

The Content Authentication Crisis

Electronic Data Content Authenticity: The New Challenge To Trust and Auditability

Steven W. Teppler, Esq.*

TimeCertain, LLC

*Copyright 2006, All Rights Reserved

What Do These Companies Have In Common?

- Enron
- HealthSouth
- Rite-Aid
- NextCard
- Ernst & Young
- Computer Associates
- Parmalat
- Adelphia

What Do These Companies Have In Common?

- Broadcom
- Brocade Communications
- cNet
- Computer Associates
- Comverse Technologies
- Intuit
- Symantec
- KLA-Tencor
- Macrovision
- Juniper Networks
- Mercury Interactive
- Michael's Stores
- Monster Worldwide
- Rambus
- American Tower
- United Healthcare
- RSA. Verisign
- Vitesse Semiconductor
- United Health
- Take Two Interactive
- Nearly 200 Other Companies

Time-Based Digital Data Manipulation

- **Acts:**
 - After the Fact Data Alteration of Financial or Business Records
 - Hundreds of Billions in Combined Losses
- **Method:**
 - Backdating Digital Data Records
- **Result:** Potential Fraud
- **Easily Accomplished:** Why, and How?

Why

Financial Gain

How

- **SOURCE DATA MANIPULATION**
 - **Most Source Data is Now Digital**
 - **Binary Data**
 - **Comprised of Zeroes and Ones**

Nature of Digital Data

- Change Document and/or Date
- Alter, Forge, Delete, Substitute
- Bury Real Data Forever
- Destroy Auditability of Data
- AND GET AWAY WITH IT

Manipulating Zeroes and Ones Take One



- Digitized full body bone scan
- Note cancerous lesions on rib in second and fourth images

Manipulating Zeroes and Ones Take Two



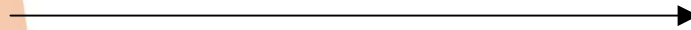
- Altered Digital Data File
- Backdated to the Same Time and Date
- New Version Can Have Its Own Valid “Digital Signature”
- Miraculously Cured
- Courtesy: Adobe Photoshop®

The Inevitable Content Challenge

- **WHOSE VERSION WINS?**
 - **How To Prove Authenticity**
 - **How Much Will it Cost to Litigate**
 - **Costs of Losing**
 - Money
 - Prison
 - **Cost of Winning**
 - Money
- **DO WE WANT A JUDGE OR JURY TO DECIDE?**
 - On the Basis of Credibility?

The Vulnerability: Time

The Network Clock



```
01010100101010  
01010000101110  
01101011010010  
11101001010101  
00101101010100
```



The Threat To Content

- **Entities that Create Digital Data Upon Which They, or Others Rely, and Which Could Result in Liability:**
 - Sarbanes-Oxley
 - HIPAA
 - Gramm-Leach-Bliley
 - State Laws
 - Insurance
 - Digital Rights Management
 - Authorship/Inventorship (Copyright and Patent)

A Constellation of Potential Liability

- **Sarbanes-Oxley**
 - § §302, 404 Public Companies
- **HIPAA**
 - Health Information
- **Gramm-Leach-Bliley**
 - Finance and Investment Markets
- **Computer Fraud and Abuse Act**
- **SEC '33 and 34 Acts**
 - Shareholder Lawsuits
- **False Claims Act**
 - Fraud against Government

Liability Potential

- **Criminal and Civil**

- **For the CxO**

- Direct Liability for Own Acts
 - Includes Upstream Liability for Downstream Acts

- **For the Security Professional**

- Liability for Conspiracy
 - Exposure as Stepping Stone Target
 - Info-Sec Targeted as a Means for Upstreaming Liability to CxO

The Content Authentication Crisis

The Paradigm Shift in Approach to Admissibility, Authentication And Custody of Digital Data

New Discovery Rules I: F.R.C.P. Rule 34 (Production)

Documents, Things, AND

- **34(a) Electronically Stored Media**
 - » Stored in Any Medium
- **34(b) Form of Production May Be Specified**
- **34(b)(ii) Form(s) Ordinarily Maintained or...Reasonably Usable**

New Discovery Rules II: F.R.C.P. 26 (Disclosures)

- **26(a)(1)(B) Initial Disclosures** - A Copy of, or Description by Category and Location, of
 - **All Electronically Stored Information** - In the Disclosing Party's Possession, Custody or Control...
 - **Why the Fuss about Electronic Information?**

The Federal Rules of Evidence

- **Fed.R. Evid. §1002** - Requires Production of The Original of A Document So That **Content** Can be Proved.
 - What Does This Mean in the Digital Data Universe?

Digital Data Content

The Bad News

- Comprised of Zeroes and Ones
- Ephemeral By Design
- Everything Digital is By Definition an “Original”
- Traditional Forensic Techniques to Determine Authenticity (or Provenance) Fail

– Why Care?

Digital Data Content, or Those Zeroes and Ones

001001011011010100
101010101010110101
101001001010010110

- Legal Memorandum?
- Financial Spreadsheet?
- Recipe for Dog Biscuits?
- Who Can Tell?

Digital Data Rules

- **92 Percent of All New Information (or Data) Currently Generated is Digital in Nature**
 - Peter Lyman & Hal R. Varian, How Much Information?, at <http://www.sims.berkeley.edu/how-much-info-2003> (last visited Aug. 1, 2006)

Discovery of Electronic Data: Seeking the Source

- **Discovery Seeks Source Evidence**

- Source Defined: (Webster's):

- First cause; place of origin from which something comes or develops; that which gives rise to anything.

Umm, I thought we're talking Discovery and Evidence here, aren't we?

Discovery Seeks Source Evidence

- That Evidence is Source Information
 - **BUT**
- Source Digital Information is Zeroes and Ones
- Why All the Fuss? We Just Use the Data Files, Don't We?

Digital Evidence Admissibility Issues (1)

- **Hearsay Rule –**
 - **Fed. R. Evid. 801** - "a statement [as defined in Rule 801(a)], other than one made by the declarant while testifying, is hearsay if it is offered to prove the truth of the matter asserted."
 - Digital Data - Clearly Hearsay and Inadmissible

Unless

Digital Evidence

Admissibility Issues (2)

- **Fed. R. Evid. Exceptions to Hearsay Rule**
 - **§803(6) Records of Regularly Conducted Activity**
 - Made At or Near the Time
 - By A Person With Knowledge
 - If Kept in the Course of Regularly Conducted Business Activity
 - It Was the Regular Practice of that Business to Make that Data Compilation
 - **ALL** As Shown By Testimony of Custodian or Qualified Witnesses...[or by certification pursuant to FRE §902(11) or (12)]
 - **UNLESS (cont'd NEXT slide)**

Digital Evidence Admissibility Issues (2)

- **F.R.E. §803(6) cont'd**
- **Unless the Source of Information or the Method or Circumstances of Preparation Indicate a Lack of Trustworthiness.**

Digital Data Content: Neither Good, Nor Evil

- Zeroes and Ones
- They Don't Know if They Are True or False



www.shutterstock.com · 106543

Evidentiary Antagonism Between Electronic Records and Digital Evidence

- **Paper Records and Filings - Permanent**
 - By Intent
- **Digital Data Records - *Ephemeral***
 - By Intent
 - **Alterable and Altered Without Sign or Symptom**
 - By Intent
 - ***No Physical-Attribute Anchors to A Firm Evidentiary Foundation***
 - What Technologists Call an “Unintended Consequence”

Digital Data as Evidence

The Issues

- Computer Generated Evidence is **Not** The Same as Physical Evidence
- Admissibility Issues Are Different
- Why Be Concerned – After All, It's Reliable, I Know, Because the Computer Said So.
- Isn't it?

Electronic Data Discovery Issues

- What are We Discovering, or Admitting?
- How Do We Know Digital Data is What it Purports to Be?
- How Do We Know It Hasn't Been Fraudulently Altered Before or After Production?
- Hierarchical Evidence: A House of Cards
 - Howzat?

Digital Evidence

Really, Views of Views

– View Number 1

- Source Data of File (0's and 1's) Structured By Application Executable File

– View Number 2

- Executable Operates On Top of Operating System (“OS”) File(s)

– View Number 3

- Application File and/or OS Files Render Source Data File into a Human Readable Electronic Representation (Screen View)

– View Number 4

- Application File and/or OS Files Render Source Data into Data Stream Further Formatted for Printing

– View Number 5

- Paper Printout

Information Security and Content Authentication

- **A Major Digital Evidence Reliability Challenge**
 - Undetectable Alteration, Manipulation or Deletion
 - Most Easily Carried Out by People In Control
 - Trusted Insiders
 - Corporate Officers, Including In House and External Counsel
 - IT Staff
 - » For More Information See Nearon, et al., *Life After Sarbanes-Oxley: The Merger of The Merger of Information Security and Accountability*, 45 Jurimetrics J. 379-412 (2005)
 - Examples: Options Backdating (200+ Disclosures, Five Indictments, and A Barrage of Shareholder Actions)

Digital Data Manipulation: Example Two

- The “News” From Beirut:
Courtesy, Reuters



Digital Evidence Custody Issues

- **Custody – Two Issues**
 - **Pre-Production (Still “Under Control”)**
 - Integrity, Content and Reliability Questionable
 - **Post-Production**
 - Integrity, Content and Reliability Still Questionable
- **So, How To Make Digital Data Immune From Content Challenge?**

Digital Evidence Reliability Tools

Digital Signatures, Etc.

- **Digital Signatures**
 - The Technology: Here Today and Usable
 - Distinguished From “Electronic” Signatures
- **Uses for Digital Signatures**
 - Identity
 - Permissions (Use Attributes)
 - Content
 - What’s the Difference

Other Technology to the Rescue?

- **WORM Storage**
 - Advertised Advantages
 - Undisclosed Vulnerability
- **Encryption**
 - Control Issues
- **Backup**
- **EnCase Type Technologies**
- **“Compliance Solutions”**
 - Vendor Gabfests

Digital Evidence Admissibility

Reliability

The Cornerstone To Admissibility

(Not Weight)

Digital Evidence Admissibility

What Courts Are Saying (One)

- **Swinton v. State** 847 A.2d 921 (Conn., 2004)
 - Seminal Digital Evidence Admissibility Analysis
 - Decided on 6th Amendment Confrontation Clause Grounds
 - Distinguishes Between Computer Generated and Computer Enhanced Data*
 - Requires Greater Degree of Reliability to Be Shown as Foundation for Admissibility of Computer Generated Evidence (vs. Computer *Enhanced* Data)
 - Excluded Computer Generated Data as Not Reliable

*In this Presenter's Opinion A Distinction without Difference

Digital Evidence Admissibility

What Courts Are Saying (Two)

- **Rodd v. Raritan Radiologic Assoc.** 860 A.2d 1003 (App. Div. N.J. Super. 2004)
 - Reversed Admission of Computer Generated Photographs –
 - **Reliability** - Problems Arising From any Computer-Generated Exhibits and the Processes by Which They are Created
 - **Insufficient Foundation** - Requires Testimony by a Person With Some Degree of Computer Expertise Who Has Sufficient Knowledge to be Examined and Cross-examined About the Functioning of the Computer and the Technology Used to Create the Exhibit.
 - Cites Swinton v. State as Precedent

Digital Evidence Admissibility

What Courts Are Saying (Three)

- **In re Vee Vinhnee** 336 B.R. 437 9th Cir.BAP (Cal.) 2005.
 - Court **Excluded** an *Unopposed* American Express Data Printout of a Debtor's Amex Charges, Despite (or in Strict Reliance on) 803(6) and 902(11), Even With the Testimony of the "IT Person" Who Made a Declaration in Support of Admissibility of the Data in Question.
 - The Reason? **Reliability**

Digital Evidence Admissibility

What Courts Are Saying (Four)

- **In re Vee Vinhnee** – Insightful Excerpts

“...The testimony of the records custodian at trial regarding the computer equipment used by American Express was vague, conclusory, and, in light of the assertion that “[t]here’s no way that the computer changes numbers,” unpersuasive...”

Digital Evidence Admissibility

What Courts Are Saying (Five)

- In re Vee Vinhnee – Insightful Excerpts

“...Regardless of the question of the declarant’s qualifications, the trial court also ruled...the declaration...deficient as to basic foundational requirements for admission of electronic records, **noting particularly the need to show the accuracy of the computer in the retention and retrieval of the information at issue.**”

Digital Evidence

Crawford v Washington Factors

- **Crawford v. Washington** 124 S.Ct. 1354 (2004)
 - **Testimonial Hearsay** - Subject to 6th Amendment Confrontation Clause
 - **Confrontation Clause Goal** - to ensure reliability of evidence, but it is a procedural rather than a substantive guarantee, in that it commands, not that evidence be reliable, but that reliability be assessed in a particular manner, i.e., by testing in crucible of cross-examination

Digital Evidence and The Florida Courts

- **The Manatee/Sarasota/Seminole County Intoxilyzer Cases**
 - State of Florida v. Ismael Almaraz, et. al (Manatee County Court, [Cons.] Case No. 2005 CT 5586 May 2006)
 - Software and EPROM Source Code are Integral Parts of Intoxilyzer, the Instrument That “Establishes an Element of a Criminal Offense”
 - Held That §316.1932(1)(f)(4) Fla. Stat. (2005), Which Provides that Defendants are Entitled To Full Information About the Instrument that Establishes Guilt, Includes Full Information About Intoxilyzer EPROM Source Code
 - Court Also Based Its Decision on Article 1, §9 of the Florida Constitution and the Confrontation Clause, Article V and Article XIV of the U.S. Constitution (Curiously, No *Crawford* Reliance)

Digital Evidence and The Florida Courts (Two)

- **The Manatee/Sarasota/Seminole County Intoxilyzer Cases**
 - **State of Florida v. Ismael Almaraz, et. al** (Manatee County Court, [Cons.] Case No. 2005 CT 5586 May 2006) [cont'd]
 - Did Not Exclude Evidence, But Granted Motion to Compel Source Code and Required State to Lay Proper Foundation (and “Scientific Predicate”) as Condition for Admissibility
 - Recognized Conflict with Other Florida Court Decisions and Certified Question to 2d DCA
 - Recognized Pending Florida Legislation to Exclude “Source Code” from “Full Information” Disclosure Requirement

Digital Evidence

Testimonial Hearsay

- **Digital Evidence Accuses** – Subject to Crawford Doctrine.
 - Digitally Generated Images
 - Digital Audio, Video, Surveillance
 - Digitally Generated Documents
 - Memoranda, Letters, Spreadsheets
 - Digitally Generated Diagnostic Data
 - Intoxilyzer Data Output
 - Computer Radar Output
 - **Guess What Else Accuses Digitally?**

Computing Environment Enables Generation of Testimonial Hearsay

- **Data Generating Environment - Enables Generation of Accusing Data**
 - **Computer Hardware** (contains firmware)
 - Firmware is Code (software data) Contained In Hardware
 - **Computer Firmware** (contains code)
 - **Computer Operating Systems** (contain code)
 - **Application Routines** (contain code)
 - **Communication Routines** (contain code)
- Arguably, Reliability Must be Shown Pursuant to Crawford v Washington

Digital Evidence Reliability Issues (One)

- **Is the Code What it Purports to Be?**
 - What Indicia of Reliability Offered?
- **Did the Computing Device Operate in the Way Intended by the User?**
 - What Indicia of Reliability Offered?
- **Has the Digital Data Output (Binaries) Been Altered Since the Event Creating It?**
 - What Indicia of Reliability Offered?

Digital Evidence Reliability Issues (Two)

- **Data Generating Environment Identical?**
 - To that of the Time the Accusing Data Was Generated?
- **Firmware Code Version Identical?**
 - To the Version in Place at the Time the Accusing Data was Generated?
- **Application Code Version Identical?**
 - To the Version in Place at the Time the Accusing Data was Generated?

Trusted TimeStamping Technology: The Solution to the Problem

- **Verifiable Third Party Timestamp**
 - Tracks and Authenticates any digital data content creation, modification or change (including transmit and receive)
 - Service Oriented Architecture/Service Oriented Business Application Aimed at Detection Rather Than...
- **Creates Trusted, Auditable, Challenge Immune Digital Data**
 - Workpapers
 - Memoranda
 - Financial Information
 - Audit Logs
 - Video, Audio Other Digital Media

Trusted Time Stamp Standards Evolution

- The Protocol:
 - IETF RFC 3161 (circa 2001)
- Policy Based Protocol
 - ANSI X9F4 9.95 (Trusted Timestamps for Financial Institutions)
- Information Assurance Consortium (2005)
 - Vendor Agnostic
 - Promotion of Technology

X9.95 Comparison RFC 3161

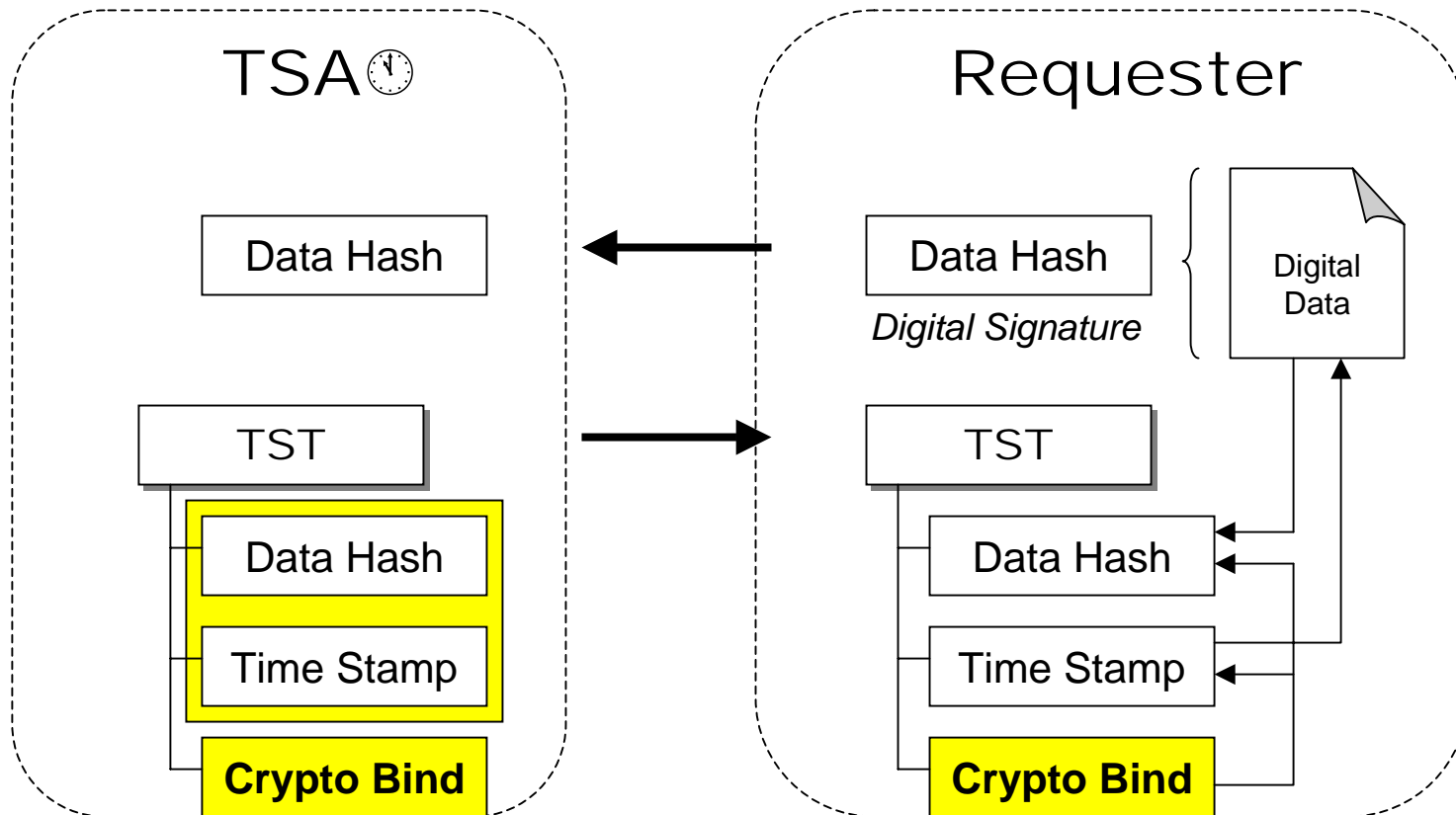
X9.95 Trusted Time Stamp

- Roles & Responsibilities
 - Time source entity
 - TSA, Requestor, Relying Party
- Requirements
- Methods
 - Digital Signature
 - Message Authentication Code
 - Linked Tokens
 - Transient Key
- Processes
 - Data Objects
 - Time Calibration
 - Process Flows
 - Error Handling
- Policy & Practice Statements
- Audit Evaluation Criteria

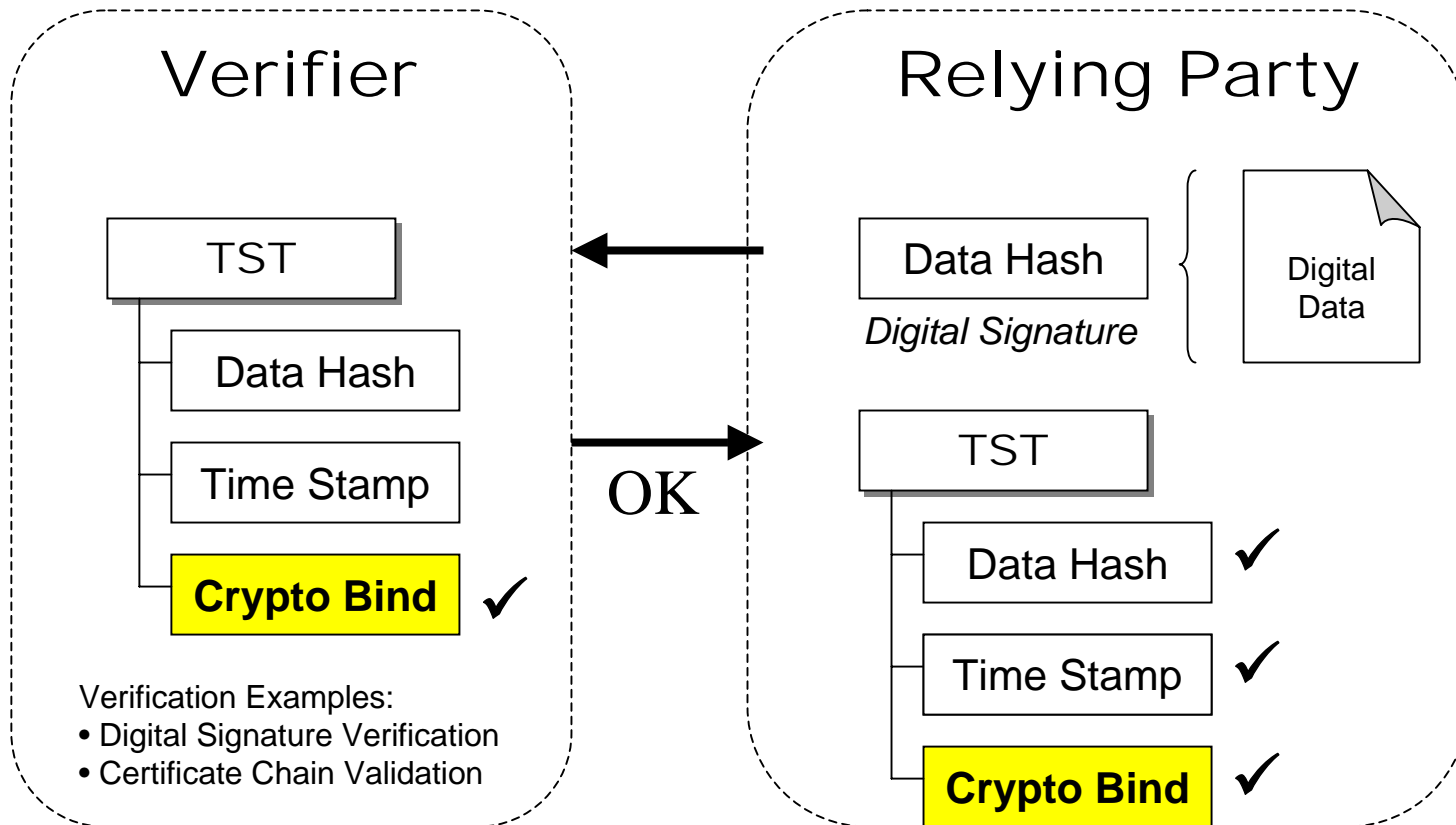
RFC 3161 Time Stamp Protocol

- Roles & Responsibilities
 - TSA, Requestor, Relying Party
- Method
 - Digital Signature
- Processes
 - Data Objects
 - Error Codes

TST Issuance by a TSA



TST Verification



Trusted Time Stamp Application

- Application Areas for Trusted Time Stamps:
 - Financial Services Trading and Transaction Systems
 - Records Management Systems for Regulatory Compliance and Legal Discovery
 - Messaging Management and Archival Systems
 - Intellectual Property Capture, R&D and Engineering Systems
 - Imaging Systems
 - Electronic Medical Records
 - Legal and Court e-Filing Systems
 - Financial and Accounting Systems (i.e. General Ledger, Contract Management, Option Grant Management, etc.)

Takeaways

- **Understand Digital Evidence Issues**
 - Software, Firmware, Application, Operating System Code
- **Be Aware of Authentication, Admissibility, and Custodial Challenges and Defenses**
 - Until Authentication and Integrity Preservation Techniques Develop Further, Attacking Digital Evidence Will Be Easy
- **Keep Up With Evolving Decisional Trends**
 - Relating to Digital Evidence Admissibility
- **Consider Trusted Time Stamps as A Solution**

Thank You – Questions?

Steven W. Teppler, Esq.
steppler@timecertain.com
(941) 929-7949