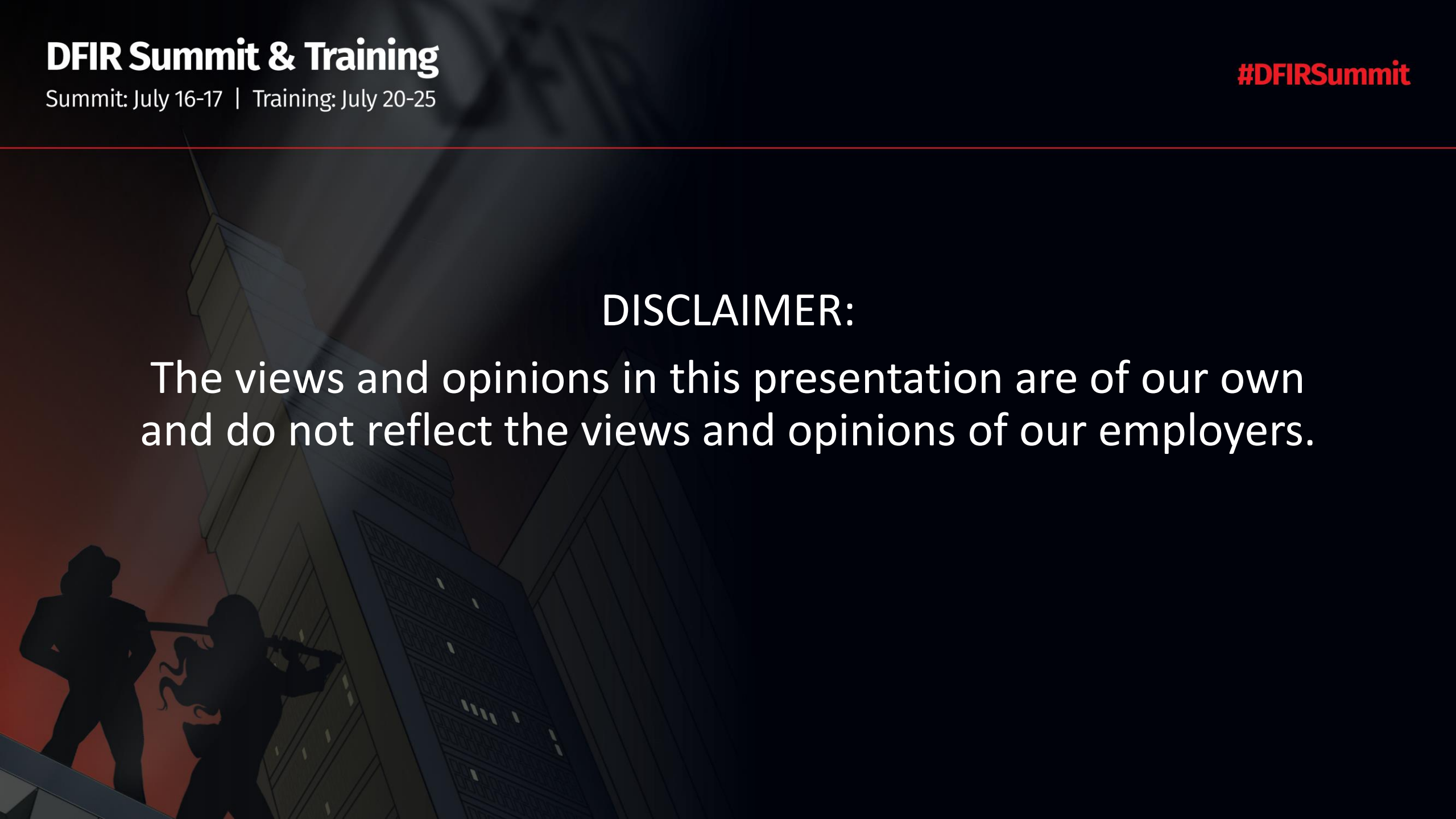
SUMMIT TALK

Forensic Marriage: The love/hate relationship between eDiscovery and DFIR

Sarah Konunchuk, CFC Response
Andrew Konunchuk, DISCO

DFIR Summit & Training | Live Online
Summit: July 16–17 | Training: July 20–25

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE



DISCLAIMER:

The views and opinions in this presentation are of our own and do not reflect the views and opinions of our employers.

What gives us the right?

- Sarah
- Senior DFIR Analyst, CFC Response
- Corporate Insider Threat investigations
- Masters degree
- Disney & Teel Tech Intern
- GCFE, GASF, GSEC, EnCE
- Social Media Obsessed
- @SarahKonun13

- Andrew
- Data Operations Specialist, DISCO
- Deloitte & Touche
- LightSpeed Legal
- Nuix, IPRO Certifications
- National Guard IT & Radio
- Reddit expert
- @AndrewKonu

Both:
Bachelor of Science in Digital Forensics
from Bloomsburg University

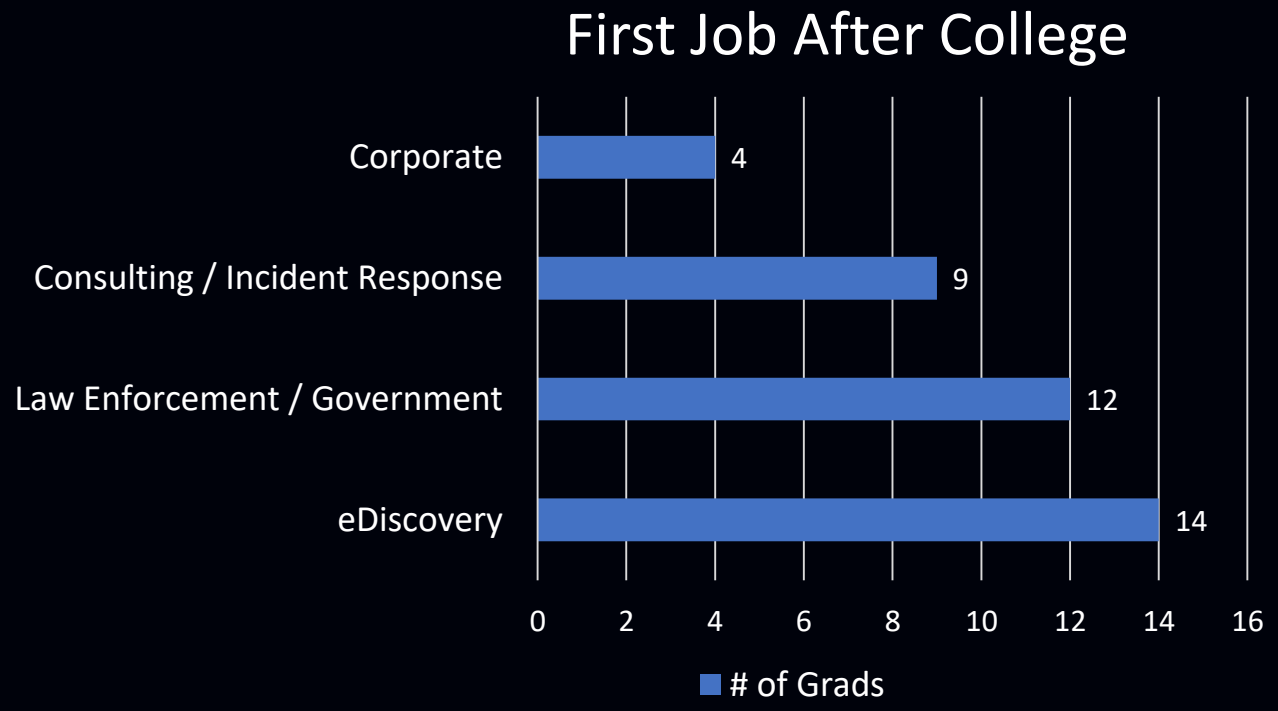
Agenda

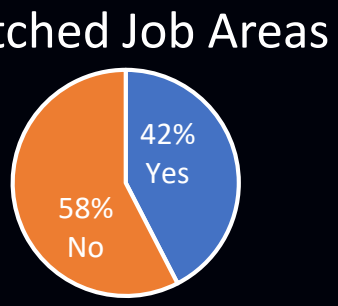
- Statistics
- Myths
- Love/Hate Relationship
- Detailed Explanation of Both
- Compare/Contrast
- Case Example

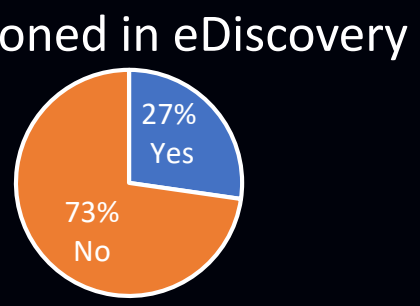
Stats from our Survey

- 7 questions
- 50% response from 2014 grads
- Students from Bloomsburg Alumni Network of 2009-2020 surveyed

- 14 eDiscovery, 25 DFIR
- 36% of students with a forensics degree get hired on in eDiscovery first
- 6 outliers from 2018-2020
- 64% of people moving jobs are to/from the eDiscovery field
- 3% myths about DFIR, whereas 30% rumors about eDiscovery







Myths about eDiscovery

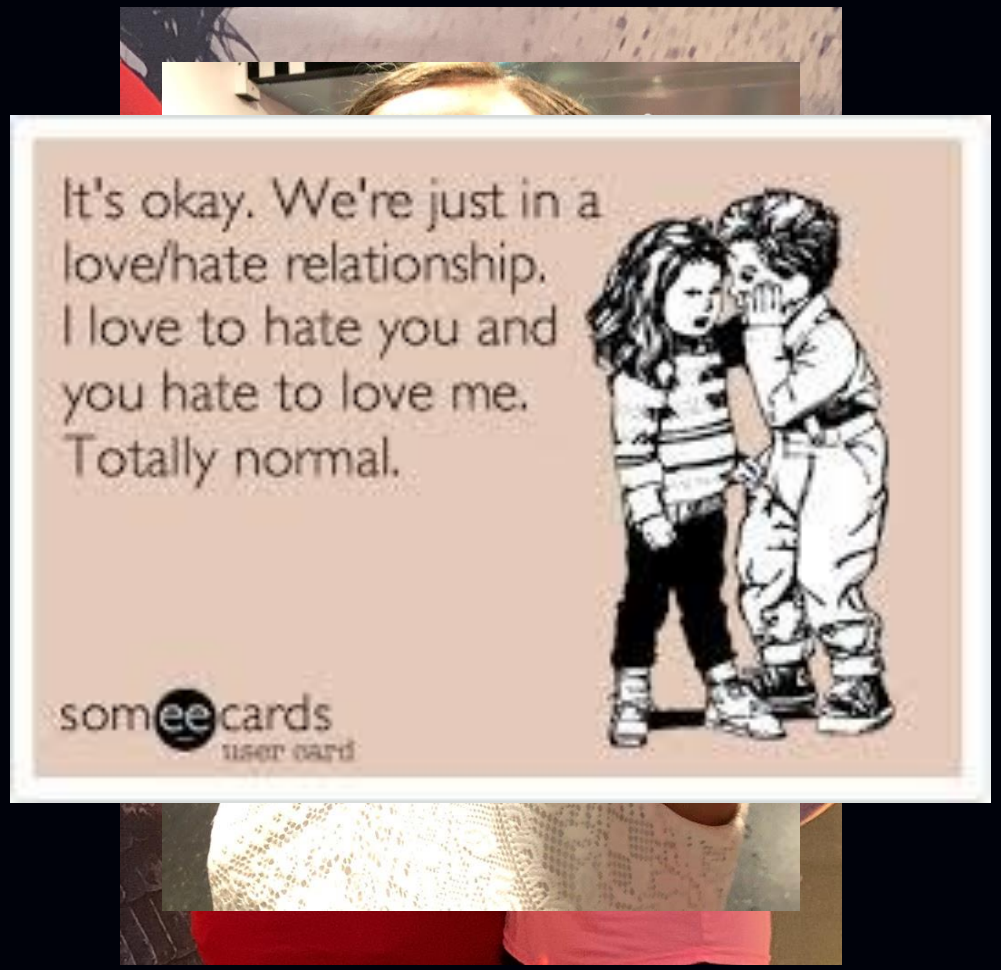
- Button pushers
- It's boring
- Won't utilize all of the forensic skill set
- Not real forensics
- Just data dumps
- Very repetitive
- Just dealing with legal
- Only looking at data and not doing investigative work
- Have I mentioned it's boring?

Myths about DFIR

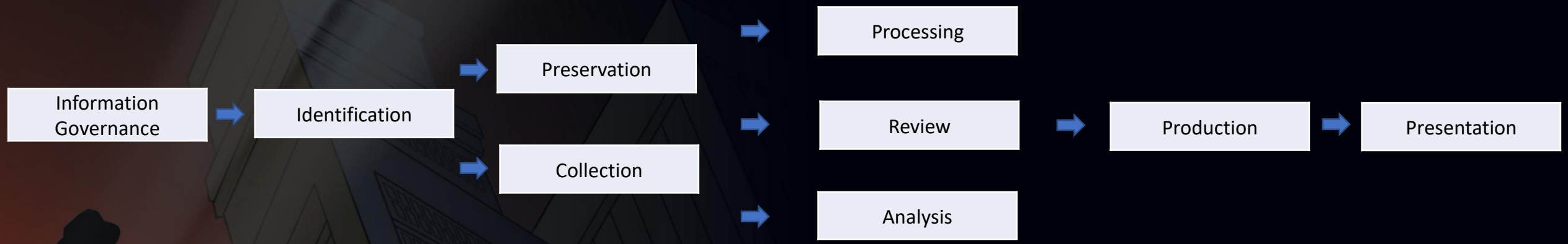
- You'll work in a SOC (Security Operations Center)
- Never see a full project start to finish
- Always looking at code to reverse engineer malware

What we love to hate about the other

"No one moves from DFIR to eDiscovery, but everyone moves from eDiscovery to DFIR."



Electronic Discovery Reference Model



Digital Forensics & Incident Response

- The process of analyzing/interpreting data from an electronic device, such as a hard drive, mobile phone, or USB.
- Name came about around the 1980s
- Really need to know the fundamentals of how a computer works
- Jobs in industry are vast
  - Different areas
    - LE, Government, IR, Consulting, corporate
  - Different subjects
    - Computer, network, memory, mobile

eDiscovery vs. DFIR

Similarities

- Involves the preservation, collection and acquisition of information or evidence
- Valuable ways to retrieve electronically stored information
- Legal and technical expertise

Differences

- Easily accessible vs. hidden/deleted
- Form of escalation
- Scalability and Complexity
- Tools used

Digital forensic stages	EDRM stages
(Preparation)	Information Governance
Identification	Identification
Preservation	Preservation
Collection	Collection
Examination	Processing
	Review
Analysis	Analysis
	Production
Presentation	Presentation

Table 1: Comparison of stages in digital forensics and eDiscovery

Case Example

- Woof CO claims Bark CO has stolen a document named “Skye.docx.”
- Skye.docx contains super sensitive information on a new dog breed
- The Kon Kompany has been hired on to investigate this matter
  - Starts w/ forensics collecting
  - Moves to eDiscovery for narrowing scope
  - Back to forensics to deep dive the 3 employees identified by eDiscovery

DFIR Summit & Training

Summit: July 16-17 | Training: July 20-25

#DFIRSummit

Resources

https://www.sans.org/reading-room/whitepapers/incident/paper/33448

https://www.edrm.net/resources/frameworks-and-standards/edrm-model/

https://brettshavers.com/brett-s-blog/entry/you-do-not-want-to-work-in-dfir

https://www.flashbackdata.com/digital-forensics-vs-ediscovery-2/

linkedin.com/in/konunchuk/
Twitter: @AndrewKonu

linkedin.com/in/sarah-konunchuk/
Twitter: @SarahKonun13

SANS DFIR