



# Presentation Title

## Presentation Subtitle

## Speaker Biography

- Tim L. Bryan, CPA/CFF/CITP, CISA, EnCE
- Senior Manager, Crowe Horwath LLP
- Forensic Technology Services Leader
- Over 13 years of professional experience and leads Crowe's Forensic Technology Services Group. Tim is an adjunct professor at UOP, and also provides consulting and expert witness services. Responsible for performing and overseeing all aspects of fraud investigations including digital forensics, reviewing internal controls and processes, data analytics and other IT-related litigation support.

## Agenda

- Digital Computer Forensics – Defined
- Evolving Forensics Standards & Tools
- Forensics Procedures & Protocols
- Computer Forensics Cases
- Using Forensic Technology to Find Evidence
- Questions

## Where is the evidence

- Servers
- Desktop Computers
- Laptop Computers
- Cell Phones
- Smart Phones
- iPads / Tablets
- iTunes Backup Files
- Cloud Based Storage (Drop Box, iCloud)
- Social Media Websites (Facebook, Twitter)
- Documents (i.e. Word, Excel)
- Accounting Databases
- Data Backups (tape, disk, online)
- Third Parties (i.e. eBay, Paypal, Financial Institution)
- USB Flash Drives

# Investigation Techniques - Digital Forensics

- What is Digital Forensics
  - The use of specialized techniques to acquire, restore, investigate and present
    - Preservation
    - Collection
    - Integrity
    - Validated Process
    - Reporting
- Does a Computer Contain Evidence?
  - Stop use immediately
  - Unplug vs. Shutdown
  - Create a backup or image
  - IT Staff vs. Forensics Expert

## Forensic Standards

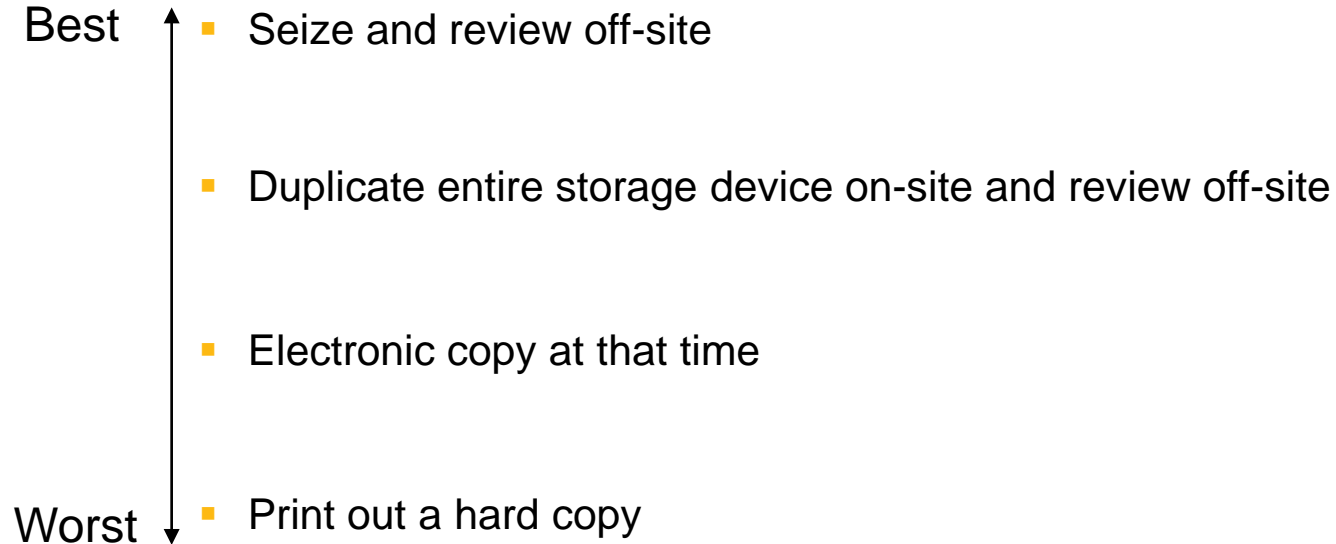
- No Formal Standards – Only Guidelines
- Primary Source – U.S. Department of Justice Publications:
  - Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations
  - Electronic Crime Scene Investigation
  - Forensic Examination of Digital Evidence
- <http://www.usdoj.gov>

## Forensic Case Initiation

- Case Background
- What Evidence
- Understand Computer Systems Involved
  - Operating Systems
  - Hardware
  - Database
  - Encryption


## Acquire

- Four Primary Seizure Options:





# Chain of Custody



**Forensic Technology Services**  
Evidence Acquisition Form

Page \_\_\_\_ of \_\_\_\_  
Engagement Name: \_\_\_\_\_  
OTS Number: \_\_\_\_\_

Date Received: \_\_\_\_\_ Method of Receipt: \_\_\_\_\_  
Received From: \_\_\_\_\_ Location: \_\_\_\_\_ Relationship: \_\_\_\_\_

Suspect Equipment Description (Use one sheet per piece of equipment i.e. one desktop with two internal HDDs or one external HDD)						
Evidence #	Equipment Type	Manufacturer	Model	Serial Number	Capacity	Power State / Condition When Received

Date Imaged: \_\_\_\_\_ Imaging Software: \_\_\_\_\_  
Location Imaged: \_\_\_\_\_ Imaging Hardware: \_\_\_\_\_

Evidence File Drive Description						
Drive	Equipment Type	Manufacturer	Model	Serial Number	Capacity	Storage Location
Primary Drive						
Redundant Drive						

Suspect Equipment: Retained / Returned \_\_\_\_\_ Retained At: \_\_\_\_\_  
Date Returned: \_\_\_\_\_ Method of Return: \_\_\_\_\_  
Returned To: \_\_\_\_\_ Location: \_\_\_\_\_ Relationship: \_\_\_\_\_

Aquisition Notes:

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_


## Restore

- Ensure NO CHANGES to Evidence
  - Use Write Blocking Device
- Authentication of Evidence
  - Make multiple bit for bit copies of evidence
  - Confirm copies are exact duplicates of original evidence
  - Use Hash Algorithm for authentication (MD5)

[illegible]

# Understanding Metadata

- Metadata
  - Data about Data
  - Document Properties



Properties ▾	
Size	44.0MB
Slides	30
Hidden slides	0
Words	1585
Notes	19
Title	AICPA – FVS Conference
Tags	<a href="#">Add a tag</a>
Comments	<a href="#">Add comments</a>
Multimedia clips	1
Presentation format	On-screen Show (4:3)
Template	AICPA FVS Con 2013 formatted
Status	<a href="#">Add text</a>
Categories	<a href="#">Add a category</a>
Subject	<a href="#">Specify the subject</a>
Hyperlink Base	<a href="#">Add text</a>
Company	Crowe Horwath
Related Dates	
Last Modified	11/5/2013 10:09 AM
Created	9/30/2013 8:40 AM
Last Printed	11/4/2013 12:52 PM
Related People	
Manager	<a href="#">Specify the manager</a>
Author	<input checked="" type="checkbox"/> Bryan, Tim
	<a href="#">Add an author</a>

# Using Forensic Technology to Find Evidence



## Commonly Misspelled Words

- 1. accommodate
- 2. a lot
- 3. arctic
- 4. calendar
- 5. cemetery
- 6. conscience
- 7. conscious
- 8. definitely
- 9. embarrass
- 10. existence
- 11. foreign
- 12. gauge
- 13. grammar
- 14. guarantee
- 15. harass
- 16. height
- 17. independent
- 18. inoculate
- 19. its/it's
- 20. liaison
- 21. license
- 22. maintenance
- 23. millennium
- 24. minuscule
- 25. mischievous
- 26. misspell
- 27. noticeable
- 28. occurrence
- 29. perseverance
- 30. playwright
- 31. possession
- 32. preceding
- 33. prejudice
- 34. principle/principal
- 35. privilege
- 36. pronunciation
- 37. questionnaire
- 38. receipt
- 39. recommend
- 40. rhythm

## Forensic Tools Demonstration

- Hardware Tools
  - Write Blocking Devices
- Software Tools
  - EnCase, FTK
- Mobile Devices
  - Cellebrite
- Search Tools
  - Intella, DT

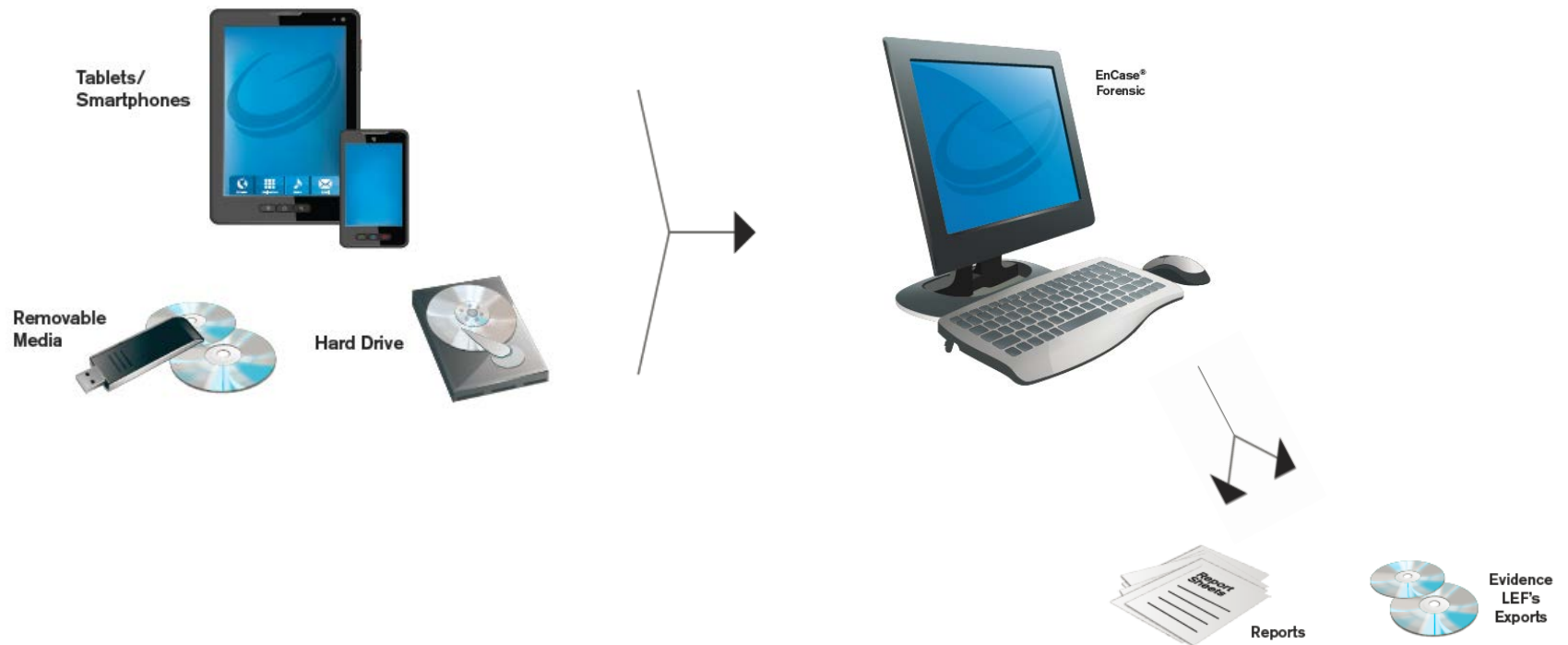


## Forensic Tools

- EnCase Imager
- FTK Imager
- iPhone Backup Extractor / iBackup Bot
- Browsing History View
- Outlook Stat View
- Outlook Attach View
- Last Activity View
- Exif Data View



# EnCase Forensic



## Mobile Devices - Cellebrite



## Forensic Demonstration & Case Studies

- Embezzlement Investigation
- Employment Matter
- Email Searching
- USB Device Tracking & Deleted File Analysis
- User Activity Analysis
- Cell Phone Investigation

# Computer Forensics Cases



## Community College Embezzlement

- Initial Allegations:
  - Receipt Forging
  - Excessive Spending
- Involved Parties:
  - Our Client – College Administration (Vice Chancellor)
  - Alleged Perpetrator – Director of Technical Support Services
- Setting:
  - Client wanted a discrete investigation
  - Alleged Perpetrator was a trusted and well respected employee
  - Client did not believe issues were very large or widespread
  - Alleged Perpetrator had resigned from the College

## Community College Embezzlement

- Client Provided Documents and Files:
  - Perpetrator's Purchasing Card Spending Detail
  - College Purchasing Policy documents
  - Perpetrator's College Emails - .pst file
- Persons Assigned to Assist with Investigation:
  - College CFO
  - IT Support Tech
- Items Requested and Not Provided:
  - Perpetrator's desktop and laptop computers

## Community College Embezzlement

- Initial Findings:
  - Irregular purchasing activity
    - Large volume of purchases from unusual websites
      - Buy.com
      - Numerous Paypal vendors
  - No odd or unusual email activity (District Acct)
  - No conclusive evidence of wrongdoing or misappropriation
- Issues Encountered:
  - Could not remote access into the Perpetrator's computers
  - Client was very hesitant to allow the collection of the computers
  - Assigned IT Support Tech was not helpful in the investigation

## Community College Embezzlement

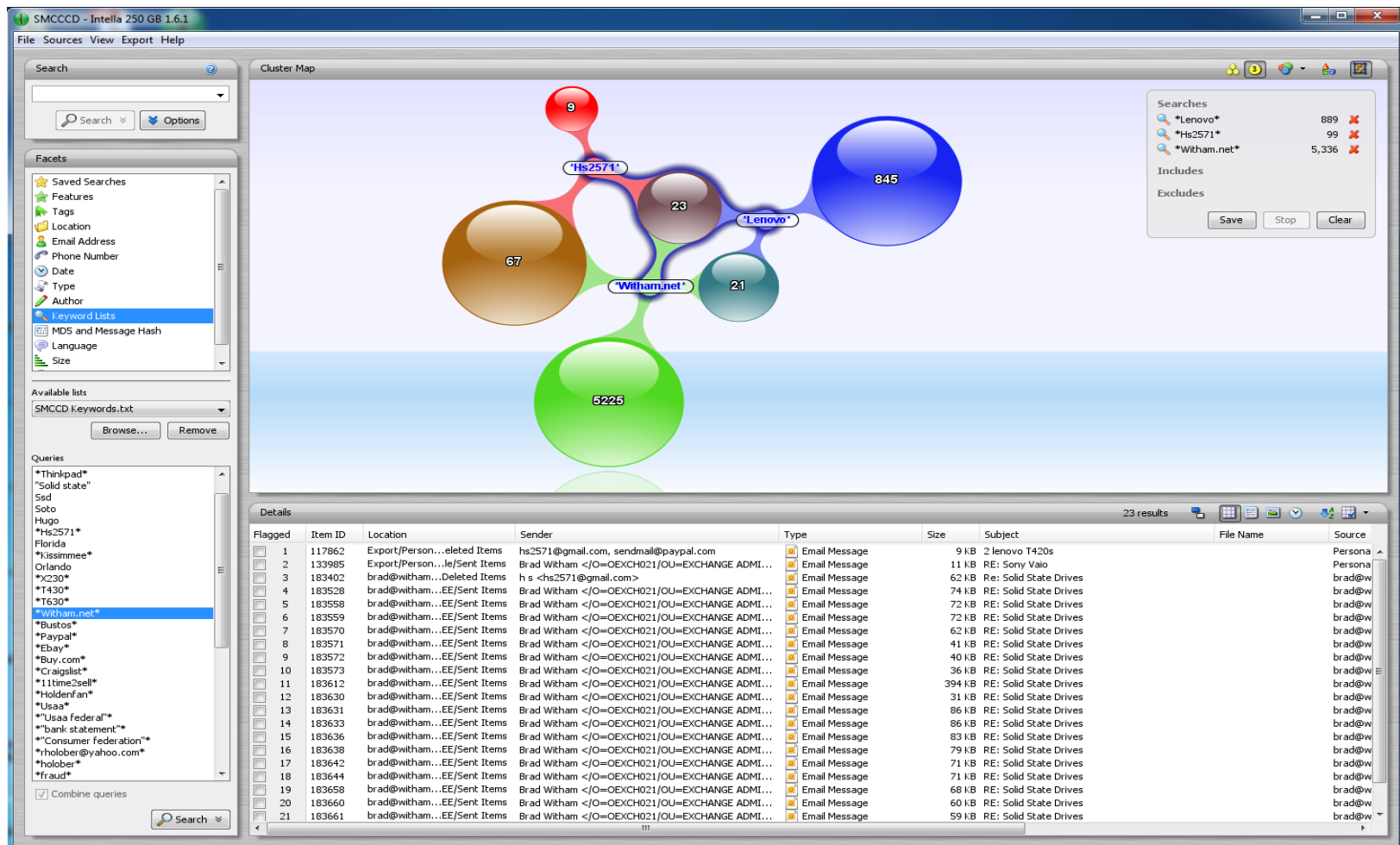
- Key Turning Point:
  - We were allowed to collect the Perpetrator's computers
  - Upon receipt of the computer we could determine that an attempt was made to reformat or erase the computer
  - The IT Tech explained the reformatting was a standard procedure
  - The computers were searched using EnCase software
  - The EnCase software located multiple hidden files
    - Including an email (.pst) file for a personal email account



## Community College Embezzlement

- The Case Materializes:
  - A cursory scanned of the emails revealed multiple sales transactions
    - The Perpetrator was selling computer and technology related equipment (laptop computers, memory, etc.)
  - The Intella software package was used to perform an in-depth analysis of the emails
  - We developed a macro to pull the purchase activity from Buy.com into an excel spreadsheet format
  - The items sold by the Perpetrator were then compared to the purchases he made using College funds
    - Transaction matches and patterns emerged

# Community College Embezzlement



## Community College Embezzlement

- Each Side Receives a Helping Hand:
- The Inside Man
  - We learned that the IT Support Tech assigned to help in the investigation was a good friend of the Perpetrator
  - The IT Tech later admits to providing the Vice Chancellor's email login credentials to the Perpetrator and attempting to reformat the computers to destroy evidence
- The District Attorney is Alerted
  - Based on the information recovered from the computers, enough evidence is available to bring a criminal case
  - The DA uses subpoena power to collect additional documents

## Community College Embezzlement

- The Case Builds and Twists:
  - We learned the Perpetrator's Paypal names from the recovered emails
  - The DA subpoenaed the necessary sales listing and transaction information from Paypal and eBay.
  - The purchases made by the Perpetrator with College funds were matched with sales made via eBay, Craigslist and private emails.
  - Total amount identified exceeded \$150,000
  - During this time the Perpetrator, an Australian native, flees to Australia

## Community College Embezzlement

- The Case is Closed:
  - The Perpetrator returns from Australia and is arrested
    - He pleaded no contest to four felony charges including forgery and embezzlement
    - He was sentenced to three years in prison and will be deported upon release from jail.
  - The IT Tech is also arrested
    - He pleaded no contest to one felony count of identity theft
    - He was sentenced to 90 days in jail

## Employment IP Theft

- Initial Allegations:
  - Withholding Company Property
  - Taking Proprietary Information
- Involved Parties:
  - Our Client – Former Employer
  - Alleged Perpetrator – SVP/Chief Business Development Officer

## Employment IP Theft

- Fact Pattern:
  - Employee slow to return his company owned laptop
  - The laptop is finally returned and upon inspection the hard drive has been encrypted (not standard practice)
  - Employee claims to forget the encryption password, but eventually we break it
  - After the laptop hard drive has been decrypted, it is determined that the drive has been 'wiped'
- Where do we start looking for evidence?

## Employment IP Theft

- HP Laptop



- IBM Laptop



- iPhones (2)



- iPads (2)



- HP Desktop



- Macbook





## Employment IP Theft

- Cloud Based



## Employment IP Theft

- Key Turning Point:
  - Within iPhone Backup file we find:

Text

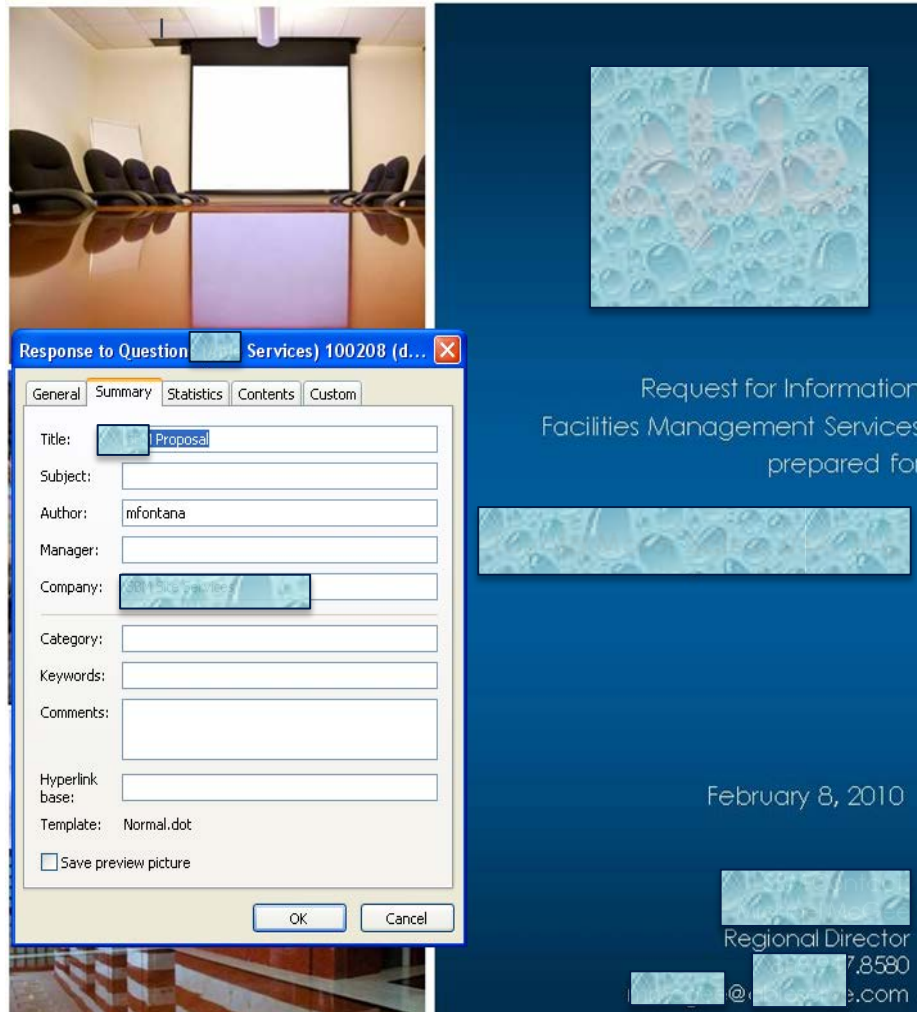
Also-please make sure to remove the Drive Erase CD from the HP laptop.

When u mail laptop, include an HP Printer disk that I believe is in the floor i

## Employment IP Theft

- The Case Materializes:
  - We identify thousands of Employer documents that have been transferred to new employers computers
  - Hundreds of documents have been used as templates for new employer

# Employment IP Theft



## Employment IP Theft

- The Case is Closed:
  - Case settles.....No additional testimony needed

---

For more information, contact:

Tim L. Bryan, CPA/CFF/CITP, CISA, EnCE

Direct 916.492.5153

Mobile 916.217.5150

Tim.Bryan@crowehorwath.com

Crowe Horwath LLP is an independent member of Crowe Horwath International, a Swiss verein. Each member firm of Crowe Horwath International is a separate and independent legal entity. Crowe Horwath LLP and its affiliates are not responsible or liable for any acts or omissions of Crowe Horwath International or any other member of Crowe Horwath International and specifically disclaim any and all responsibility or liability for acts or omissions of Crowe Horwath International or any other Crowe Horwath International member. Accountancy services in Kansas and North Carolina are rendered by Crowe Chizek LLP, which is not a member of Crowe Horwath International. © 2014 Crowe Horwath LLP