



Forensic Investigation

For my capstone I had to perform a forensic investigation

Overview

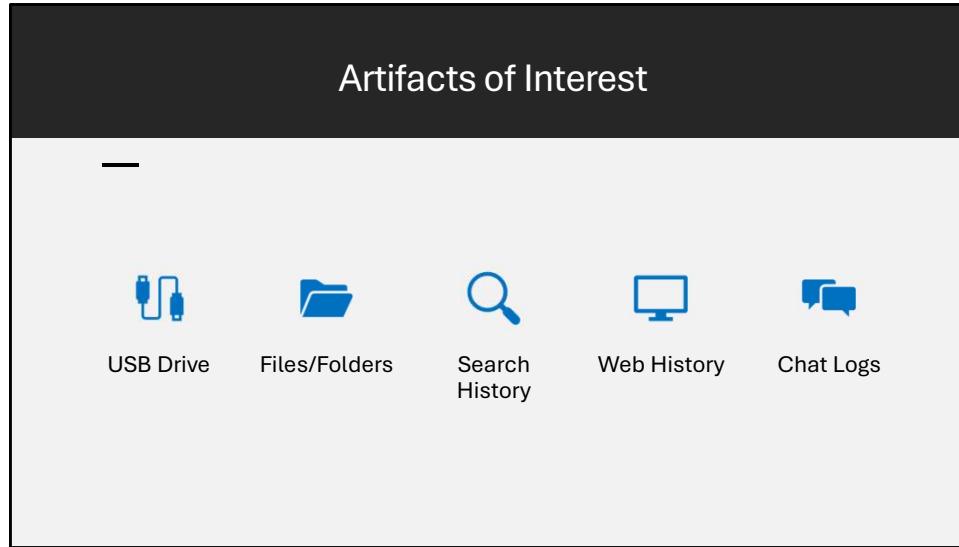
Ever since the CEO's RTO mandate was announced on June 26th Manager A's supervisor, Senior Manager, has noticed that his performance has not been up to standard.

Senior Manager has spoken with the General Manager, but no decision has been made about placing Manager A on leave without pay. HR has given Cyber permission to investigate Manager A's laptop.



Manager A's performance has been down ever since CEO's RTO mandate.

I have completed a week of Magnet AXIOM training, and I have been tasked with remotely capturing an image of the laptop. I used AXIOM Process and Examine to process and analyze the image. The timeline for the investigation is June 26th to July 15th.

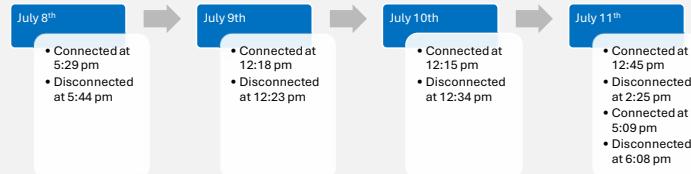


5 artifact types that I discovered during my investigation

USB Artifact

VendorCo ProductCode USB Device

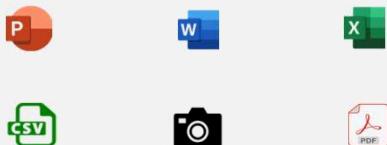
- Was assigned drive letter E:
- First connected on 7/8 at 5:29 pm
- Had a series of 5 connects and disconnects



VendorCo ProductCode USB Device is the name of this usb.
This usb device was leveraged across multiple days as shown

File Types on USB

Corporate Shared Drive → C:
Drive → E: Drive



These are the file types that were transferred to the USB

All the files on the USB originated from the company's corporate shared drive then they were copied to the C: drive,
and finally they were copied to the E: drive which is the USB device

Due to internal use only data classification, I can only provide an overview of the content

Files on USB

- Files contained customer billing info
- There were other files containing pertinent information



These files were opened on the USB on July 11

These files had .lnk files on the USB

One file was corrupted

Due to internal use only data classification, I can only provide an overview of the content

Files on USB

- Files contained images from a generating station
- Financial information
- C-Staff information

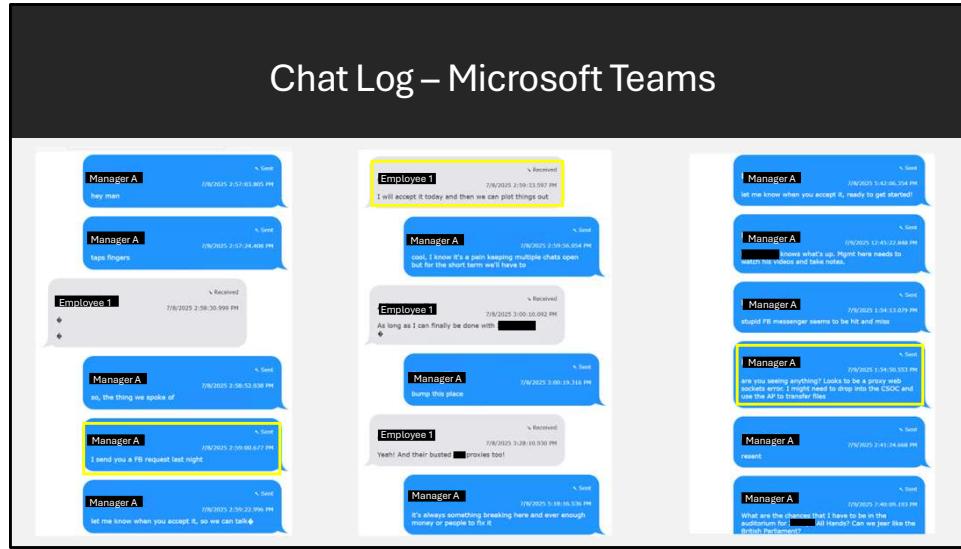


These files were also opened on the USB on July 11th

These files did not have .lnk files present on the drive, but I found evidence of them being opened after they were copied

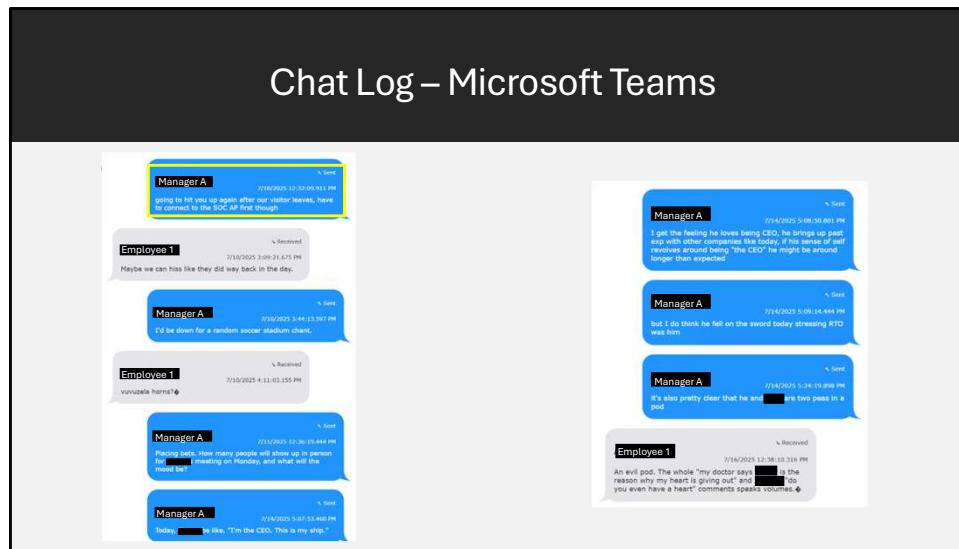
All the files that were transferred to the USB originated in file path **Users***\Documents\research**

Due to internal use only data classification, I can only provide an overview of the content



Conversation between Manager A and Employee 1

Chat Log – Microsoft Teams

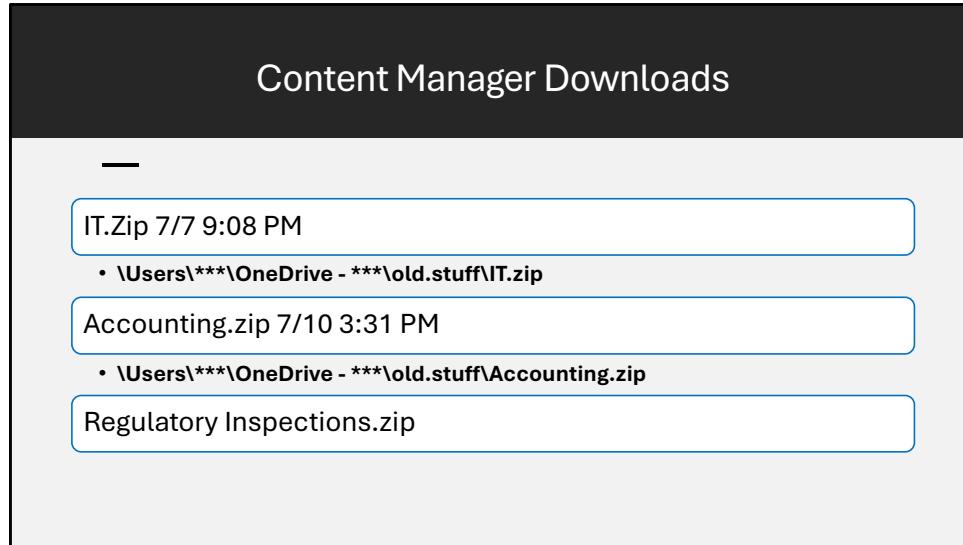


Facebook URL Artifacts

- There were 156 hits for Facebook URL Artifacts
- Facebook was visited using Chrome and Edge.
- User was checking Facebook friend requests on 7/8 5:32 pm

 Facebook URLs 156

As previously stated, the timeline for the investigation is June 26th to July 15th.



These three files were downloaded from the content manager
The first two files were uploaded to OneDrive to Manager A's account

Chrome Artifacts – Web History

No more hybrid schedules for state workers as remote work slashed | News From The States

How rising 'return to office' calls might effect SC differently than other states

HR-17.09,
"Telecommuting

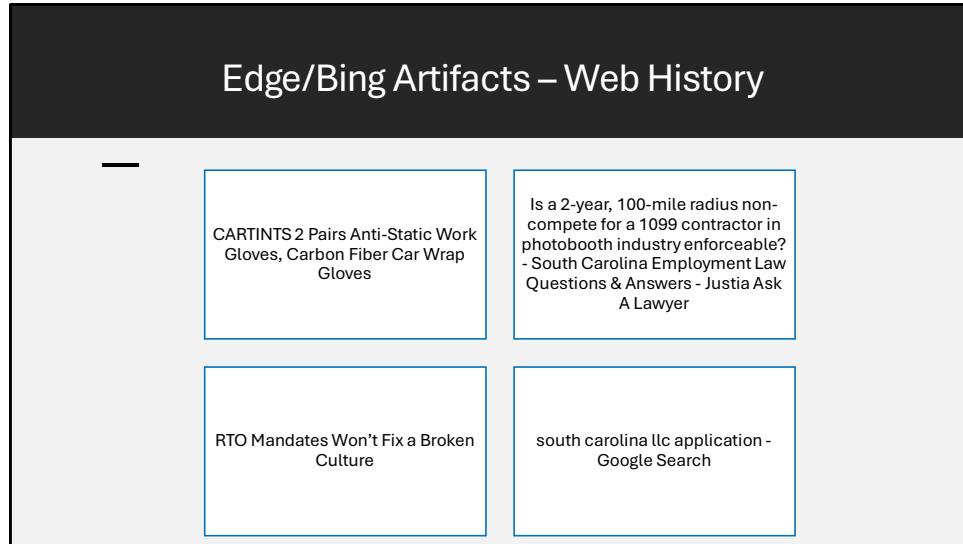
How to Get an LLC
and Make a Limited Liability Company

These are artifacts from the chrome web history

Chrome Artifacts – Google Searches



This slide contains Google search history



Here are some of the Edge Web History Artifacts

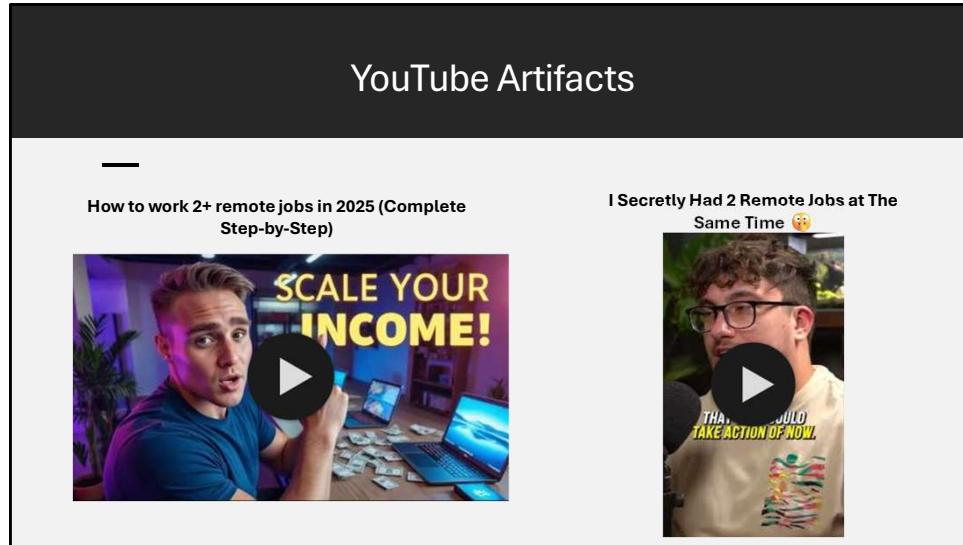
Edge/Bing Artifacts – Web History

17 hits for Indeed

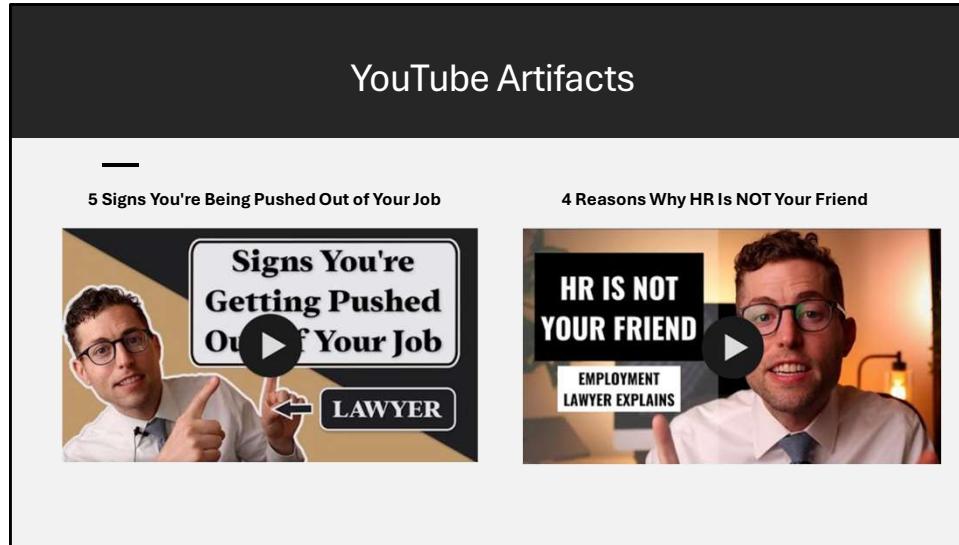
2 hits for legal
searches regarding
RTO

Flexible Cyber Security Manager \$130,000 Jobs – Apply Today to Work From Home

Legal searches: bcattorneys.com



These YouTube videos were accessed through edge
The first youtube video is from Youtuber Delaney William
The second video is a youtube short from Caleb Hammer



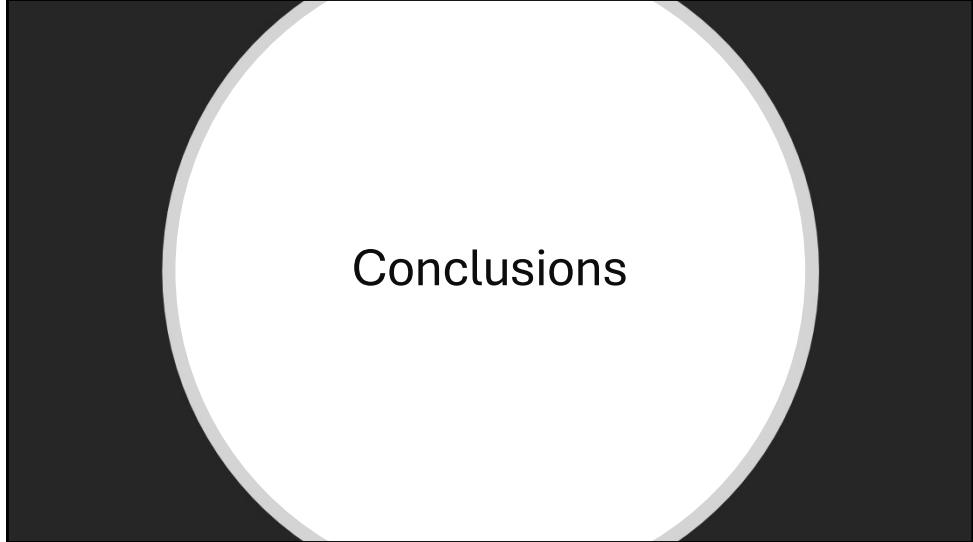
Both of these youtube videos are made by an employment attorney Ed Hones.

1. This youtube video explain tactics employers may use to cause a “Constructive Discharge”
 1. Constructive discharge is a tactic used to make working conditions intolerable so an employee will leave
 2. Offers legal advice
2. This video details how HR is there to protect the company, but not the employees. It offers legal advice on how an employee can protect themselves.

Edge & Chrome Keyword Search Terms

	Keyword Search Term	URL	Last Visited Date/Time	Artifact type
1	how to balance two remote jobs	https://www.google.com/search?q=how+to+balance+two+remote+jobs	7/9/2025 7:49:34.815 PM	Edge Keyword Search Terms
2	legal protections when leaving a company	https://www.google.com/search?q=legal+protection+when+leaving+a+company	7/7/2025 3:54:43.491 PM	Edge Keyword Search Terms

	Keyword Search Term	URL	Last Visited Date/Time	Artifact type
1	can you sue your state over rto	https://www.google.com/search?q=can+you+sue+your+state+over+rto	7/3/2025 12:35:00.524 PM	Chrome Keyword Search Terms



Conclusions

Takeaways

How digital forensic software works

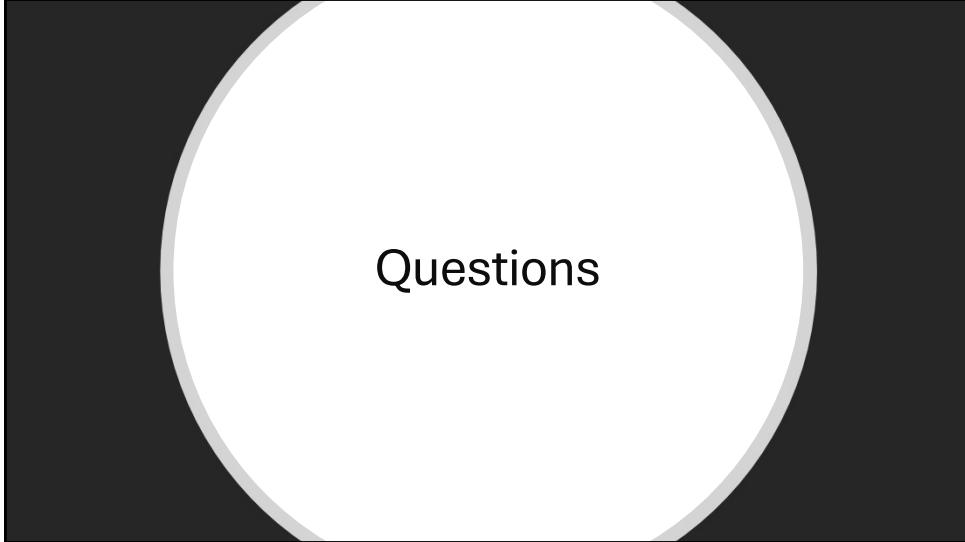
Never assume anything

User activities are recorded in the Registry

Logs are kept of deleted files

Look at the bigger picture

As a digital forensic analyst, you should never assume anything because that can cause you to overlook data or misinterpret results from your own bias. Making assumptions can lead to false accusations, and that can compromise an investigation. It's important to stay unbiased and only rely on evidence.



Questions

Does anyone have any questions?