***Shubham Paikrao***

# Digital Forensics Walkthrough – Investigating Data Exfiltration

## 🎯 Case Summary:

A critical data leak occurred at the company. Suspicion falls on Liam, a recently terminated system engineer. Given his access level, odd working hours, and suspicious behavior (e.g., taking photos near the server room), I was tasked with analyzing his workstation disk image using Autopsy to uncover evidence. Here's a full breakdown of my investigation:

---

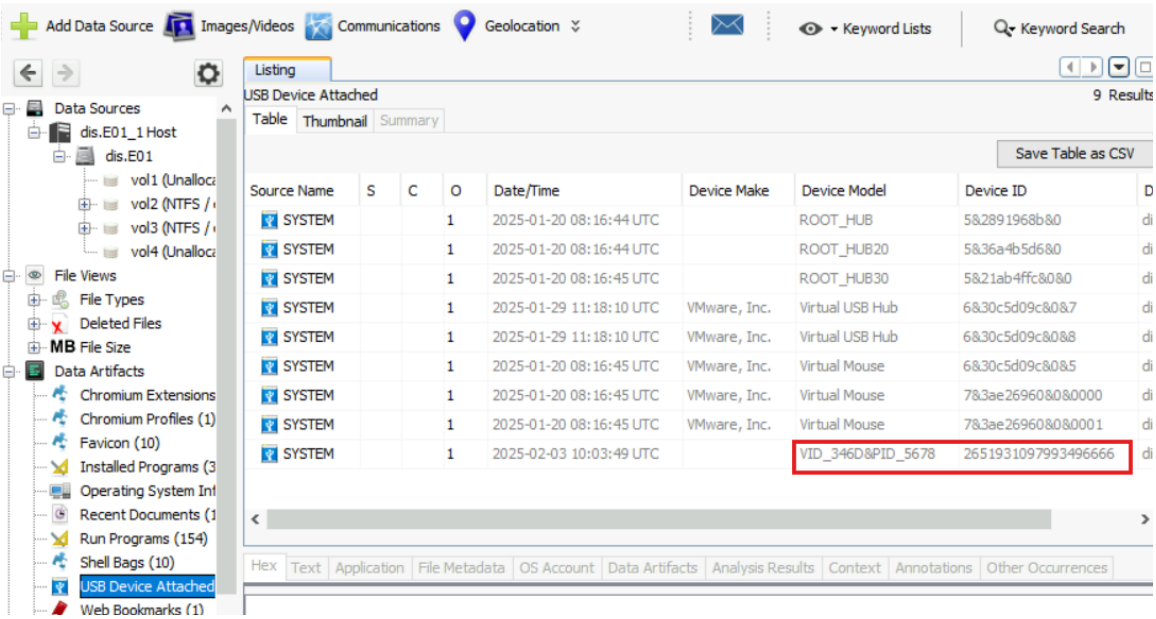
## 🛠️ Tools Used

- Autopsy – primary disk forensics analysis
- ExifTool – metadata extraction from files
- HxD – hex editor to identify file signatures
- Windows Registry Viewer – for user/hardware info

---

## 🔍 Investigation Steps

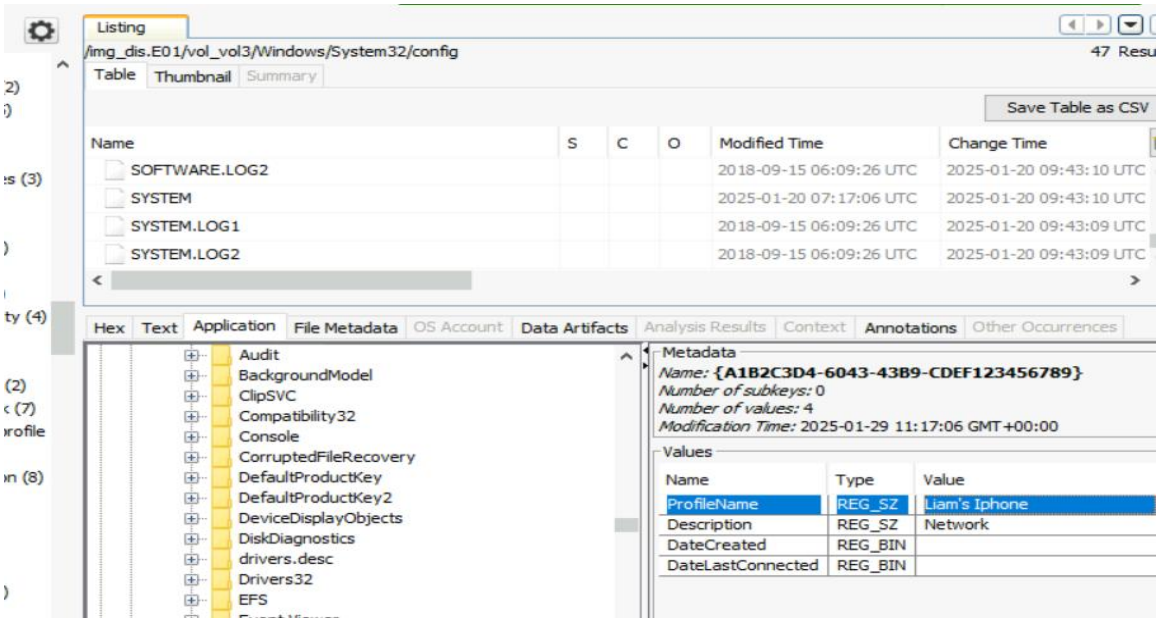
1. **Mounted the Disk Image in Autopsy**
   I started by opening the disk image in Autopsy. From the USB Devices Attached section, I spotted a suspicious USB device.
   Serial Number Identified: 2651931097993496666



2. **Registry Hive Analysis – Found Hotspot Name**

I navigated to: **Under the Microsoft > Windows NT > NetworkList,** I located recent network profiles and discovered the personal hotspot name Liam used.

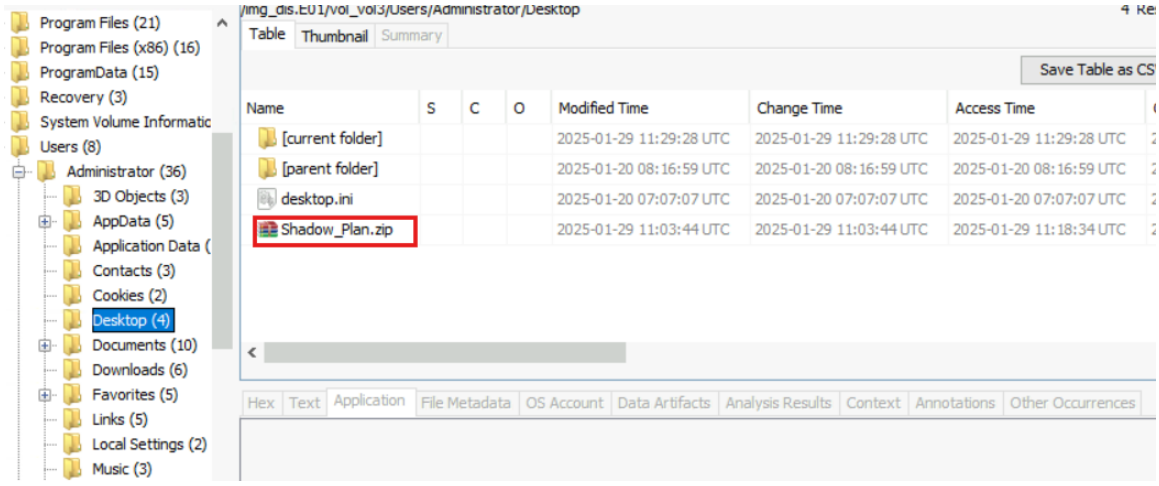
Hotspot Profile Name: **Liam's iPhone**




3. **Searched the Desktop for Suspicious Files**

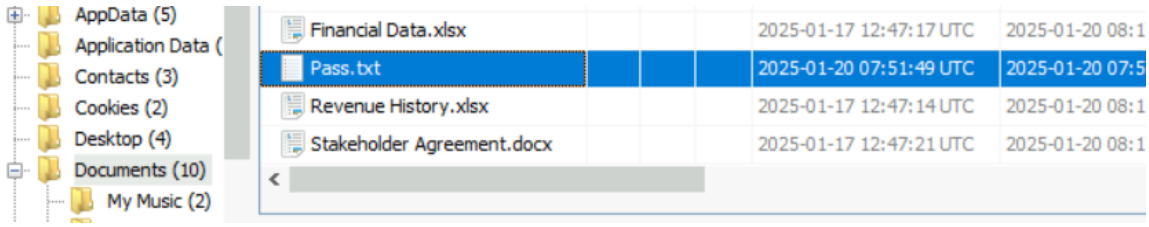
I checked Liam's Desktop folder and found a zip file:

Zip File Name: **Shadow_Plan.zip**



### 4. Password Protection – Discovered Pass.txt

The zip file was password-protected. I browsed the Documents folder and found a file named **Pass.txt.** It contained the password for the zip: **Qwerty@123**




### 5. Extracted the Zip and Ran ExifTool

After extracting the contents of Shadow_Plan.zip, I found a PDF file named breach_plan.pdf. Using ExifTool, I checked the metadata and found the author's name:

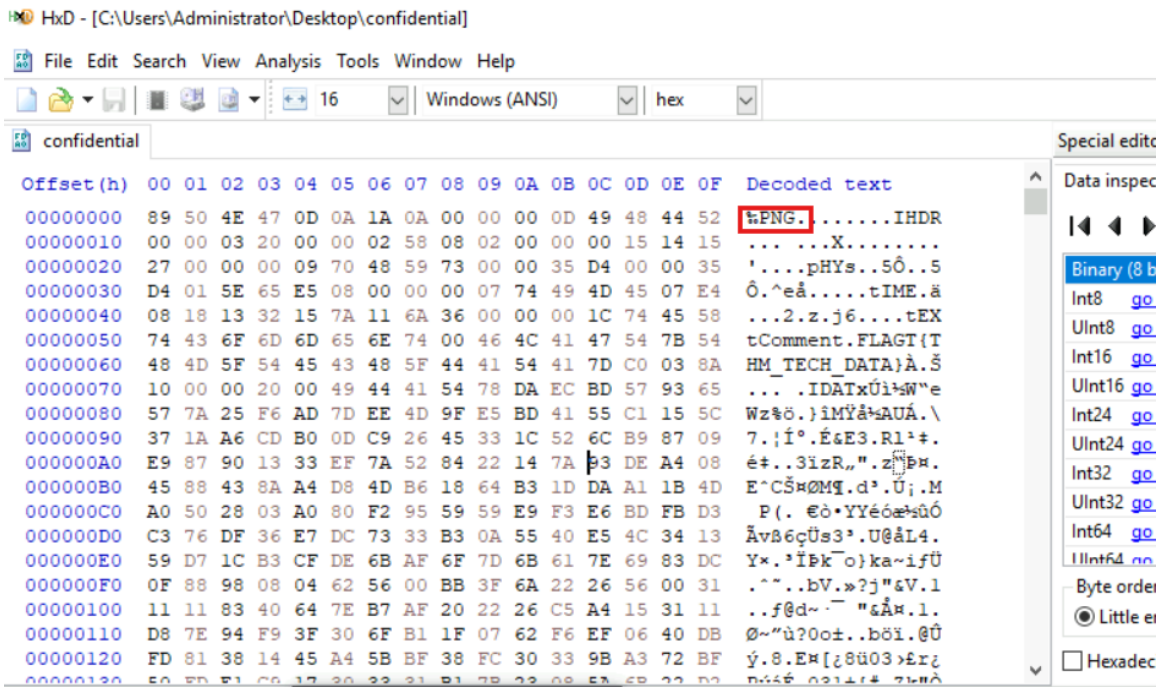
External Entity Identified: **Henry**

```
C:\Users\Administrator\Desktop\Forensic Tools\Exiftool>exiftool.exe ..\..\breach_plan.pdf
ExifTool Version Number         : 13.25
File Name                       : breach_plan.pdf
Directory                       : ../..
File Size                       : 1403 bytes
File Modification Date/Time     : 2025:01:29 10:43:23+00:00
File Access Date/Time           : 2025:04:19 16:32:18+00:00
File Creation Date/Time         : 2025:04:19 16:32:18+00:00
File Permissions                : -rw-rw-rw-
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.3
Linearized                      : No
Page Count                      : 1
Producer                        : ReportLab PDF Library - www.reportlab.com
Author                          : Henry
Create Date                     : 2025:01:29 05:43:23-05:00
Creator                         : ReportLab PDF Library - www.reportlab.com
Modify Date                     : 2025:01:29 05:43:23-05:00
Subject                         : unspecified
Title                           : untitled
Trapped                         : False

C:\Users\Administrator\Desktop\Forensic Tools\Exiftool>
```

6. **Unknown File Without Extension**

   Another file inside the zip named confidential had no extension. I opened it in HxD and analysed the header: File Type Identified by Signature: **PNG**




7. **Searched for File Access Patterns**

   Using the recent files and search artifacts in Autopsy, I discovered that Liam searched for: **Financial, Revenue**

8. **Explored USB Content**

   I reviewed the USB drive contents and listed the folders present on it:

   Folders on USB**: Critical Data TECH THM, Exfiltration Plan**

9. **Tracked Executable Use – file_uploader.exe**

   The PDF (breach_plan.pdf) instructed Liam to execute a tool named file_uploader.exe. From file metadata and execution artifacts:

   Last Execution & Count: **2025-01-29 11:26:09, 2**

10. **Tracked File Deletion**

    Liam attempted to cover his tracks. I discovered the deletion timestamp of an important file: Tax Records.docx.

    **Deletion Timestamp: 2025-01-29 11:29:02**

11. **Observed Suspicious Web Activity**

    In an attempt to appear normal or possibly mislead investigators, Liam visited a known social media site.

    URL Visited via Web Browser: **https://www.facebook.com/**

12. **PowerShell Command Execution**

    Lastly, as per the breach plan, Liam executed a PowerShell command to enumerate shared directories:

    PowerShell Command Executed:

    **Get-WmiObject -Class Win32_Share | Select-Object Name, Path**

---

🧩 **Final Thoughts:**

This forensic investigation clearly links Liam to the data exfiltration incident. By correlating USB usage, deleted files, network evasion tactics, metadata in documents, and execution history, I was able to identify not just Liam's direct actions but also reveal collaboration with Henry, the external party.

---

✅ **Recommendations to Prevent Insider Data Exfiltration**

- Implement Data Loss Prevention (DLP) Solutions
- Restrict and Monitor USB Device Usage
- User Activity Monitoring (UAM) and Behavioral Analytics
- Apply Least Privilege Access Controls
- Network Segmentation & Zero Trust Architecture
- Implement Strong Offboarding Processes
- Audit and Monitor Registry & PowerShell Usage
- Digital Forensics and Incident Response Readiness
- Security Awareness Training
- Conduct Red Team Exercises & Insider Threat Simulations