**Laboratory Exercise – Windows Registry Forensics Analysis**

Name: Afeefah Manzoor

**1. Overview**

This exercise provides hands-on experience applying concepts learned during the Windows registry forensics discussion.

**2. Resources required**

This exercise requires a virtual machine with Regripper software installed. Cyber Range users should use the Introduction to Digital Forensics environment. This virtual environment includes various forensics software, as well as digital artifacts required for this exercise.

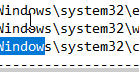
The following filesystem image is provided for this exercise and other exercises in this module:

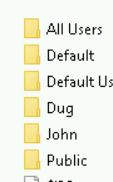
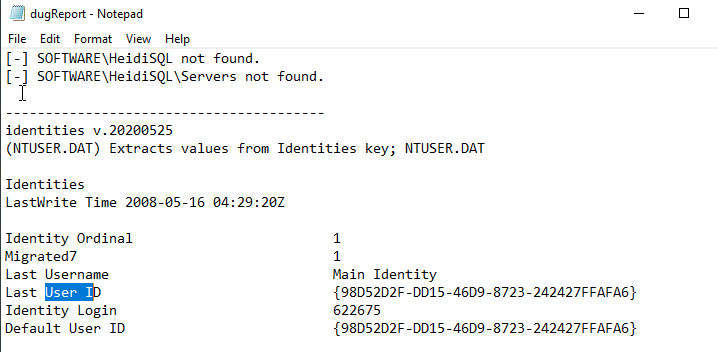
* Win7\_Laptop.tar.gz

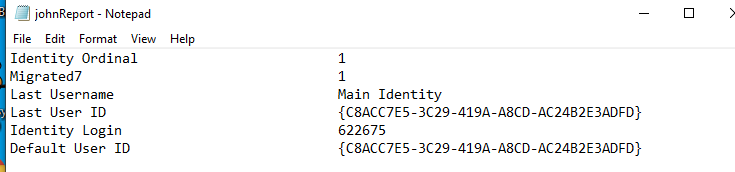
**4. Tasks**

**Windows Registry Forensics**

1. What service pack level is the Windows 7 computer and when was it installed?

 windows 7 32bit. 2-25-2016

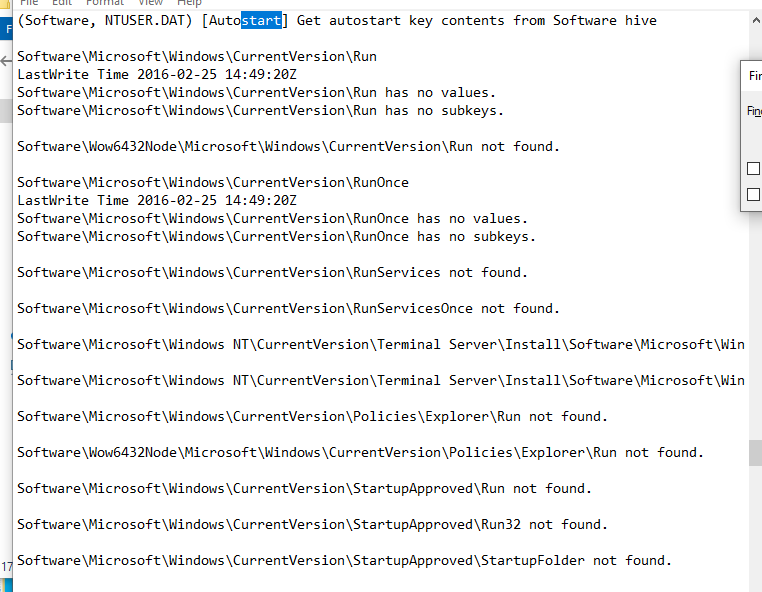
1. List the users and SIDs on the system



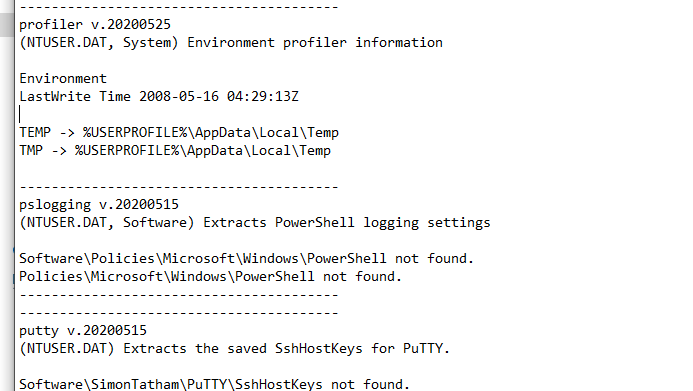
John:C8ACC7E5-3C29-419A-A8CD-AC24B2E3ADFD

Dug:98D52D2F-DD15-46D9-8723-242427FFAFA6

1. Are there any programs designated to run at system startup? If so, list them here. Nope, it looks like the system just updates



1. Is the system a workstation or a server (hint, see producttype plugin)

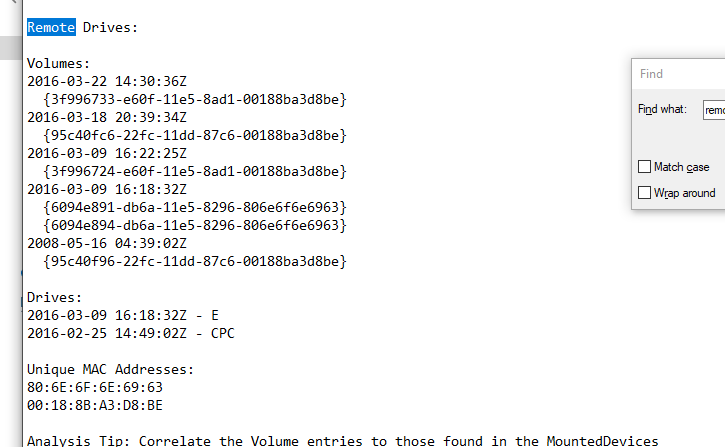
no

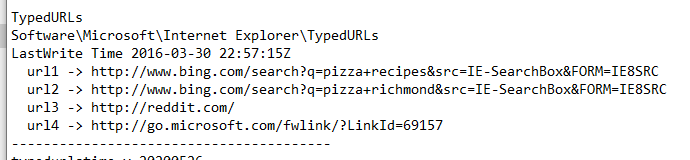
1. Have any USB devices been used on the system? List them here.

no

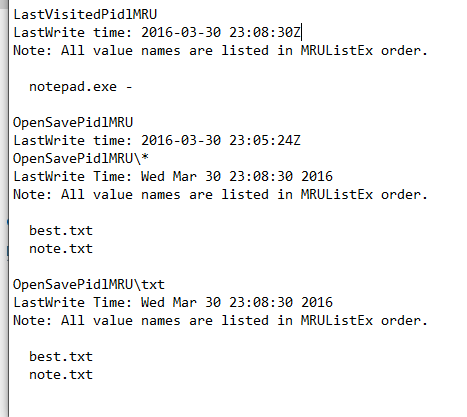
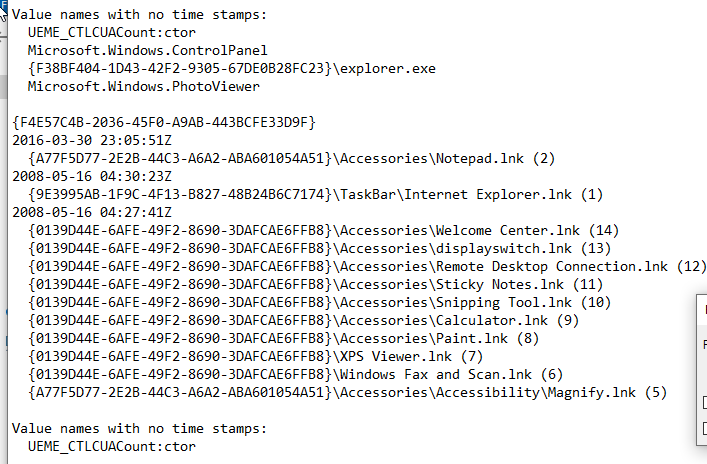
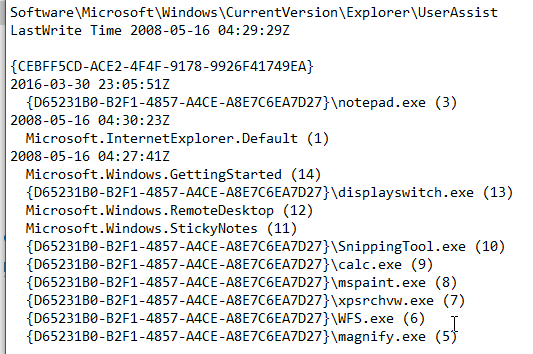
1. When was the system last shut down?

5-16-2008

1. Is the computer set up to listen for Remote Desktop (RDP) connections? If so, what port is it listening on? Yes, 3389
2. Which URLs did the user Dug visit using Internet Explorer?



He looked up pizza recipes, pizza Richmond on bing, went on reddit and a Microsoft page.

1. Did the user Dug open any .txt files (what are the filenames)?he opened best.txt and note.txt
2. What else can you find out about Dug’s activities on the system?

Dug looks like he opened notepad, went online, opened a remote system, the used a snipping tool, calculator, and paint.