A red sign with white text

Description automatically generated

Cardiff University

School of Computer Science and Informatics

**CMT216 - Computer and Network Forensics**

**Assessment – Coursework**

**This assessment is submitted in partial fulfillment of the requirements for the qualification of Master of Science in Cyber Security[MSc Cyber Security]**

Supervisor: Shancang Li

Author: Sharwari Sanjeet Dali

(Student id: 23088177)

Date of Submission:09/05/2024

Court Report

1. Executive Summary:

The forensic examination of the material collected from the Lard&land Donuts case has uncovered the subsequent crucial discoveries:   
  
1. Taurus Smith, also referred to as Mona Simpson, is under suspicion for her alleged participation in a cyber intrusion targeting her job, Lard&land Donuts, with the intention of pilfering the company's confidential "Honey Duff Donuts" recipe.

2. The information acquired from the USB flash drive image and network traffic analysis suggests that Taurus Smith may have collaborated with an accomplice, possibly her son H.J. Simpson, to carry out this attack. The details of the image file are shown in the screenshot below.

3. The suspect's laptop held multiple recipes and secret material from Lard&land Donuts, which had been camouflaged using advanced techniques such as steganography and encryption.

4. Based on network activity, it appears that Taurus Smith intended to travel to Hawaii, either to meet with her collaborator or to continue the theft of the secret recipe.

A screenshot of a computer

Description automatically generated

1. Detailed Finding:

A. Suspect Identification and Accomplice

- The individual identified as "Taurus Smith" was revealed to be using a fictitious name. The suspect's genuine identity is Mona Simpson.   
- The presence of a secondary user account branded "hacker" on the suspect's laptop, together with an SSH private key, shows the involvement of a collaborator.   
-A message retrieved from a deleted file suggests the involvement of two people known as "Dad" and "Lisa," who may have a relationship to the suspect.

A screenshot of a computer

Description automatically generated

B. Data Theft and Concealment Techniques

- The USB flash drive image depicted a laptop hard drive, implying an attempt to duplicate or get access to sensitive information.

- The suspect's laptop held several recipes and confidential information from Lard&land Donuts, which were concealed using a variety of methods.

- When inspected with steganography tools, two PNG image files were found to contain secret recipes.

- An encrypted email was discovered, which revealed the presence of two additional PNG files with recipes.

- A password-protected PDF file called "Lardland Super Donuts Instructions" was uncovered, which required a password to open.

The password was encrypted using a password-cracking tool, which revealed another recipe.

- The pink donut png file named 1.png had encoded document of the secret recipe of honey duff donuts as given below.

A screenshot of a recipe

Description automatically generated

C. Network Activity and Travel Plans

* According to a review of the PCAP files' network activity, Taurus Smith's computer (192.168.1.158) was sending instant messaging packets to an unexpected laptop on the company's wireless network, suggesting a potential case of computer misuse attack.
* The network data also made clear Taurus Smith's plan to travel to Hawaii, either to meet up with her partner or to further the theft of the trade secret recipe.

A screenshot of a computer

Description automatically generated

1. Conclusion and Recommendations:

The forensic investigation discovered significant evidence that Taurus Smith (Mona Simpson) was involved in a computer misuse attack against her employer, Lard&land Donuts, with the purpose of stealing the company's trade-secret "Honey Duff Donuts" recipe. The suspect's use of advanced means to conceal the stolen data, such as encryption and steganography, as well as the suspected involvement of an accomplice, indicate to a well-planned and coordinated operation.   
  
It is recommended that the authorities investigate Mona Simpson's behaviour in greater detail, particularly any connection to her likely travel schedule and suspected collaborator. To determine the entire degree of the data theft and any potential impact to Lard&land Donuts, the retrieved data—including secret recipes and confidential information—should be thoroughly scrutinised.