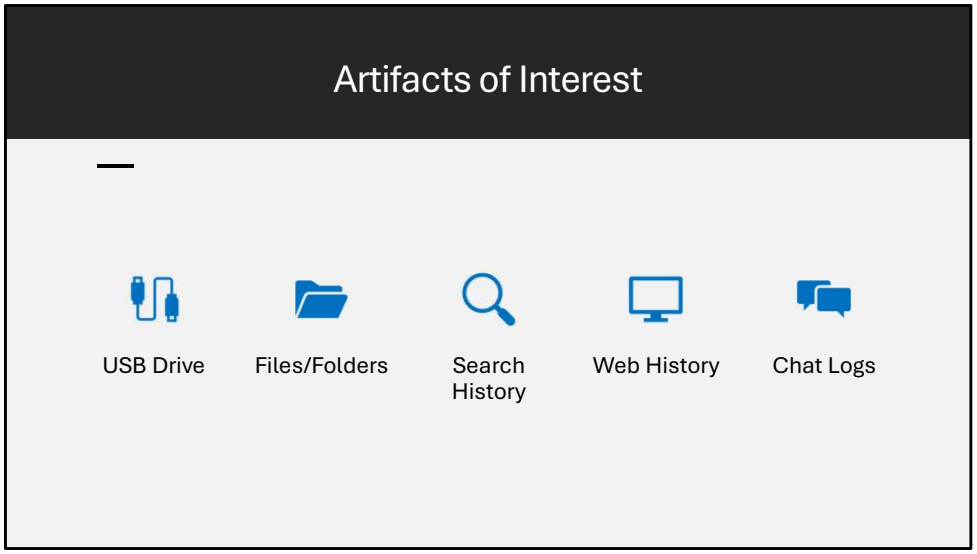
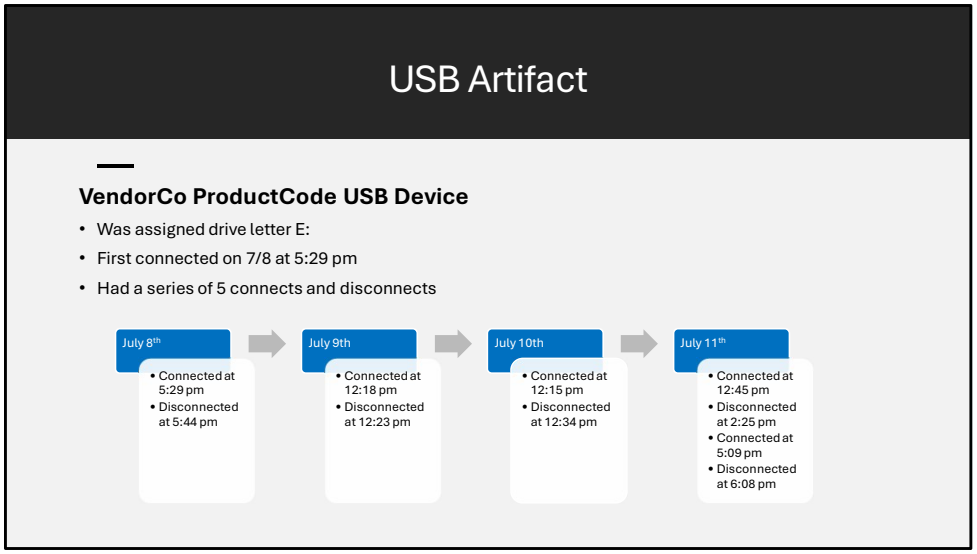
For my capstone I had to perform a forensic investigation

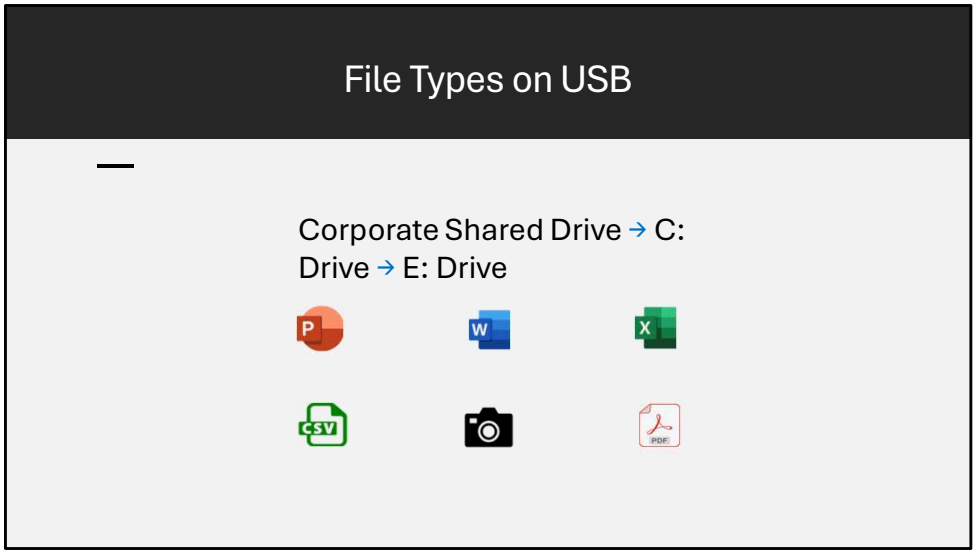
Manager A's performance has been down ever since CEO's RTO mandate.
I have completed a week of Magnet AXIOM training, and I have been tasked with remotely capturing an image of the laptop. I used AXIOM Process and Examine to process and analyze the image.
The timeline for the investigation is June 26th to July 15th.



5 artifact types that I discovered during my investigation



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

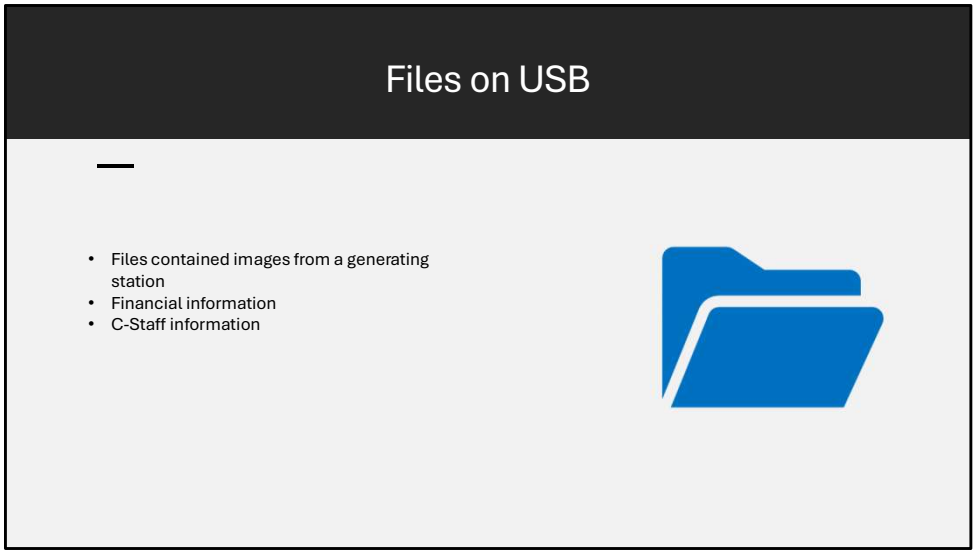


These are the file types that were transferred to the USB
All the files on the USB originated from the company's corporate shared drive then they were copied to the C: drive, and finally they were copied to the E: drive which is the USB device
Due to internal use only data classification, I can only 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 was corrupted
Due to internal use only data classification, I can only provide an overview of the content



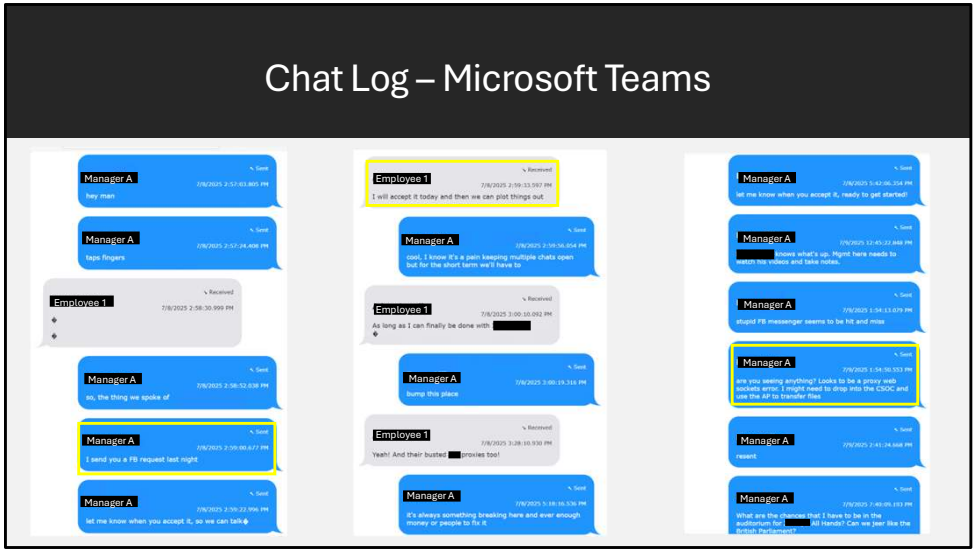
These files were also opened on the USB on July 11th

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**

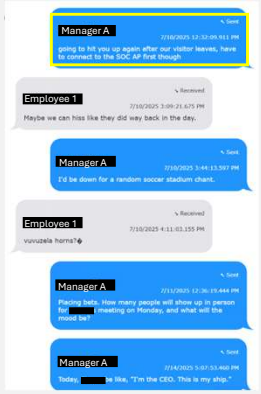
Due to internal use only data classification, I can only provide an overview of the content

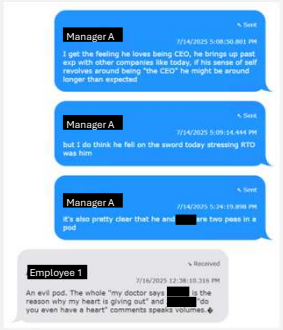
Chat Log – Microsoft Teams



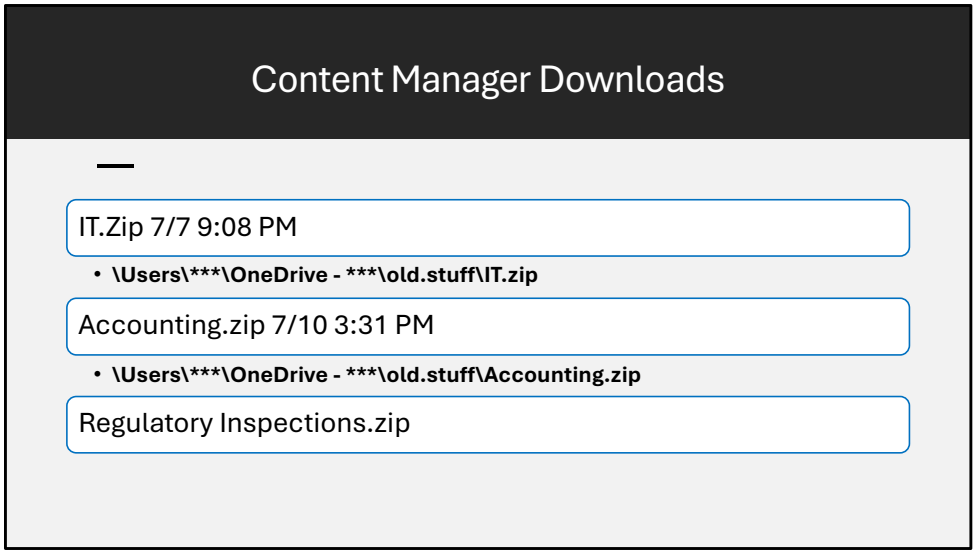
Conversation between Manager A and Employee 1

Chat Log – Microsoft Teams

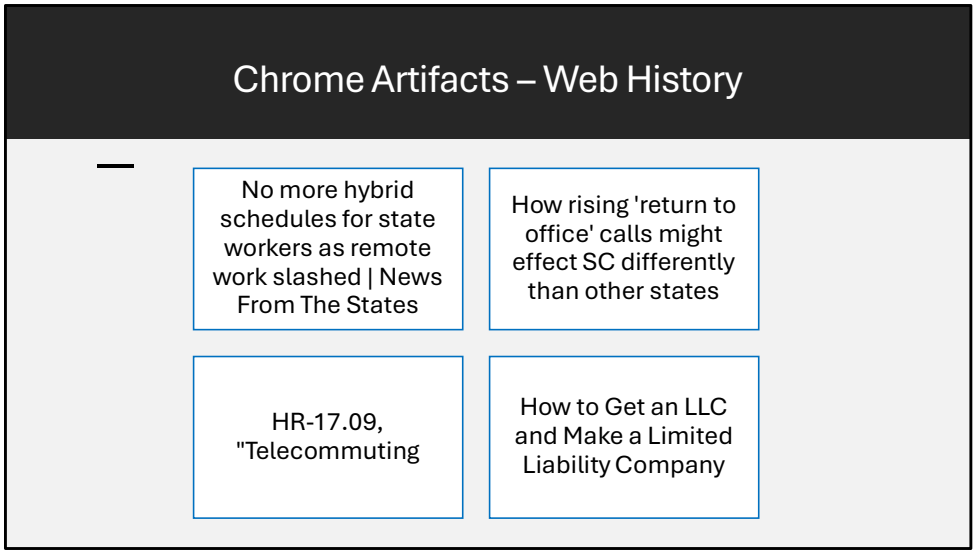




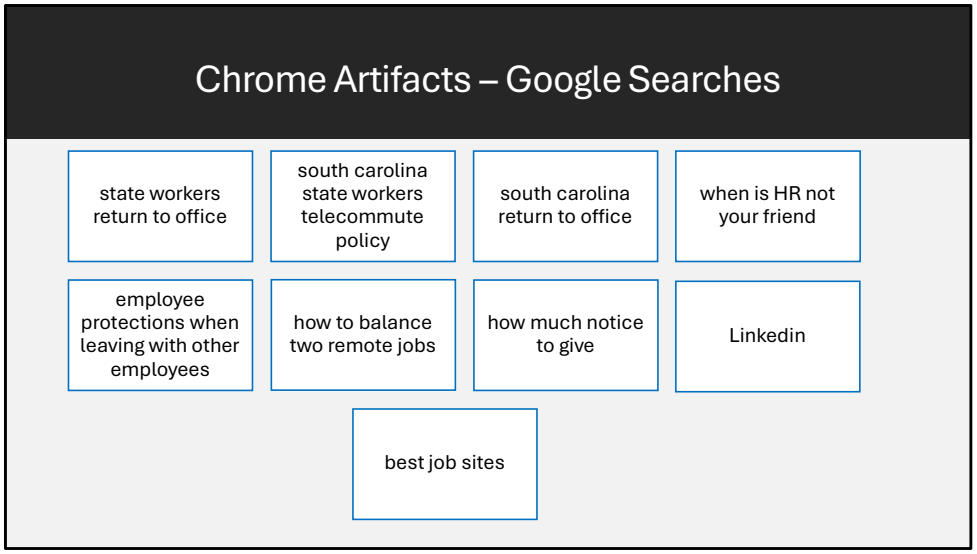
As previously stated, the timeline for the investigation is June 26th to July 15th.



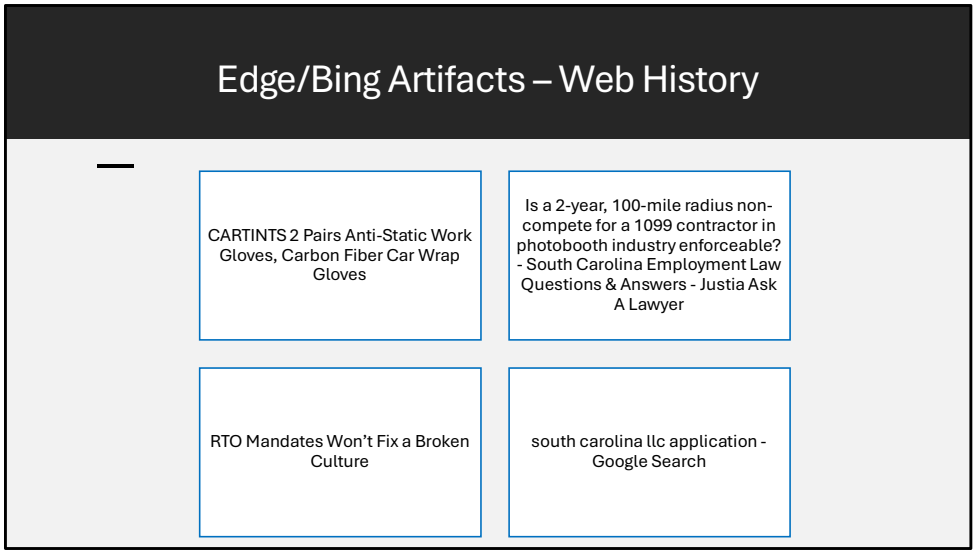
These three files were downloaded from the content manager
The first two files were uploaded to OneDrive to Manager A's account



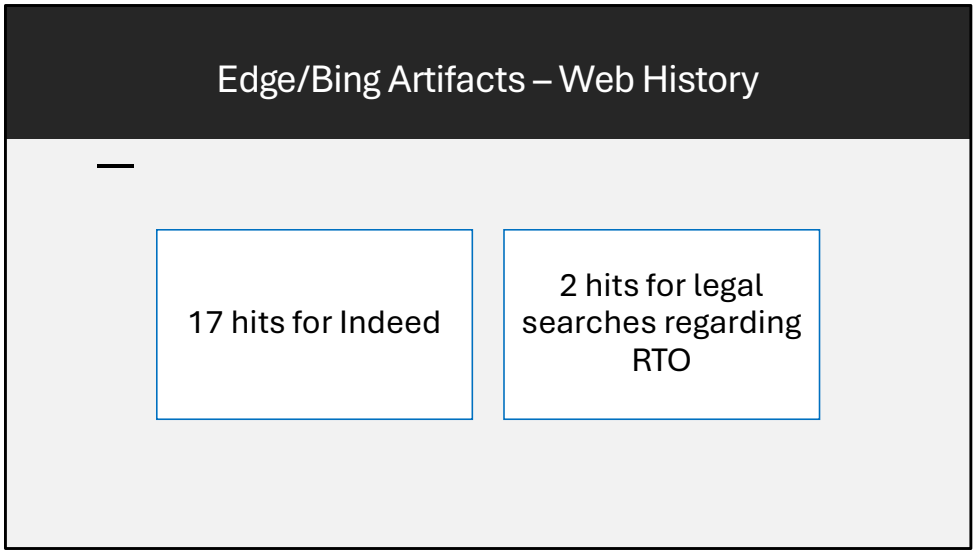
These are artifacts from the chrome web history



This slide contains Google search history



Here are some of the Edge Web History Artifacts



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

Legal searches: bcattorneys.com

YouTube Artifacts

How to work 2+ remote jobs in 2025 (Complete Step-by-Step)

I Secretly Had 2 Remote Jobs at The Same Time 😱

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

YouTube Artifacts

5 Signs You're Being Pushed Out of Your Job

4 Reasons Why HR Is NOT Your Friend

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

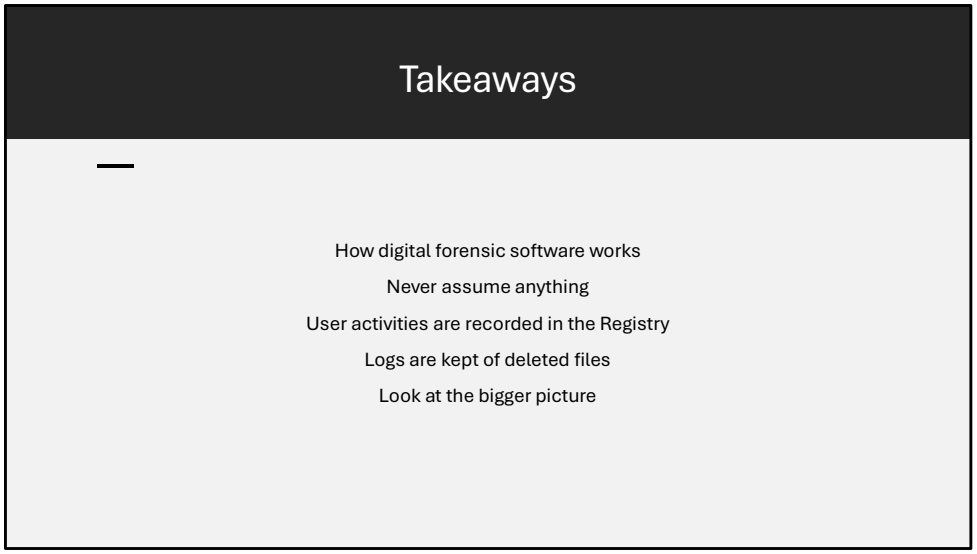
1. This youtube video explain tactics employers may use to cause a “Constructive Discharge”’
    1. Constructive discharge is a tactic used to make working conditions intolerable so an employee will leave
    2. Offers legal advice
2. This video details how HR is there to protect the company, but not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

Edge & Chrome Keyword Search Terms

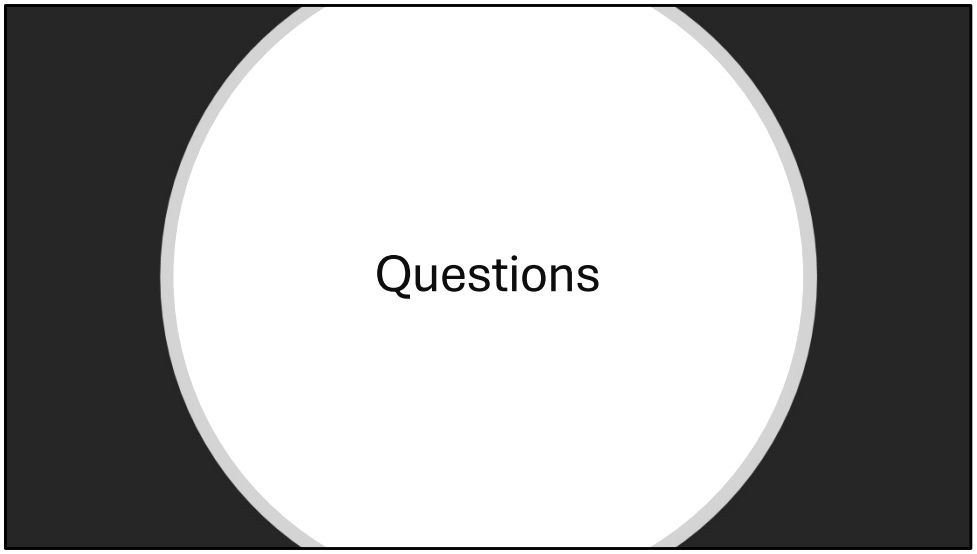
Keyword Search Term	URL	Last Visited Date/Time	Artifact type
how to balance two remote jobs	https://www.google.com/search?q=how+to+balanc...	7/9/2025 7:49:34.815 PM	Edge Keyword Search Terms
legal protections when leaving a company	https://www.google.com/search?q=legal+protectio...	7/7/2025 3:54:43.491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

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

Conclusions



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.



Does anyone have any questions?