WEEK -34

Submitted By: **Raunak Kr Singh**

Submitted To: **Mr Mukesh Tiwari**

1. LECmd Output.csv: Was there any user interaction on this machine with an optical disk drive? If yes, when did that happen?

   Yes, User Interaction with an optical disk drive occurred on **2002/06/04 12:02:55 AM UTC.**

2. LECmd Output.csv: Was there any user interaction on this machine that shows that an *index.htm* file was stored in a removable storage media? If yes, which **day** the interaction happened?

   Yes, User Interaction with an index.html file on removable storage occurred on **2002/06/03 08:05:20 PM UTC. Monday** was the day**.**

3. LECmd Output.csv: Was there any user interaction on this machine that shows access to a folder created by an Online Service? Whenthis happened?

   Yes, there was an interaction indicating access to folders created by an online service i.e. **Currex**.

   2002/05/14 5:26:24 PM UTC.

4. LECmd Output.csv: Was there any user interaction that shows a zip file was stored in a folder? If yes, which folder? When this particular folder was last accessed?

   Yes, Interaction was shown that a zip file was stored in a folder.

   Path: **C:\Users\rauna\OneDrive\Documents\DATA\Traget\D\Documents and Settings\Bob Hunter\Recent\103-0356_IMG.zip.lnk**

   Last Access Timestamp: **2002-06-03 9:24:10 PM UTC.**

   Path: **C:\Users\rauna\OneDrive\Documents\DATA\Traget\D\Documents and Settings\Bob Hunter\Recent\CURREX~1.zip.lnk**

   Last Access Timestamp: **2002-05-14 5:26:24 PM UTC.**

   Path: **C:\Users\rauna\OneDrive\Documents\DATA\Traget\D\Documents and Settings\Bob Hunter\Recent\hourz11.zip.lnk**

   Last Access Timestamp: **2002/05/14 5:26:04 PM UTC**.

5. PECmd Output.csv: When Internet Explorer was last run?

   Internet Explorer was last run on **2002-06-04 11:40:38 PM UTC.**

   Last Run: **2002-06-04 11:40:38 PM UTC**

   Row in PECmd_Output: **11**

   Executable: **\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\INTERNET EXPLORER\IEXPLORE.EXE**

6. PECmd Output.csv: What was the name of last executable file that was run on this computer? What is this file related with?

   The name of the last executable file that was run on the computer was **IMAPI.EXE**.

   Last Run: **2002-06-05 12:40:08 UTC**

   Last Executable: **\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\IMAPI.EXE**

   Row in PECmd_Output: **4**

   Info: IMAPI.EXE is an anti-forensic system file commonly used for CD/DVD burning processes.

7. PECmd Output.csv: Which 2 programs that were used in the last 3 days were mostly run in this system?

   Two programs that were used in the last 3 days are:

   1. **RUNDLL32.EXE**

      Run Count: **20**

      It is a system utility used for running DLLs.

   2. **IMAPI.EXE**

      Run Count: **22**

      It is a system utility for optical media burning.

8. PECmd Output.csv: Did this user attempt to access his/her emails in these last three days? If yes, when did this happen?

   Yes, the user accessed an e-mail related program.

   Program: **\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\OUTLOOK EXPRESS\MSIMN.EXE**

   Last Access Time: **2002-06-03 09:08:20 PM UTC**

   Row in PECmd_Output: **20**