Computer Forensics: Assignment 2: Registry: Chanakya Gaur

1. What is the file path within the Windows Registry of each file that you copied to the “Registry Exercise” folder?

C:\ Windows\ System32\Config\SAM

C:\ Windows\ System32\Config\System

C:\ Windows\ System32\Config\Security

C:\ Windows\ System32\Config\Software

C:\Documents and Settings\Buddy\_NTUSER.dat

C:\Documents and Settings\Elly\_NTUSER.dat

C:\Documents and Settings\Granny\_NTUSER.dat

C:\Documents and Settings\Jed\_NTUSER.dat

C:\Documents and Settings\Jethro\_NTUSER.dat

C:\Documents and Settings\Kaykay\_NTUSER.dat

1. What are the names of these user accounts?

Administrator

Buddy

Elly

Granny

Guest

HelpAssistant

Jed

Jethro

Kaykay

Support\_388945A0

1. What is the “SID unique identifier” for each account identified in step 2?

Administrator - 500

Buddy - 1008

Elly - 1007

Granny - 1006

Guest - 501

HelpAssistant -1000

Jed - 1004

Jethro - 1003

Kaykay - 1005

Support\_388945A0 – 1002

1. What are the last logon times for each of the accounts found in step 2?

Administrator - Never

Buddy – 7/4/2009 13:15:17 UTC

Elly – 7/4/2009 13:06:51 UTC

Granny – 7/3/2009 23:10:23 UTC

Guest – 7/3/2009 22:34:14 UTC

HelpAssistant – Never

Jed – 7/4/2009 13:11:38 UTC

Jethro – 7/4/2009 7/4/2009 2:21:28 UTC

Kaykay – 10/14/2009 13:15:29 UTC

Support\_388945A0 – Never

1. In the System Registry Hive there are two control sets named “ControlSet001” and “ControlSet002”. Which control set is the current one?

ControlSet001

1. What time zone is this computer configured for?

Pacific Standard Time

1. What is the name of the computer you are examining and where did you find this answer?
   1. Jethro812
   2. ControlSet001/ComputerName/ComputerName
2. What is the name of the version of the Microsoft Windows Operating System that is installed on the computer that you are examining? What is the version number of the operating system? What is the build number for the operating system? Which Service Pack is installed? What is the product ID of the operating system? When was the operating system installed?
   1. Microsoft Windows XP
   2. 5.1
   3. 2600
   4. Service Pack 2
   5. 76487-OEM-0040012-30561
   6. Tue Jun 30 04:51:49 2009
3. How long does this system wait before it creates the next restore point?

86400 seconds = 1 day

1. What is the Gmail password for the Jethro account?

alamode10

1. Which programs were most recently run within the Jethro user account?

Cmd

Regedit

ipconfig

1. Which URLs did the user of the Jethro account type into InternetExplorer?

Jethro\_NTUSER.dat\SOFTWARE\InternetExplorer\TypedURLs

Check Screenshot

1. Which URLs did the user of the Jed account type into InternetExplorer? Where is this information found?

Jed\_NTUSER.dat\SOFTWARE\InternetExplorer\TypedURLs

Check Screenshot

1. Which printer is the Jed account configured to use?

HPDeskJet 880C, winspool, Neo2

1. What is the Windows Registry?

The Registry is a hierarchical database that stores low-level settings for the Microsoft Windows operating system. The kernel, device drivers, services, Security Accounts Manager (SAM), and user interface all use the Registry.

1. What are the five (5) primary files that store the Windows NTFS Registry Information?

* Sam
* Security
* Software
* System
* Default

1. TRUE or FALSE: The Security Accounts Manager (SAM) file contains user account management and security settings such as user logon passwords.

True

1. Within which Windows NTFS registry file will one find information regarding the last known good configuration (that is, the last configuration the system successfully booted with)?

System

1. Within which Windows NTFS registry file will one find information regarding whether a particular user is allowed to reboot the computer?

Security

1. Within which Windows NTFS registry file will one find information regarding a listing of all installed programs, their settings, paths to application files and directories, licensing, and expiration date information for the operating system?

Software

1. Within which Windows NTFS registry file will one find information regarding the Most Recently Used (MRU) list of files?

NTUSER.DAT

1. A security identifier (SID) is a unique, alphanumeric-character string that identifies each operating system and each user in a network of Windows NT, 2000, and XP systems. Below is an example of a SID. The last four characters of the SID (“1000”, in this example) are called the Relative Identifier (RID). What does the RID identify?

S-1-5-21-436374069-842925426-1343024091-1000

It identifies the first created controller of the domain.

1. Different file systems allow the Windows operating system to track different amounts and different types of data. When comparing the FAT file system and the NTFS file system, which file system allows a Windows operating system to track more data?

NTFS