upon completion of the course, to prepare, students to: (1) develop an understanding of the impact of law, regulation and public policy mechanisms on the collection of electronic information from various repositories for use in investigations, counter-terrorism, litigation, regulation and other dispute resolution activities; (2) understand the basic concepts and policy issues of computer forensics; (3) gain familiarity with how privacy, security, pre-trial discovery rules and rules of evidence constrain available methods of defending against attacks, and the forensics techniques used to investigate the aftermath; and (4) develop an understanding of how law enables various security policies (e.g., authentication, integrity, confidentiality) and the implementation of information technology governance in organizations.

Cyberforensics Law (IST 453) focuses on applicable constraints on cyberforensics activities imposed by legal, regulatory and public policy considerations. The course is designed to teach students the fundamentals of identifying, screening and accessing electronic data for use as proof of unlawful activity and misconduct involving computer information systems security, computer communications, abuse of access control and unlawful access to trade secrets and covers the major legal, regulatory and policy issues in cyber-forensics including, pre-trial discovery, production of electronic documents (EDD), chain of custody, EDD cost balancing, admissibility of electronic evidence, "business records," expert witness roles and qualification, constitutional rights to privacy and confidentiality, privilege, litigation support, forensic service providers, document retention standards, legal constraints on ERN, EDD employment policies, key EDD laws, civil, criminal and regulatory procedure and evidence, "litigation holds," spoliation, obstruction of justice, interaction with inside and outside service providers, consultants and legal counsel, EDD strategy, audit trails, and multi-disciplinary teamwork relations with computer and network forensic experts. Students are exposed to the failure and successes of particular cyberforensic techniques in both the legal and regulatory forums. These topics are developed more fully in the next sections of this article.

Cyberforensics law, IST 453 employs a combination of homework, quizzes, examination(s), team project(s), outside class research, reports, in-class presentations and various class participation methods. Grading weights can vary depending on the instructor and the course emphases given in a particular institution's program. The technology needs for the course include desktop or laptop access and access to web resources both during and outside class. Cyberforensics, IST 453 is a junior or senior level course with one mandatory pre-requisite, IST 110, "Information, People and Technology." IST 110 is a three semester credit lower division (freshman, sophomore) course on the use, analysis and design of information systems and technologies to organize,

coordinate, and inform human enterprises.[6] The IST 110 prerequisite course also satisfies general education requirements in the sciences. The pedagogies used in the cyberforensics course are developed more fully in later sections of this article.

3.1 The Cyberforensics Law Curriculum

A cyberforensics law curriculum could conceivably take several forms selectively emphasizing or diminishing its major components. In building this curriculum, the authors have conducted research stretching for several years that reviews traditional forensics curricula and electronic discovery practices. This base is expanded with a close examination of the emerging cyberforensics and practices as they relate to EDD. Adjustments have been made to this definition of the field with a view to the adequate preparation of graduates to maximize their employment opportunities and career flexibility. This analytical process has resulted in a course design with four units: (1) investigations, litigation and tribunals, (2) pre-trial discovery, (3) evidence admissibility and (4) cyberforensic applications.

3.1.1 Unit I: Investigations, Litigation and Tribunals

Unit I is foundational, a critical pre-requisite to all other discussions. An

---

[6] The full course description for IST 110 states:

> Information, People and Technology presents the high points of an education in the School of Information Sciences and Technology. It opens an intellectual journey through the ideas and challenges that IT professionals face in the world. It will address major questions such as: How can we use technology to organize and integrate human enterprises? How can technology help people and organizations adapt rapidly and creatively? What can we do about information overload?
>
> Three perspectives (or facets) address the core issues: information or the basic science of data encoding, transmission and storage; people or the interactions among technologies, institutions, regulations and users; and technology or the design and operation of basic information technology devices. Students completing the course will be confident users and consumers of information technology. Students will develop research and analytical skills to evaluate specific devices and understand how those devices function in larger socio-technical systems. Students will be able to predict and anticipate the impact of new technologies on human institutions as well as understand the potential impact of institutions on the use and design of information technologies.
>
> The course employs an action-oriented approach. Students learn by doing—formulating and solving problems drawn from professional contexts, detecting and recovering from errors related to technology use, and locating, reading and studying materials that support their analysis and problem-solving. Students will accomplish this by participating in team-based learning. The course provides students with the opportunity to use, modify, and evaluate software to search for, frame, and express ideas with fluency. A variety of mechanisms are used to assess student performance. These evaluation methods typically include exams, quizzes, homework assignments, group projects, and peer and self-assessments.

See http://www.psu.edu/bulletins/bluebook/long/ist/110.htm retrieved 3.7.06.

introduction to the foundations of legal process, litigation and legal decision-making is typical in the traditional pedagogy of legal, regulatory and policy environments in various undergraduate fields such as business, administration of justice, information sciences and technology and telecommunications. Given the limitations of undergraduate preparation in these topics, students need exposure to the legal system, legal process, litigation, jurisdiction and the key distinctions in the relevant range of forums in which cyberforensics is most useful: civil, regulatory, criminal, self-regulatory, internal investigations and alternative dispute resolution (ADR) methods. Unit I is designed to introduce the differences in burdens of proof, constitutional protections, the differing stakes in outcomes, the process model of litigation, pre-trial activities, appeals, integration of investigations, incentives and resources likely available for investigation, enforcement or litigation and the roles of the key parties and other participants.

Unit I is the proper place to lay the foundation for the differences in forensic techniques used in counter-terrorism and non-judicial internal investigations. Constraints and opportunities in these contexts differ from those in dispute resolution such as civil litigation, criminal justice, regulatory enforcement as well as professional self-regulatory and ADR tribunals. Evidence gathering in the first area are increasingly performed without much judicial oversight, and may lead ultimately to deployment of counter-measures. This is a hotly controversial area as of this writing. The second group consists largely adversarial proceedings governed by judicial and procedural requirements. Nevertheless, the two broad categories are often linked. Society increasingly demands some cooperation among disputants in adversary tribunals because dispute resolution relies heavily on the discovery of facts known to or possessed by parties and others in possession of relevant facts, both independent and contractually-related parties. Investigations that yield useful evidence for litigation are no longer conducted solely by forensic experts in the physical, chemical, bio-medical and psychological sciences. Indeed, most legal and administrative proceedings usually involve some aspect of pre-trial discovery that intimately depends on electronic records of transactions, communications or other activities. Electronic evidence is increasingly a determining factor for factual issues in all forms of dispute resolution.

This introductory unit is also the optimal place to integrate some constitutional law relevant to the role and structure of government, the separation of powers among executive, legislative, judicial and regulatory branches of government, checks and balances, the dual federalism system extant in many nations like the U.S. and the bill of rights impact on law enforcement, privacy and confidentiality. The constitutional background lays a better foundation for the deployment of cyberforensics beyond the traditional counter-measures and criminal justice realms into civil litigation, regulatory enforcement, discipline of individual professionals by SROs, NGO powers, corporate shareholder

inspection privileges and the basis for electronic evidence gathering through and from government.

3.1.2 Unit II: Pre-Trial Discovery

Unit II discusses the complex process of pre-trial investigation and the use of rights granted in the U.S. by both state and federal rules of procedure to discover relevant evidence to issues in dispute from the parties in the litigation. Several critical processes and concepts are explained. The most important is a longstanding U.S. tradition of advancing justice through overcoming proprietary claims of confidentiality or individual claims of privacy with expansive requirements that permit litigants to access relevant evidence from nearly any custodial source. This generous pre-trial discovery ethic is and excellent context for international comparison because in many foreign nations the parties can hide evidence injurious to their personal interests. Pre-trial discovery of electronic information is becoming known as EDD.

Next the course may explore the emerging concept of evidence life-cycle management (ELM) as a conceptual foundation that clearly exposes the many difficulties of the discovery process for cyberforensics professionals such as maintaining chain of custody and the validity of search and seizure procedures. Finally, discovery difficulties from Week are used to illustrate the growing trend to organize ICT functions to better enable EDD efficiency and responsiveness. The electronic records management (ERM) model can be used to minimize the cost and disruptions of responding to electronic record discovery requests and minimize the risk of sanctions for spoliation or obstruction of justice for non-responsiveness to judicial requirements.

Much of the course materials devoted to legal requirements for discovery are derived from the Federal Rules of Civil Procedure (Fed.R.Civ.P.), the Federal Rules of Criminal Procedure (Fed.R.Crim.P.) and the Administrative Procedure Act (APA). There are always difficulties in generalizing about these matters because of differences between state and federal law as well as even larger differences between the laws of various nations. Indeed, there is still a significant minority of the U.S. states without discovery procedures that directly parallel the above mentioned federal laws and some states are developing their own approach to electronic discovery.[7] Nevertheless, the federal discovery and procedural rules are the most relevant in the U.S. and constitute models for the U.S. states as well as other nations. Some special rules and cases are used when relevant to illustrate progressive or antiquated laws as well as the unique requirements of dispute resolution in special

[7] *See* National Conference of [State] Chief Justices, Working Group on Electronic Discovery, *Guidelines for State Trial Courts Regarding Discovery of Electronically Stored Information* (Review draft, September 2005). Available at http://www.ncsconline.org/What'sNew/E-Discovery%20Guidelines.pdf.

circumstances (e.g., privacy in domestic relations) and of specialized regulatory programs (e.g., Food and Drug Administration).

This unit discusses the sequential pre-trial discovery process from discovery planning and the discovery conference through the traditional discovery methods of interrogatories, depositions, admissions and examinations and to the culmination of discovery at the pre-trial conference. Of course, the major focus is on the primary cyberforensics interest in the production of documents including traditional paper as well as electronic information contained in electronic files. References should be made throughout this unit to admissibility because mishandling and chain of custody difficulties arise during investigations and pre-trial discovery and such negligence can frustrate successful use of the discovery process results.

3.1.3 Unit III: Admissibility of Evidence

Unit III presents the rules of evidence that very intimately impact admissibility. Again, U.S. federal law figures prominently, particularly the Federal Rules of Evidence (Fed.R.Evid.) because much attention is constantly focused to modernize these rules. As with the procedural and discovery rules discussed in Unit II, the Fed.R.Evid. are widely copied by many states. Nevertheless, this should not detract from the occasional opportunities for the examination of unique differences between some states or foreign laws that are appropriate to explore: (1) progressive advances, (2) the difficulties imposed when law does not keep pace with technology and (3) unique cultural differences.

There are many key evidence admissibility issues under the Fed.R.Evid. and the considerable interpretive caselaw addressing the product of cyberforensics and electronic evidence. These include threshold issues of the relevance, materiality and (in)competence of proffered evidence, authentication and the chain of custody. Of central importance is the hearsay rule and its many exceptions – some more directly relevant to electronic evidence while some only tangentially relevant when electronic evidence is at issue. The most important hearsay exception for electronic information, the business records exceptions, should be discussed including the exception's complex contours when adapted to electronic evidence. Also relevant to EDD and cyberforensics are the testimonial privileges including attorney-client, attorney work product, and several other relationship privileges potentially useful in blocking discovery and admissibility.[8]

A particularly useful sub-topic in this evidence unit is the so-called "junk science" controversy that has resulted in new rules of admissibility for

[8] Situation dependant additional but typically narrowly construed privileges, include the spousal privilege, the doctor-patient privilege, the priest-penitent privilege, the psycho-analyst- patient privilege and in much more limited situations, there may apply an accountant-client privilege and a self-evaluation privilege.

scientific evidence and the expert witnesses needed to sponsor useful reports about electronic evidence and the results of cyberforensic techniques. A discussion may be appropriate about the watershed *Daubert*[9] case and its progeny, also known as the *Daubert* Trilogy. This often begins with the history of scientific evidence and experts from the 1923 *Frye*[10] case's general acceptance standard still in use in some states and then through the modern federal law from the *Daubert*, *Joiner*[11] and *Kuhmo*[12] cases. These cases help cyberforensics experts better understand that the cyberforensics field is a respected area of recognized expertise and qualified experts are eligible to testify. The *Daubert* focus also assists in establishing how electronic evidence must link to the facts at trial, that many emerging disciplines are candidates for scientific testimony and that judges are the ultimate gatekeepers of scientific evidence admissibility. Analogies can also be drawn from several other major areas of recurring need for proof of scientific facts as sponsored, interpreted and applied by expert witnesses to better inform future cyberforensic experts of the evolving challenges as technology changes. Other analogous disciplines can include: statistics and multiple-regression, survey research methods, the estimation of economic damages, epidemiology, toxicology, various engineering practices, DNA testing, medical diagnosis and treatments, environmental and workplace exposures and various employment issues.

3.1.4 Unit IV: Cyberforensic Applications

Recent studies suggest an alarming incapacity at most business firms, government agencies and non-governmental organizations (NGO) with respect to EDD compliance, the avoidance of spoliation or obstruction sanctions and the attendant public relations damages. According to the Cohasset Study: "the majority of organizations are not prepared to meet many of their current or future compliance and legal responsibilities."[13] Indeed 46% of surveyed firms have no formal recordkeeping procedures and 65% do not include electronic documents among the documents that are systematically retained. Such recent studies strongly suggest that there is still considerable under served opportunity for EDD and cyberforensics professionals with good training. This Unit IV can provide some coherence to additional matters not readily classified in the first three units and therefore create opportunities for EDD and cyberforensics applications.

---

[9] *Daubert v.. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993).

[10] *Frye v. U.S.*, 293 F. 1013 (D.C. Cir. 1923).

[11] *G.E. v. Joiner*, 522 U.S. 136 (1997).

[12] *Kumho Tire Co., v. Patrick Carmichael*, 526 U.S. 137 (1998).

[13] Williams, Robert F. and Lori J. Ashley, *Electronic Records Management Survey: A Renewed Call to Action*, Cohasset Associates Inc. (2005).
http://www.merresource.com/pdf/survey2005.pdf

In the inaugural delivery of this course the authors have found that real legal cases, integrated throughout the course, retain student interest and illustrate the concepts well. This Unit IV can be deployed to concentrate on particular and important EDD and cyberforensics problems. For example, the now famous and watershed *Zubulake* litigation is a key series of related cases that illustrate the need for organized ERM, the importance of EDD to employment issues as well as relevance to many financial services sector concerns.[14] The Morgan Stanley litigation illustrates that recalcitrance in discovery response may be severely punished, even without additional litigation.[15] The Microsoft litigation reveals the potential for reputational damage. Like these high visibility cases, there are hundreds of cases useful to the cyberforensics curriculum. As in other legal studies, some cases are redundant, but most are nevertheless of direct and immediate interest in cyberforensics and EDD such as the cases that have established mandatory EDD procedures such as the "litigation hold." Cases are a common law compendium that reveals emerging document retention standards and thereby establish the legal constraints on ERM practices.

Unit IV can also contribute to cyberforensics law as an end-stage degree program culminating experience. Cyberforensics law permits an integration of the various tools of cyberforensics law through application in a problem based learning (PBL) environment. For example, end-stage course integration is an ideal forum for learning the identification, retention and management of consultants and third-party EDD service providers. Similarly, exposure to the whole field of cyberforensics is most useful to enable students to understand EDD strategy, a classic culmination of a degree program. With the benefit of understanding the whole process, students are better enabled to contribute to EDD audits and have acquired skills to address the difficulties of bridging multi-disciplinary relations with computer and network forensic experts and litigators or regulators. Table 1 summarizes the content in IST 453 organized by semester weeks, but not by the four unit divisions that are described above.

---

[14] Eight related *Zubulake* decisions were issued between 2003 and 2005: *Zubulake v. UBS Warburg*, 217 F.R.D. 309 (S.D.N.Y. 2003) (Zubulake I: allocating discovery costs for email production from backup tapes); *Zubulake v. UBS Warburg*, No. 02 Civ. 1243, 2003 WL 21087136 (S.D.N.Y. May 13, 2003) (Zubulake II: Zubulake's reporting obligations); *Zubulake v. UBS Warburg*, 216 F.R.D. 280 (S.D.N.Y. 2003) (Zubulake III: allocating costs between parties for restoration of email backup tapes), *Zubulake v. UBS Warburg*, 220 F.R.D. 212 (S.D.N.Y. 2003) (Zubulake IV: duty to preserve emails; defendant bears plaintiff's re-deposition costs); *Zubulake v. UBS Warburg*, 2004 WL 1620866 (S.D.N.Y. July 20, 2004) (Zubulake V: sanctions granted; UBS ordered to pay costs; defense counsel ordered to monitor compliance and preserve with a litigation hold); *Zubulake v. UBS Warburg*, 231 F.R.D. 159 (S.D.N.Y. Feb.2, 2005) (Zubulake Va); *Zubulake v. UBS Warburg*, 382 F.Supp.2d 536 (S.D.N.Y. March 20, 2005) (Zubulake VI: preventing admission of various evidence); and *Zubulake v. UBS Warburg*, 02-CV-1243 (April 6, 2005) (Zubulake jury verdict: $29.3 million in damages of which $9.1 million compensatory, nearly $20.2 million punitive discovery sanctions).

[15] *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, 2005 WL 679071 (Fla. Cir. Ct. Mar. 1, 2005).

Table I: Class Syllabus Schedule

IST 453 Cyberforensics Law

Sessions	Topics
Week 1:	Investigation and Litigation: Criminal, Civil, ADR, Regulatory, Non-Judicial Tribunals
Week 2:	Traditional Discovery: Interrogatories, Depositions, Discovery Requests
Week 3:	Electronic Data Production and EDD Project Planning
Week 4:	Litigation Hold on Electronic Data
Week 5:	Admissibility of Electronic Evidence
Week 6:	Computer Forensic Expert Witnesses
Week 7:	Scientific Evidence and *Daubert* Constraints on Admissibility of Electronic Evidence
Week 8:	Evidentiary Aspects of Modern Communications Technologies
Week 9:	Cost Balancing of Electronic Document Production
Week 10:	Privilege and Privacy of Electronic Evidence
Week 11:	Spoliation and Obstruction of Justice
Week 12:	Regulated Electronic Records Management
Week 13:	Third Party Service Providers
Week 14:	Team-Project Presentations
Week 15:	Team-Project Presentations

Inevitably, there are pressures to modularize courses and cyberforensics law may not be an exception. One obvious strategy might be to compress this semester long course down to a quarter or trimester configuration. While this can be done, great caution is recommended because these are significant adjustments that should be carefully considered. If the three credit, semester-long (14 or 15 weeks) course discussed herein is condensed into the ten week format of the typical quarter-length term course, the following approaches are recommended to making adjustments. On threshold analysis, many instructors might simply eliminate or condense some topic coverage. Another predictable condensation strategy is to reduce or even eliminate in-class time devoted to the particular, time-consuming pedagogies suggested here. While successful delivery may still be possible with such adjustments, great care should be taken because there is critical value in each topic and in the coverage depth as defined herein as well as to the skills derived from these well-respected pedagogies.

There is some promise to achieve topic compression by aligning this course with the emphasis given cyberforensics at particular programs or the emphasis given that is derived from the perspective of particular instructors. For example, some programs are largely oriented to counter-terrorism and do not give much emphasis to the litigation perspective. Graduates from such programs may largely target public-sector, government and criminal law investigation employment opportunities rather than to the broader consulting, regulatory, ADR and civil litigation deployments of cyberforensics. Under this strategy, a cyberforensics law coursework package might reduce some of the instruction responsive to private-sector demand for information assurance coursework preparation and/or third party cyberforensic service providers that support eCommerce, the telecommunications industry, Internet service providers (ISP) and other non-governmental sectors. However, framing cyberforensics primarily for counter-terrorism or targeting graduates to employment primarily in government agencies may limit graduates from the largest growing portion of the employment market. Similar difficulties may accompany the narrowing of scope of this course or the program primarily to careers serving only civil litigation.

Another alternative is pedagogical curtailment that would allow some programs and instructors to condense course coverage by replacing in-class student presentations with outside-of-class activities. For example, individuals can write papers rather than do in-class presentations of their research. Teams can create websites presenting their work rather than consuming in-class time with debates. Similarly, at many institutions, quizzes and examinations can be delivered in additional sessions held outside class time such as using online testing or group delivery during separately scheduled and additional evening sessions.

4. CYBERFORENSIC LAW PEDAGOGIES

The cyberforensics law course described here benefits greatly from several foundations that form the core of Penn State's curricular standards in information sciences and technology. These are pervasive tools that endow students with both perspective and expectations that most instructors find useful in delivery of their coursework. Cyberforensics law benefits greatly from these pedagogical perspectives generally deployed at Penn State and many are detailed in later sections of this paper.

One important perspective is problem based learning (PBL) in which students learn by solving problems and through their independent research to inform their proposed solution. PBL recognizes a somewhat diminished role for instructors to pervasively teach primarily facts in favor of an instructor's role in coaching student-driven quest for solutions, learning from failure, extensive

feedback and frequent project foci.[16] Cyberforensics may be an ideal context for the implementation of PBL in team settings. Many effective PBL implementations use critical thinking techniques in which developing then testing propositions is the key to considering a range of plausible views.

> "Critical thinking is the processing of information by using inquiry and logical analysis. It involves reasoning by acquiring and testing information to develop independent conclusions, to analyze advocacy representing points of view, to examine assumptions and test allegations of fact, and to reconcile inconsistencies between new information and existing personal beliefs. Critical thinkers must uncover bias that can affect the accuracy and persuasiveness of oral or written expression. Critical thinking permits you to evaluate evidence or advocacy, evaluate the quality of expression, support assertions or formulate effective rebuttals, write convincing essays, contribute to class discussions, evaluate public policy arguments, and test claims supported by empirical evidence."[17]

Many PBL problems also require the use of high quality project management. EDD and cyberforensics projects, particularly because they are so fundamentally constrained and influenced by law, regulation and public policy, are series of related tasks susceptible to the project management skills-building regimen of systematic subtask inventories, efficient scheduling and implementation management generally developed in quality project management coursework. In programs benefited with prerequisite work in project management, cyberforensics law should build effectively on this skillset. However, even in programs without formal project management skill building, it is possible to use team projects to build basic project management skills. These skills can be introduced with outside readings and then these skills better developed over the term with application and feedback on numerous assigned projects.

The above discussion of standard pedagogical elements in information sciences and technology argues for their ubiquity in any curriculum in which cyberforensics law is a component. However, the unique mix of skills training that any particular program is capable of delivering varies greatly. It may still be possible to achieve some integration of these skills even if they are not omnipresent in a particular program's other coursework or if the cyberforensics law course cannot practically be preceded by such prerequisites. For example, cyberforensics law is also an ideal forum for the initial introduction of critical thinking, PBL and the integration of people, information and systems. Litigation and the policies underlying cyberforensics law are classic critical

---

[16] *See generally* Albanese, M. A. and S. Mitchell, *Problem-based learning: a review of literature on its outcomes and implementation issues*, Academic Med (1993) 68(1): 52-81.

[17] Bagby, John W., *eCommerce Law*, p.10 (2003; West Publishing Co. Mason OH).

thinking contexts. These nearly always involve controversies with plausible opposing advocacy, the continuing need for assessment of issues and reasoning, and there are presented numerous opportunities for developing alternative hypotheses, rationales and conclusions. Case studies are a popular legal education method making cyberforensics law an ideal opportunity to resolve hypothetical and simulated problems or revisit real cases for analysis. Cyberforensics is an ideal application of the integration of people, information and systems.

Many institutions now deploy course management systems to enable instructors, teaching assistants and students to use online course materials and communications technologies that enhance course management without costly website development and maintenance. For example, WebCT,[18] Blackboard (now merged into WebCT)[19] and Angel[20] are three from among dozens of such systems[21] adaptable to almost any academic discipline and with flexibility that does not require deployment of any mandatory pedagogies or instruction methodologies. IST 453 Cyberforensics Law makes a majority of the course materials available only to registered students or invited guests including syllabi, schedules, announcements, lecture notes, quizzes, readings, access to multimedia resources, distribution of assignments to students and subsequent electronic submission of deliverables by students and teams. Course management software permits computer access from nearly any physical location in the world with reliable Internet access to manage course administration. Course management systems automate repetitive tasks and thereby enhance student learning opportunities and collaboration. Importantly, properly implemented course management systems can make course compliant with the TEACH Act's 2002 reformulation of educational fair use under U.S. copyright law.[22]

4.1 Group/Teamwork

Most students in the College of Information Sciences and Technology are actively engaged in group teamwork in all their IST coursework. Students required to think, write, talk and argue about course content learn better and retain more. Teamwork is a basic foundation of the program's pedagogy

[18] *See* http://www.webct.com/ retrieved 3.7.06.

[19] *See* http://www.blackboard.com/webct retrieved 3.7.06.

[20] *See* http://angellearning.com/ retrieved 3.7.06.

[21] *See* Western Cooperative for Educational Telecommunications' comparison of course management systems at http://www.edutools.info retrieved 3.7.06.

[22] On November 2nd, 2002, the Technology, Education and Copyright Harmonization Act (TEACH Act), was passed as part of the Justice Reauthorization legislation Pub. Law 107-273 (Nov. 2002), 116 Stat. 1758

107th Cong.

deployed to enhance the various group work settings in practice at most employers.[23] IST 453 students are expected to fully participate in required group activities, including, mini-presentations, in-class discussions and the culminating portal project research. Team assignments are detailed in the syllabus and posted to the course management system. Teams are immediately necessary to prepare for class and team processes are used throughout the semester for work on research projects and point-counterpoint debates (mini-presentations). Teams are also recommended to meet and confer to study together and prepare for quizzes and exams. Team member evaluation of other team members is deployed to discipline equal contribution and to provide additional learning from inter-student evaluations.

4.2 Class Attendance and Preparation

Attendance in IST 453 is mandatory for all class meetings, for quizzes and examinations and for all group activities. Each week a team representative makes an electronic submission of a team attendance record. Attendance and class preparation is mandatory because law is complex and requires interpretation. These skills are not generally acquired in a few hours of last minute cramming or in a vacuum without interaction with the law domain expert. Understanding of law materials is acquired continuously through steady, consistent and progressive exposure over the whole term. Also outside preparation of considerable readings is required because viewgraph slides used in class by many instructors generally are highly abbreviated, representing mere condensations used primarily to focus attention on particular topics. Indeed, bulleted phrases on overhead slides sometimes lure students to presume course content is simple and abbreviated. Clearly viewgraph excerpts are seldom complete thoughts so they lack the details needed for adequate learning and ultimate success in upper division coursework. Therefore, students' sole focus on in-class immersion without outside preparation is insufficient preparation for exams in cyberforensics law. Furthermore, detailed note taking is essential to fill in the many important details, to note how the law applies in the many class examples and as an repetitive imprinting behavior.

Outside class preparation requires careful reading and reasoning through all the written materials. Students accustomed to reading too quickly or merely skimming to finish just-in-time find such preparation is generally insufficient when compared with more intensive study. Students in IST 453 are expected to come to each class having prepared the assigned readings before attending the lecture on the topic covered by assigned readings. Readings in cyberforensics law are best "prepared," that is the readings are not be simply read, instead,

[23] *See* Spence, Larry, *Working in Teams*, (IST Learning Initiatives, 2005). http://pbl.ist.psu.edu/teamwork/

they must be read carefully, sometimes re-read to highlight and confirm understanding for key terms, definitions and examples. Many good students take notes that restate the concepts in the student's own words as they read, making summaries in the margins or in separate notes. This note-taking is helpful because rewriting and paraphrasal serves to imprint the knowledge. Highlighting enables retrieval of key textual references when reviewing for exams, quizzes or homework and also serves to imprint.

Textbooks and educational materials in law are often of greater length than in other coursework making the pace of reading for each class sufficiently high so that students must give increased attention to keeping up throughout the course. Careful reading of technical legal text has been the primary technique for law study for centuries. Law study is somewhat different than study for the computational, systems architecture or programming disciplines. Law necessarily involves considerable, close study of relevant texts including excerpts from constitutions, statutes, regulations, cases and interpretive texts. Reading and discussion about law is the predominant pedagogical method to learn law. This makes law study much more like the pedagogy used successfully in the humanities and social sciences, language arts, philosophy, applied sociology, history or applied political science. Successful students in cyberforensics law study must recognize these differences and adapt immediately to the greater expectations for preparatory reading and outside study. It is often useful to periodically remind students of this pedagogical difference and to deploy quizzes or Socratic dialogue in class to provide sufficient incentive for adequate preparation of the readings. This differences in needed student study and preparation also highlights the interdisciplinary challenge in professional cyberforensics practice because skills learned by this technique must be accurately applied to technical processes.

Law instruction has a long tradition of deploying the Socratic method and the much copied case method. Indeed, Prof. Christopher Columbus Langdell at Harvard Law School invented the case method in the nineteenth century nearly 50 years before the case method was adopted more widely by business schools in the 1920s or by medical schools in the mid-1980s.[24] The case study method is becoming pervasive across most disciplines. The case method is important to cyberforensics because cases produce many of the key precedents that constrain cyberforensics, cases provide real-life examples of the legal concepts, often with well-known parties, cases can be adapted to provide PBL opportunities and critical thinking is essential to a successful delivery of the case method. Course instructors and librarians are good resources to provide guidance for the effective identification of cases and other literature organized by legal citations. This can include original source materials for student

[24] *See* Garvin**,** David A. *Making the Case: Professional education for the world of practice*, Harvard Magazine, Vol. 106, No 1, pp. 56-65 & 107 (Sept.-Oct. 2003).

research as well as interpretive viewpoints that can engender interest in further study. Many online search and legal resources are also useful in cyberforensics law study, including the proprietary legal databases Lexis-Nexis and Westlaw.

4.3 Team Research and Portal Projects

Various courses in law, regulation and public policy in schools of engineering, business and information sciences and technology deploy team research projects. In IST 453 these are configured as team portal projects, essentially electronic reports that require research by all teams. The project culminates in a final report configured as a webpage or portal that provides an electronic gateway to an understanding of the topic for use by all other classmates. Portals should enable other users to explore and gain a deeper understanding of an important aspect of cyberforensics law and EDD. In IST 453, all students in the class are examined on the instructor's selection of topics covered in all other team's portals. This configuration is intended to expand all student's breadth and depth in the subject matter while endowing teams with responsibility for development of an area of curricula in this fast evolving subject matter.

Portal projects implement PBL in group settings to accomplish the identification and analysis of a research problem. These projects generally enhance research and critical thinking skills by requiring the search and retrieval, filtering and analysis of relevant information organized into an effective web-based presentation report format. There is an optional opportunity for each team to select its topics that can be used to enhance student commitment by providing group work consistent with personal interests.

The particular implementation of portal projects in IST 453 discussed here requires a phased delivery of preliminary work, then progress checkpoints to encourage sufficient accretive work culminating in a final portal deliverable. Phased deliverables provide feedback opportunities, usually require significant revisions and refinement and this process is proven to lead to higher quality work products. Portal project teams should also benefit through further enhancement of group work skills. For example, most teams report active participation together through conferring and collaborating to identify important issues, using group processes to select topics appropriate both to most teammate's interests and the cyberforensic law subject matter and finally team project management dynamics results in considerable research that informs the preparation of the portal.

Classmates can be greatly enriched by the work of every other group's work. That is, each portal can be evaluated on how well it is designed to engage the interest of others from the whole class outside each group. Classmates can obtain a clearer understanding with greater depth about each other group's legal, regulatory and/or public policy research issues through web access and

class presentations than would be possible without this considerable team-based, outside class activity. Portal projects expand the potential material covered beyond what is possible for in-class only exposure.

These team-based research portal projects are focused on a final deliverable report, configured as a website or portal, which provides a problem statement, explanatory text discussing the problem, a textual synthesis of divergent views and well-defended clear conclusions. It is expected and rewarded when there is appropriate and considerable use of working hotlinks, provided throughout the report, linking to various relevant online materials. Linked materials are evaluated on how directly the underlying materials relate to the topic, and generally are expected to include such resources as laws, regulations, articles, commentaries, research reports and other relevant information from academic, trade, professional and law publications. Critical thinking is a key analysis method that should be deployed to identify the topic, most likely a controversial one, which will then require investigation about the problem, including the positions of various advocates. The report should synthesize these materials, possibly proposing and defending a solution.

Many successful teams design and implement their project steadily throughout the course. The phased checkpoints require timely progress report submissions according to the schedule of deliverables described below. These checkpoints implement a project management regimen that are intended to assure that the process culminates with the project's timely completion and electronic submission. Portals are evaluated then posted to the course website so that all other class members can view them during the final two to three weeks of class culminating in the final examination. Each student is expected to study and navigate every other team's portal. Some content from all the portals is tested on the final exam.

Team or group portal projects are approached in stages of a project, much like the work of cyberforensics professionals. Each of the three stages culminates in an electronic submission using the course management system for uploading, evaluation and feedback. Implicit in this schedule and then explicitly required in the second deliverable is a general project workplan inspired by students' project management training. Teams are encouraged to modify their workplans so long as the scheduled reports are timely filed.

4.3.1 Team Portal Deliverable #1: Topic Bids

Each team's selection of portal topics are expected in title and abstract form of approximately one page in length. The abstract identifies and describes legal, regulatory and/or public policy issues in cyberforensics law. The abstract commits all team members to this project. Cyberforensics law uses a team bidding system for the selection of research portal topics. Bids can be drawn from a list the instructor constructs of preferred topics or alternatively could be initiated without such prompting.

Bidding is intended to assure a diversity of topic among the teams, provides breadth to all students' class experience by expanding their exposure to many more important topics, reduces redundancy between different teams' research and provides valuable experience in proposing the acceptance of a team's effort to win a service project. The portal project bidding attempts to achieve the course's pedagogical and PBL goals because: (1) all teams commit to topics that are both relevant to the course subject matter and represent personal interests of the whole team and (2) bid quality is improved while team consensus and commitment are enhanced when more background research is conducted early on in the project when the scope is still flexible rather than later on in the project timeframe when the scope has become fixed. A basic rubric is used for the portal bidding process.[25] The instructor and teaching assistants are engaged in evaluating each portal bid using the rubric factors in the formulation of a bid acceptance or in the rejection[26] and any follow-on instructions for second round bidding or bid resubmissions.[27]

---

[25] The evaluation and bid award is based on the following rubric:

1. reason topic was chosen,
2. team's apparent understanding of the topic,
3. quality, quantity and breadth of background information on the topic,
4. a start of a bibliography, expressed as the names of statutes, regulations, articles, reports, either in standard bibliographic form or simply as links,
5. the clarity of writing and satisfaction of requirements for team number, team member names and timely submission,
6. clear evidence of specific aspects of the broad topic that separates each team's bid from other team's bids on a similar topic.

[26] In some instances a particular team's bid might be rejected either due to quality insufficiency or simply are of comparatively lower quality when judged against another team's bid on the same or similar topic. If another team is awarded a topic because the winning team's bid is better conceived, researched and articulated in the first round of bidding, the losing team(s) is directed to resubmit with a changed topic in a second round of bidding. Tertiary rounds of bidding are possible but some instructors may strive to avoid too many additional bidding rounds because they can impose significant delay and therefore be counterproductive. When a new bid is made on a different topic, the bidding team must necessarily perform additional, time consuming and in-depth background research to inform the revision. It may be useful to alert teams of this time constraint suggesting at least some superficial consideration of a back-up bid during the less time-constrained first round period. Revised bid resubmissions are required within only a few days following the instructor's distribution of feedback that rejected the previous bid. All teams' awarded bids are posted for all other classmates to view following the final acceptance of all teams' bids.

[27] In some cases, more than one team could be awarded a similar topic but this generally results only from clear statements in all overlapping bids that each team is committed to address some specific and substantially separate aspects of the topic sufficient to differentiate each team's portal. This overlap is evaluated at the instructor's discretion and may arise in two ways. First, this severability of a single topic may arise when more than one team submits high quality bids that initially evince the sufficiency of these significant differences in the first round of bidding. Second, up to two teams could achieve severability of a single topic if they engage in reasonable negotiations that re-scopes each bid and this severance satisfies the instructor. Such negotiations can achieve additional pedagogical benefits, particularly for the negotiating teams.

4.3.2 Team Portal Deliverable #2: Outline and Workplan

A detailed outline and workplan are due approximately one month after bids are awarded. The outline must be a detailed substantive topic breakdown and organization revealing that the team has already conducted considerable information search and retrieval and that this initial research shows a developing understanding of the major issues involved. This second deliverable serves as a progress report that should also specify a workplan: an expected set of tasks scheduled so that the project will be timely completed. A variety of workplan formats can be useful including project management software diagrams, but in all cases should clearly reveal students have made estimates of the time required, made an initial allocation of work and are realistic in their scheduling - all the hallmarks of successful project planning.

4.3.3 Team Portal Deliverable #3: Final Portal

The final portal submission must be a substantially revised and polished final submission. Portals are posted to the web for use by all other classmates in studying for the final exam. Final submissions must be in a format easily posted without link changes and viewable using various browsers. Students are generally prohibited from posting their portals on their personal webspaces because of the risk the portals might become unavailable for other classmates during the intensive final exam study period. All deliverables are evaluated and graded. The heaviest weight is allocated to the final deliverable. Portals are generally evaluated by these criteria: (i) the timeliness and completeness of all progress reports and final portal submission, (ii) the depth of analysis, (iii) the clarity of writing and other exposition, (iv) the accuracy, navigability and extent of relevant links and (v) the effectiveness of a required visual representation of the research project.[28]

---

[28] A visual representation is required for all portal projects and are recommended for the shorter, point-counter, mini-presentations discussed in the next section. A visual is helping to naive readers to recall, organize, and represent graphically the pertinent information from a research topic. Visual learning techniques or graphical ways of representing information help in understanding, organizing and teaching processes, in the organization of complex phenomena and in the prioritization of new information. In the support of others' decisionmaking, researchers must often provide simplified assistance with perspective, clear reasoning, and solid information. In the analysis of large data sets, the clarification of trends and patterns, in identifying irregularities and enabling of quick reactions, visual representations are becoming crucial support for the reports made by nearly every discipline or profession. Therefore, the visual requirement for IST 453 cyberforensics law coursework aids in skillbuilding for teammates in their problem solving, it helps build team support, and it accelerates evaluation and approval by instructors, supervisors or clients.

Each team must design and refine some type of visual graphic to illustrate their key points, the major institutional players, and/or the policy arguments made their portal project. Teams are given considerable freedom to select the type of visual they find is most useful to conveying important matters in each specific topic. Experience in these projects from among students in information sciences and technology over several years illustrates that particular

4.3.4 Selecting Suitable Topics for Bidding

The authors have experimented with several formats for topic selection in individual and team project contexts. One method is free-form, allowing students to identify and describe topics entirely on their own. While this method initially raises student satisfaction, there are nevertheless risks that students may choose topics before they have had enough exposure to the cyberforensics law subject matter and this too likely will result in suboptimal choice on relevant topics or the impracticality of a project's scope. Therefore, it seems advisable to either work more closely with individual students or with teams to negotiate topics. Another alternative is for a knowledgeable instructor, who ostensibly knows a relevant range of researchable and relevant topics, to set a topic range. The portal bidding process described here is premised on this latter, instructor-induced, topic pre-selection. The side benefits are that a defined range of relevant topics can be selected and each class in each successive year is benefited with good breadth and depth of topic coverage. Another side benefit is that when instructors remain current in the field of cyberforensics law, they can adapt the list to the most pressing problems. For example, in 2006 the electronic eavesdropping controversy unexpectedly became a very timely portal topic. A full list of contemporary topics in the year 2006 appear in a footnote.[29]

---

visual styles can be effective such as one or more from this potential list: concept mapping, Gantt charts, flow charts, T-charts, decision trees, data flow diagrams, schematics, systems architecture models, data flow diagrams or object models. An online primer showing the appropriate use of these and other types of visuals is available to IST 453 classes.

[29] Listing of portal project topics available for IST 453 team bidding during spring term 2006:

1. Wiretap, Trap and Trace under CALEA, Communications Assistance for Law Enforcement Act of 1994 (CALEA), Pub. L. No. 103-414, 108 Stat. 4279;
2. *Zubulake* cases and their impact on balancing EDD costs;
3. Analysis of the forthcoming Revisions to Fed.R.Civ.Proc., Fed.R.Crim.Proc. and Fed.R.Evid. in relation to EDD and Cyberforensics;
4. Analysis of EDD/Cyberforensics industry's organizaiton: third party service providers, EDD consultants, electronic records management providers;
5. Analysis of evidentiary and testimonial privileges in relationship to Cyberforensics & EDD: types, history, justificaitons, etc.
6. Spoliation and obstruction: causes, pitfalls, caselaw, effects, EDD and ERM impact;
7. Litigation holds: definitions, Week, discussion of various parties' duties, discussion of prohibitions and sanctions, integration of legal constraint into ERM practices;
8. Development of the activity-investigation-evidence supply chain discussing the constraints and opportunities of evidence lifecycle management;
9. National Association of Securities Dealers (NASD) electronic records management (ERM) requirements: analyze rules, discuss duties & processes, discuss recordkeeping; discuss file organization & document retrieval architecture, discuss targeted records (e.g., IM, email, communication logs);
10. Discussion of the Sedona Principles: their history, recent revisions, their objectives, proffered means to implement,

4.4 Team Debate, Point-Counterpoint or Mini-Presentations

Cyberforensics law uses another team-based research project, a form of team researched debate against another team. These are also known as mini-presentations or point/counter activities that have a point-counterpoint character and are made in an in-class oral format. Each topic is assigned to two teams just one week prior to the presentation necessitating quick responses like often occur in real work environments. Each team is expected to prepare a report for the class to support their debate posture (either for or against) as assigned and on the particular topic. Mini-presentations require research that is intended to provide deeper understanding of a selected topic to the team as research group and ultimately through the presentation to the whole class. The presentation of opposing arguments may also contribute to students' personal but better-informed views and critical thinking skills. The mini-presentation projects are designed to implement PBL in group settings. Such research and advocacy projects on controversial issues in cyberforensics law generally the search and retrieval, filtering and analysis of relevant information organized into an effective class-based presentation. Teams are also expected to strive to engage classmates in discussion centering on their topics. Careful selection of provocative topics by the instructor helps assure that critical thinking educational benefits occur.

In IST 453 each team prepares two mini-presentations on a schedule set by the instructor, once on the "advocacy for" side of some controversy and the second time on the "advocacy against" side. The instructor generates a list of current and provocative topics in cyberforensics law and the topics are assigned exactly one week prior to the in-class "debate." Each presentation is limited to approximately ten minutes and there is time allotted for follow-up discussion time engaging the whole class. The presentations are expected to provide sufficient background information for classmates to clearly understand the issue discussed and the team's viewpoint. After clarifying the problem statement, evidence either in support or to refute the topic as assigned is expected. The evidence used should generally rely on an accumulation of materials, which will require outside research by each participating teams, including sources on law, regulations, articles, commentaries, research reports and op-eds. Each team's final report is expected to be concise, particularly in

---

11. New applications of electronic eavesdropping for national security counter-terrorism interdiction and criminal enforcement: email, IM, web-surfing history, search engine use history, telephony (wireline, wireless, VOIP), geo-location (toll tags, Onstar or wireless tracking, credit card use, etc.)
12. Internet archives as electronic repositories of Internet content: use as evidence, illustrative case(s) (e.g., *Echostar Satellite*), various archives available (i.e., archive.org, Wayback, webcite system), validity of resistance to archiving under copyright and opposition to results when offered as evidence, hearsay rule application, costs, use of proxies, etc.

comparison with the more substantial portal research projects discussed above. Each team is evaluated with a rubric simplified from that discussed above in the more extensive portal project: the quality of their presentation, the persuasiveness of their presentation and logic, and their ability to provoke class' questions and respond defending their position on the topic. Teams are required to submit a short deliverable, detailing their argument. Class members evaluate each team's presentation on using the same rubric that is used by the instructor.

5. EDUCATIONAL MATERIALS

An enormous amount of literature on cyberforensics and EDD has emerged in the last few years largely resulting from several recent watershed cases that are only now serving to alert firms, government agencies and NGOs of the dire need to give this area greater attention. Instructors may need to prepare themselves to do considerable screening to find the most efficient and useful literature, accessible by upper division undergraduates and within manageable reading expectations. The literature takes several key forms, many portfolios of which may be useful to support a well-designed cyberforensics law course. There are many websites from EDD and cyberforensics service providers that address best practices and lessons learned from the watershed cases. Instructors of cyberforensics law should consider a collection of articles from cyberforensics academic journals, articles from practitioner journals, articles from academic law reviews, white papers and other research reports to sponsor, online cases and statutory compilations. Much, if not most of this material is freely available from the Internet and permission for the use of electronic copies of many substantial works is easily obtained.

While none of the college-level textbooks available at this time are directly keyed to the body of knowledge identified in this article, there are nevertheless several textbooks with useful parts. Also recognize that textbooks largely covering cyberforensics technical skills are not likely appropriate for a cyberforensics law or EDD coursework. These technical texts typically address computer, network and file access techniques and have very limited and shallow integration of the many policy constraints imposed by the legal system. Potential instructors of cyberforensics law should carefully examine the candidate texts listed in Table II as well as the other literature listed in the bibliography to determine the cost effectiveness of each and the optimal method to integrate each part.

Table II: Textbooks

Lange, Michele C.S. and Kristin M. Nimsger, ELECTRONIC EVIDENCE AND DISCOVERY: WHAT EVERY LAWYER SHOULD KNOW, (2004, Am.Bar Assn.; isbn#1-59031-334-8);
Britz, Marjie T., COMPUTER FORENSICS AND CYBER CRIME, (2004, Pearson/Prentice-Hall, isbn#0-13-090758-8)
Mack, Mary and Steve Pattison, ELECTRONIC EVIDENCE MANAGEMENT: FROM CREATION THROUGH LITIGATION, (2005, FIOS; isbn#0-9725542-5-4).
Kruse, Warren G. II and Jay G. Heiser, COMPUTER FORENSICS – INCIDENT RESPONSE ESSENTIALS, Addison-Wesley. ISBN: 0-201-707199
Nelson, Bill, Amelia Phillips, Frank Enfinger and Chris Steuart, GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS, 2d edition. Course Technology Incorporated, 2006. ISBN: 0-619-21706-5.
Mandia, Kevin and Chris Prosise, INCIDENT RESPONSE: INVESTIGATING COMPUTER CRIME. Osborne/McGraw-Hill, 2001. ISBN: 0-07-213182-9.
Casey, Eoghan, DIGITAL EVIDENCE AND COMPUTER CRIME: FORENSIC SCIENCE, COMPUTERS AND THE INTERNET. Academic Press, 2000. ISBN: 0-12-162885-X
Schiffman, Mike, HACKER'S CHALLENGE: TEST YOUR INCIDENT RESPONSE SKILLS USING 20 SCENARIOS. Osborne/McGraw-Hill, 2001. ISBN: 0-07-219384-0
The Honeynet Project, KNOW YOUR ENEMY: REVEALING THE SECURITY TOOLS, TACTICS, AND MOTIVES OF THE BLACKHAT COMMUNITY. Addison-Wesley, 2002. ISBN: 0-201-74613-1

6. COURSE AND CURRICULUM EVALUATION

Cyberforensics law is amenable deployment of evaluation techniques similar to other courses in information and computer sciences as well as in undergraduate

law and policy coursework. Both the evaluation of student performance and evaluation of the course can be accomplished with these traditional methods. While much of the evaluation and feedback methods peculiar to the chosen pedagogies are described above, this section discusses evaluation more generally.

The most important starting place is to assure the course is developed by domain expert(s) in cyberforensics law. Cyberforensics is an inherently interdisciplinary field. However, there is considerable experience at many universities with faculty possessing well-developed technical skills but who may not fully appreciated how the law, policy and regulation constrain their activities. Another possible difficulty is that there is widespread misperception in technical fields that the law is an easily represented deterministic field.[30] Second, the course and students can be better evaluated when there have been adequate educational objectives established and evaluation rubrics designed and tested. Third, a review by various faculty on and off campus for demand, pedagogical coherence, and the inclusion of an appropriate body of knowledge for baccalaureate programs seems essential for sustained success. This consultation also provides a useful opportunity to discover other pockets of demand for EDD and cyberforensics, other instructional resources and may defuse turf difficulties.

Fourth, there can be developed evidence that this coursework is beginning to proliferate at other institutions. While these authors found such evidence, a faculty team proposing a cyberforensics law course may need to do additional research that demonstrates a clear demand. For example, it can be useful, where feasible, to offer cyberforensics law on an experimental basis then generalize to the future from such past deliver(ies) of the course. Fifth, the emergence of educational materials reasonably adaptable and already available helps to evaluate a particular course's design. Sixth, it is advisable to deploy pedagogies empirically proven effective or so traditionally accepted as to be defensible. Indeed, it is advisable to link pedagogies to each major unit or topic of the subject matter. This approach should not stifle innovation so new pedagogies can be rationally extended or adapted from validated, existing pedagogies. Seventh, it is useful to have other quantitative and qualitative evidence from the cyberforensics course's pilot testing, including student evaluations, student quality teams, pre-/post-testing of students knowledge and skills, and instructor peer visitations.

[30] *See generally*, Bagby, John W. & Tracy Mullen, *Legal Ontology of Contract Formation: Application to eCommerce*, Proceedings of the AAAI Workshop on Contexts and Ontologies, held in conjunction with the Twentieth National Conference on Artificial Intelligence (AAAI-05) Pittsburgh PA.

7. CONCLUDING COMMENTS

EDD and cyberforensics is a professional pursuit presently in its start-up phase. Coherent organization of development efforts are also largely in the start-up phase resulting in a wide variety of approaches, guidance and "best" practice advice from professional groups like the American Bar Association[31] that are only now filtering down to impact rules of procedure and evidence in the U.S. state and federal courts. Indeed, at this juncture, private sector consortia may still have impact on this field's development as exemplified by the emerging influence of the Sedona Conference.[32] To compound this lack of precise guidance is the current lack of ERM readiness at what is inferred to be a majority of private and public sector organizations. Indeed, many, if not most, of all private-sector firms, not-for-profit organizations (e.g., trade associations, SROs, NGOs, foundations) and government agencies are not adequately deploying ERM, document retention and EDD litigation planning. While this is an unfortunate circumstance, it likely offers plentiful opportunities for near to medium-term employment prospects for graduates in the information and computer sciences. Necessarily, and working backward, the clear implication is that there will be strengthening demand and generally acknowledged needs for coursework on cyberforensics techniques, cyberforensic law and EDD.

[31] Civil Discovery Standards, American Bar Association, Section of Litigation (Aug.1999, revised: Aug. 2004)
http://www.abanet.org/litigation/discoverystandards/2004civildiscoverystandards.pdf

[32] *See generally*, the Sedona Principles, The Sedona Conference, (Sept. 2005)
http://www.thesedonaconference.org/dltForm?did=TSG9_05.pdf

APPENDIX:

Selected Bibliography

Week 1: Investigation and Litigation: Criminal, Civil, ADR, Regulatory, Non-Judicial Tribunals

Bazan, E.B., & Elsea, J.K. (January 5, 2006). Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information. In *Congressional Research Service Report to Congress*. http://www.fas.org/sgp/crs/intel/m010506.pdf .

Granick, J. (January 18, 2006). *Mass Spying Means Gross Errors*. http://www.wired.com/news/columns/0,700351.html?tw=wn_story_page_next1.

Dubey, P. & Stevens, T. (2005). *The Litigation Balancing Act: No Pressure to Measure?* http://fiosinc.com/resources/pdfFiles/200505_corporate_counsel.pdf.

Week 2: Traditional Discovery: Interrogatories, Depositions, Discovery Requests

American Lawyer Media, Inc. (No Date). *Interrogatories.* http://dictionary.law.com/definition2.asp?selected=1005&bold.

Committee on the Judiciary; 108th Congress. (2004). *Federal Rules of Civil Procedure; with forms.* http://judiciary.house.gov/media/pdfs/printers/109th/civil2005.pdf.

Dubey, P. & Araujo, N. (2005). *Evidence lifecycle management – the new frontier.* http://www.fiosinc.com/resources/pdfFiles/200507_evidenceLifecycle.pdf.

Mack, Mary. (2004). *Taming the litigation beast: Are you ready?* http://www.cioupdate.com/insights/article.php/11049_3342321_1.

Rinkle, Ralf. (No Date). *The 'Lectric Law Library's Lexicon on Deposition.* http://www.lectlaw.com/def/d041.htm.

No author. (2005). *Rule 26: General rules governing discovery; duty of disclosure.* http://www.law.cornell.edu/uscode/html/uscode28a/usc_sec_28a_06000026----000-.html.

No author. (2005). *Rule 34: Production of documents and things and entry upon land for inspection and other purposes.* http://www.law.cornell.edu/uscode/html/uscode28a/usc_sec_28a_06000034----000-.html.

No author. (2005). *Rule37: Failure to make disclosure or cooperate in discovery; sanctions.* http://www.law.cornell.edu/uscode/html/uscode28a/usc_sec_28a_06000037----000-.html.

Redgrave, J. M. ed. (2005). *The Sedona Principles: Best practices, recommendations, & principles for addressing electronic document production*. http://www.kenwithers.com/articles/sedona/principles.pdf.

Sommer, P. (2005). *Directors and corporate advisors' guide to digital investigations and evidence.* http://www.iaac.org.uk/Portals/0/Evidence%20of%20Cyber-Crime%20v08.pdf.

Week 3: Electronic Data Production and EDD Project Planning

Brown, C. L. T. (2003). *Bate's numbering – What's in a number anyway?* www.techpathways.com/uploads/BatesNumbering.pdf.

Hedges, R. J. (2004). *Discovery of digital information.* http://www.kenwithers.com/articles/hedges092704.pdf.

Kinnaman, M. (2005). Let's Get Relevant: Using document analytics to reduce total discovery cost. *E-Discovery Law & Strategy, 2 (2).* www.attenex.com/newsEvents/inTheNews/pdf/Lets_Get_Relevant_Ediscovery_LS_06_2005.pdf.

No Author. No Date. *Guidelines for the discovery of electronic documents in Ontario.* http://www.krollontrack.com/library/ontario.pdf.

No author. No date. *Embedded information in electronic documents: Why meta data matters.*

http://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI_MetaData.pdf.

Reisinger, S. (2005). *In-house attorneys become IT gatekeepers: Big damages in botched e-discovery cases up the ante for in-house lawyers as they take on a new role.* http://www.law.com/servlet/jsp/ihc/PubArticleIHC.jsp?id=1128342926735.

Roitblat, H. L. (2005). *Proactive solutions: The next generation of eDiscovery.* Retrieved http://www.discoveryresources.org/pdfFiles/Proactive_Solutions.pdf.

Week 5: Admissibility of Electronic Evidence

Preserving chain of custody in e-discovery cases. http://www.lexisnexis.com/applieddiscovery/clientResources/techTips9.asp.

Preston, Gates, & Ellis. (2005). *Motion for exclusion of evidence or adverse inference denied as untimely and because defendant produced all responsive documents.* http://www.ediscoverylaw.com/case-summaries-269-motion-for-exclusion-of-evidence-or-adverse-inference-denied-as-untimely-and-because-defendant-produced-all-responsive-documents.html.

St.Clair v. Johnny's Oyster & Shrimp, Inc., 76 F.Supp.2d 773 (S.D.Tx.1999)

Weeks 6 and 7: Computer Forensic Expert Witnesses and Scientific Evidence and *Daubert* Constraints on Admissibility of Electronic Evidence

Frye v. U.S., 293 F. 1013 (D.C. Cir. 1923)

Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579 (1993)

GE v. Joiner, 522 U.S. 136 (1997)

Kumho Tire Co., v. Patrick Carmichael, 526 U.S. 137 (1998)

Martinez v. Bynum, 461 U.S. 321 (1983)

Rink v. Cheminova, 400 F.3d 1286 (11th Cir. 2005)

Week 8: Evidentiary Aspects of Modern Communications Technologies

McAree, D. (2005). *New liability frontier: Instant messages.* http://www.law.com/jsp/article.jsp?id=1125392711384.

McCurdy, G. S. & Dawson, M. J. (2004). *Are instant messages discoverable? Is this digital medium more like emails or phone calls? http://www.prestongates.com/images/pubs/Dawson NLJ.pdf.*

Sharpe, L. & Lange, M. C. S. (2004). *Juggling the worlds of paper and electronic discovery.* http://www.krollontrack.com/include/document.asp?file=/publications/abtl.pdf.

Skupsky, D. S. (1996). Discovery and Destruction of E-mail. In *The internet and business: A lawyer's guide to the emerging legal issues* (chapter 5). http://www.itechlaw.org.

Verizon Online Services, Inc. v. Ralksy, 203 F. Supp. 2d 601 (E.D. Va. 2002).

Waters, J. K. (2006). *Zantaz launches first discovery e-mail search.* http://www.law.com/jsp/ltn/pubArticleLTN.jsp?id=1138701909475.

Week 9: Cost Balancing of Electronic Document Production

Blouin, D. (2004). *The discovery dance.* http://www.law.com/special/supplement/e_discovery/discovery_dance.html.

Gawlicki, S. M. (2005). *GCs find new ways to cut e-discovery costs: Altria and Cisco bring e-discovery in-house.* http://www.insidecounsel.com/issues/insidecounsel/15_169/technology/236-1.html.

Plotkin, J. (2004). *White Paper: E-mail discovery in civil litigation: Worst case scenarios vs. best practices.* http://www.veritas.com/Products/www?c=collateral&refId=322.

Robichaud, T. D., & Gilinsky, M. (2004). Zubulake V: Emerging trends in the duties regarding electronic evidence. *Mealey's Litigation Report: Discovery, 1(12)*. www.discoveryresources.org/ pdfFiles/04_zubulakeV_092004.pdf.

Sachdev, A. (2005). *Costly electronic discovery 'part of potentially every case in the 21st Century.'* www.evestigate.com/PDFS/chicagoTribune_041005.pdf.

Eight related *Zubulake* decisions issued between 2003 and 2005 detailed in ftn.13.

Week 10: Privilege and Privacy of Electronic Evidence

Lucchetti, A. & McDonald, I. (2006). *Spitzer's targets use his tactics: Grasso, Greenberg seek documents on attorney general's operations; impact on the governor's race.* The Wall Street Journal, C.1.

Weeked States Department of Justice (2002). *Searching and seizing computers and obtaining electronic evidence in criminal investigations.* Retrieved December 16, 2006, from http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm.

Reino de Espana v. American Bureau of Shipping (SDNY Dec. 14, 2005).

Week 11: Spoliation and Obstruction of Justice

Ballon, I.C. (1999). *Spoliation of e-mail evidence: Proposed intranet policies and a framework for analysis.* http://library.findlaw.com/1999/Feb/22/131004.html.

Leddin, B. J., & Gonsowski, D. (2005). Spoliation of Electronic Data: The wages of sin in a virtual world. *New Jersey Law Journal, CLXXIX(3).* http://www.fiosinc.com/resources/pdfFiles/20050117_spoliation.pdf.

Redgrave, J. M., Cook, R. C., & Ragan, C. R. (2005). *Looking Beyond Arthur Anderson: The impact on corporate records and information management policies and practices.* www.rdrw.com/pdf/arthur092005.pdf.

Week 12: Regulated Electronic Records Management

Launchbaugh, C. (2004). *E-Records management: A sad state of affairs or golden opportWeeky? Records management professionals have an opoprtuntiy – and an obligation – to communicate the importance of including electronic records in their organization's records management program.* www.discoveryresources.org/pdfFiles/Launchbaugh.pdf.

Murphy, B. (2005). *Sarbanes-Oxley records management implications.* http://www.s-ox.com/feature/detail.cfm?articleID=924.

Talcott, K. D. (2005). *Dealing with third-party providers: Spell out expectations before entering a relationship.* http://www.cowengroup.com/news/thirdparty.html.

All weeks: additional links to selected online resources:

http://www.usdoj.gov/usao/iln/osc/

http://www.fiosinc.com/

http://www.daubertexpert.com/

http://www.dauberttracker.com/

http://www.daubertexpert.com/old2004/index.html

http://www.applieddiscovery.com/

http://www.krollontrack.com/

http://www.uscourts.gov/library.html

http://www.lawpartnerpublishing.com/

http://www.ironmountain.com/Index.asp

http://www.forensic-evidence.com/site/Link_wo.html

http://www.senseient.com/default.asp?page=main.htm

http://www.syngence.com/ediscovery.asp?return=ediscovery&width=1152

http://www.thesedonaconference.org/publications_html

http://www.law.com/special/supplement/edd/

http://www.waybackmachine.org/

http://www.acxiom.com/

http://www.iwar.org.uk/