**CIS-484-50-4242 Project 4 Report**

**April 5th, 2024**

**Case Number: CIS-484-50-4242**

**Investigator: Tristan Rogers**

**Executive Summary**

**Overview of investigation.**

This report is in relation to Mr. Perry Winkler, who has been under investigation by the LMPD for several month due to Mr. Perry Winkler’s suspected involvement with the dealing of drugs. LMPD obtained a search warrant for the home of Mr. Winkler and was able to find a damaged PC that they believed to be owned and used by Mr. Winkler. LMPD handed off the computer to lead computer forensic investigator Tristan Rogers.

**Summary of findings.**

The investigation into Mr. Winkler's computer yielded several key findings. A user profile was discovered named “Perry” as well as a deleted .rtf file was found that was signed with “Perry”. We believe that this ties Mr. Winkler to the found computer. We also discovered several files which were pictures of guns, marijuana, and money which we believe was obtained by illegal activities performed by Mr. Winkler. Several deleted files were also uncovered which were letters and a file program called “Evidence Eliminator”. Finally, we found contacts of individuals who could potentially be working with Mr. Winkler as well as a ledger of potential clients of Mr. Winkler.

**Conclusions and recommendations**

The computer forensics investigation conducted on Mr. Winkler's computer produced significant findings that provide a great insight into the illegal activities of Mr. Winkler. The analysis of the computer found outside of Mr. Winkler’s home uncovered a variety of incriminating files and communications that indicate Mr. Winkler is most likely on the run due to his suspicion of law enforcement investigation of his illegal activities, drug dealing. Based on the evidence collected and analyzed, it is obvious that Mr. Winkler was involved with drug dealing and was aware that law enforcement was on to him. It is important to make aware that while the evidence found is compelling, further investigation may be necessary to create a stronger case against Mr. Winkler and to further guarantee his conviction.

Regarding the investigation's findings, it is recommended that if Mr. Winkler is found, he should be prosecuted due to his involvement in the drug trade, evading police, and knowingly destroying evidence. Overall, the thoroughness of the investigation has provided great insights that will help with prosecuting Mr. Winkler for his crimes should law enforcement feel the need to.

**Introduction**

**Background**

For several months LMPD’s drug enforcement team has been investigating Perry Winkler for suspected drug trade involvement. LMPD was able to obtain a search warrant for the home of Mr. Perry Winkler but when arriving at the suspects home they found that it was abandoned and left without any usable evidence. After searching the perimeter of the property LMPD found a dumpster with a damaged PC inside. They believed the damage to be caused by an attempt to prevent anyone from reading the data, however the hard drive was intact and not damaged. The drive was then transported back to LMPD facilities where it was imaged and handed over to lead forensic investigator: Tristan Rogers.

**Purpose and scope of the investigation**

The purpose of the forensic investigation is to examine the computer image given to us by LMPD to find digital evidence that proves Mr. Perry Winkler’s drug trade involvement and his potential whereabouts. This investigation aims to provide evidence of Mr. Winkler’s illicit activities that may have occurred on the computer system as well. By investigating the contents of the computer image provided, we seek to piece together a full understanding of the activities of Mr. Winkler.

The scope of this forensic investigation will be a complete examination of all files, directories, system configurations, user activities, etc within the provided computer image. Investigators will analyze metadata, logs, system artifacts, and any other digital traces to provide evidence to LMPD and their prosecutors to find and ultimately convict Mr. Winkler for his crimes. The scope also includes identifying other sources of evidence, such as deleted files or hidden data, and making sure that the integrity of the forensic analysis process is not harmed. Finally, the investigation will follow established forensic methodologies and legal requirements to avoid admissibility of any findings in the legal process.

**Methodology used in the investigation.**

A comprehensive methodology was used to fully analyze the image extracted from Mr. Winkler's computer. This methodology included several phases which are identification, preservation, collection, analysis, documentation, and presentation of evidence. The identification, preservation, and collection were already done by LMPD as they had already identified the computer as evidence, preserved the evidence by creating an image thus making sure that nothing on the machine was changed. The analysis phase involved a full examination of the collected evidence to find incriminating files, communications, and other relevant pieces evidence against Mr. Winkler. Throughout the investigation, documentation was kept recording every step of the process to make sure the evidence was usable in court proceedings. Finally, the findings were presented which provides an overview of the investigation's conclusions and recommendations.

**Evidence Identification and Collection**

**Description of the evidence sources**

In the investigation, multiple sources of evidence were identified and examined on Mr. Winkler's computer which was run on a Microsoft Windows operating system. These evidence sources were the computer's file system, email accounts, chat logs, internet browsing history, and logs. The file system contained many potentially incriminating files. These were documents and images as well as executable programs. Email logs provided a glimpse into Mr. Winkler's communications and interactions, which may reveal conversations related to the investigation. Internet browsing history allowed us to look into Mr. Winkler's online activities which may allow us to further prove Mr. Winkler’s nefarious activities.

**Details of how evidence was identified and collected.**

In the investigation, the previously mentioned methodology was followed to identify and collect evidence from Mr. Winkler's computer using FTK Imager, supplemented by other forensic tools. FTK Imager and other forensic tools were used to search through the forensic image provided by LMPD which allowed us to identify and extract evidence. Advanced features within FTK Imager allowed for the targeted collection of specific file types which made the process much more efficient. Additionally, complementary forensic tools were employed to supplement FTK Imager's capabilities so that there are not any potential leads overlooked. Through the use of FTK Imager and other specialized tools, we were able to provide LMPD with a complete package of digital evidence against Mr. Winkler.

**Evidence Preservation**

**Integrity of the evidence**

Ensuring the integrity of the evidence throughout the investigation was of great importance in order to maintain its reliability and usability in legal proceedings. Measures were implemented to safeguard the integrity of the evidence collected at each stage of the investigation. First, upon identification and collection, a forensic image of Mr. Winkler's computer was created. This forensic image was a bit for bit copy of the original storage device in the computer, which allows us to examine the machines data without any chance of changing the original device nor allowing anyone argue that the device was changed. Strict chain of custody procedures were followed as well. During the investigation, the integrity of the evidence was maintained through the following previously mentioned measures which ensures the credibility and reliability of our findings.

**Forensic imaging process**

For the investigation of Mr. Winkler, LMPD created an exact copy of the computer’s hard drive. This copy is called a forensic image or bitstream image, ensures that the original data is preserved and maintains the integrity of the evidence. Before beginning the imaging process, LMPD verified the integrity of the hard drive, meaning that they checked for damage and made sure that the hard drive functioned normally. Write blocking software is used to prevent any changes to the data on the hard drive-in order to maintain the integrity of the data inside. Documentation is also crucial. Chain of custody and everything done to the hard drive must all be annotated and recorded in order to make sure that the evidence recovered is usable in court.

**Evidence Analysis**

**Overview of the forensic analysis techniques used**

In the investigation of Mr. Winkler's computer, we used a number of forensic analysis techniques in order to uncover digital evidence against the suspect. The first technique we used was file system examination. We used this technique to analyze the structure and contents of the file system, to allow us to identify and extract files and directories that could prove illegal activity. Deleted file recovery techniques were also used to recover data that had deleted from the system, to allow us to find evidence that Mr. Winkley may have tried to hide from law enforcement. We also analyzed Internet history to find Mr. Winkler's browsing activities, which showed us visited websites, search queries, and online behaviors. These behaviors could be important to the investigation and provide us leads to other forms of evidence. We also employed keyword searches to narrow our search for specific terms or phrases relevant to Mr. Winkler’s activities. Finally, we examined the devices metadata in order to find timestamps, file properties, and other potentially helpful information that could provide context for other evidence discovered during our forensic investigation. With these forensic analysis techniques used together, we were able to conduct a complete analysis of Mr. Winkler’s machine which brought forth important information that will help LMPD.

**Findings**

**Summary of the key findings from the analysis**

The evidence findings from the investigation reveal several significant findings:

Identification of user: Evidence suggests that the computer found by LMPD was used by an individual named Perry. This is supported by the presence of a deleted .rtf file in the recycle bin signed as "Perry," as well as a user profile labeled "Perry" containing various files and documents.

Incriminating Photos and other documents: Within Perry's user profile, photos were discovered depicting money and marijuana, suggesting potential illegal activities. The images were named "mikes desk.jpg" and "da stuff.jpg" were found in Perry's photos folder. Additionally, a spreadsheet was found that appears to be a ledger for individuals that owed the suspect money which further indicates that the suspect was dealing illegal drugs.

Attempted Evidence Deletion: Perry appears to have deleted incriminating evidence, as indicated by the discovery of a deleted .rtf file labeled "letter" containing a message mentioning the disposal of items in the kitchen and bedroom, along with a question to someone about cleaning the computer.

Data Erasure Software: Evidence of data erasure software, such as "Evidence Eliminator" and the SDelete program, suggests attempts to hide or completely remove digital evidence from the computer system.

Communication with Accomplices: A document titled "Letter3.rtf" found in Perry's documents references communication with an accomplice, indicating potential collaboration in illegal activities.

Identification of Possible Accomplices: We found two saved contacts, Rick Shoner and Larry Spitz, on the computer which raises our suspicion of their involvement as Perry’s potential accomplices.

Discovery of Plans.zip: We discovered A .zip file named "plans.zip" found within Perry's documents, alluding to the existence of plans that may be related to Perry’s dealings and current location.

In summary, the evidence we discovered point towards Perry's involvement in illegal activities, including attempts to delete incriminating evidence, communication with accomplices, and the possession of incriminating images and documents. Additionally, the discovery of data erasure software and a discarded damaged computer further suggests efforts to conceal or manipulate digital evidence.

**Identification of any suspicious or incriminating evidence**

Evidence #1 $RSU8VAG.rtf: Found in partition two’s recycle bin, is a letter to an unknown person that “Thanks for your help! I will do wat you said with the task thing on the computer. Im glad you printed instructions for me or i woudl never figure it out lol. anyways ill destroy this and will look for your email with further instructions. cant wait to ditch this place! Yours truly, Perry”

Evidence #2 Rick Shoner.contact: Found under user Perry in the contacts folder. This contact was created on 2016-02-16. The email address associated with this contact is [rickyboy579@aol.com](mailto:rickyboy579@aol.com).

Evidence #3 Larry Spitz.contact: Found under user Perry in the contacts folder. This contact was created on 2016-02-16. The email address associated with this contact is [spitzmeister@rocketmail.com](mailto:spitzmeister@rocketmail.com)

Evidence #4 Plan.zip: Found under user Perry, Documents, emails folder.

Evidence #5 SDelete.zip: Found under user Perry under the Downloads folder.

Evidence #6 Mike’s desk.jpg: Found under user Perry in Pictures. This is a picture of a large bag of marijuana and a large stack of money.

Evidence #7 Da stuff.jpg: : Found under user Perry in Pictures. This is a picture of a large plastic grocery bag full of marijuana.

Evidence #8 Evidence Eliminator in partition 2 > noname > unallocated space > 00000048 > 00052506. “Evidence Eliminator is one of the best applications that can professionally deep clean your computer. You can use your computer and Internet with confidence.”

Evidence #9 Letter3.rtf: Found under user Perry inside the documents folder. This is a letter that states “What should I do? I havent hurd from you and im getting worried. are you there yet? i need an email to know. Also, i bought those credit card numbers you showd me. There supporsed to be all prepaid too so we are set! lol well i hope your safe and will look for your email. Sincerely, perry”.

Evidence #10 Letter.rtf: Found under user Perry inside the documents folder. This is a letter that states “I think there onto us. What shud I do ? I know about getting rid of the stuff in the kitchen and bedroom but what about the computer? Please call me - i need to fugure this out. Signed Perry”

Evidence #11 Book2.xlsx: Found under user Perry inside the documents folder. This appears to be a ledger that kept track of who owed Perry money. A list of names, amount due, and favorite drug of each client appears.

**Interpretation of the evidence in the context of the investigation**

Evidence #1: Suggests Perry's communication with an unknown individual about tasks related to the computer and plans to leave his current location, hints at a potential attempt to evade authorities.

Evidence #2 and #3: Reveals two contacts named Rick Shoner and Larry Spitz, potentially implicating them as accomplices or associates.

Evidence #4: Plan.zip, suggests the existence of plans or documentation relevant to Perry's activities and may lead to where Perry left to.

Evidence #5: The discovery of SDelete.zip, indicates attempts to erase digital traces and potentially hide illegal activities.

Evidence #6 and #7: Incriminating images of marijuana and money, support the suspicion of Perry's involvement in drug-related activities.

Evidence #8: The presence of Evidence Eliminator, reinforces the implication of Mr. Perry trying to sanitize the computer and eliminate evidence.

Evidence #9 and #10: Letters expressing concern and attempts to conceal incriminating evidence, provide a further look into Perry's intentions and actions.

Evidence #11: The ledger in Book2.xlsx, suggests Perry's involvement in the drug trade, with records of clients, owed amounts, and preferred drugs. Additionally, despite only finding pictures of marijuana, the ledger indicates that Mr. Perry may be dealing other drugs base on his clients favorite drug listed.

Overall, the evidence paints a clear picture of Perry's involvement in criminal activities, including drug trafficking, evading police, and attempts to conceal evidence of these activities.

**Conclusion**

**Summary of the investigation's findings**

The forensic investigation yielded great evidence indicating Perry's involvement in a number of illicit activities, including drug trafficking, evading police, and tampering with evidence. Perry's communication with an unknown individual(s) about computer-related tasks and plans to leave his current location indicates an effort to evade authorities. The two contacts that may be associated with Perry, Rick Shoner and Larry Spitz, raise suspicion of their involvement as accomplices or associates. The finding of Plan.zip and SDelete.zip indicates attempts to hide/delete digital evidence, while incriminating images of marijuana and money support the suspicion of Perry's drug activities. Additionally, letters of concern and attempts to conceal/delete evidence provide a look into Perry's intentions and confirm that what he knows what he’s doing is wrong in some way. The presence of Evidence Eliminator further supports the Perry’s attempts to remove evidence from his computer, while a ledger indicates Perry's involvement in the drug trade. Overall, the forensic investigation's findings create a full picture of Perry's involvement in criminal doings.

**Assessment of the strength of the evidence**

The strength of the evidence in this investigation is strong, providing information that supports LMPD’s suspicion of Perry's involvement in illicit activities. Many pieces of evidence connect to each other, providing credibility to the overall findings. For instance, Perry's communication with an unknown individual about computer-related tasks line up with the discovery of the SDelete and Evidence Eliminator programs, indicating attempts to conceal/delete digital evidence. The existence of contacts named Rick Shoner and Larry Spitz may support the idea of Perry having accomplices or associates. Additionally, incriminating images of marijuana and money, along with letters expressing concern and attempts to conceal evidence, provide evidence of Perry's involvement in drug-related activities. Finally, the ledger found offers documentation of Perry's involvement in the drug trade, strengthening the case against him. Overall, the links and consistency of the evidence strengthen its credibility and add to a strong case against Perry.

**Recommendations**

**Recommendations**

We, the forensics team, recommend that LMPD take this evidence and use it to further build a case against Mr. Perry as the evidence provided is sound. The individuals Rick Shoner and Larry Spitz should also be investigated as they may be able to provide additional evidence to Mr. Perry’s illegal activities and LMPD may be able to build cases against them as well. Finally, we also recommend that LMPD take the names listed in the ledger and investigate those individuals as well. Building cases against all parties involved will ultimately lead to more arrests and a safer community.

**References**

**Tools**

SDelete: SDelete stands for Secure Delete. It is a command-line utility developed by Microsoft that securely deletes files, directories, and free space on a disk. The main purpose of SDelete is overwrite data so that it cannot be easily recovered by data recovery tools. It works by using various algorithms to overwrite data multiple times, making it much harder to recover.

FTK Imager: A forensic imaging and analysis tool developed by AccessData. It is used by digital forensic investigators, law enforcement agencies, and cybersecurity professionals for getting, analyzing, and examining digital evidence from computers and many other digital devices.

Evidence Eliminator: A software program is used to securely delete sensitive data and remove digital traces of users' activities on their computers. Additionally, it is used to erase browser history, cookies, cache files, and other traces of online activity.

**Appendices**

**Pictures**

Evidence #6

**A bag of money and a bunch of marijuana

Description automatically generated**

Evidence #7

A bag of marijuana in a chair

Description automatically generated

Evidence #11

A screenshot of a table

Description automatically generated