2025

Digital Forensics Investigative Report
ACME Construction Company: Intellectual Property Theft Case

Prepared by: Juliano Alves de Souza
Date: October 26, 2025

I. Executive Summary

This report documents the digital forensic investigation into the suspected intellectual property (IP) theft by **Drew Patrick**, a director-level employee and senior manager at ACME Construction Company. ACME, a manufacturer of high-end excavators, maintains its competitive advantage and industry reputation through painstaking, innovative design work. This proprietary data is the basis for their ability to charge a premium on their products. Drew Patrick's abnormal behavior and the subsequent identification of large files and suspicious emails by IT triggered a multi-disciplinary internal investigation involving IT, HR, legal counsel, and the digital forensics team.

The investigation uncovered clear and compelling evidence of deliberate attempts by Drew Patrick to exfiltrate proprietary design data for personal gains specifically, seeking a promised managerial position with a competitor. This was achieved by bypassing security controls using an anonymous account and peer-to-peer (P2P) applications. This incident constitutes a significant security breach that compromised ACME's core competitive assets, risking substantial financial loss, reputational damage, and loss of market share. The findings outlined herein precisely detail the motive, method, and opportunity, supporting a robust case for both civil and criminal proceedings against Drew Patrick.

II. Legal Concerns

The core legal concern centers on the unauthorized access, transmission, and attempted sale of ACME's proprietary excavator design data. Drew Patrick's actions constitute intellectual property theft, a breach of confidentiality, and a violation of internal data handling policies. Given the clear intent to profit from high-end development secrets and the confirmed transfer of files to external, non-ACME-controlled IP addresses, the case is being built for both civil litigation (Defend Trade Secrets Act) and criminal prosecution (Economic Espionage Act).

The legal and forensic teams are collaborating closely with the following primary objectives:

- **Validating Evidentiary Integrity for Admissibility:** The forensic process is meticulously documented, including the creation of a forensic image using **FTK** and hash verification of the Western Digital hard drive (serial NB497356F). This step provides a legally sound

foundation, preemptively mitigating defense challenges to the evidence's authenticity and ensuring compliance with federal laws governing data protection.

- **Demonstrating Intent to Profit and Exfiltration:** The objective is to uncover artifacts that explicitly prove Drew Patrick's intent to profit and the pre-meditated nature of the theft. Evidence such as emails promising design information for a managerial position, searches on YouTube for "selling intellectual property", and the creation of a dark web email address, constructionseller@darkweb.com, are crucial in establishing this intent.
- **Establishing a Comprehensive Timeline:** The correlation of network and endpoint logs is vital to establish the chronology of unauthorized access. For example, Active Directory logs, which indicated Drew was not logged in during the transfers, directly led to the discovery of the anonymous account created on 9/17/2016 at 9:57 p.m., demonstrating the deliberate circumvention of security controls (two-factor authentication).
- **Ensuring Compliance:** All investigative steps must comply with federal laws governing data protection, employee monitoring, and surveillance boundaries, confirming that the collection of digital evidence did not infringe on any of Patrick's rights.

III. Relevant Procedures

A. Processes and Procedures

Handling a criminal situation involving an internal employee requires a structured, multi-step incident response process to ensure the integrity and legal admissibility of evidence.

1. **Initiate Incident Response and Notification:** The process begins immediately upon detection of suspicious activity, such as the SIEM alert for P2P traffic from Drew's IP. Prompt notification of the **HR and legal teams** is critical to ensure all subsequent steps comply with employment law and legal procedure. *Reasoning: Immediate legal and HR involvement is necessary to establish a clear legal basis for monitoring and seizure, preventing procedural missteps that could invalidate evidence.*
2. **Isolate the Suspect's Workstation and Preserve Volatile Data:** Drew Patrick's computer must be physically and logically disconnected from the network to halt

any ongoing data exfiltration or potential remote wiping attempts. *Reasoning: Volatile data (RAM contents, active network connections) is transient and must be preserved before the system is powered down or seized, as this data can often contain active encryption keys or running processes that prove intent.*

3. **Seize Physical Evidence:** The hard drive must be physically seized using documented protocols. The target drive, in this case, the **Western Digital 500 GB hard drive (serial NB497356F)**, is clearly labeled and documented. *Reasoning: A formalized seizure protocol prevents accusations of evidence tampering or chain of custody breaks before analysis even begins.*

4. **Forensic Imaging (Acquisition):** A bit-for-bit, forensically sound image of the drive is created using specialized tools like **FTK Imager** or similar functions in **FTK**. *Reasoning: This step ensures that all analysis is performed on the copy, leaving the original evidence unaltered – a fundamental rule of digital forensics necessary to avoid contamination.*

5. **Cryptographic Hashing:** A cryptographic hash (SHA-256 or MD5) is generated for both the original hard drive and the forensic image. *Reasoning: Comparing the hash values proves that the image is an exact, unaltered replica of the original drive, providing a mathematically sound basis for evidence integrity.*

6. **Analyze Artifacts and Correlate Logs:** Non-invasive analysis is performed on the image using tools like **Autopsy** and **FTK**. This includes correlating endpoint data (emails, file activity) with network logs (SIEM, IPS). *Reasoning: Corroboration across multiple evidence sources (network and endpoint) eliminates the possibility of isolated error or misinterpretation, strengthening the overall conclusion.*

7. **Maintain Confidentiality and Objectivity:** The analysis must be conducted impartially, avoiding any bias, and all investigative notes must remain confidential. *Reasoning: Objectivity ensures the findings are scientifically sound and not influenced by the desired legal outcome.*

B. Chain of Custody

Maintaining the **Chain of Custody** is essential for the legal admissibility of digital evidence. It provides an unbroken, documented timeline of who possessed the evidence and what was done to it, from the moment of seizure to presentation in court.

- **Seizure and Documentation:** The process began with the seizing of the physical evidence, specifically the **Western Digital 500 GB hard drive (serial NB497356F)**, and its immediate documentation in the chain of custody log.
- **Imaging and Verification:** A forensic image was created using **FTK**, and the cryptographic hashes generated for both the original drive and the copy were recorded. *This log entry proves that the analysis was conducted on an identical, verified copy.*
- **Transfer and Access Logging:** Every transfer of the evidence and every instance of personnel accessing it for analysis was meticulously logged, including **timestamps and the specific personnel involved**. *This prevents any legal challenges arguing that unauthorized access occurred or that the evidence was exposed to contamination.*
- **Secure Storage and Analysis:** The original evidence was stored in a secure evidence locker, and the forensic image was analyzed using **Autopsy and FTK** without altering the original image file. *This ensures that the original evidence remains untouched and verifiable, supporting accountability and integrity*.

IV. Details of Investigation

A. Resource Needs

An effective investigation required a **multidisciplinary team** with diverse technical and legal expertise. The success of the investigation was a direct result of coordinating the knowledge and tools of these specialized roles. Lab experiences emphasized the importance of team coordination, especially when correlating network logs with endpoint data.

Resource Needed	Expertise (Knowledge, Skills, Abilities)	Lab-Informed Examples/Tools Used
Network Forensics Analyst	Deep knowledge of network protocols, SIEM event analysis, and log correlation (Active Directory, DHCP/DNS).	Use of **Wireshark** for deep packet inspection, **Snort** for SIEM alert analysis (P2P traffic). Experience with **Analyzing Traffic Captured from Site Survey Software** and **NetWitness Investigator** to trace the external file transfers.
Endpoint Forensic Examiner	Expertise in filesystem analysis (NTFS), artifact recovery, and non-volatile data preservation.	Proficiency with **FTK** for forensic imaging and hash verification; **Autopsy** for non-invasive artifact recovery and indexing; and skill in **Using the dd Utility** (hypothetical lab experience) for creating bit-for-bit disk copies.
Legal/Compliance Specialist	Knowledge of data protection laws, employee surveillance boundaries, and legal admissibility standards (Chain of Custody).	Ensuring all evidence collected complies with the strict protocols learned from labs like **Sanitizing and Cloning Hard** Drives to maintain evidentiary integrity.
Data/Application Analyst	Skill in analyzing application-specific files like SQL, Excel, and proprietary formats.	Use of **Autopsy's** sort and index functions to rapidly isolate files like SQL, Excel, and email for review. Experience with **Viewing the Contents of index.dat** to reveal browser activity.

The coordination between the SOC (Snort/SIEM analysis) and the Endpoint team was vital: the network logs detailing P2P traffic and external IP transfers served as the initial evidence and provided the necessary justification for the forensic imaging of Drew's hard drive, demonstrating how SOC analysis directly fed into forensic imaging and investigation success.

B. Methods

The forensic approach was methodical and ensured comprehensive coverage while minimizing oversight.

1. **Disk Imaging and Verification:** Drew's **Western Digital 500 GB hard drive** was imaged using **FTK**, and the integrity was confirmed by generating and verifying cryptographic hash values.
2. **Filesystem and Artifact Analysis:** Autopsy and Windows Forensic Toolchest were used to analyze the **NTFS** file structure. This included an in-depth analysis of slack space (hidden data), where incriminating temporary internet files were recovered.
3. **Data Sorting and Indexing:** The sort and index functions within **Autopsy** and **FTK** were leveraged to rapidly isolate and review key files by type, including emails (Outlook), SQL files, Excel documents, messaging logs, and HTML cache.
4. **Log Correlation and Timeline Reconstruction:** Timestamps from various sources were correlated to build a definitive timeline:
    - **SIEM/Snort Alerts** identified the P2P traffic originating from Drew's IP.
    - **Active Directory** Logs showed no login by Drew's *named* account during the transfers, which led to the discovery of an anonymous account created at 9:57 p.m. on 9/17/2016.
    - **IPS** Logs traced the data movement from R&D servers to Drew's desktop and then to the external IPs.

C. Findings

The evidence gathered through a non-invasive, structured forensic process confirms the intent, method, and motive for intentional intellectual property theft by Drew Patrick. The findings are grouped below to provide a synthesized explanation, with the overall impact on the organization being the breach of its core competitive advantage and the risk to its premium reputation.

Category	Finding	Forensic Tactic/Technology Employed	
Technical Method of Exfiltration		**P2P Traffic and Unauthorized Account:** SIEM, utilizing **Snort**, detected P2P traffic from Drew's IP. Active Directory logs confirmed the transfers occurred via an **anonymous account** created at 9:57 p.m. on 9/17/2016, specifically bypassing Drew's name, two-factor authenticated account. **IPS logs** traced the files' movement from the R&D servers to Drew's desktop and then to external, non-ACME IPs.	**SIEM/Snort Analysis** (network-level), **Active Directory Log Review** (authentication), and **IPS Log Correlation** (data movement).
Evidence of Motive and Intent		**Dark Web Activity and Searches:** HTML cache revealed searches for "proprietary information brokers" and the creation of the email address constructionseller@darkweb.com **Slack space** analysis recovered hidden temporary internet files on	**HTML Cache Analysis** (using Autopsy/FTK to recover browser history and temporary files), and **Slack Space Analysis** (revealing

		searches for "advertising stolen data" and "hacking SQL servers".		hidden, deleted data).
Stolen IP and Communication		**Proprietary Files and Communication:** Hard drive analysis recovered **Excel files** with parts specifications, **SQL database files** containing proprietary information, and two encrypted SQL databases. **Emails** promised design data to non-ACME accounts, and follow-up emails requested assurance of a promised managerial position. **Messaging logs** discussed the possession of these proprietary documents.		**File Indexing and Sorting** (SQL, Excel, Email, Messaging logs), **Keyword Search**, and **Metadata Analysis**.

These findings confirm intent, method, and motive, supporting legal action.

V. Investigative Journal Notes Integration

The investigative journal entries provided critical insights into the forensic process:

1. The initial detection of P2P traffic led to a multi-layered investigation.
2. Evidence was corroborated across network and endpoint sources.
3. Ethical considerations were addressed, including employee privacy and surveillance boundaries.
4. Chain of custody was maintained from seizure to analysis.
5. Tools like Autopsy and FTK enabled non-invasive artifact recovery.
6. The investigation demonstrated best practices in digital forensics, aligning with real-world standards and legal expectations.

VI. Conclusion

As the lead forensic investigator on this case, I can definitively conclude that the evidence gathered provides unambiguous proof of intentional intellectual property theft by Drew Patrick. Every procedural step, from the initial Snort alert signaling policy violation to the forensic imaging of the Western Digital Hard Drive (serial **NB497356F**) using FTK, was executed with uncompromising integrity, guaranteeing the legal admissibility of all findings via an unblemished Chain of Custody.

The meticulous analysis, leveraging tools like Autopsy and FTK, recovered a synthesized body of evidence—including proprietary Excel and encrypted SQL files, dark web activity revealing a buyer-seller relationship, and internal messaging logs—that collectively establish Patrick's motive, method, and opportunity to profit from ACME's proprietary designs.

This investigation is not merely a successful evidence recovery operation; it is a critical organizational risk assessment. The deliberate circumvention of security (using an anonymous account to bypass two-factor authentication) represents a catastrophic failure point in ACME's internal controls. The findings are now poised to support robust civil litigation and potential criminal prosecution, thereby safeguarding ACME's competitive market position. Moving forward, the strategic recommendations provided—strengthening internal controls, rigorously enforcing data policies, and continuing investment in forensic readiness—are essential to ensure the long-term protection of ACME's vital intellectual assets against future insider threats.

References

1. Pollitt, M. (2007). *The key to forensic success: Examination planning is a key determinant of efficient and effective digital forensics*. Retrieved from **NIST SP 800-86**.

2. Scientific Working Group on Digital Evidence (SWGDE). (2020). *Best Practices for Digital Evidence Collection*. Retrieved from https://www.swgde.org

3. SalvationDATA. (2023). *How to Write a Digital Forensics Report Step-by-Step*. Retrieved from https://www.salvationdata.com

4. Al Khater, N., & Overill, R. E. (2015). Forensic Network Traffic Analysis. *Proceedings of The Second International Conference on Information Security and Cyber Forensics*, 1–9.

5. Ayers, R., Brothers, S., & Jansen, W. (2014). *Guidelines on Mobile Device Forensics* (NIST Special Publication 800-101 Revision 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-101r1

6. Cundiff, V. A. (2009). Reasonable measures to protect trade secrets in a digital environment. *IDEA: The Intellectual Property Law Review*, *49*(3), 359–394.

7. International Organization for Standardization (ISO/IEC). (2012). *Information technology—Security techniques—Guidelines for identification, collection, acquisition and preservation of digital evidence* (**ISO/IEC 27037:2012**).

8. Ieong, R. S. C., Lai, P. K. Y., Chow, K. P., Kwan, M. Y. K., & Law, F. Y. W. (2010). Forensic investigation of peer-to-peer networks. In J. R. R. S. Ieong, K. P. Chow, P. K. Y. Lai (Eds.), *Handbook of Research on Computational Forensics, Digital Crime, and Investigation* (pp. 513–530). IGI Global.