CSCI 476 - Lab 1

The current Point of Sale (PoS) system does not require cardholder's data to be encrypted when they are saved in non-persistent memories (e.g. RAM). This design flaw, unfortunately, allows attackers to install malware on a PoS system to steal the credit card information. In 2005, "Target Corp. was hit by an extensive theft of its customers' credit-card and debit-card data over the busy Black Friday weekend [1]. "

In this lab, you are asked to implement a Java program to validate if a Point of Sale (PoS) system has unencrypted credit card data in memory, i.e., your program needs to identify both Track I and Track II data. While working on your program, you could make the following assumptions; otherwise, your program would generate too many false alarms.

Track I Data:

- "Primary Account" field contains 13-19 digits
- "Name" field contains a first name and a last name, separated by "/"
- First/Last name contains 2-26 letters
- "Additional Data" field contains a 2-digit expiration year, a 2-digit expiration month, a 3-digit service code, and discretionary data
- There is no Longitudinal Redundancy Check (LRC) field

Track II Data:

- "Primary Account" field contains the same information as it in Track I
- "Additional Data" field contains a 2-digit expiration year, a 2-digit expiration month, a 3-digit service code, a 4-digit encrypted PIN, a 3-digit CVV and discretionary data
- There is no LRC field

A sample memory data of a PoS system, called *memorydump.dmp*, is provided on Brightspace LE/D2L. Although the memory data can be obtained via memory dump tools, this sample file is hand-made. A sample output of your program may look like:

There is 1 piece of credit card information in the memory data!

<Information of the 1st credit card>:
Cardholder's Name: Qing Yang
Card Number: 4128 1234 1234 1234
Expiration Date: 09/2015
Encrypted PIN: 1930
CVV Number: 108

[1] http://www.wsj.com/articles/SB10001424052702304773104579266743230242538