Assignment 2 (Due Feb 7th, 11:30pm)

The current version of the Point of Sale (PoS) system does not require cardholder data to be encrypted when they are saved in non-persistent memory (e.g. RAM). This design flaw, unfortunately, allows attackers to install malware on a PoS system to steal the credit card information of cardholders. 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 assignment, you are asked to implement a Java program to validate if a Point of Sale (PoS) system has unencrypted credit card track I data in memory. A sample memory data of a PoS system is provided on the course webpage, called *memorydump.dmp*. Although the memory data can be obtained via existing memory dump tools, this sample file is hand-made. A sample output of your program may look like:

There is 1 track I record in the memory data
<Information of the 1st record>
Cardholder's Name: BinhaiZhu
Card Number: 4128 1234 1234 1234
Expiration Date: 09/2015
CVC Number: 101

As in the first assignment, you can form a team (preferrably with no more than 3 students) to finish this one. Hand in your output as well as the Java code on D2L (in 2 separate files, similarly as in Assignments 1, e.g., family_name.output and family_name.java).

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