

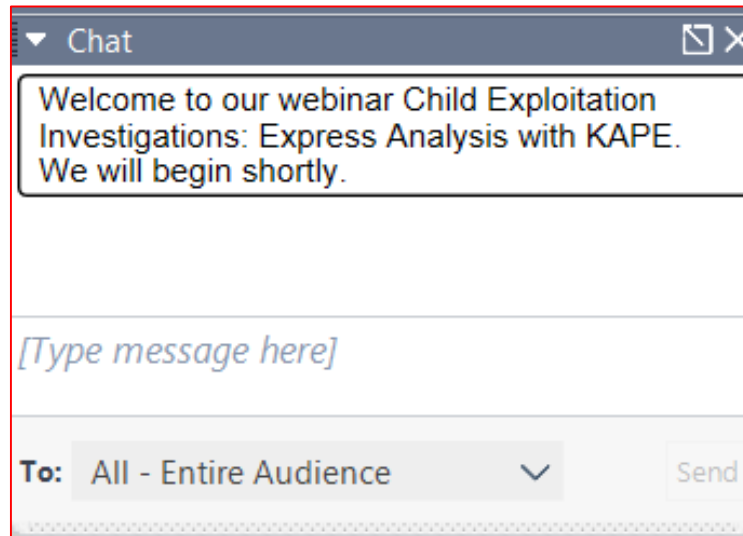
# Conducting Efficient Insider Threat Investigations using KAPE

September 2020

Private and Confidential

# Notes:

- Session is being recorded, You'll receive access to the recording in a couple days



- Ask questions via chat >

- We'll try to answer as many questions as possible

# Upcoming KAPE Intensive Training and Certification

- Virtual live sessions
- Max 25 students

[bit.ly/kape2020](https://bit.ly/kape2020)

SCHEDULE	INSTRUCTORS
September 30, 2020 10:00 a.m. – 7:00 p.m. (EST)	Eric Zimmerman Mari DeGrazia Sean Straw Scott Zuberbuehler
October 8, 2020 8:00 am – 5:00 pm (BST)	Paul Wells James Thoburn

---

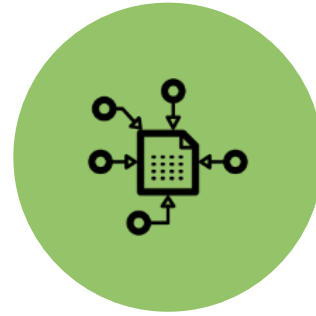
# About Tony & Aaron

- Senior Vice Presidents at Kroll
- Former in-house experience leading insider threat investigations

# Overview



Insider Threat  
Investigations



Collection Efficiency

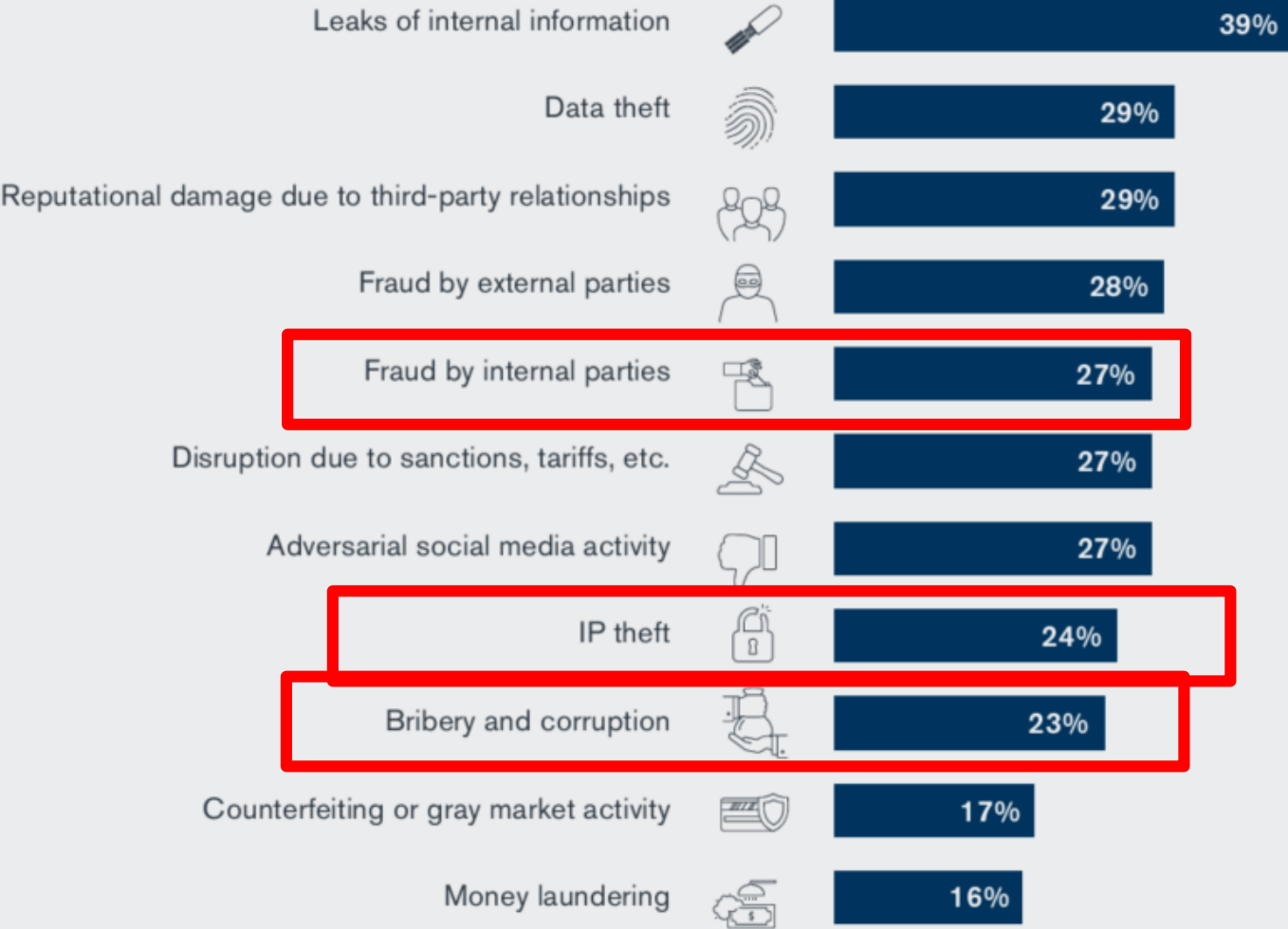


Analysis Efficiency



KAPE Case Studies

# WHICH INCIDENTS HAVE SIGNIFICANTLY AFFECTED YOUR ORGANIZATION IN THE LAST YEAR? \*



# 17%

KROLL IR CASES RELATED TO UNAUTHORIZED ACCESS

\* Kroll Global Fraud and Risk Report, 2019-20

\* Kroll internal data as of August 2020

---

# Insider Threat Investigations | Why Does This Matter?

- What is insider threat – intentional/unintentional
- Based on management, policies, etc.
- Plethora of scenarios – this affects everyone, etc.
- Time is of the essence
- Exigent circumstances – departing employees (NDAs, non competes, etc.), leaving the country, etc.
- ROI = Time = more investigations

---

KAPE

# Collection Efficiency



---

# Collection Efficiency | Overview

- KAPE targets key forensic artifacts required for analysis and runs in a matter of **minutes**
- Can be used for remote and/or automated collections
- Can be shared on a USB for single-click collections for non-technical users
- Can send to various destinations, including SFTP, S3, etc.

# Collection Efficiency | !BasicTargets








Category	Target File Contents
Event Logs	Windows Event Logs
Evidence of Execution	Prefetch RecentFileCache Amcache Syscache
File System	\$MFT \$LogFile \$UsnJrnl:\$J \$Secure:\$SDS \$Boot \$Tops:\$T
LnkFilesAndJumpLists	User Jumplist directories User Office Recent .LNK files User Recent and Desktop .LNK files Restore Point (XP) .LNK files

# Collection Efficiency | !BasicTargets




Category	Target File Contents
PowerShellConsole	ConsoleHost_history.txt
RecycleBinMetadata	Contents (including deleted files) of User Recycle Bin folders
RegistryHives	User (including UsrClass.dat) and system Registry hives and transaction logs
ScheduledTasks	SchedLgU.txt and scheduled task files
SRUM	Contents of Windows\System32\sru folder
ThumbCache	User thumbcache_*.db files
USBDevicesLogs	Setupapi.log and Setupapi.dev.log
WindowsIndexSearch	Windows.edb

# Collection Efficiency | Build a KAPE Package

## Default KAPE Files & Folders (~150 MB)

-  Documentation
-  Modules
-  Targets
-  ChangeLog.txt
-  Get-KAPEUpdate.ps1
-  gkape.exe
-  kape.exe

## Files & Folders Needed for Triage Collection (< 10mb)

-  Targets
-  kape.cli
-  kape.exe

# Collection Efficiency | \_kape.cli

```
--tsource C: --tdest .\%m --target !BasicCollection --vhdx %m
```

Argument	Value	Description
--tsource	C:	Use C:\ as the collection source
--tdest	.\%m	Write output to subfolder named by hostname in directory where KAPE is run
--target	!BasicCollection	Use the !BasicCollection set of Targets
--vhdx	%m	Write output into a VHDX file named by the hostname

# Collection Efficiency | Running KAPE

2.17%: Files remaining to be copied: 1,309 (Copied: 18 Deferred queue count: 11 Deduped count: 0 Skipped count: 0 Errors: 0)

KAPE version 0.9.3.0 Author: Eric Zimmerman (kape@kröll.com)

KAPE directory: E:\Kape

Command line: --tsource C: --tdest .\LT-11234 --target !BasicCollection --vhdx LT-11234

Using Target operations

Creating target destination directory 'E:\Kape\LT-11234'

Found 12 targets. Expanding targets to file list...

Cannot find target file 'Re

Found 1,338 files in 0.702

Deferring 'C:\Windc Copied deferred file 'C:\users\aarón.j.read\AppData\Local\Microsoft\Windows\Explorer\thumbcache\_48.db' to 'E:\Ka

Deferring 'C:\Windc pe\LT-11234\C\users\aarón.j.read\AppData\Local\Microsoft\Windows\Explorer\thumbcache\_48.db'. Hashing source file...

Deferring 'C:\Windc Copied deferred file 'C:\users\aarón.j.read\AppData\Local\Microsoft\Windows\Explorer\thumbcache\_96.db' to 'E:\Ka

Deferring 'C:\Windc pe\LT-11234\C\users\aarón.j.read\AppData\Local\Microsoft\Windows\Explorer\thumbcache\_96.db'. Hashing source file...

Deferring 'C:\Windc Copied deferred file 'C:\users\aarón.j.read\AppData\Local\Microsoft\Windows\Explorer\thumbcache\_idx.db' to 'E:\K

Deferring 'C:\Windc ape\LT-11234\C\users\aarón.j.read\AppData\Local\Microsoft\Windows\Explorer\thumbcache\_idx.db'. Hashing source file...

Deferring 'C:\Windc Copied deferred file 'C:\programdata\microsoft\search\data\applications\windows\Windows.edb' to 'E:\Kape\LT-1123

tant.evtx' due to IOExcepti4\C\programdata\microsoft\search\data\applications\windows\Windows.edb'. Hashing source file...

Deferring 'C:\Windc Copied 1,093 (Deduplicated: 245) out of 1,338 files in 193.0738 seconds. See '\*\_CopyLog.csv' in the VHD(X)/Zip located i

leshooter.evtx' due to IOEx Copied 1,093 (Deduplicated: 245) out of 1,338 files in 193.0738 seconds. See '\*\_CopyLog.csv' in the VHD(X)/Zip located i

Deferring 'C:\Windc 'E:\Kape\LT-11234' for copy details

to IOException... Initializing VHDX creation. This may take a while...

Deferring 'C:\Windc VHDX file 'E:\Kape\LT-11234\2020-09-23T185526\_LT-11234.vhdx' created.

to IOException... VHDX file 'E:\Kape\LT-11234\2020-09-23T185526\_LT-11234.vhdx' created.

Deferring 'C:\Windc Cleaning up files in 'E:\Kape\LT-11234'...

IOException... Cleaning up files in 'E:\Kape\LT-11234'...

Compressing VHDX file to 'E:\Kape\LT-11234\2020-09-23T185526\_LT-11234.zip'...

Done. Original size: 2.4GB, Compressed size: 477.7MB

Total execution time: 274.7489 seconds

E:\Kape>\_

# Collection Efficiency | Storage/Transfer Options

- Local drive (USB)
- Network share
- Transfer to SFTP, S3, Azure, etc.

The screenshot shows a configuration window with two tabs: "Target variables" and "Transfer options". The "Transfer options" tab is active. At the top right, there are two checked checkboxes: "Zip container" and "Transfer". Below the tabs, there are three selection buttons: "SFTP", "S3", and "Azure storage". The "SFTP" button is highlighted with a red border. Below these buttons are several input fields: "Server" (Required), "Port" (22), "Comment", "Username" (Required), and "Password".

Field	Value/Requirement
Server	Required
Port	22
Comment	
Username	Required
Password	

---

KAPE

# Analysis Efficiency



# Analysis Efficiency

```
Description: 'LECcmd: process .lnk files'  
Category: FileFolderAccess  
Author: Eric Zimmerman  
Version: 1  
Id: 1b66f0e2-2ccf-449c-ae02-a1b3dc59df08  
BinaryUrl: https://f001.backblazeb2.com/file/EricZimmermanTools/LECcmd.zip  
ExportFormat: csv  
Processors:  
-  
  Executable: LECcmd.exe  
  CommandLine: -d %sourceDirectory% --csv %destinationDirectory% -q  
  ExportFormat: csv  
-  
  Executable: LECcmd.exe  
  CommandLine: -d %sourceDirectory% --html %destinationDirectory% -q  
  ExportFormat: html  
-  
  Executable: LECcmd.exe  
  CommandLine: -d %sourceDirectory% --json %destinationDirectory% -q  
  ExportFormat: json
```

## What are Modules?

- The actual “processing” of the artifacts you collected
- Grouped in Categories

## Can be Tailored

- What works for someone may not work for you
- Special Programs/Scripts can be utilized

---

# Creating a Module

- Benefits of KAPE:
  - Open Sourced
  - Well Documented
  - Modules written in YAML
  - Frequently Updated by Community
  - Internally Created do not need to be shared
  - Select the Result format for your needs
  - Automation and Speed
  - Small Storage Footprint
- Creating the Internal Toolkit:
  - Proprietary based Investigations
  - Create Case Specific Modules
    - » Run certain processes for certain investigations
  - If its Command Line, you can run it

---

KAPE

## Case Studies

- Intellectual Property Theft
- Exceeding Authorized Authority
- Custom Targets

---

# Case Study – Intellectual Property Theft

- A senior engineer recently left the company and created his own business with a competing product offering.
- You are requested to determine if evidence exists that the engineer took data leading up to their departure.
- Artifacts of Interest:
  - USB Devices
  - File/Folder Access
  - Program Execution

# Case Study – Intellectual Property Theft – USB Devices

## Module: Registry\RECmd

HiveType	Description	Category	KeyPath	Deleted	LastWriteTimestamp
System	USB Devices	USB Devices	\ControlSet001\Enum\USBSTOR\Disk&Ven_SanDisk&Prod_Extreme&Rev_0001	FALSE	03/27/2018 09:22:22
System	USB Devices	USB Devices	\ControlSet001\Enum\USBSTOR\Disk&Ven_SanDisk&Prod_Extreme&Rev_0001\AA010215170355310594&0	FALSE	03/27/2018 09:22:22
System	USB Devices	USB Devices	\ControlSet001\Enum\USBSTOR\Disk&Ven_SanDisk&Prod_Extreme&Rev_0001\AA010603160707470215&0	FALSE	03/27/2018 09:22:22

## Module: Event Logs

TimeCreated	EventId	Channel	MapDescription	PayloadData3
03/27/2018 09:22:13	1006	Microsoft-Windows-Partition/Diagnostic	USB Insertion/Removal	ParentId: USB\VID_0781&PID_5580\AA010215170355310594
03/27/2018 09:22:22	1006	Microsoft-Windows-Partition/Diagnostic	USB Insertion/Removal	ParentId: USB\VID_0781&PID_5580\AA010603160707470215
03/27/2018 09:56:22	1006	Microsoft-Windows-Partition/Diagnostic	USB Insertion/Removal	ParentId: USB\VID_0781&PID_5580\AA010603160707470215
03/27/2018 12:11:42	1006	Microsoft-Windows-Partition/Diagnostic	USB Insertion/Removal	ParentId: USB\VID_0781&PID_5580\AA010215170355310594

# Case Study – Intellectual Property Theft – File/Folder Access

Module: File-Folder Access\Shellbags

AbsolutePath	CreatedOn	ModifiedOn	FirstInteracted	LastInteracted
Desktop\D:\			3/27/2018 9:22	3/27/2018 9:22
Desktop\D:\\Project-912328	1/12/2018 15:31	12/20/2017 11:12		
Desktop\D:\\Project-547891	2/1/2018 11:14	12/16/2017 16:22		
Desktop\D:\\Project-672341	3/11/2018 14:50	3/1/2018 12:50		3/27/2018 9:23
Desktop\D:\\Project-672341\Schematics	3/11/2018 14:51	3/1/2018 21:12		3/27/2018 9:23
Desktop\D:\\Project-672341\Project_Plan	3/11/2018 14:52	3/1/2018 11:34	3/27/2018 9:23	3/27/2018 9:23
Desktop\D:\\Project-672341\Parts	3/11/2018 14:53	3/1/2018 11:34		
Desktop\E:\			3/27/2018 9:23	3/27/2018 9:50
Desktop\E:\\Project-672341	3/27/2018 9:23	3/1/2018 12:50		3/27/2018 9:50
Desktop\E:\\Project-672341\Schematics	3/27/2018 9:24	3/1/2018 21:12		
Desktop\E:\\Project-672341\Project_Plan	3/27/2018 9:25	3/1/2018 11:34		
Desktop\E:\\Project-672341\Parts	3/27/2018 9:26	3/1/2018 11:34		

# Case Study – Intellectual Property Theft – Program Execution

Module: Registry\UserAssist

BatchValueName	ProgramName	RunCounter	LastExecuted
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\abgrcnq.rkr	{System32}\notepad.exe	7	03/27/2018 09:23:15
Zvpebfbsg.ZvpebfbsgRqtr_8jrxlo3q8oojr!ZvpebfbsgRqtr	Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge	1	03/27/2018 09:28:51
P:\Hfref\wpybhql\Qbjaybnqf\vafgnyyonpxhcnaqflap.rkr	C:\Users\jcloudy\Downloads\installbackupandsync.exe	1	03/27/2018 10:40:33
P:\Hfref\wpybhql\Qbjaybnqf\Renfre 6.2.0.2982.rkr	C:\Users\jcloudy\Downloads\Eraser 6.2.0.2982.exe	1	03/27/2018 10:43:48
P:\Cebtenz Svyrf\Renfre\Renfre.rkr	C:\Program Files\Eraser\Eraser.exe	1	03/27/2018 10:51:12
P:\Hfref\Choyvp\Qrfxgbc\Renfre.yax	C:\Users\Public\Desktop\Eraser.lnk	1	03/27/2018 10:51:12

---

# Case Study – Exceeding Authorized Access

- Alert received for IT employee emailing sensitive data outside of the company.
- You are requested to determine what the materials are and where they came from.
- Artifacts of Interest:
  - LNK Files
  - \$MFT



# Case Study – Exceeding Authorized Access – File/Folder Access

## Module: FileFolderAccess\LECmd

SourceFile	SourceCreated	SourceModified	WorkingDirectory	MachineID
D:\users\djones\AppData\Roaming\Microsoft\Windows\Recent\Profile Pic.jpg	6/6/2020 11:45	6/6/2020 11:45	\\dt-cperry\c\$\users\cperry\Desktop\Profile Pic.jpg	dt-cperry
D:\users\djones\AppData\Roaming\Microsoft\Windows\Recent\Perry Taxes.pdf	6/6/2020 11:47	6/6/2020 11:47	\\dt-cperry\c\$\users\cperry\Documents\Taxes\2019\Perry Taxes.pdf	dt-cperry
D:\users\djones\AppData\Roaming\Microsoft\Windows\Recent\EmployeeDetails20200101.xlsx	6/6/2020 11:51	6/6/2020 11:51	\\dt-cperry\c\$\users\cperry\Documents\Projects\HR\EmployeeDetails20200101.xlsx	dt-cperry
D:\users\djones\AppData\Roaming\Microsoft\Windows\Recent\All.Employee.Listing.2020-03-01.csv	6/6/2020 9:37	6/6/2020 9:37	\\dt-ljones\c\$\users\ljones\Documents\All.Employee.Listing.2020-03-01.csv	dt-ljones
D:\users\djones\AppData\Roaming\Microsoft\Windows\Recent\Img6001.jpg	6/6/2020 12:49	6/6/2020 12:49	\\lt-sjohnson\c\$\users\sjohnson\OneDrive\Documents\Pics\Img6001.jpg	lt-sjohnson
D:\users\djones\AppData\Roaming\Microsoft\Windows\Recent\Img5123.jpg	6/6/2020 12:53	6/6/2020 12:53	\\lt-sjohnson\c\$\users\sjohnson\OneDrive\Documents\Pics\Img5123.jpg	lt-sjohnson
D:\users\djones\AppData\Roaming\Microsoft\Windows\Recent\Img5124.jpg	6/6/2020 12:54	6/6/2020 12:54	\\lt-sjohnson\c\$\users\sjohnson\OneDrive\Documents\Pics\Img5124.jpg	lt-sjohnson

# Case Study – Exceeding Authorized Access – File/Folder Access

Module: FileSystem\MFTECmd\_\$\$MFT

ParentPath	FileName	Extension	Created0x10	Created0x30	LastModified0x10	LastModified0x30
.\Users\djones\Downloads\Tickets\cperry	Profile Pic.jpg	.jpg	06/06/2020 11:45	06/06/2020 11:45	03/30/2020 22:49	03/30/2020 22:49
.\Users\djones\Downloads\Tickets\cperry	Perry Taxes.pdf	.pdf	06/06/2020 11:47	06/06/2020 11:47	05/02/2020 14:01	05/02/2020 14:01
.\Users\djones\Downloads\Tickets\cperry	EmployeeDetails20200101.xlsx	.xlsx	06/06/2020 11:51	06/06/2020 11:51	01/03/2020 08:00	01/03/2020 08:00
.\Users\djones\Downloads\Tickets\ljones	All.Employee.Listing.2020-03-01.csv	.csv	06/06/2020 09:37	06/06/2020 09:37	03/01/2020 16:24	03/01/2020 16:24
.\Users\djones\Downloads\Tickets\sjohnson	Img6001.jpg	.jpg	06/06/2020 12:49	06/06/2020 12:49	5/27/2020 9:12	05/27/2020 09:12
.\Users\djones\Downloads\Tickets\sjohnson	Img5123.jpg	.jpg	06/06/2020 12:53	06/06/2020 12:53	5/1/2020 14:32	05/01/2020 14:32
.\Users\djones\Downloads\Tickets\sjohnson	Img5124.jpg	.jpg	06/06/2020 12:54	06/06/2020 12:54	5/1/2020 14:32	05/01/2020 14:32
.\Users\djones\Downloads\Tickets	tickets_6-6-20.7z	.7z	06/06/2020 13:37	06/06/2020 13:37	06/06/2020 13:37	06/06/2020 13:37

---

# Case Study – Custom Target/Modules

- Corporate Proprietary Investigation
  - Not an IR Event
- Geographically separated
  - No Travel permitted
- User may have stored IP in folders throughout the OS Structure
  - Files had a unique file extension
- Needed to be as forensically sound as possible
  - Kape created .zip file + password protection

---

# Case Study – Custom Target/Modules – What We Did

- Created a unique Target that would look for specific file extension
- Created a unique Module for fast processing of specific artifacts
- Remoted into the machine when the user had the machine on network
- Initiated KAPE Target to pull the artifacts
- Ran KAPE Module to process the artifacts needed, which included a nice file listing
- On the machine for less than 10 minutes
- Processing of the Targeted artifacts took even less than that
- Customer was provided preliminary reports within 8 hours of our involvement

---

# Case Study – Custom Target/Modules – Quick Wins

- Insider Threat allegation was substantiated very quickly
- Amount of dwell time was minimal
  - customer was not even prepared for returned results
- No Expenses
  - Saved thousands of dollars alone on no expenses needed
- Internally proved the tool could be leveraged for more than just IR
  - Tailoring to specific files relevant to the matter
- Tailoring the tool saved countless hours on the target system
  - User never knew we were there

---

# Questions



# For More **KAPE**: Intensive Training and Certification

- Virtual live sessions
- Max 25 students

[bit.ly/kape2020](https://bit.ly/kape2020)

SCHEDULE	INSTRUCTORS
September 30, 2020 10:00 a.m. – 7:00 p.m. (EST)	Eric Zimmerman Mari DeGrazia Sean Straw Scott Zuberbuehler
October 8, 2020 8:00 am – 5:00 pm (BST)	Paul Wells James Thoburn

For more information about our global locations and services, please visit:

[www.kroll.com](http://www.kroll.com)

#### About Kroll

Kroll is the leading global provider of risk solutions. For more than 45 years, Kroll has helped clients make confident risk management decisions about people, assets, operations and security through a wide range of investigations, cyber security, due diligence and compliance, physical and operational security, and data and information management services. For more information, visit [www.kroll.com](http://www.kroll.com).

#### About Duff & Phelps

Duff & Phelps is the global advisor that protects, restores and maximizes value for clients in the areas of valuation, corporate finance, investigations, disputes, cyber security, compliance and regulatory matters, and other governance-related issues. We work with clients across diverse sectors, mitigating risk to assets, operations and people. With Kroll, a division of Duff & Phelps since 2018, our firm has nearly 3,500 professionals in 28 countries around the world. For more information, visit [www.duffandphelps.com](http://www.duffandphelps.com).