Breakfast Meeting:
"Securing your Secured Data"
Digital Forensics, Fraud and Forensic Advancements

9 April 2013

Facilitator:
Dr. Sheau-Dong Lang, Coordinator
Master of Science in Digital Forensics
University of Central Florida
Orlando, Florida, USA
Email: slang@ucf.edu

Outline:

- What is Digital Forensics
- Digital Evidence: Technical, Legal, Ethical Issues
- Digital Forensics: Criminal Investigation or Civil Litigation
- Cyber Fraud: Case Studies
- Digital Forensics applied to Fraud Investigation
- Challenges

What is Digital Forensics

- "Computer forensics" was coined in 1991 in the first training session held by the International Association of Computer Investigative Specialists (IACIS, http://www.iacis.com), is largely a response to a demand for service from the law enforcement community
- Computer forensics is "the application of science and engineering to the legal problem of digital evidence"

Digital Evidence

- Information of "probative value" that is stored or transmitted in binary form, i.e., evidence which is sufficiently useful to prove something important in a trial









Technical, Legal, Ethical Issues

- Identification (bagging and tagging)
- Acquisition (legal constraints, acquiring evidence without tampering)
- Preservation, Transport, and Storage (chain of custody, security)
- Extraction and examination (authenticating evidence, tools and best practice for data analysis, keyword searches, establishing timeline of events, corroborating evidence, who-what-when-where-why-how questions)
- Reporting (documenting, composing forensic reports)
- Interpretation (testifying, expert witness)
- Ethics (maintain the highest standards of ethical conduct)

Criminal Investigation

- Search Warrant: law enforcement apply to a judge for search warrant based on the probable cause for:
  - a crime has been committed
  - evidence of crime exists
  - evidence of crime can be found at the specified location
- Digital Forensic Examination: search the seized items for evidence related to the alleged crime
- Individual's Rights: protected against unreasonable search and seizure by government (US Constitution, 4th amendment)

TRINIDAD AND TOBAGO CHAMBER OF INDUSTRY AND COMMERCE
www.chamber.org.tt
The Chamber means BUSINESS

Civil Litigation - eDiscovery

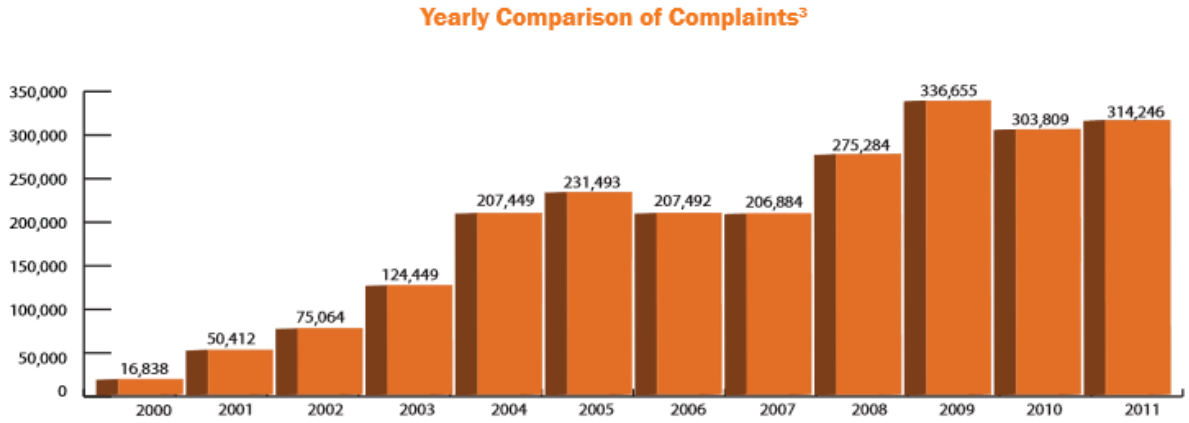
- Parties in a dispute are required to provide each other relevant information and records related to the case
- Electronically stored information (ESI) is identified by attorneys, evidence is extracted and analyzed using digital forensic procedures, then the extracted evidence is reviewed for privilege and relevance by the attorney before turning over to the opposing counsel
- Stages of eDiscovery Process: Identification, Preservation, Collection, Processing, Review, Production

Types of Digital Evidence

- Documents: spreadsheets, PDF files, resumes, letters
- Graphics and Multimedia Files: pictures, photos, audio, video, and movie files
- Applications: movie players, SMS messengers, Skype, file-sharing software, Internet browsers, hacking tools
- Emails: MS Outlook, Yahoo! mail, Gmail, Hotmail
- Internet Browser Artifacts: history, cookies, temporary Internet files, browser bookmarks
- Deleted Files: may be recovered by tools
- Metadata: date/time when files were created, last modified
- Encrypted or Password Protected Files

Cyber Fraud

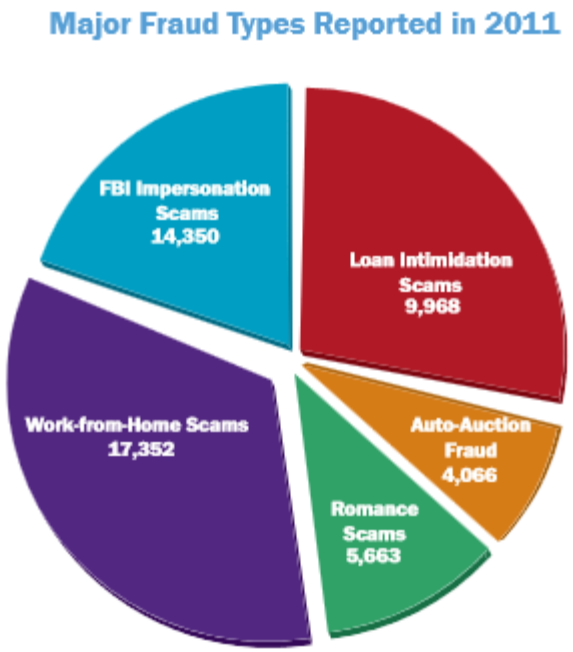
- Fraud: wrongful or criminal deception intended to result in financial or personal gain



2011 FBI Internet Crime Complaint Center (IC3) Report (11 May 2012) (http://www.ic3.gov/media/annualreport/2011_IC3Report.pdf)

TRINIDAD AND TOBAGO CHAMBER OF INDUSTRY AND COMMERCE
www.chamber.org.tt
The Chamber means BUSINESS

Cyber Fraud Cases



- FBI-related Scams:
  Scams in which a criminal poses as the FBI to defraud victims
- Work-from-Home Scams:
  Organized cyber criminals identify their victims through newspaper ads, online employment services, unsolicited emails or "spam," and social networking sites advertising work-from-home "opportunities."

2011 FBI Internet Crime Complaint Center (IC3) Report (http://www.ic3.gov/media/annualreport/2011_IC3Report.pdf)

TRINIDAD AND TOBAGO CHAMBER OF INDUSTRY AND COMMERCE
www.chamber.org.tt
The Chamber means BUSINESS

More Cyber Fraud Cases

- Deceptive Marketing:

  consumers complained of receiving and being billed for products they did not order

- Romance Scams:

  Scammers, often a criminal with a well-rehearsed script,

  target individuals who search for companionship or romance online, and victims believe they are “dating” someone decent and honest

TRINIDAD AND TOBAGO CHAMBER OF INDUSTRY AND COMMERCE
www.chamber.org.tt
The Chamber means BUSINESS

More Cyber Fraud Cases

- Auto-Auction Fraud:

  Criminals create an attractive deal by advertising vehicles for sale at prices below book value, instruct the victim to send payment to a third-party agent via a wire transfer payment service; the criminal pockets the payment but does not deliver the vehicle

- Identity Theft:

  Unauthorized use of a victim's personal identifying information to commit fraud or other crimes

- Distributed Denial of Service (DDoS) Attack:

  Attacks that cause websites to be knocked offline from numerous requests from outside computers at one time

Recent Fraud Alerts

- (17 September 2012) cyber criminals targeting financial institution employee credentials to conduct wire transfer fraud
- (12 October 2012) smartphone malware targeting mobile devices, stealing information and taking over the phone
- (30 November 2012) Citadel malware continues to deliver Reveton ransomware, compromise computers, in attempts to extort money

TRINIDAD AND TOBAGO CHAMBER OF INDUSTRY AND COMMERCE
www.chamber.org.tt
The Chamber means BUSINESS

Digital Forensics in Business Fraud Investigation

- Establish Computer Incident Response Procedures

  (preserve evidence, form incident response team, identify and control compromise systems, notify affected parties, evaluate damages, and apply security measures)
- Conduct personnel training

  (system security, penetration testing, incident response, data recovery, digital forensics)
- Report to Law Enforcement and collaborate
- Legislate Cyber laws and statutes

TRINIDAD AND TOBAGO CHAMBER OF INDUSTRY AND COMMERCE
www.chamber.org.tt
The Chamber means BUSINESS

Challenges

- Technology advances too fast
- Society becomes too inter-connected
- Information security becomes ever-increasingly more complex
- Criminals become smarter and more motivated by potential financial gains
- Cyber fraud investigation is complex and time consuming
- Cyber laws lag behind technology

TRINIDAD AND TOBAGO CHAMBER OF INDUSTRY AND COMMERCE
www.chamber.org.tt
The Chamber means BUSINESS

Thank You!

Q & A

Facilitator:
Dr. Sheau-Dong Lang, Coordinator
Master of Science in Digital Forensics
University of Central Florida
Orlando, Florida, USA
Email: slang@ucf.edu