INVESTIGATIONS: SOLVING COMPLEX PROBLEMS

+Alan Nelson, CPA, CFF, FEXCE, PI, XAMN, XRY +Catherine Clifton, JD, MBA, SPHR

Texas Municipal Human Resources Association Conference May 8, 2025

The Trust Trap . . . 20 years in the making

Long time employee

Rarely took vacations

Gained the trust and admiration of co-workers and people in the community

Advanced through the organization to become the comptroller.

Campbell Soup Company "inheritance".

12 weeks of unpaid leave . . . Reveals the past . . .



The Finale



Learning Objectives

×1 vox	Plan	Learn how to develop an effective Investigation & Incident Response Plan.
	Investigate	Learn how to investigate allegations of fraud, misconduct, and misappropriation of assets from your organization.
•	Workflow	Learn where you and your organization fit into the Investigation and Incident Response workflow.
	Leverage	Learn how to leverage forensic technology into your compliance program and incident response plan.

Additional Learning Objectives







you can leverage tools like IDEA, Forensic Explorer and Tableau to streamline your investigation process.





Utilizing forensic technology will broaden your reach and deepen your understanding of your case elements.



Allowing for better outcomes for you and the client.

withum[#]

Planning Your Investigation

INVESTIGATIONS – SOLVING COMPLEX PROBLEMS



POWER IN THE PLUS[™]



Planning -Solving Complex Problems

Do you have an Investigative & Incident Response Plan ("IRP")?

Has your internal investigative team been assembled?

Does the investigative team have experience handling evidence?

Does your investigative team include individuals with strong interviewing skills?

Is your investigative team experienced in investigating sensitive matters?

Planning -Solving Complex Problems

- Policy and procedures guide.
- Uhistleblower Hotline.
- Internal Audit | Program Compliance Reviews Findings
- □ IT Department Friend vs. Foe
- How will your ongoing investigative efforts be communicated to your stakeholders?

Planning – Discovery & Incident Response – Ask the questions?

- Who was involved?
- What happened?
- Where did the incident occur?
- When the the incident occur?
- Why did the incident occur?
- How did the incident happen?

withum[#]

Investigation Protocols

INVESTIGATIONS – SOLVING COMPLEX PROBLEMS



POWER IN THE PLUS™



Investigation -Investigative & Incident Response Protocols



Issue identification.



Identify all the stakeholders.



Isolated event or an entity-wide systemic practice.



Nature of the allegation(s) – Data exfiltration, fraud, procurement.



Where did the source of the allegation(s) arise from?

Investigation – Investigative & Incident Response Protocols



Will outside counsel be brought in?

Do we have the appropriate resources internally – SME's?

What is the Audit Committee's role?

withum[#]

Workflow

INVESTIGATIONS – SOLVING COMPLEX PROBLEMS



POWER IN THE PLUS[™]



Where it all starts . . .



Peeling Back The Layers of an Onion

- Triggering Event.
- How was the event communicated?
- Nature of the allegation.
- Has and allegation been documented?
- Does the allegation involve external parties?
- Does the allegation involve a current employee?

Are there multiple individuals involved?

- □ Is personal safety and welfare at risk?
- □ Have all stakeholders been notified?
- Are external subject matter experts needed?
- □ Has sensitive data been compromised | exfiltrated?

Complex Internal Investigations

- Conflict of Interest
- Discrimination
- Harassment
- Misappropriation of Assets
- Procurement | Purchasing Activities.
- Secure Employee Offboarding
 - + Involuntary
 - + Voluntary

Investigation Source Lead



Administrative Proceeding



Confidential Informant



Ethics Hotline



External Law Enforcement (LEO) Agency



Outside Counsel Representing Victim.

withum[#]

Leveraging Forensic Technology

INVESTIGATIONS – SOLVING COMPLEX PROBLEMS



POWER IN THE PLUS[™]





Digital Forensics

- What is Digital Forensics?
- Collecting, preserving, and delivering digital evidence



eDiscovery

- What is eDiscovery and what it is <u>NOT</u>
- Digital Forensics vs. eDiscovery



Data Analytics & Visualization

- You got the data, now how can you use it
- Tools to get the insights you want

Important Key Words in Digital Forensics

A digital forensic expert must *always*:



MAINTAIN A STRICT CHAIN OF CUSTODY

A Chain of Custody document is created at the start of every investigation identifying the evidence source, content being acquired, and the date and time the investigator takes possession of the evidence.

2

3

4

5

PERSERVING INTEGRITY OF INFORMATION

The evidence acquired must maintain it's original format and condition. Copies of the "image" can be used for reviewing and testing.

SCIENTIFIC METHOD

The forensic processes performed are peer and court accepted.

ACCURATE, RELIABLE

Data validation through hash algorithms which demonstrate the integrity and the reliability of the forensic images.

REPEATABLE

The results derived from digital evidence processing can be replicated with the same outcomes. Evidence is typically processed with multiple tools.

Sources Of Evidence

Through Digital Forensics



Computers

Laptops, PCs, peripheral devices such as USBs and printers.



Internet of Things

The IoT is the connection between networks and devices such as Alexa or printers that are connected.



Mobile Devices

Cellphones, iPads, Tablets, Smart Watches, GPS devices.



Cloud Sources

Microsoft 365, Gmail, Google Drive, OneDrive, iCloud.

Digital Forensics allows you to analyze:

TIMELINES OF COMPUTER ACTIVITY

Helpful to determine when and who utilized the computer, to corroborate what the user was accessing and performing while using the device..

COMMUNICATIONS

Beyond emails, communications such as chats, Teams, Slack, and text messages

INTERNET USAGE

Websites visited, keyword searches conducted, and login credentials.



Recovering deleted information such as emails

and/or files.

SOCIAL NETWORKS

Login credentials, alternate aliases, and connected individuals. Open-source intelligence (OSINT)

PHOTOS, MOVIES, RECORDINGS

Screenshots, voice recordings or video footage.

INSTALLED APPS, PROGRAMS, & PERIPHERAL DEVICES

Prohibited programs, tracking programs, USBs or documents sent to printers.

The Goals of Digital Forensics

Quotes

"The binary data doesn't care about innocence or guilt. It gives you the information that you need to make your expert conclusions."

- Gus Dimitrelos

11

Utilizing Forensic Technology to Conduct Fraud Investigations



What is eDiscovery?

A complex process – simplified:



PARTIES INVOLVED IN A LEGAL CASE

In the event a legal case will ensue, parties will enter the eDiscovery process to preserve, collect, review, and exchange information that has been electronically stored, also known as ESI.

DETERMINE THE SCOPE

Attorneys of both parties will determine the scope of the eDiscovery, identify, and attempt to ensure relevant ESI is preserved.



()4

02

MAKE REQUESTS & CHALLENGES

Requests will be made by each attorney as well as challenges.

ESI COLLECTED, ANALYZED, AND FORMATTED FOR COURT

Once ESI is collected, the legal team will analyze and prepare data into a reviewable format for counsel to utilize in trial as evidence.

Sources Of Evidence

Through eDiscovery



Computers

Laptops, PCs, peripheral devices such as USBs and printers.



OSINT

Publicly available data or information such as arrest records, court filings, social media, data on public trading.



Mobile Devices

Cellphones, iPad, Tablets, Smart Watches,



Cloud Sources

Microsoft 365, Gmail, Google Drive, OneDrive, iCloud.

Triggering Events – Why are we Investigating

• Occupational misconduct / Asset Misappropriation

• Corruption / Bribery / Conflicts of Interest

• Accounting Irregularities / Financial Stmt. Fraud



Digital Forensics & eDiscovery

The Hybrid Approach



We have data! Now what...

Using the information/evidence you've collected to provide insights about your case

Let's look at some data

1		I		III		IV		
x	Y	x	у	x	У	x	У	
10	8.04	10	9.14	10	7.46	8	6.58	
8	6.95	8	8.14	8	6.77	8	5.76	
13	7.58	13	8.74	13	12.74	8	7.71	
9	8.81	9	8.77	9	7.11	8	8.84	
11	8.33	11	9.26	11	7.81	8	8.47	
14	9.96	14	8.1	14	8.84	8	7.04	
6	7.24	6	6 6.13		6 6.08		5.25	
4	4.26	4	3.1	4	5.39	19	12.5	
12	10.84	12	9.13	12	8.15	8	5.56	
7	4.82	7	7.26	7	6.42	8	7.91	
5	5.68	5	4.74	5	5.73	8	6.89	

Visualization and Tableau Introduction, 2019

Turn Data into Analytics

Using the information/evidence you've collected to provide insights about your case

Let's look at some data...with statistical analysis

1		II		Ш		IV		
×	У	x	y	x	Y	x	У	
10	8.04	10	9.14	10	7.46	8	6.58	
8	6.95	8	8.14	8	6.77	8	5.76	
13	7.58	13	8.74	13	12.74	8	7.71	
9	8.81	9	8.77	9	7.11	8	8.84	
11	8.33	11	9.26	11	7.81	8	8.47	
14	9.96	14	8.1	14	8.84	8	7.04	
6	7.24	6	6.13	6	6.08	8	5.25	
4	4.26	4	3.1	4	5.39	19	12.5	
12	10.84	12	9.13	12	8.15	8	5.56	
7	4.82	7	7.26	7	6.42	8	7.91	
5	5.68	5	4.74	5	5.73	8	6.89	
9	-	9	-	9	-	9	-	Mean of x
11	-	11	-	11	-	11	-	Variance of x
-	7.5	-	7.5	-	7.5	-	7.5	Mean of y
	4.122		4.122		4.122		4.122	Variance of y
0.816	0.816	0.816	0.816	0.816	0.816	0.816	0.816	Correlation between x and y
y = 3 + 0.5x	Linear regression line							

Visualization and Tableau Introduction, 2019

Turn Analytics into Trend Lines

Using the information/evidence you've collected to provide insights about your case

Let's look at some data ... visually!



Data Analytics Tools



AUDIT COMMAND LANGUAGE (ACL)

Another analytics tool used by auditors but can also be applied to fraud investigations. Rather than sampling the data, ACL can test 100% of the available data.

The IMPACT Model

Analytics Tools put into Action with ACL, IDEA, or Power Query

IDENTIFY THE QUESTIONS Understand the case problems that need to be addressed. MASTER THE DATA **TRACK OUTCOMES** Know what data is available and how it relates to Follow up on the results of the analysis. . the case problems. COMMUNICATE INSIGHTS PERFORM THE PLAN Communicate effectively using clear language and Select an appropriate model to find a target ********** ******** variable. visualization,.

ADDRESS & REFINE RESULTS

Identify issues with your analyses or possible issues, and refine the model.

Do you have Dirty data?

Junk in = Junk out



Sneaky Screenshots

Don't be fooled... it's not as easy as you think

ERIC	12203	ANKE KRUSE ORGANICS INC	12/22/2020	AB 3265 M	C51021	1/19/2021	1000974	HMV	820.63		
ERIC	20028	BETONSTEIN GMBH	12/22/2020	21569	B52204	1/14/2021	1000927	TLW	52845.00	Bulk Gold Purchase	
MIA	20041	BIJOUTERIE CARMEN	12/22/2020	21569	B52207	2/19/2021	1000930	HMV	790.68	Changes made by refinery	
MIA	20129	BILEVICH BOEDO	1/12/2020	G34-567	A52637	3/27/2020	1000831	TLE	1000.00		
MIA	20133	BISHOP PUBLISHING INC.	12/23/2019	82 64 1	A52638	1/25/2020	1000800	H.M.V.	18682.41		
SOUB	20133	BISHOP PUBLISHING INC.	12/27/2019	99799ABC-123	A52639	1/15/2020	1000801	HMV	2713.16		
MIA	20204	BOREAL LABORATORIES LTD	12/31/2019	AZ278	A52641	2/21/2020	1000803	TLW	54721.86		
MIA	20352	GUESS INC.	1/11/2020	81340	A52642	2/5/2020	1000828	BC	75373.66		
KSA	20403	BRIDDIG	1/8/2020	971004A	A52643	2/6/2020	1000809	СВ	6844.63		
CW	20414	CITIZEN INC.	12/25/2019	10000 A	A52644	1/20/2020	1000825	BC	4522.28		
SOUB	20508	FOSSIL INC.	1/5/2020	100139	A52645	1/29/2020	1000821	HMV	37754.37		
CW	20508	FOSSIL INC.	12/30/2019	TJ9729	A52646	1/23/2020	1000820	HMV	9620.16		
CW	20532	BTLS INTERNATIONAL	12/27/2019	000496CJW	A52647	1/21/2020	1000899	H.M.V.	64592.51		
KSA	20532	BTLS INTERNATIONAL	1/1/2020	2828 BNA	A52649	1/21/2020	1000833	TLW	1185.46		
CW	20532	BTLS INTERNATIONAL	1/2/2020	147865CTR	B52116	1/22/2020	1000863	HMV	397.05		
KSA	20535	BURKHARDT	12/30/2019	54976/10	050117	1/20/2020	100004117777	უგეკი	1 5ትናና ራን		
SOUB	20535	BURKHARDT	1/3/2020	CS - 563 -97	No searchab	le text				×	
Quick Tip: Try performing a text search in Adobe. (Ctrl+f) If you get this					This is a scanned PDF and cannot be searched. Run text recognition (OCR) to search text? you have dirty data!						
					Do not sh	ow this message ag	gain				
								Yes	No		
								12010	100100	771 ⁰	

Photo Metadata

Don't be fooled... it's not as easy as you think



Quick Tip: Check your image properties. You should be able to see the photo's metadata, if you can't...you have *dirty data*!

Cellphone Stats

- 97% of Americans own a phone (325.4 million people)
- 92% own "smart" phones
 - Up from 81% in 2019. It was 35% in 2011.
- 4 hours 25 minutes (The average time per day spent using a mobile phone)
- Average of 80 apps on phone (not all in use)
- Phones can range in size from 32GB to 1TB.

 Sources:
 https://www.consumeraffairs.com/cell_phones/cell-phone-statistics.html#:~:text=Americans%20spend%20an%20average%20of,photos%2C%20and%20surfing%20the%20internet.

 https://financesonline.com/smartphone-addiction-statistics/
 https://www.pewresearch.org/internet/2019/06/13/mobile-technology-and-home-broadband-2019/

 https://techreport.com/statistics/app-statistics/
 https://techreport.com/statistics/app-statistics/

Data Collection Challenges

Digital Forensics, eDiscovery, and Data Analytics



1



3

5

Lack Of Sufficiently Skilled IT Staff

Attorneys rely heavily on the IT Staff to collect, preserve, and analyze ESI. Without a firm understanding of what is needed and how to get ESI creates a challenge for attorneys to communicate and for IT to deliver.

Cost Of Technology

eDiscovery technology is available to clients and attorneys, however, for smaller operations and/or cases, the cost may very well be prohibitive.

Managing Data Quality & Quantity

Cloud storage and data collection software has increased ESI exponentially. The volume is diverse, often unstable, and unusable.

Deficient Information Governance (IG)

IG policies, procedures, and controls define how companies manage ESI. The eDiscovery process will yield unproductive results without an effective IG practice in place.

Cost of Review

Much of the case cost is tied to the eDiscovery process, more specifically, the review of the ESI. Attorneys estimate the eDiscovery costs to be between 70-80% of the total cost of the case.

Do you have the skills

To conduct a digital forensic/eDiscovery/data analytics investigation?



Questions?

Don't be shy!



Quotes

Quotes

11 "success usually comes to those who are too busy to be looking for it "

"



Alan Nelson, CPA, CFF, FEXCE, PI, XAMN, XRY <u>anelson@withum.com</u> 214.662.0681 Catherine Clifton, JD, SPHR <u>CC@GannawayClifton.law</u> 817.442.7133