

# CERTIFIED INSPECTOR GENERAL INVESTIGATOR

---

## DIGITAL EVIDENCE

**JOHN  
JAY** COLLEGE  
OF  
CRIMINAL  
JUSTICE



**ADAM SCOTT WANDT, J.D., M.P.A.**  
ASSISTANT PROFESSOR OF PUBLIC POLICY  
JOHN JAY COLLEGE OF CRIMINAL JUSTICE

[awandt@jjay.cuny.edu](mailto:awandt@jjay.cuny.edu)

<http://wandt.us>

# ADAM SCOTT WANDT

ASSOCIATE PROFESSOR OF PUBLIC POLICY  
JOHN JAY COLLEGE OF CRIMINAL JUSTICE

ATTORNEY AND COUNSELOR AT LAW  
(NEW YORK STATE)

CO-CHAIR NYC BAR ASSOCIATION:  
TECHNOLOGY, CYBER & PRIVACY LAW COMMITTEE

FORMER SWORN LAW ENFORCEMENT OFFICER

INSTRUCTOR:  
ASSOCIATION OF INSPECTORS' GENERAL

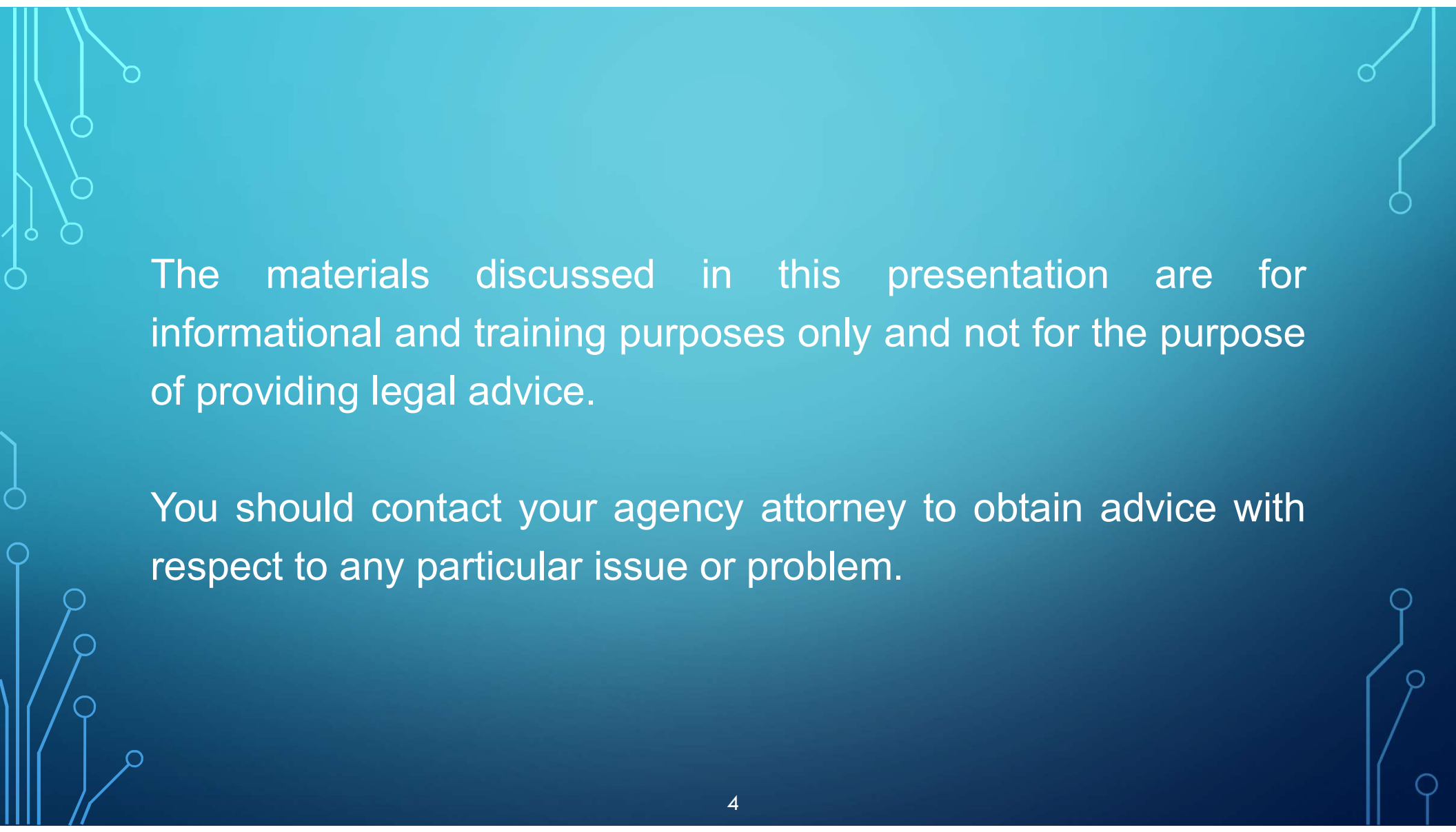
MASTER SCUBA DIVER  
UNDERWATER PHOTOGRAPHER



<https://wandt.us>

wandt.us/aig





The materials discussed in this presentation are for informational and training purposes only and not for the purpose of providing legal advice.

You should contact your agency attorney to obtain advice with respect to any particular issue or problem.



# LEARNING OBJECTIVES



Understand how digital evidence is generated and where it might be found.



Understand the role digital forensics plays in investigations.



Understand key legal decisions regarding the collection and use of digital evidence.



Gain basic knowledge on the use of cellular and ISP records.







**CASEY ANTHONY TRIAL**





Home / Daily News / Cops in Casey Anthony Case Missed Internet...

---

EVIDENCE

## **Cops in Casey Anthony Case Missed Internet Search for 'Fool-Proof Suffocation'**

POSTED NOV 27, 2012 02:30 PM CST

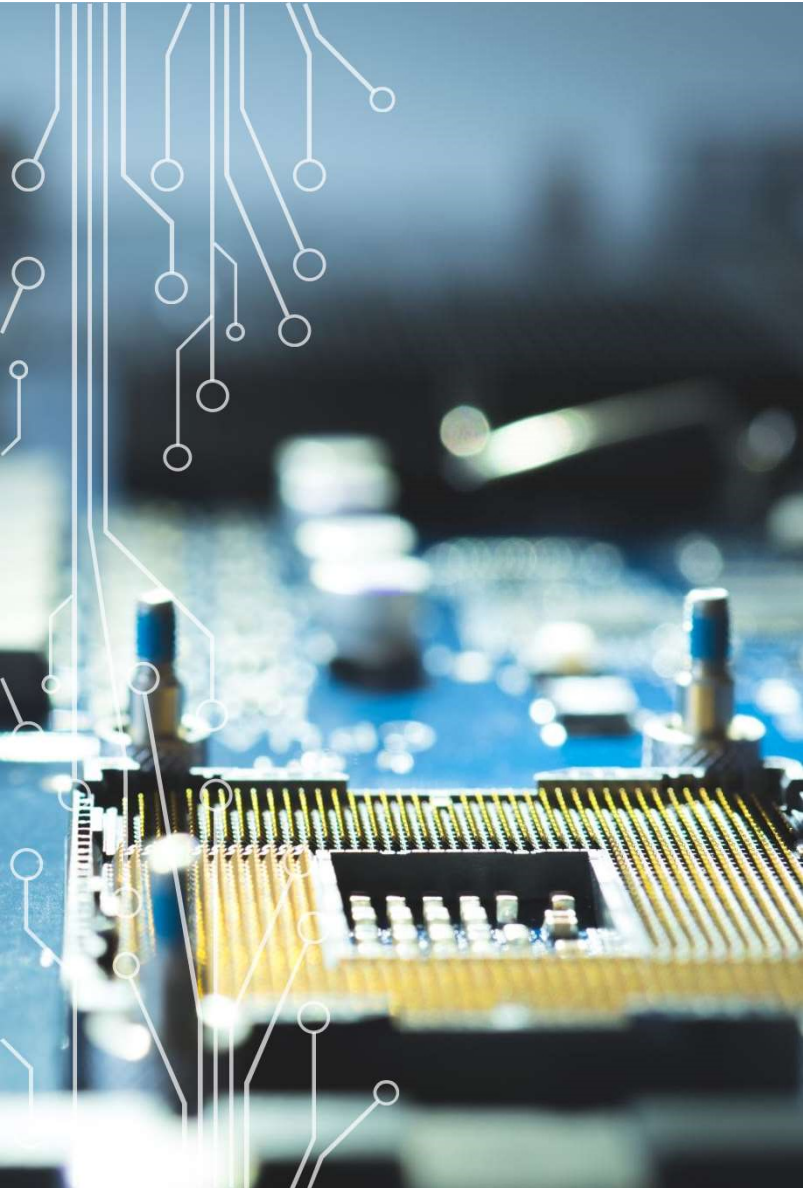
BY DEBRA CASSENS WEISS ([HTTP://WWW.ABAJOURNAL.COM/AUTHORS/4/](http://www.abajournal.com/authors/4/))

---

Police investigating the disappearance of Caylee Anthony overlooked an Internet search for the misspelled phrase “fool-proof suffocation” on the family computer.

The problem: Orange County sheriff’s police checked out the search history on the Internet Explorer browser, but not the Mozilla Firefox browser, report the Associated Press (<http://www.usatoday.com/story/news/nation/2012/11/25/casey-anthony-suffocation-google/1725253/>) and CBS News Crimesider ([http://www.cbsnews.com/8301-504083\\_162-57554037-504083/casey-anthony-](http://www.cbsnews.com/8301-504083_162-57554037-504083/casey-anthony-)





“THOSE COMPUTER CRIME  
PEOPLE I WORK WITH.”

# PURPOSE OF DIGITAL FORENSICS



PROVE INTENT (STATE OF MIND)



PROVIDE RELEVANT EVIDENCE TO A CASE.



FIND HIDDEN OR DELETED FILES AND DATA.

# PURPOSE OF FORENSICS



WHO?



WHEN?



WHERE?



HOW?



SOMETIMES  
WHY

## TYPICAL CASES

Criminal

Child Sexual Abuse  
Materials

White Collar Crimes

Identity theft, money  
laundering, credit card  
fraud, etc.

Acts of Terrorism

Internal Affairs and  
Inspectors General

Regulatory/Compliance

Administrative (HR)

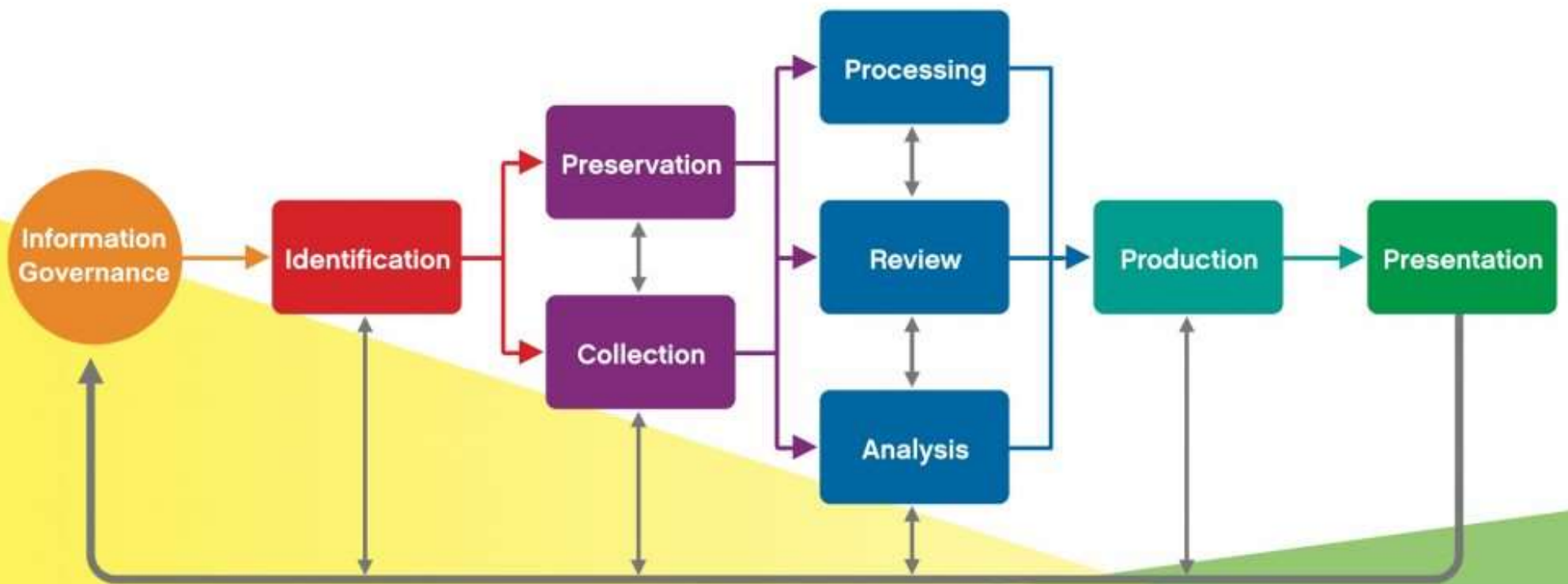
## OPERATIONAL DEFINITIONS

**Digital forensics** is the collection, preservation, analyses, recovery & investigation of evidence found in digital devices that can be used in civil, criminal or regulatory cases.

**E-Discovery** is the process by which (IT/other) examiners find & produce documents stored in electronic form in response to civil or criminal litigation, internal corporate policies, or regulatory investigations.



# Electronic Discovery Reference Model



**VOLUME**

**RELEVANCE**

<b>CATEGORY</b>	<b>eDiscovery</b>	<b>Digital Forensics</b>	<b>Incident Response</b>
<b>SCOPE</b>	Narrowed to a specific dataset	All encompassing (active, deleted and carved files in unallocated space, unlocking password protected files, decrypting encrypted files)	All encompassing OR specific to process.
<b>EXAMINER</b>	Any power user	"Expert"	"Expert"
<b>DATA MINING</b>	Data gathering	Data digging	Data digging
<b>STATE</b>	Active	Reactive	Proactive

# Digital/Computer Forensic Certifications



CFCE: Certified Forensic Computer Examiner

- <https://www.iacis.com/certification/cfce>



EnCE: Encase Certified Examiner

- <http://www.guidancesoftware.com/computer-forensics-training-ence-certification.htm>



CCE: Certified Computer Examiner

- <https://www.isfce.com/certification.htm>



CHFI: Computer Hacking Forensic Investigator

- [http://www.eccouncil.org/certification/computer\\_hacking\\_forensic\\_investigator.aspx](http://www.eccouncil.org/certification/computer_hacking_forensic_investigator.aspx)

# Digital/Computer Forensic Certifications



## GCFC: GAC Forensic Examiner Certification

- <http://computer-forensics.sans.org/certification/gcfc>



## CDFE: Certified Digital Forensic Examiner

- <http://mile2.com/digital-forensics-courses/certified-digital-forensics-examiner.html>

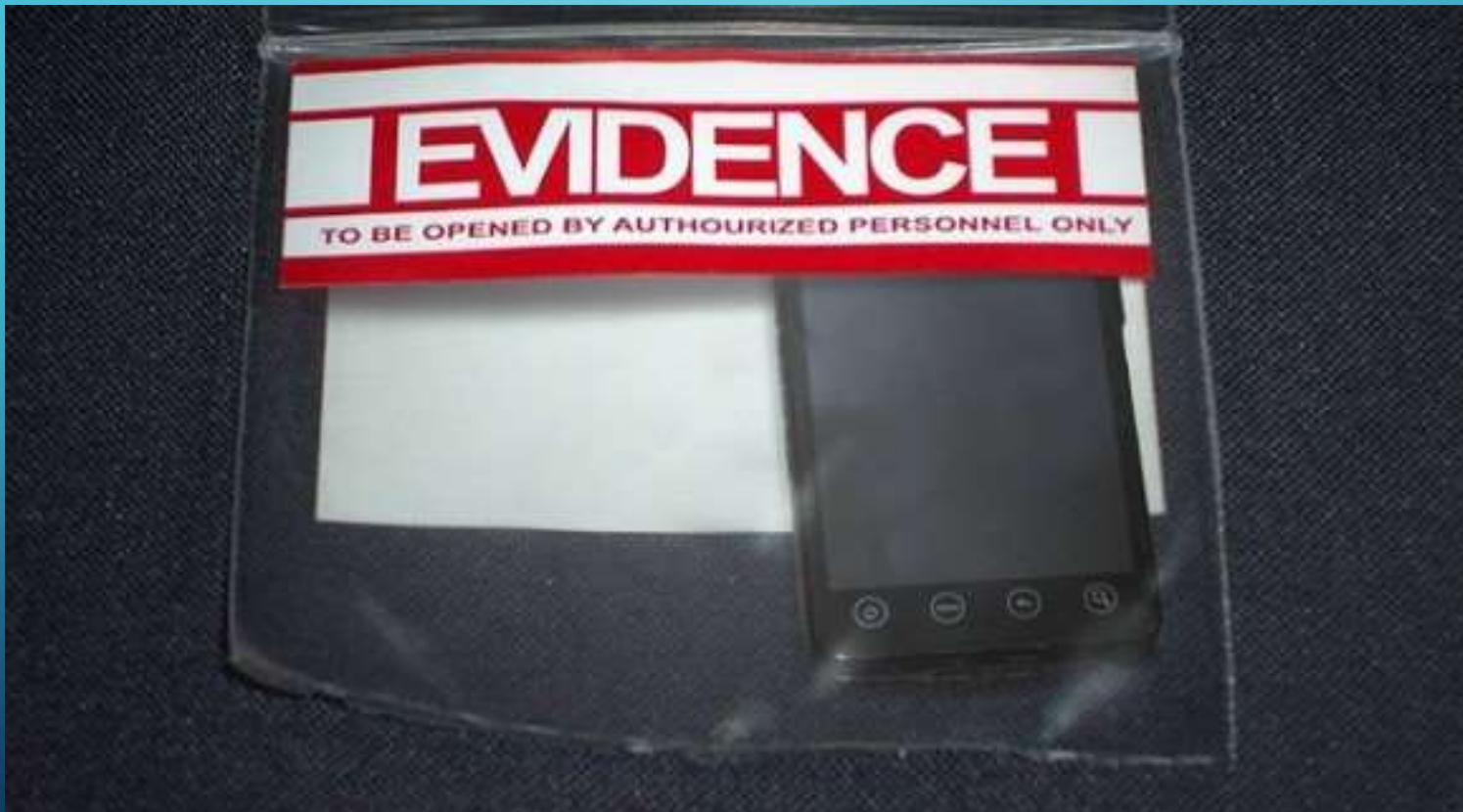


## \*CFE: Certified Fraud Examiner

- <http://www.acfe.com/membership/becoming-cfe.asp>

\* Not a Digital Forensics expert by itself

# EVIDENCE PRESERVATION (EASY??)





# EVIDENCE PRESERVATION





NYPD / DOI EVIDENCE WEARHOUSE



**REPAIRED AND IMPROVED**



## 'Nightmare' Warehouse Fire Erases Evidence in Many Unsolved Cases

Lawyers say evidence in cold cases and bids for exoneration disappeared or was ruined when a Police Department storage facility in Brooklyn went up in flames.

[Give this article](#) [Share](#) [Bookmark](#)



The waterfront compound held everything from impounded vehicles to fibers from decades-old murders and cold cases. Andrew Seng for The New York Times

# EVIDENCE PROCESSING AND EVIDENCE ANALYSIS

As Collected? Storage Until Needed?

1% vs 100%

High Skill Set Individuals

Computer Assisted Analysis

Data Mining / Big Data

# FORENSIC RECOVERY OF EVIDENCE DEVICE (FRED UNIT)



# MOORE'S LAW

A DECADE OF PROGRESS IN SEMINOLE  
COUNTY, FL



*We began operations in 2000/2001  
with one workstation.*





*Digital  
Intelligence's  
FRED Senior,  
our first  
workstation*

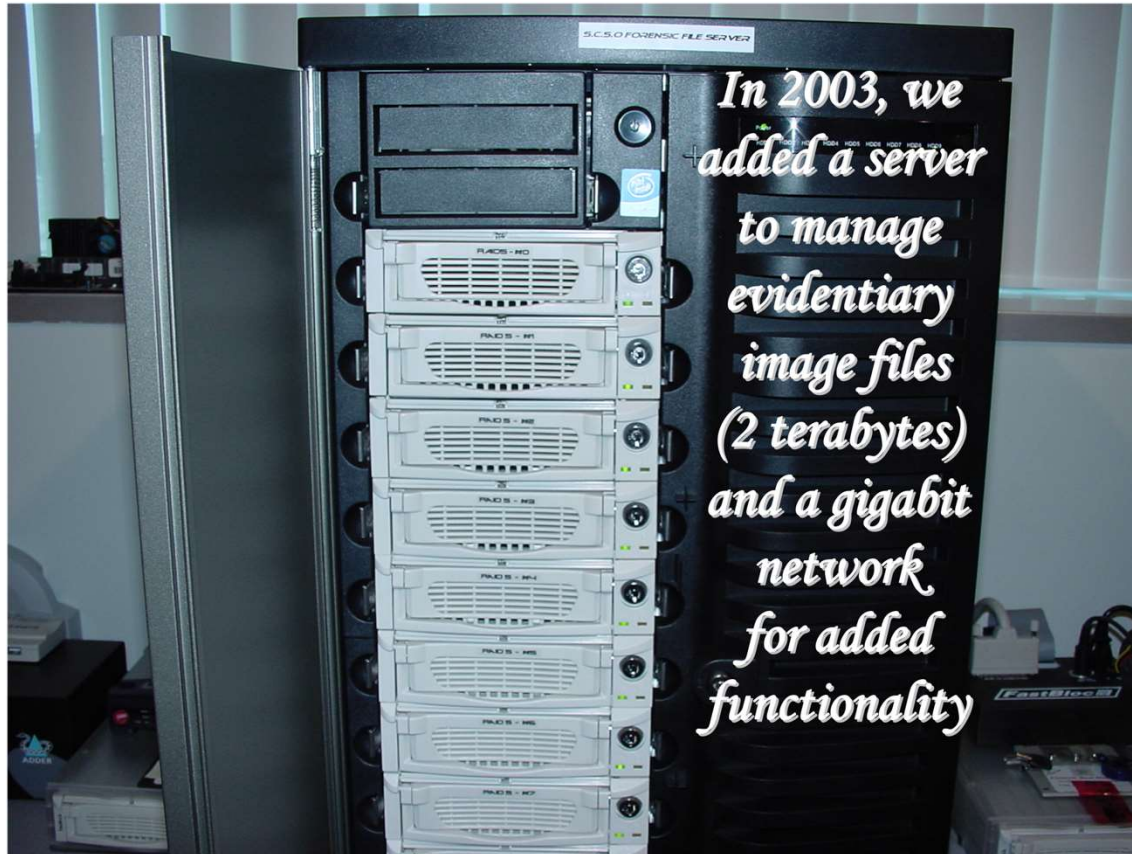
# *2002 Computer Forensic Lab*



*2003 Computer Forensic Lab*







## *2 of 3 Forensic Workstations - 2003*



*In 2004, we added an additional 3 terabytes of storage to manage increasing evidence*

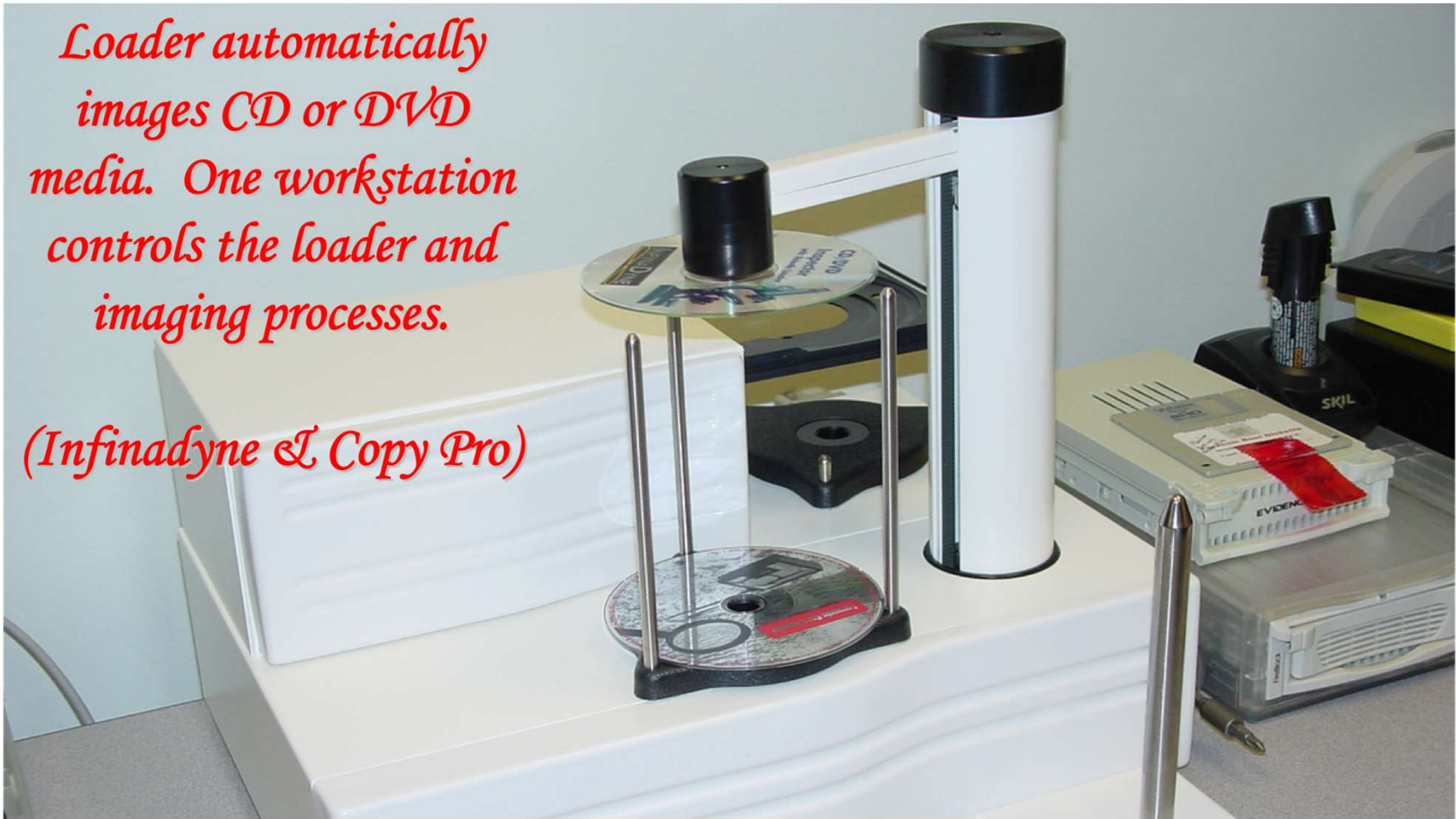


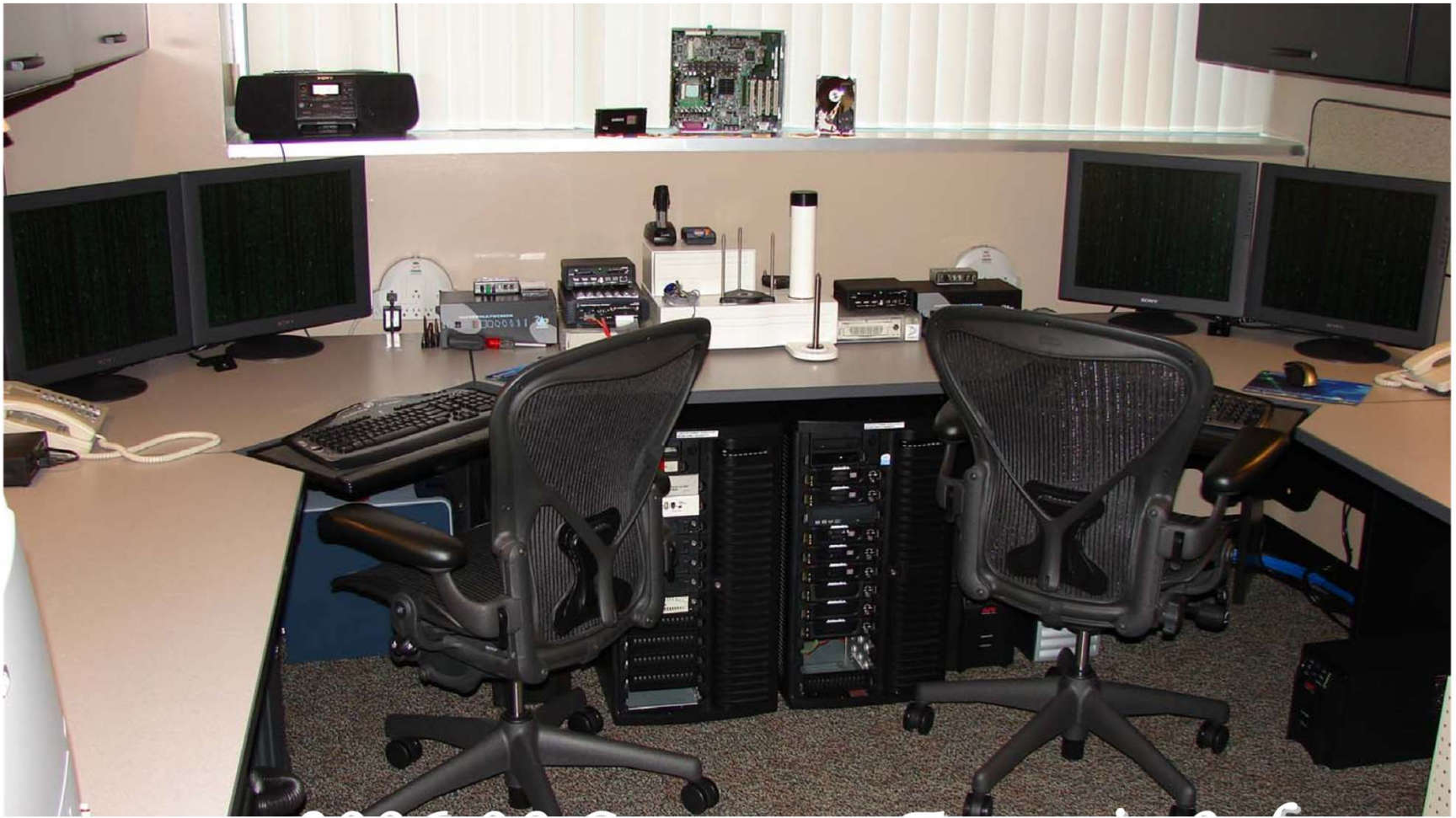
# *2004/05 Computer Forensic Lab*



*Loader automatically  
images CD or DVD  
media. One workstation  
controls the loader and  
imaging processes.*

*(Infinadyne & Copy Pro)*





*In 2005, we added a 42U rack to consolidate server components. A 6,000w battery backup/UPS was added to provide continuous power to all components in the rack and each workstation in the lab. Through the end of 2006, the server managed roughly 10+ terabytes of storage.*



*In 2007, we moved our rack out of the lab and to the agency's data center. This was done for better fire suppression, A/C and climate control, and improved power/battery backup systems. We also added an additional 6TB array. (16 TB)*





# 2007-08 Server and Arrays





*2009 Computer Forensic Lab*

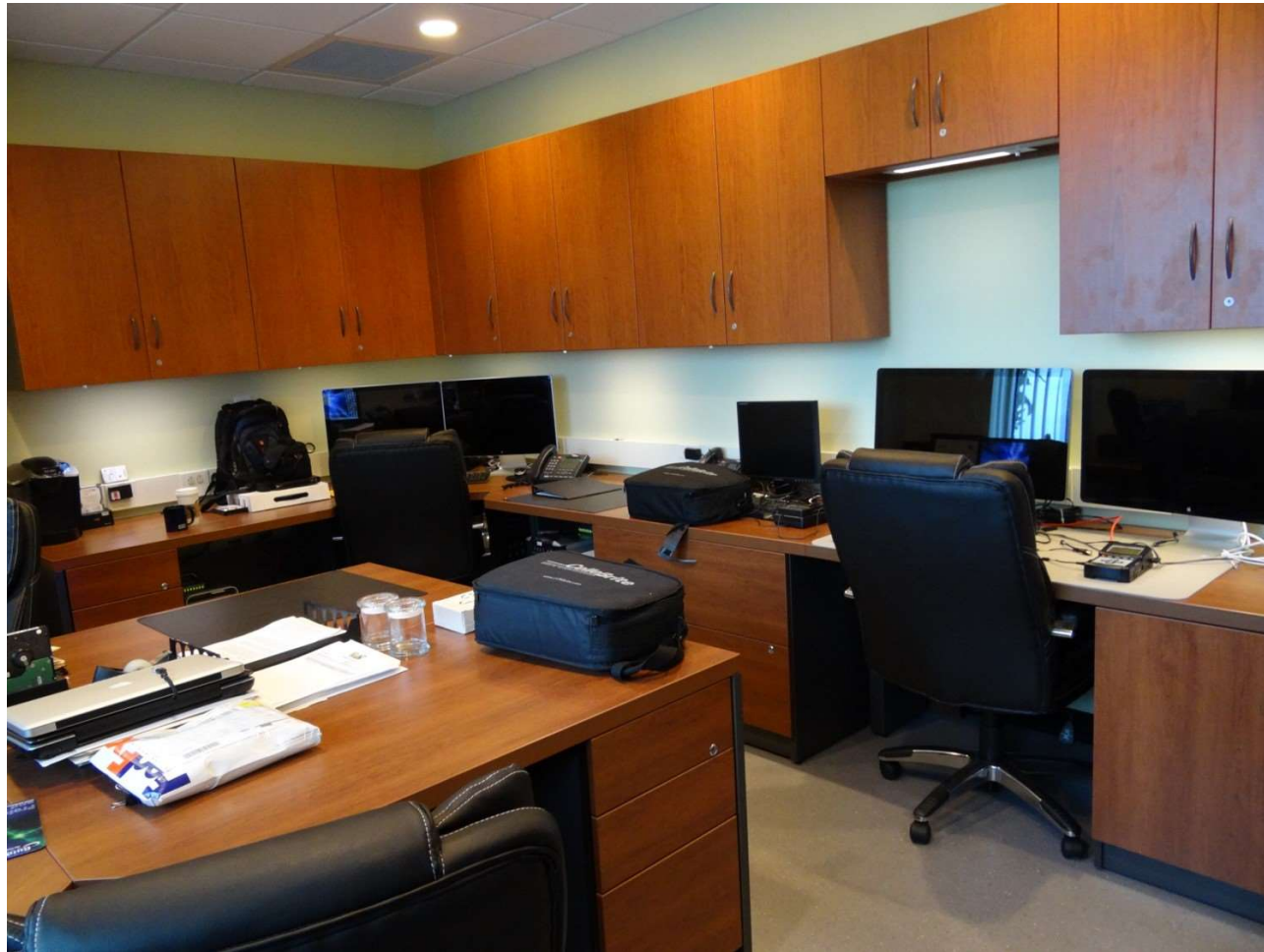


*Sergeant's Office: FRED and Dell Laptop*





TEN + YEARS LATER



Lab expanded from 2 examiners up to 5 digital forensic examiners. Each examiner was issued 3 FRED computers and double monitors



Chip-Off station for removing microchips from cell phones for further analysis



Senior examiner was provided his or her own office











