**YMT 549 Digital Forensics**

**Lab 3 (32 Points)**

**Due: At the end of class**

**(Use back side of this paper for your answers)**

**Policies and Procedures**

1. **List 3 ways to access a password protected BIOS?**
2. **If you find an application that is installed to your computer is used recently. However, you were not able to find any files based on signature (header) analysis. What can be the reason for that?**

**Data, PDA and Cell Phone Forensics**

1. **How do you differentiate EIDE type hard drive from SATA?**
2. **In which case do you need to use master/slave configuration in devices?**
3. **Documentation of chain of custody should answer which questions?**

|  |  |  |
| --- | --- | --- |
| **1** | **Download Excel KeyDemo** | Location: Flash Drive |
| **2** | **Download Book1.xls** | Location: Flash Drive |
| **3** | **Install Excel Key Demo** | Regular Settings |
| **4** | **Run Excel Key Demo** | Click on **“Continue with outdated demo”** |
| **5** | **Change Settings** | Click on **“Settings”** in the main screen.  Click on “**Dictionary”** tab.  Change the values of **“Run for Passwords from …”**. New values will be 2 to 6.  Click on **“Xieve optimization”**  Change the values of **“Run for Passwords from …”.** New values will be 2 to 6.  Click **“OK”**. |
| **6** | **Uploading file** | Click on **“Recover”** in the main screen.  Locate and select the **“Book1.xls”**  Wait until the process is done.  Take a note of the **“File-Open Password”** |
| **7** | **Opening the Book1.xls file** | Use the identified password and open the **“Book1.xls**” file |
| **8** | **Questions:** | 1. What is the password to open **“Book1.xls”**? 2. How many different attacks conducted in order to find the password? 3. What is the last password tested with Xieve attack? 4. Total of how many passwords have been tried to find the password? (include the values from all different attack strategies) |
| **9** | **Learn to Use the DOS Shell in Windows** | Click **“Start”** and then click **“Run”** in Windows Operating System  Type **“cmd”** in the dialog box and click **OK**.  Type the command **“help”** and press **Enter**.  Use the help command to find help on several commands listed. Practice with commands to display a list of directories, copy a file, rename a file, and make a directory.   1. What is the command line to display a list of directories, includes the subdirectories? 2. What is the command line to copy **“abc.doc”** from C drive to A drive. 3. What is command line to rename **“abc.doc”** to **“def.doc”** 4. What is the command line to create a folder? 5. Write the appropriate DOS command for searching files that is named as “readme” on the C drive. How many did you find? 6. Assuming you have “input.txt” file located in your C root folder. What would be the command line prompt to change the attribute of the file to *hidden*? 7. What is the command line to display *hidden* files? |