Assignment 7: Password Recovery and Encrypting File Systems: Chanakya Gaur

1. For which languages does PRTK provide dictionaries by default? [2 points]

* English
* Spanish
* Italian
* French
* German
* Arabic
* Russian

2. What is a biographical dictionary? [2 points]

A biographical dictionary is a dictionary derived from biographical information. For example, names, birthdays etc.

3. What are the four (4) types of attacks used by PRTK to unlock/decrypt a file? [5 points]

Password reset, Decryption, Dictionary, Key Space

4. Export an FTK word list and use it to find the passwords for the following three files found within the Clampet18.aff evidence image. What are the passwords? [15 points]

* Customers.xls - shine
* Laundry List.doc - capone
* TheBigOne.zip - capone

5. When you unlock the file named “The Big One”, you will be able to access an audio file. Play the audio file. What is the “tail number” of the red and white Cessna (airplane) that is mentioned in the audio file? [5 points]

N0234Z

6. Obtain the NTUSER.DAT file for the Jethro account, and the SAM, SECURITY, SOFTWARE, and SYSTEM registry files from the Clampet18.aff evidence image file. (One way to do this is to open the Clampet18.aff evidence image with FTK Imager and export these files.) Drop each file into PRTK and process them. Do any of these files reveal any passwords? If so, what are they? [10 points]

SAM = no (“Empty”)

SECURITY = “liniment”

SOFTWARE = no

SYSTEM = no

NTUSER.DAT for Jethro = alamode1

7. What is the Encrypting File System (EFS)? [2 points]

The Encrypting File System (EFS) on Microsoft Windows is a feature introduced in version 3.0 of NTFS that provides filesystem-level encryption. The technology enables files to be transparentlyencrypted to protect confidential data from attackers with physical access to the computer.

8. What is a “File Encryption Key” (FEK)? [2 points]

EFS works by encrypting a file with a bulk symmetric key, also known as the File Encryption Key, or FEK. It uses a symmetricencryption algorithm because it takes less time to encrypt and decrypt large amounts of data than if an asymmetric key cipher is used.

9. According to AccessData Training Manual, three (3) pieces of information are needed to decrypt EFS encrypted files. One of the items is the “Protect” folder, which FTK automatically collects for you. (p. 733) The second item is the “EFS Alternate Data Stream” for the file that is going to be decrypted. What is the third piece of information that is required to decrypt EFS encrypted files? (Hint: it is a piece of information that you must provide to FTK.) [2 points]

Login password

10. Moonshine is any distilled spirit made in an unlicensed still. As with all distilled spirits, yeast ferments a sugar source to produce ethanol, then the alcohol is extracted through distillation using a still.