NISGTC Lab 16: Forensic Case Capstone Challenge 2

Alex Arnold

Summary of Case:

Jimmy Jamison has been arrested for stealing credit cards. He has used five different credit cards that were not his. A police officer has acquired an image of his hard drive. Law enforcement has requested that a forensic investigator examine the image of the suspect’s hard drive. The goal of the investigation is to examine the contents of his user profile for documents that contain credit card info. Screenshots of any relevant documents will be added to this report.

Tools:

Tools for this investigation will be a Linux based system that will be running PTK investigation software.

Method:

The hash of the files that was sent with the image was verified to match in both the MD5 and sha1 sum to ensure that the file that was sent matched the image acquired by the police. After this the image was loaded up into PTK and the User account files were examined for the requested information. Upon investigation 5 files were found which were examined then extracted for further examination. Upon investigation with a text file editing application, it was seen that the files contained images of credit cards in the suspected files.

Findings:

After investigation a total of five files were found on the users account, each file contained a single image of a credit card.

A screenshot of a computer

Description automatically generated

Files on the suspects hard drive that were later extracted and examined further.

A screenshot of a computer

Description automatically generated

File called Doc1.doc Containing a single image of a Mastercard credit card with an angry birds image on the card. Text may be Cyrillic script for the bank name. This card does not have an individuals name that it is affiliated with.

A computer screen shot of a credit card

Description automatically generated

The second document called Doc2.doc containing another credit card. This card is a Visa card from Hong kong University. This card is in the name of an individual called MR Yip Yau Shing.

A computer screen shot of a credit card

Description automatically generated

The third document was called Doc3 and contained a credit card image with no affiliation. This card is in the name of an individual named Firstname Lastname.

A computer screen shot of a credit card

Description automatically generated

The fourth document was called Doc4.doc and contained a single image of a credit card from the Bank Of Anywhere. There was no country affiliation with this card. This card is in the name of an individual called Name O Cardholder.

A computer screen shot of a card

Description automatically generated

The fifth document contained a single image of a credit card. This card was a Visa card associated with Amazon.com and is a rewards card. Belonging to a D. Barrett.

Conclusions:

Upon the conclusion of the investigation and the collection of the evidence available. There were five different credit cards stored on the suspect’s machine. These credit cards were stored in five different files as images within the .doc files. From further examination of the images four of the cards are affiliated with different names while one has no name. Three of the five cards are unaffiliated with a country or origin while two of the cards are from other countries based on the bank / org name on the card.