Cyber and Internet Evidence:
Admission and Investigation

Chair: Adam P. Tyksinski, Esq., ***Assistant Public Defender, Major Crimes Section***
Oneida County Public Defender, Criminal Division

Presented by: ***Oneida County Bar Association***
Oneida County Public Defender, Criminal Division
Oneida County District Attorney's Office
New York State Defenders Association, Inc.

Speakers: **Michael A. Coluzza, Esq.,** ***First Assistant District Attorney***
Oneida County District Attorney's Office

Patrick J. O'Connor, Director
Oneida County Child Advocacy Center

Sgt. Tony Martino, Computer Forensics Expert
Utica Police Department

Adam P. Tyksinski, Esq., Assistant Public Defender

Saturday, April 30, 2011

Oneida County Child Advocacy Center
930 York Street
Utica, New York 13502

9 A.M. – 12 P.M.

MCLE Credits: (2) Professional + (1) Ethics

Cyber and Internet Evidence:
Admission and Investigation

Saturday, April 30, 2011

Oneida County Child Advocacy Center
930 York Street
Utica, New York 13502

8:30 a.m. – 9:00 a.m.	**REGISTRATION**
9:00 a.m. – 9:15 a.m.	**Introduction to the role computer forensics plays in the prosecution and defense of criminal cases.** **Adam P. Tyksinski, Esq.,** ***Assistant Public Defender, Major Crimes Section, Oneida County Public Defender, Criminal Division***
9:15 a.m. – 10:15 a.m.	**What's Inside That Box? Gathering Evidence in Cyberspace** **Patrick J. O'Connor,** ***Director*** ***Oneida County Child Advocacy Center*** **Sgt. Tony Martino,** ***Computer Forensics Expert*** ***Utica Police Department***
10:15 a.m. – 10:30 a.m.	**BREAK**
10:30 a.m. – 12:00 a.m.	**Cyber Evidence: Foundations and Usage at Trial** **Michael A. Coluzza, Esq.,** ***First Assistant District Attorney*** ***Oneida County District Attorney's Office.***

MCLE Credits: (2) Professional + (1) Ethics

Speakers

Adam P. Tyksinski, Esq., ***Assistant Oneida County Public Defender***
Major Crimes Section

Born and raised in Clinton, Adam Tyksinski graduated from Clinton High School in 1997 and attended Union College where he received his Bachelors of Science in Economics, Concentrating in Managerial Economics and Political Science in 2001. He received his Juris Doctor in 2006 from the Thomas Jefferson School of Law. In 2008, he became a member of the New York State Bar and was appointed an Assistant Oneida County Public Defender, City Courts Section in February, 2009. On August 10, 2010, Adam was promoted to the Major Crimes Section. Mainly focused on mid-level felonies in Oneida County Court, the Major Crimes Section focuses on drug, child pornography, burglary, criminal contempt and grand larceny cases. Mr. Tyksinski attended the week long Defender Institute Basic Trial Skills Program sponsored by the New York State Defenders Association and has participated in numerous DWI training programs. He is a member of the Criminal Track Committee which develops low cost training programs for assigned counsel, public defenders, district attorneys and private criminal law practitioners. He has lectured to the bar on the fundamentals of criminal practice and is on the faculty and a member of the curriculum committee for the Criminal Law Academy scheduled for this fall at Mohawk Valley Community College.

Michael A. Coluzza, Esq., ***First Assistant Oneida County District Attorney***

Michael A. Coluzza received his Bachelor's Degree from the State University of New York at Albany in 1987 and his Juris Doctorate from the Boston University School of Law in 1990. Born and raised in Utica, NY, Michael joined the Oneida County District Attorney's Office in 1991. Starting as a local criminal court prosecutor, Michael went on to general felony assignments and then to major felony assignments. To date, Michael has handled well in excess of thirteen hundred felony cases since joining the District Attorney's Office.

Mike's current caseload includes robberies, burglaries, assaults, arsons, and homicides. Mike has handled numerous homicide cases and has been involved in the prosecution of all three of the only dual-jury murder trials in Oneida County history. Mike has prosecuted cases that have received national attention, including People v. Robert Hayes (17 year old murder case from 1987 that was originally ruled a suicide), and People v. Alan Baird (volunteer Deputy Fire Chief who caused a training death of a young recruit in 2001)

In 2001, Mike was promoted to the position of First Assistant District Attorney. Since that time, in addition to his regular caseload, Mike's daily duties also now include supervising prosecutions, attorney training and various other administrative issues arising in his office of twenty-two full time attorneys.

He instructs police personnel in basic and advanced training courses at the Mohawk Valley Police Academy, and has lectured for the Oneida County Arson Task Force Fall

Seminar, Law Day, and Constitution Day. He serves as a judge in the New York State Bar Association High School Mock Trial Competition, has served as guest faculty for the New York State Prosecutors Training Institute in both basic and advanced courses, has lectured for the New York State Office of Fire Prevention and Control, has guest lectured in the area of Elder Abuse prosecutions for Lifespan of Greater Rochester and has served as a board member and panelist for "The Art of Innocence", a local educational program sponsored through The Innocence Project. He has also lectured to fellow attorneys on the topic of presentation of electronic evidence through the Oneida County Family Court and the Oneida County Bar Association.

He currently serves on the New York State District Attorney's Association's Best Practices Committee and has assisted in the development and refinement of statewide practice standards for prosecutorial ethics, police identification procedures and suspect interviewing.

Sgt. Tony Martino, Computer Forensics Expert, Utica Police Department

Tony Martino is a 17-year veteran of the Utica, N.Y Police Department where he holds the rank of Sergeant. He is a 1992 graduate of the State University of New York at Geneseo where he received a his Bachelor of Arts in Communications and Utica College where he received his Masters of Science in Economic Crime Management in 2004. His Masters Thesis was on the subject of wireless data network security.

Tony is currently the supervisor of the Management Information Systems Unit and directs the operation of the digital forensics laboratory at the Utica Police Department. In this role, Tony conducts approximately 100 forensic examinations per year. In 2003, Tony founded the Central New York Computer Crime Coalition, and the Central New York Internet Crimes Against Children Task Force.

Sgt. Martino is currently an adjunct instructor at Utica College where he developed and now teaches courses in intermediate and advanced computer forensics and works in the Computer Forensics Research and Development Center. Tony is also a contributing author to the book, "The New Technology of Crime, Law and Social Control" published by Criminal Justice Press in 2007.

Since 2004, Tony has been a deputized U.S. Marshal as a participant in the United States Secret Service electronic crime task force. He has testified in numerous computer crime cases including as an expert witness in Oneida County Court and U.S. District Court in the Northern District of New York.

Training – specific to computer crimes investigation
Evidence Technician certification – New York State DCJS
Basic Data Recovery & Analysis - National White Collar Crime Center (NW3C)
Advanced Data Recovery & Analysis NT Systems – NW3C
Advanced Data Recovery & Analysis ILook – NW3C
Basic Computer Crime Investigation – United States Secret Service
Ultimate Toolkit Forensic Bootcamp – Access Data Inc.
Windows Forensics – Access Data Inc.
Cellular Forensics Examiner – Paraben Inc.

Windows Vista Forensics – Access Data Inc.
Cellular Forensics – BK Forensics Inc.
Encase Intermediate Forensics – Guidance Software Inc.
Advanced Forensic Tools – United States Secret Service

Related Professional Activities

U.S. Defense Cyber Crime Center – academic curriculum committee member – Current
Guest Speaker – New York City Computer Forensics Show – April 2010
Lead Researcher – Malicious software analysis project – Utica College – Jan. 2010
Guest Lecturer Cybercrime Investigation – Syracuse University – November 2009
Guest Speaker – Economic Crime Institute Conference – Potomac, Maryland – Oct. 2009
National Institute of Justice – Digital Evidence in the Courtroom – committee member

Patrick J. O'Connor, Director, Oneida County Child Advocacy Center

Pat O'Connor received an Associates Degree in Science majoring in Business Management from Mohawk Valley Community College before enrolling at the State University of New York Institute of Technology where he received his Bachelor of Business Administration. He earned his Master of Science Degree in Criminal Justice from Southwest University. Pat began his career in law enforcement in 2000 with the Whitestown Police Department and has since served with the Kirkland and Whitesboro Police Departments. Mr. O'Connor joined the Oneida County District Attorney's office in 2009 as a Senior Confidential Investigator assigned to the Oneida County Child Advocacy Center. He has received extensive training in conducting investigations into allegations of sexual abuse and serious physical abuse against children and specialized training in combating the possession, receipt, and distribution of child pornography via the internet, as well as online solicitation of minors for the purposes of sex. During the course of his assignment at the Child Advocacy Center, Pat has conducted numerous investigations into child sexual exploitation by means of the internet and drew dozens of Search Warrant Applications resulting in the seizure of hundreds of items of digital evidence, which subsequently led to the arrests of perpetrators and sexual offenders across Oneida County culminating in several successful State and Federal prosecutions. In October of 2010, he was promoted to the position of Director of the Child Advocacy Center where he continues to conduct investigations on a regular basis.

Oneida County District Attorney's Office

Senior Investigator Patrick J. O'Connor, Director

Oneida County Child Advocacy Center

Child Exploitation

- Traditional crime that has been perpetrated for centuries.

- Computers & the Internet:
  - Enable predators to cover long distances
  - Provide a cover of anonymity
  - Offer a false sense of security
  - Reduce inhibitions of both offender & victim

3 Types of Online Child Exploitation

- Child Pornography
- Luring (travelers)
- Disseminating indecent material

Characteristics of child pornography

- Two federal court cases help provide basic guidelines in determining what is or isn't child pornography.
- United States v. Dost
- Arizona v. Gates

Child Pornography

1. Whether the focal point of the visual depiction is on the child's genitalia or pubic area;

2. Whether the setting of the visual depiction is sexually suggestive, i.e, in a place or pose generally associated with sexual activity;

3. Whether the child is depicted in an unnatural pose, or in inappropriate attire, considering the age of the child;

Child Pornography

4. Whether the child is fully or partially clothed, or nude;

5. Whether the visual depiction suggests sexual coyness or a willingness to engage in sexual activity;

6. Whether the visual depiction is intended or designed to elicit a sexual response in the viewer.

Erotica vs. Pornography

- Erotica is legal and is often mistaken for child pornography.
- Includes images that do not meet Dost test
  - Nudism
  - Swimsuits
  - Animation (anime)

Where do C.P. Come From?

- Homemade
- Magazines
- Web Sites (limited)
- Peer 2 Peer
- Trading
  - Groups
  - Chat Rooms (IRC)

Identifying Victims

- The image must be of a real child
  - May use medical expert testimony for age
- In NYS not legally necessary to know the identity of the child
- NCMEC – Maintains an international database of known victim images

Luring Crimes

- Use of Internet communication tools to meet minors for the purpose of engaging in sexual contact.

- NYS lacks a law specific to luring
  - Federal & many states have one.

Where Luring Crimes Start

- Chat Rooms
- Instant Messenger
- Social Networking Sites (myspace)

Luring Crimes M.O.

- Hanging out in inappropriate online places
- Using deceptive age, photo, interests
- Grooming
- Profiling Victims (Googling)
  - Studying minutia of conversations

Disseminating Indecent Material to a Minor

- NYS law Sec. 235.22
- Uses a computer to send a depiction of pornography to a minor AND
- Invites that minor to engage in sexual acts

Disseminating Indecent Material to a Minor

- Can charge attempted crime for disseminating to a person the suspect believes to be a minor
- Graphic sexual chat is considered an image for the purpose of this section

How to Catch a Predator

- Citizen Complaints
  - Vigilante Groups
- Undercover online operations
  - ICAC guidelines
  - Evidence Collection
  - Suspect Identification
  - Entrapment

Sr. Inv. Patrick J. O'Connor

Contact:
Oneida County Child Advocacy Center
930 York Street
Utica, NY 13502
(315) 732-3990 (Office)
(315) 725-6538 (Cell)
poconnor@ocgov.net

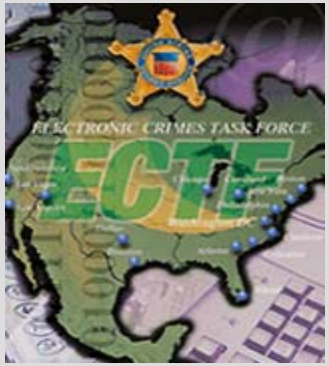
Managerial Issues in Cyber Investigations

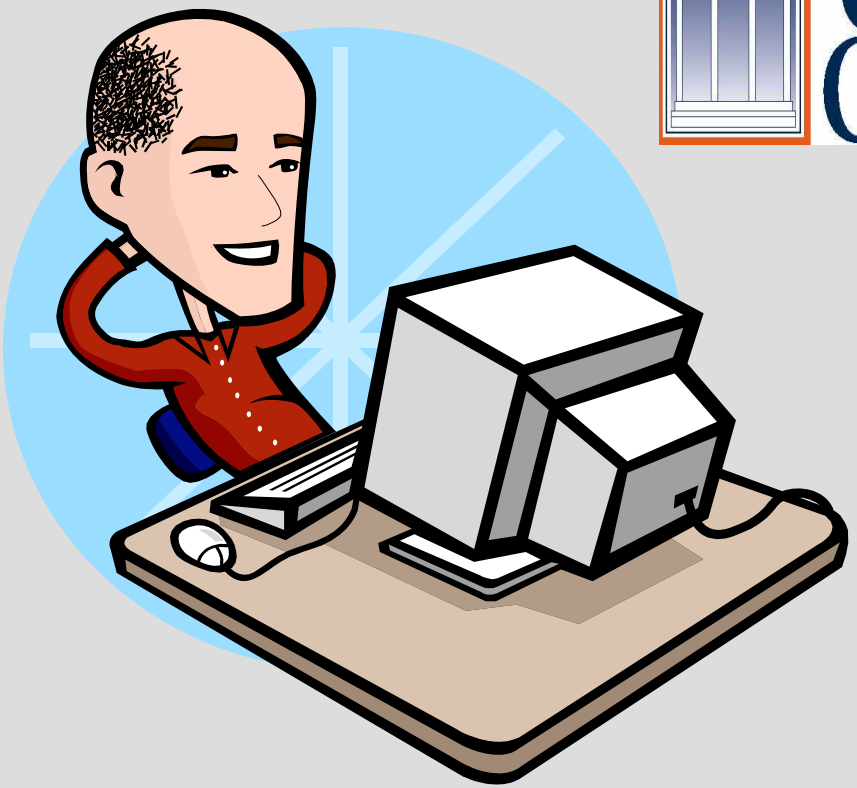
Oneida County Child Advocacy Center

April 30, 2011

Tony Martino

Who is the Bald Guy?





UTICA COLLEGE

Agenda

- Define & explain digital investigations & computer forensics
- Identify unique needs of cyber investigations
- Discuss managerial issues related to cyber investigations

What is computer crime?

The computer is fruit, instrumentality, or evidence

What is computer crime?

Technology has aided many traditional crimes:

- Harassment
- Stalking
- Theft
- Trafficking stolen goods

What is computer crime?

Some crimes are unique to an Internet connected world:

- Identity theft
- Hacking
- Phishing
- DOS attack

What is computer crime?

Some minor crimes have flourished online:

- Auction fraud
- Credit card fraud
- Scams (Nigerian 419 …)
- Child Exploitation
- Copyright Infringement

Computer Crime Law

NYS Penal Law Section 156

Unauthorized use of a computer

Computer trespass

Computer tampering

Unlawful duplication of computer material

Computer Crime Law

Federal Statutes

Many existing wire fraud statutes used
Interstate Nexus often needed

- Parties in different states?
- ISP in different state?
- What route did the communication take?

Enhanced Penalties

Demystifying Computer Crime

DO NOT be afraid of computers

Use Standard Investigative Techniques

- Treat as any other investigation
  - Just happens to involve a computer

Find what you know & work backwards

Need for Forensics

Digital evidence is very important

Computer data far more evasive than conventional evidence

Deleted Data

- Can remain on hard drive for extended periods of time

Forensics is a Specialty

- Hardware, Software, Training are unique

Computer Forensics Definition

- Identification, collection, preservation, examination, analysis and presentation of computer digital evidence in a manner that is legally acceptable.

What Does This Mean?

Computer Forensics

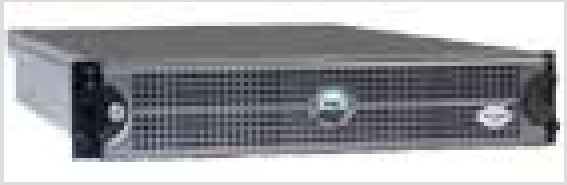
- The ability to conduct analysis of digital data in a manner that:
  - Does not alter the original information
  - Conforms to industry accepted practices
  - Provides repeatable results
  - Meets the standards necessary to support criminal, civil or internal litigation

Forensic Capabilities

- Recovery of deleted information
- Analysis of user activity
- Timeline creation of data changes
- User attribution for activity on shared systems
- Preservation of data for future analysis or litigation.
- Qualification as an expert witness

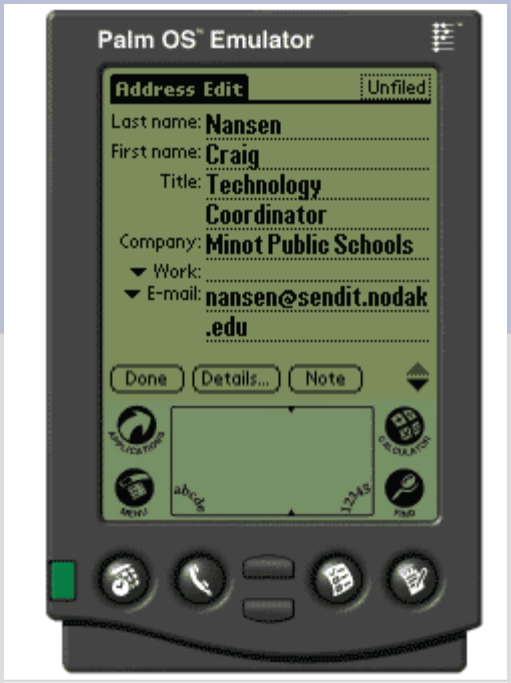
Digital Evidence

- Comes in many flavors



?

Think Outside the Box!


Palm OS Emulator
Address Edit
Unfiled
Last name: Nansen
First name: Craig
Title: Technology Coordinator
Company: Minot Public Schools
Work:
E-mail: nansen@sendit.nodak.edu
Done
Details...
Note


ARCHOS
Jukebox Studio 20


iPod
Playlists
Browse
Extras
Settings
About


MOTOROLA


MOTOROLA


MOTOROLA
01:JGA@jga-inc.com |JGA
ALERT TOOL1 | 09/13/01
12:19! TRANS PRESS DUR
FLEX
SkyTel

Magnetic

Optical

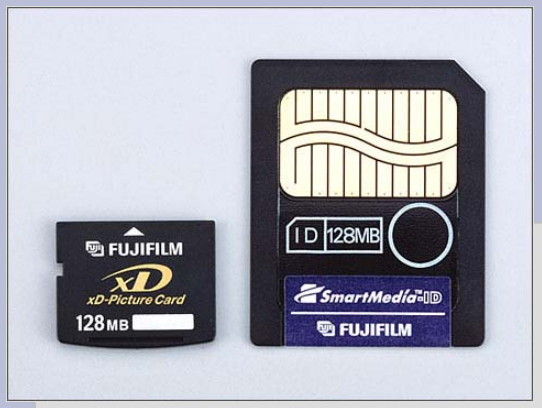

Blu-ray Disc


CD-RW


USB 2.0
compatible
Bundled with
USB 2.0 PCI Card
for Desktop PC
USB 1.1 compatible
Windows
98 SE/ME/2000
ARCHOS
DEx-CDRW2


Memorex
DVD-R
Memorex
3 PACK
DVD-R
4.7GB
120
SINGLE SIDED
DVD

Chip

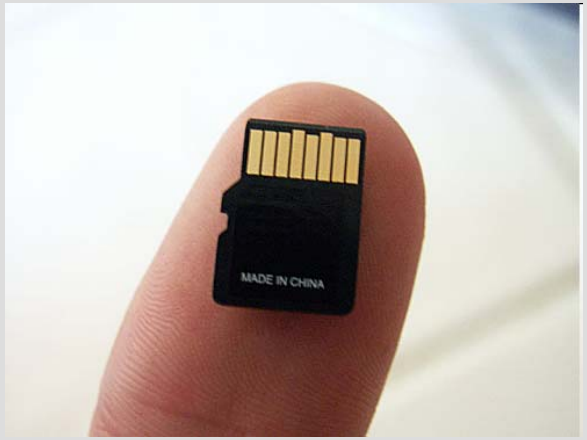

FUJIFILM
xD
xD-Picture Card
128MB
ID 128MB
SmartMedia ID
FUJIFILM

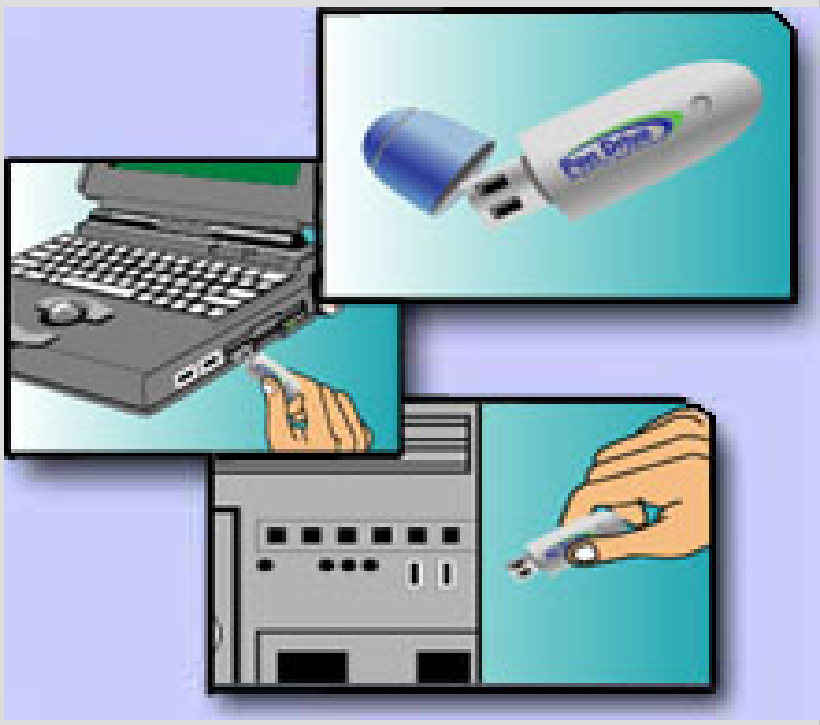

SanDisk
64MB
SD card


SanDisk
64MB
Memory Stick


SanDisk
1.0GB
CompactFlash


SCAN
www.scan.co.uk
64 Mb of data in a pen!
Check out
This
USB
pen
drive
Pen Drive


MADE IN CHINA


Pen Drive

Unconventional

Questions

Contact

Sgt Tony Martino

315-223-3590

amartino@uticapd.com

CYBER EVIDENCE:

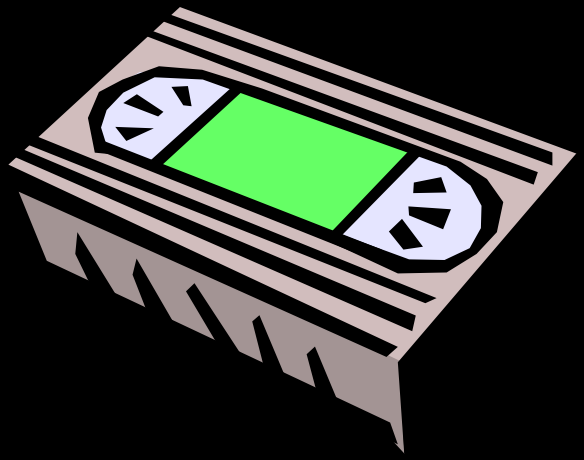
FOUNDATIONS

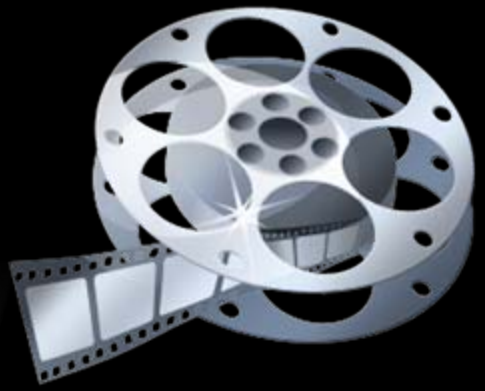
AND USAGE AT TRIAL

Michael A. Coluzza, Esq.

Office of the Oneida County District Attorney

THE WAY IT WAS:





THE WAY IT IS NOW:

TECHNOPHOBIA

- THE PERSISTENT AND DEBILITATING FEAR THAT TO UNDERSTAND, USE AND PRESENT EVIDENCE STORED IN AN ELECTRONIC MEDIUM, YOU HAVE TO BE PART COMPUTER SCIENTIST, PART MATHEMATICIAN, PART MAGICIAN, ABLE TO LEAP TALL BUILDINGS IN A SINGLE BOUND.

TWO BIG QUESTIONS, ASKED BY LAWYERS EVERYWHERE:

- HOW DO I GET THIS EVIDENCE IN?

OR

- HOW DO I KEEP THIS EVIDENCE OUT?

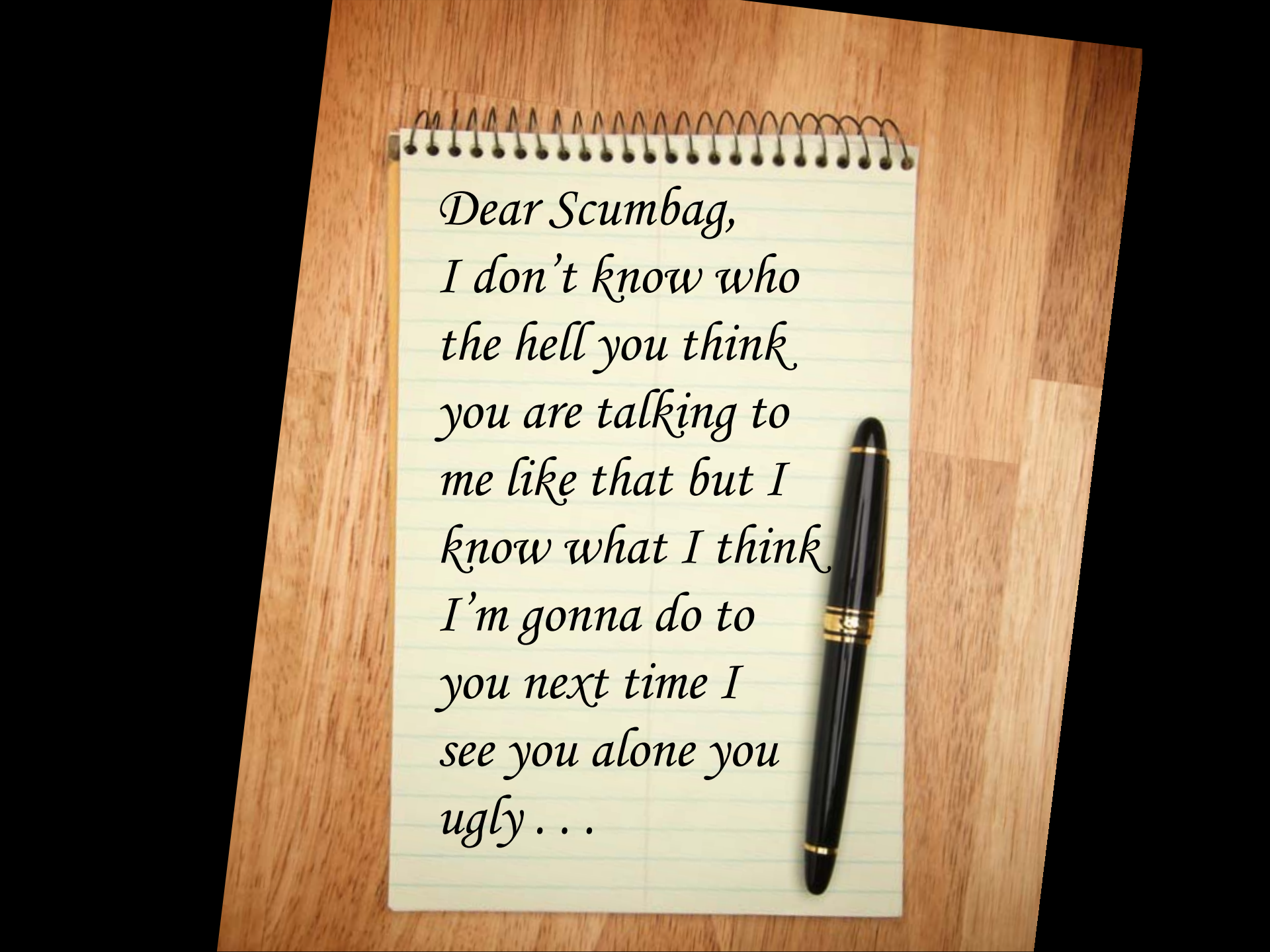
DON’T WING IT AND HOPE FOR THE BEST

HOW DO I FIGURE THIS OUT?

AS A START POINT, ASK YOURSELF THE FOLLOWING:

HOW WOULD I HAVE DONE THIS ONE HUNDRED YEARS AGO?

HOW DO I LAY A FOUNDATION FOR ONE OF THESE NOW, OR ONE HUNDRED YEARS AGO:


Dear Scumbag,
I don't know who
the hell you think
you are talking to
me like that but I
know what I think
I'm gonna do to
you next time I
see you alone you
ugly . . .

Personal letter foundation

- Who signed it?
- Is it on stationary that the recipient recognizes/attributes to the ostensible maker?
- How was it delivered?
- If handwritten, does the recipient have a basis upon which to recognize the handwriting?

- How many witnesses can recognize the handwriting?
- Is the subject matter such that can circumstantially connect the ostensible maker/sender to the letter?
  - Info. only the ostensible sender could know
  - Acknowledgement by such person of the communication before/after the fact, etc.

Consider The Quaint Telephone:

The Court of Appeals did just that in 1980:

People v. Lynes, 49 NY2d 286 (1980)

It is for the trial judge to determine whether or not a sufficient foundation has been laid to permit a jury to find that a telephone conversation was one with the person against whom it is offered.

- Such issues are to be decided upon their own peculiar facts
- Judge must determine whether the proffered proof permits the drawing of inferences which make it improbable that the caller's voice belonged to anyone other than the purported caller
- Where the voice is unknown to recipient, there must be more than self-serving declaration of identity by caller
- **Can still be admitted where alternate indices of reliability are found in the surrounding facts and circumstances**

Court’s Examples of Indices:

- Look up person’s number in standard phone book, call & see if answering party confirms identity;
- Subject matter discussed confirms identity as ostensible caller;
- Person to be identified references facts only the ostensible caller could have ;

LYNES INDICES

- Detective called phone listed to the defendant and left message with brother to call him back
- Detective receives call from someone claiming he is defendant and that he knows the detective is looking for him
- Defendant reacts emotionally when detective reveals that the perpetrator left his knife behind at the scene – a detail only known to detective, victim and perp.

- “In sum, taking these facts and inferences in various combinations or in concert [the Judge did not err] in leaving it to the jury – aided by the instruments of cross examination, counsel’s arguments and other fact finding tools available at the trial level, to decide whether, as Learned Hand put it, ‘THE CHANCE THAT THESE CIRCUMSTANCES SHOULD UNITE IN THE CASE OF SOMEONE OTHER THAN THE DEFENDANT SEEMS SO IMPROBABLE THAT THE SPEAKER IS SUFFICIENTLY IDENTIFIED’.

THE MORAL OF THE STORY

- PRESENT ENOUGH EVIDENCE TO MAKE IT CIRCUMSTANTIALLY IMPROBABLE THAT THE SENDER IS ANYONE ELSE
- IT'S ADMITTED AND BECOMES A JURY QUESTION

FLASH FORWARD TO THE PRESENT:

- Instant Messaging cases
- Text Messaging cases
- Cell Phone cases
- Email cases
- Chat Room Transcripts
- Websites/Webpages
- Social Networking sites
- Downloaded or Stored Pictures, Photos or Videos
- Caught on Video cases

SAME BASIC RULES APPLY!

- Each of these evidence types are akin to the letter or phone call of old, only better.
- Better because of these:

- Tiny electronic footprints that reveal a host of information about the source of a communication, picture or collection of data, including:
- Where it came from
- Where it was sent
- When it was sent
- Who sent it
- Whose computer/account it was sent from
- Whether or not a deletion was attempted
- Whether or not it was altered in any way and when that occurred

AUTHENTICATION:

- Still involves the introduction of evidence sufficient to demonstrate that the “writing” is what the offering party claims is to be.

- For example, where witness can testify that he/she has seen an email previously in its original electronic form, and that a paper printout exhibit is a fair and accurate reproduction of the original.

People v. Clevenstine, 68 AD3d 1448 (3rd Dept. 2009)

- Rape Third Degree and Endangering the Welfare of a Child
- Family friend committed various acts upon two preteen daughters over a twenty month period.
- Victims' mother discovered sexually explicit instant message communications to daughters on their own computer from defendant's MySpace account, wherein admissions to sexual contact were made by the defendant

- Instant messages were burned to disc from victims' computer – used at trial over objections that they hadn't been sufficiently authenticated.

- Third Department disagreed, acknowledging that "the foundation necessary to establish these elements may differ according to the nature of the evidence sought to be admitted" relying upon People v. McGee, 49 NY2d 48 (1979).

Indices of Reliability in Clevenstine:

- Investigator from NYSP Computer Crime Unit testified to retreiving suspect messages from victim computer & burning to disc
- MySpace legal compliance officer testified that messages exchanged on disc were from accounts created by defendant and victims respectively
- Defendant's wife testified she recalled seeing same conversations on defendant's MySpace account when she was using their computer

- Defense argued that such conversations could have easily been initiated by someone else gaining access to his MySpace account.

- But Court found that, once the above basis for authenticity had been established, defense argument became a question of fact for the jury to consider and not an obstruction to admissibility [relying upon Lynes].

So What Does All of This Mean?

Some Practical
And Practice
Considerations

MOST IMPORTANT RULE:

- **Preserve the information** – send preservation letter to the legal compliance office of the particular company that is involved in conveying the suspect communication AS SOON AS YOU DISCOVER ITS EXISTENCE - SOME TYPES OF COMMUNICATIONS AREN'T KEPT BY THE COMPANY FOR A LENGTH OF TIME

- Get consent for release of the information from your client/victim and try to sufficiently identify the communication with all available information as to date and time

- Retreive the Cell Phone/Internet/Social Networking provider's records – do not simply rely upon what is in your victim/witness/client's cell phone, laptop
- The company is going to be your best source for corroborative circumstantial evidence as to the authenticity of the communication sought to be introduced
- SUBPOENA DUCES TECUM

- MAKE IT EASY ON YOUR JUDGE WITH GOBS AND GOBS OF CORROBORATIVE EVIDENCE

INTERVIEW YOUR RECIPIENT THOROUGHLY

- Why does he/she think that the message is from the ostensible sender?
- Has he/she received such messages in the past from such person?
- Who would have access to the sender's computer at that time of day?
- Is there info. In the communication itself, known only to the sender?

Cell Phones:

- Records from the provider – grid of numbers with a decoding key
- Business record that is easily proferred by any company employee with knowledge
- Yields tons of information – incoming phone #’s, outgoing #’s – rollovers to voice mail – call duration - *69 calls
- MURDER CASES HAVE BEEN SOLVED ON SUCH DATA!!!!!!!!!!!!

Websites & Webpages

- Authenticity can be established by person who viewed it on the relevant date/time
- Witness can testify to the URL (web address) that he/she inputted to access the site/page
- Witness can then compare that recollection with a hard copy of the webpage and attest that it is fair & accurate reproduction

Efforts to Delete

- Good consciousness of guilt evidence
- Recovery software is LEGION
- Leave to experts
- Often deleted files are recoverable from electronic “trash cans”, temporary internet files, backup files and archive files, just to name a few
- Good circumstantial evidence of authenticity if files were attempted to be deleted from ostensible maker’s own phone/computer

Overcoming Objections

- HEARSAY – Is that what it is? Is it really being offered to prove the truth of the matter asserted, or is there another purpose?
- Communications to show mere contact between parties, regardless of the content of the communication, are not excludable as hearsay
- Declarations against interest of the ostensible maker – not excludable as hearsay

Methodical, Brick-By-Brick Approach Will Yield Results

REFERENCES

- Authenticity of Electronically Stored Evidence, Including Text Messages and Emails, 34 ALR6th 253
- People v. Lynes, 49 NY2d 286 (1980)
- People v. Clevenstine, 68 AD3d 1448 (3rd Dept. 2009)
- People v. Foley, 257 AD2d 243 (4th Dept. 1999)
- People v.Givans, 45 AD3d 1460 (4th Dept. 2007)
- People v. Pierre, 41 AD2d 289 (1st Dept. 2007)