ACME Construction Company:

Digital Forensics Report and Memo of Findings

Jeremy Willett

**Executive Summary**:

ACME Construction Company investigated Senior Manager Drew Patrick based on initial reports and suspicion of theft of intellectual property. Upon notification of potential peer-to-peer (P2P) traffic, from the Security Information and Event Management (SIEM) system, Snort, security operations personnel reported the incident to human resources and legal teams. The security team initiated an investigation, at the request of the legal team, based on the P2P notification from Snort as this type of traffic violates company policy. Analysis of Active Directory logs indicated that Patrick was not logged into his account at the time the files were transferred via the P2P application, but ACME enforces two-factor authentication and does not allow for computer sharing. At face value, this would appear that Patrick was not the one to perform the action however, because of ACME’s established policies, and the additional fact that the account active on Patrick’s computer was an “Anonymous” account, would point to this being a suspected attempt to cover the tracks of the suspect and divert suspicion away from the only person with authorized access to the suspected device. Analysis of server access logs indicated that Patrick had been logging into the R&D database for several weeks prior to the external file transfers taking place. Network logs from the Intrusion Prevention Systems (IPSs) indicated that the files of interest had been transferred to Drew’s desktop computer prior to the external transfer. ACME has a strict policy against maintaining intellectual property anywhere other than the designated servers. File access logs on the R&D servers confirmed that the account belonging to Patrick had copied the files in question. These contributing factors lead ACME to employee a digital forensics team to further the investigation at this point. The forensics team captured log files, made a forensically sound of the Patrick’s computer’s hard drive, and collected log files from the firewall and intrusion detection systems. The details found from this investigation revealed the file transfers of intellectual property were performed from Patrick’s computer, without his employee account logged in.

Leadership was informed throughout the process of the progress of the investigation. All actions taken were approved by the Legal team prior to performing any actions to ensure the legal basis of the investigation was sound. The HR team consulted to maintain adherence to company policy. IT leaders were made available for all necessary access to the company network and to clarify any suspicious activities that needed to be verified during the investigation. Executive leaders received regular updates and supported the investigation from the outset.

Further evidence to support the incrimination of Patrick was obtained from deeper analysis of the information on the hard drive of Patrick’s computer. Emails, chat conversations, internet browser cache files, and temporary files on the hard drive provided incriminating evidence to corroborate suspicions of malintent by Patrick to steal the intellectual property of ACME Construction and take it with him to a new company in exchange for a management position. This report discusses the legal concerns, relevant procedures, and details of the investigation in deeper context to support the filing of civil and criminal charges against Drew Patrick.

**Legal Concerns**:

“Intellectual property (IP) refers to creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce” (World Intellectual Property Organization (WIPO), 2023). There are multiple types of Intellectual Property protected by law such as Trademarks, Copyrights, Patents, and Trade Secrets. “Trade secrets are pieces of information that are valuable to the creation of your product, process, or business that are not public” (Peek, 2020). ACME Construction is concerned with maintaining and protecting the trade secrets they have developed that give them an edge for their product. ACME has spent hundreds of thousands of hours redesigning their premier excavator. Every piece that goes into the excavator is individually designed to maximize the longevity of the equipment. Known for attention to detail, high-quality work, and industry innovation, this painstaking work is what sets ACME Construction company apart and is attributed for the excellent reputation they enjoy. As a result, theft of their designs and inventions for their products could result in great financial loss for the company if these were to be copied by a competitor. For this reason, ACME is very concerned with protecting its Intellectual Property from theft, whether internal or external, and has set up their systems and networks to protect this information as much as possible. Drew Patrick’s role as a senior manager directly involved in the overall development of ACME’s products provides him with access to design documentation, schematics, support documents, and any other technical references maintained in the company’s research and development (R&D) database.

The main legal defense against Intellectual Property theft is the Fair Use law that states, “certain types of usage, such as criticism, comment, news reporting, teaching, scholarship, and research, may qualify as fair use. There are four factors in determining if something is protected under fair use:

* **Purpose and character of the use:**If the party is using the copyrighted work for noncommercial and nonprofit educational uses, then it may be determined that the usage is fair. This is not an umbrella defense and courts will balance the purpose with the factors below as well.
* **Nature of the copyrighted work:**The type of work that is being used is also a factor in determining the validity of its usage. A creative work, such as a book, play or movie, is less likely to be considered fair than that of a factual work, such as a news article or technical journal.
* **Effect of use on the market:** The court will determine to what extend the unlicensed use hurts the market for original owner’s work. They will determine if sales have been displaced and the hit the business could take of the usage became widespread.
* **Amount used:** Another factor is how much of the work was used in relation to the copyrighted work as a whole. If a small clip from a movie is used for a criticism relative to the whole film being used, that may fall under fair use.” (Peek, 2020)

This defense does not apply in the case against Drew Patrick based on information found during the investigation that proves malintent with the stolen information by providing it to a competitor. The goal is to prove Drew Patrick was the actor responsible for copying proprietary information with the intent to profit from it personally. This is done through a forensic investigation performed by a hired digital forensics team.

**Relevant Procedures**:

**Processes and Procedures**:

While handling the criminal investigation of an internal employee, it is vital that the suspect is not alerted to their suspicion and the investigation taking place until the devices they have access to that can access company systems and networks can be secured. This is to prevent them from deleting or covering their tracks. The first step that should be taken is securing the suspects devices to preserve them as evidence and ensure they are unaltered or destroyed. Once the initial incident was reported and further investigation was requested by the legal team. Drew Patrick’s computer was seized and secured in evidentiary lock up to prevent anyone from accessing it or altering it. This was then handed over to the digital forensics team when they took over the investigation. As part of this investigation team, the hard drive was duplicated using Forensic Toolkit (FTK) to preserve the original hard drive image. A hash was then generated for the original and the copied image to prove both images were the same and remain unaltered throughout the investigation. This step is vital to maintain evidentiary integrity and the chain of custody of the drive and its image. The image was analyzed to ensure nothing happens to the original drive and it is preserved in the state it was seized. Evidence preservation is key to proving the case and later using it in a criminal or civil case against the suspect.

The hard drive was analyzed using Autopsy and Windows Forensic Toolkit as the hard drive image was a Windows-based system. Using the sort and index functions on these tools, the tile types isolated for analysis were SQL, Excel, Email, Chat, and HTML files. The slack space on the drive was also analyzed to look for hidden or deleted artifacts left behind from internet searches and chat remnants.

Log files were also captures from all relevant computer systems and networks. Log files for corporate mail, DNS, and DHCP servers were captured to trace the steps taken through the network and what was done by the suspected system. Packet capture logs were analyzed from the firewall and intrusion detection systems to trace access to information throughout the company network. These logs were used in conjunction with the hard drive image analysis to confirm suspicion of the actions taken by Drew Patrick.

**Chain of Custody**:

The primary source of evidence for this case is the hard drive that was imaged for analysis. Maintaining the chain of custody of the hard drive and the integrity of the data on the drive is vital to success of the case. As discussed earlier, to maintain the chain of custody, when the computer was initially seized from the possession of Drew Patrick, this was recorded according to company policy, the time, date, and the name of the person taking possession was recorded as well as the time, date, and name of the person that placed it in evidentiary lockup. All evidence was handled in a similar manner to a forensic investigation by Law Enforcement. All evidence was accompanied by a chain of custody form. This for proved the details of the item including when it was collected, where it was collected, how it was collected, the case number, the serial number of the item (if it had one), the person handling the evidence, when they received it, when they returned it, the purpose for handling the evidence, and the actions performed with the evidence. This form stayed with each piece of evidence throughout the investigation. The use of this form provided a paper trail for every person that handled the evidence during the investigation from the time it was collected to the time it was returned to the company with the investigation report.

When removed from the lockup, the same information was recorded to maintain a chain of custody that was traceable to see who, when, and where the evidence was at all times. Once the digital forensics team had it in possession, they continued to record the chain of custody as they began their process to analyze the data on the computer. the hard drive was duplicated using Forensic Toolkit (FTK) to preserve the original hard drive image. A hash was then generated for the original and the copied image to prove both images were the same and remain unaltered throughout the investigation. The creation and use of the hash is vital to maintaining the integrity of the evidence as the hash reveals if any of the information has been altered and proves that the image is identical to the original drive. If the hash of the image changes and becomes different from the original, the image is no longer forensically sound and can no longer be used as evidence to prove the suspect’s guilt.

**Details of Investigation**:

**Resources Needs**:

Digital forensic investigations into the theft of intellectual property by an employee require a variety of resources and skill sets. These include:

1. Digital Forensic Tools: Digital forensic tools are used to collect, preserve, and analyze digital evidence. These tools can range from basic software programs to advanced hardware devices. Common tools used in digital forensic investigations include EnCase, FTK, and X-Ways Forensics (Casey, 2011). This investigation required the use of FTK, Autopsy, and Windows Forensic Toolkit. These tools were used to create a forensically sound copy of the hard drive. This was verified by the creation of a hash at the time the copy was made. The hard drive was then analyzed using Windows Forensic Toolkit and Autopsy to scan the drive and locate the files in question during the investigation.
2. Knowledge of Digital Forensic Procedures: Digital forensic investigators must have a deep understanding of digital forensic procedures, including the preservation of evidence, chain of custody, and data recovery. This knowledge is critical to ensure that evidence is collected and analyzed properly, and that it can be presented in court if necessary (Casey, 2011). This is the purpose and justification for the use of a third-party digital forensics team. To ensure thorough knowledge of forensic procedures and to maintain the integrity of the evidence and the investigations outcome, the third-party was brought in to perform the investigation once it was confirmed further investigation was necessary.
3. Knowledge of Intellectual Property Laws: Digital forensic investigators must also have a solid understanding of intellectual property laws. This includes knowledge of copyright, trademark, and patent laws, as well as trade secret laws. This knowledge is important to properly identify and classify stolen intellectual property (Association of Certified Fraud Examiners (ACFE), 2021). The Legal team worked hand in hand with the investigation team to protect the company’s interests and ensure the company’s intellectual property was recovered.
4. Knowledge of Computer Networking: Digital forensic investigators must understand computer networking, including how data is transmitted and stored on networks, and how to identify suspicious activity on networks. This knowledge is critical to identify potential sources of stolen intellectual property and to trace the movement of data across networks (Casey, 2011). The IT team worked with the investigation team to provide needed information on the layout and structure of the company network. This allowed the investigation team to navigate the company network to identify what happened and how it applied to the investigation.
5. Analytical Skills: Digital forensic investigators must have strong analytical skills to identify patterns and anomalies in data. This includes the ability to identify suspicious patterns in network traffic, analyze metadata associated with digital files, and interpret system logs and other sources of data (Association of Certified Fraud Examiners (ACFE), 2021).

**Methods**:

This investigation utilized hard drive analysis, log analysis, slack space analysis, email and chat log analysis, and SQL database log analysis. These different information types allowed for the investigation to lead to proving the actions of Drew Patrick as originally suspected.

1. Hard Drive Analysis: Hard drive analysis involves examining the physical storage media of a computer system to recover digital evidence. Digital forensic investigators can recover deleted files, analyze file metadata, and identify evidence of file copying or transfer. This analysis can help to identify intellectual property theft by an employee (Carrier, 2014). The hard drive was analyzed using Windows Forensic Toolkit. Because the computer’s used at ACME Construction all run on Windows operating systems, this tool was the best choice to sifting through the hard drive to find determine the actions taken on the computer to steal the sensitive data as well as find the motive by recovering chat records detailing the intent.
2. Log Analysis: Log analysis involves analyzing system logs to identify suspicious activity. This includes examining system logs, application logs, and security logs to identify activity such as file transfers, network connections, and login activity. This analysis can help to identify suspicious activity that may be indicative of intellectual property theft (Garfinkel, 2010). Log analysis was performed by looking through the log files on the operating system and web browser to determine searches made on information pertaining to the sale and use of IP data. The network logs were analyzed to see all traffic from the computer’s IP address and find what connections it made throughout the network as it accessed servers containing proprietary and sensitive data. These connections were compared to the times of the data copies to determine the computer making the request and performing the copy.
3. Slack Space Analysis: Slack space analysis involves examining the unused portions of a computer's storage media to identify fragments of deleted files or other data. This analysis can help to identify files that may have been deleted or modified to hide evidence of intellectual property theft (Carrier, 2014).
4. Email and Chat Log Analysis: Email and chat log analysis involves examining email and chat logs to identify evidence of intellectual property theft. This analysis can help to identify employees who may have sent or received intellectual property or communicated about intellectual property theft (Garfinkel, 2010). Forensic Toolkit was used to recover the email and chat logs left behind detailing intent of Mr. Patrick to provide proprietary information in exchange for a position with another company.
5. SQL Database Log Analysis: SQL database log analysis involves examining logs associated with database transactions to identify suspicious activity. This includes examining transaction logs and audit logs to identify data access, modification, or transfer. This analysis can help to identify employees who may have accessed or transferred intellectual property through a database system (Quick, 2017). The SQL database logs were analyzed to determine when the information was accessed and by who.

**Findings**:

During the hard drive analysis, evidence was gathered that led to the determination that Drew Patrick was stealing intellectual property with the malicious intent to sell it and share it with other companies in exchange for a job. When looking through the emails found on the hard drive, Numerous emails were found that contained references to proprietary information. Some emails were to non-ACME Corporation email accounts, and they promised information pertaining to equipment design. Follow-up emails were found that asked for assurance of a promised managerial position. Chat messages from AOL messenger were also found containing information about possession of proprietary documents. This information was recorded and flagged as evidence of the suspected crime.

SQL database files revealed proprietary information and connection logs to a remote SQL server. Two additional SQL database files were encrypted and were not successfully unencrypted. These files correspond with the information suspected to have been copied through the P2P traffic that triggered the initial notification by Snort to the security operations center.

Numerous Excel files were located on the hard drive. These files contained parts list and parts specifications concerning proprietary construction equipment. These files could be relevant to the investigation but they could also apply to the daily job of Drew Patrick, this information is not necessarily indicative of the suspected crime.

Recovered internet web browser cache revealed that the dark web was searched for proprietary information brokers. An email address was created to correspond in the dark web for buyer transactions called constructionseller@darkweb.com. Internet cache also revealed that YouTube was searched for the subjects “selling intellectual property” and “selling on the dark web.” Recovered internet browser history revealed pictures and illustrations on encrypting SQL database files. Internet browser history also revealed searches concerning how to exploit the vulnerabilities of an SQL database. Hidden information in the slack space was revealed to contain temporary internet files on searches for “advertising stolen data” and “hacking sql servers.” These files, once revealed, were in plain text and read using Notepad. This information was found using Autopsy through searching through the files on the hard drive image. This information combined with other findings paint the picture and prove the intent of Drew Patrick to use the stolen information for personal gain. The search history found in the internet temp files also suggests that this was a premeditated act by Drew Patrick and was planned out for some time and then acted upon. This information all combines to prove that Drew Patrick stole intellectual property from ACME Construction and intended to sell it for personal gain and provide it to competitors of ACME Construction in exchange for a management level position.

# References

Association of Certified Fraud Examiners (ACFE). (2021). *Digital Forensics: The Basics*. Retrieved from Association of Certified Fraud Examiners (ACFE): https://www.acfe.com/resources/fraud-examiner/fraud-examiner-vol-6-no-1-digital-forensics-the-basics/

Carrier, B. (2014). *File System Forensic Analysis (3rd ed.).* Upper Saddle River, NJ: Addison-Wesley.

Casey, E. (2011). *Digital Evidence and Computer Crime (3rd ed.).* London: Academic Press.

Garfinkel, S. (2010). *Digital Forensics Research: The Next 10 Years.*

Peek, S. (2020, March 17). *How to Prove Intellectual Property Theft*. Retrieved from U.S. Chamber of Commerce: https://www.uschamber.com/co/start/strategy/intellectual-property-theft-guide

Quick, D. C. (2017). SQL Injection Forensics: An Overview and Analysis. *Journal of Digital Forensics, Security and Law*, 23-38.

World Intellectual Property Organization (WIPO). (2023). *What is Intellectual Property?* Retrieved from World Intellectual Property Organization (WIPO): https://www.wipo.int/about-ip/en/

# Memo:

# MORPHEUS WIDGETS

“The difference between knowing widgets and walking the widget path”

TO: Trinity Weaving

FROM: Jeremy Willett

DATE: 03/23/2023

RE: Findings and Next Steps for Case # 56789

**[Key Details:]**

The results of the investigation into Senior Manager Drew Patrick’s actions have provided information leading to the conclusion that Mr. Patrick was responsible for the unauthorized access and duplication of proprietary information vital to the business of ACME Construction. The incident was triggered by an alert from Snort to the security operations team. An investigation was performed at the request of the legal team to determine the actions taken by Mr. Patrick, what was accessed and copied, and potential intent with the stolen information. Based on the information recovered from the computer of Mr. Patrick and log details from company monitoring systems, the digital forensics team was able to determine the actions taken by Mr. Patrick as he collected and copied information on the intellectual property of ACME Construction. The results of this investigation, as reported to ACME construction, allow for resolution of the incident, and identify areas that changes are required to improve security and protection of intellectual property vital to the company’s success.

The investigation highlights multiple areas that worked successfully and as intended for ACME Construction’s network, intrusion detection, and incident response process. These procedures were vital to a successful investigation by providing necessary information that led to the incrimination of Mr. Patrick. Resolution of the incident was reached, aided by the investigation, by uncovering the actions taken on the network and supporting evidence pointing to his motives. The emails discovered on Mr. Patrick’s work-computer alluded to his desire to take the proprietary information and give it to a competing company in exchange for a high-level position. Log files showed Mr. Patrick researched ways to sell the information on the Dark Web for monetary gain as well. This information combined with other findings paint the picture and prove the intent of Drew Patrick to use the stolen information for personal gain. The search history found in the internet temp files also suggests that this was a premeditated act by Drew Patrick and was planned out for some time and then acted upon. This information all combines to prove that Drew Patrick stole intellectual property from ACME Construction and intended to sell it for personal gain and provide it to competitors of ACME Construction in exchange for a management level position.

The notifications sent to the security team that initiated the entire process acted as intended. Unauthorized access was flagged, and suspicious traffic led to the security team involving the HR and Legal teams. This investigation proved the necessity of the any monitoring and logging systems ACME Construction employs to protect their network and their information. Proper procedure was followed by the necessary personal to address this incident quickly and resolve it. While it is not common to suspect a Senior Manager of acting in this manner, this incident highlights the need to implement new policy and the adoption of the “Principle of Least Privilege” regarding network and system access. “In practice, the principle of least privilege applies not only to individuals but also to networks, devices, programs, processes, and services. When it comes to access control, all of these are considered subjects (active entities) that request access to resources, or objects (passive entities that contain or receive information), such as systems, files, applications, directories, databases, ports, and more. It’s critical for organizations to understand that the principle must apply to all of these entities because if compromised, any could potentially put the organization or its data at risk” (Walkowski, 2021).

**[Implications for Legal Action:]**

Maintaining evidentiary integrity is vital to a successful investigation and the results in produces to be usable in a legal setting to justify the actions taken by ACME Construction because of the investigation. Once the Legal team has determined that a digital forensic investigation was necessary, a third party was called in to perform this investigation to prevent any bias on behalf of an in-house team. The processes used in the investigation were forensically sound, beginning with an image of the computer hard drive taken from Mr. Patrick’s computer that was validated with a hash generated of the original and the image. This allows for checking of the evidence to ensure neither piece was altered and remained the same from the collection time. Chain of custody was always maintained for any evidence gathered during the investigation. This began from the moment the security team of ACME Construction began their initial investigation and continued when it was handed over to the external forensics team. Industry standard tools were used for evidence analysis. Forensic Tool Kit, Autopsy, and Windows Forensic Toolkit were used during this investigation. By adhering to industry standard and approved methods, the validity of the collected evidence was documented and usable in a legal setting.

In an investigation such as this, it is important to keep in mind civil rights of individuals being investigated. While ACME Construction administers a User-Agreement upon initial employment with any individual, the protections of the fourth amendment need to be kept in mind for cases where personal information is seized. The computer taken from Mr. Patrick was a company provided device, and while Mr. Patrick used it for personal reasons, the User-Agreement signed at the time of his initial hiring dictates that he has no reasonable expectation of privacy to anything accessed or stored on the computer as it does not belong to him. With this, ACME Construction did not violate any rights of Mr. Patrick in seizing the computer and analyzing it during this investigation.

# References

Walkowski, D. (2021, December 21). *What Is the Principle of Least Privilege and Why is it Important?* Retrieved from F5 Labs: https://www.f5.com/labs/learning-center/what-is-the-principle-of-least-privilege-and-why-is-it-important