CIS 484-78-4212

Project 2 Notes:

- All files and/or tools required for this project may be downloaded using the links posted on Blackboard or provided during lecture.
- Provide all answers in UTC format.
- Download the Project 2.7z archive from Blackboard under Projects\Project 2. Extract the contents of the downloaded archive using 7-Zip. Upon extraction, there should be two folders: “Recent” and “Reg”. The “Recent” folder will contain the LNK files and jump lists related to this project; the “Reg” folder will contain the registry hives related to this project. Provide all answers in UTC format.

Parse and Analyze LNK Files

Parse the LNK files located in the “Recent” folder using LECmd and answer the following questions:

1) What was the file size in bytes of “Great Horned Owl.jpg” the last time it was opened? 64,476 bytes

2) What is the VSN associated with the volume from which a folder called “rust” was opened? 6c191b65

3) How many different computer names are present in the collection of LNK files? 4 ids

4) Based on analysis of the LNK files, what time did the Max Powers user account start downloading a KeePass .zip archive? 4/26/2018 4:29:30 PM **or** 4/26/2018 3:56:16 PM **– Maybe earlier for creation date**

5) How many different cloud storage services are referenced by the LNK files? 3, OneDrive, Google Drive, and DropBox

6) What is the name of the computer on which the “rich.pdf” file is stored? Stored on a USB

7) Based on analysis of the LNK files, what type of animals is the user of the “Sarah M” account interested in? Owls

8) What is the MFT record number (in decimal) of the file opened from a removable device on 02/02/2017 22:38:36 UTC? 3769120

9) When was the file “Owl_Emergency_Care.pdf” last modified in the “New Pet Care” directory? 1/31/2017 7:09:01 PM

Parse and Analyze Jump Lists

Parse the Jump Lists located in the “Recent\AutomaticDestinations” folder using JLEmd and answer the following questions:

10) What is the name of the largest file referenced by the jump list records? SnowyOwl.jpg

11) What is the name of the subdirectory within the “maxpowers” user account folder where a Python script appears to be stored? Stuff **or** Documents

12) When was the file “C:\Users\Win7\Documents\Personal.docx” last opened? 3/2/2014 6:45:20 PM

13) When was the file “Pygmy Owl.jpg” created in the “Pets” directory? 1/27/2017 4:52:02 PM

14) What is the computer name of the system from which “EventIpAddresses.xlsx” was opened? desktop-edslqm8

15) 15) How many different computer names are present in the collection of jump list records? 3

16) Based on AppID, how many different versions of Excel are represented in the collection of jump list records? 2

17) Based on the jump list records available for analysis, what is the most recently used web browser? Edge Browser

Analyzing the NTUSER.DAT Registry Hive

Parse the NTUSER.DAT registry hive located in the “Reg” folder using RegRipper and/or view the hive contents using Registry Explorer to answer the following questions:

18) What version of Python was downloaded to this system? 2.7.14

19) What is the name of the directory in which “Starter.docx” is stored? C:\Users\maxpowers\Documents\Starter.doc

20) What version of KeePass appears to be installed or used on this system? 1.35

21) When was the file “Database.kdb” last opened? 2018-04-26 16:32:46Z **or** 2018-05-04 21:55:06Z

22) What is the file extension most recently opened by this user account? .msc

23) Based on the UserAssist subkey, how many times was “mspaint.exe” executed by this user account? 7

24) Based on the “Run” subkey, how many programs are configured to start when this user account logs on to the system? o

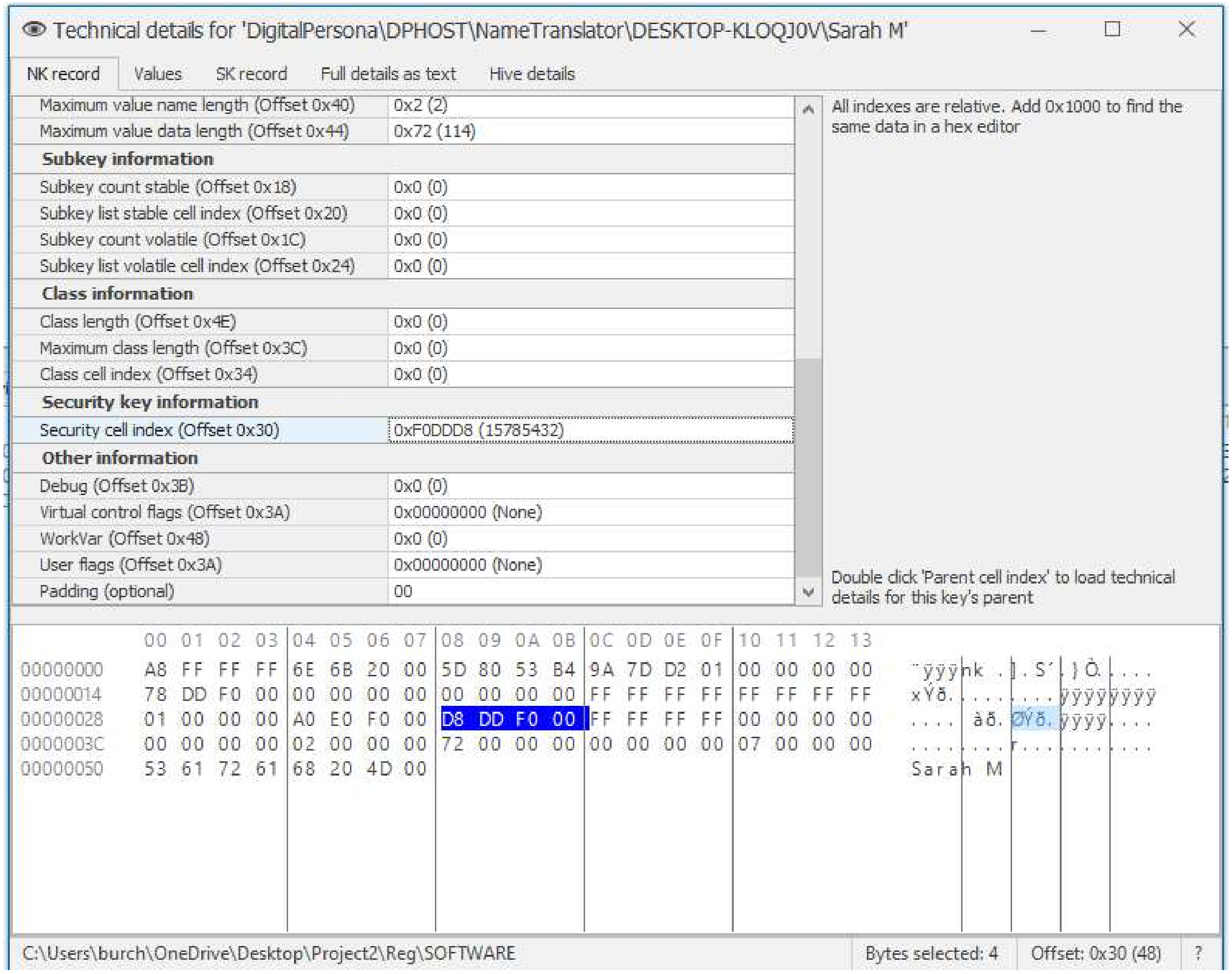
25) When was the program “atom” installed on the system? 2017-09-29 13:41:38Z

Analyzing the SOFTWARE Registry Hive

Parse the SOFTWARE registry hive located in the “Reg” folder using RegRipper and/or view the hive contents using Registry Explorer to answer the following questions. NOTE: If you receive a Due: 03/02/2021 11:59 PM prompt from Registry Explorer requesting to replay the transaction logs, select “No” to proceed without replaying the transaction logs, then “Yes” to load the ‘dirty’ registry hive.

26) Based on the “Run” subkey, how many programs are configured to start when this computer starts? 4

27) What is the Security Identifier (SID) associated with the "Sarah M" user account? Ends in 1002



Technical details for 'DigitalPersona\DPHOST\NameTranslator\DESKTOP-KLOQJ0V\Sarah M'
NK record
Values
SK record
Full details as text
Hive details

Maximum value name length (Offset 0x40)	0x2 (2)
Maximum value data length (Offset 0x44)	0x72 (114)
Subkey information	
Subkey count stable (Offset 0x18)	0x0 (0)
Subkey list stable cell index (Offset 0x20)	0x0 (0)
Subkey count volatile (Offset 0x1C)	0x0 (0)
Subkey list volatile cell index (Offset 0x24)	0x0 (0)
Class information	
Class length (Offset 0x4E)	0x0 (0)
Maximum class length (Offset 0x3C)	0x0 (0)
Class cell index (Offset 0x34)	0x0 (0)
Security key information	
Security cell index (Offset 0x30)	0xF0DDD8 (15785432)
Other information	
Debug (Offset 0x3B)	0x0 (0)
Virtual control flags (Offset 0x3A)	0x00000000 (None)
WorkVar (Offset 0x48)	0x0 (0)
User flags (Offset 0x3A)	0x00000000 (None)
Padding (optional)	00

All indexes are relative. Add 0x1000 to find the same data in a hex editor

Double click 'Parent cell index' to load technical details for this key's parent

```
          00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13
00000000  A8 FF FF FF 6E 6B 20 00 5D 80 53 B4 9A 7D D2 01 00 00 00 00   ¨ÿÿÿnk .].S´.}Ò.....
00000014  78 DD F0 00 00 00 00 00 00 00 00 00 FF FF FF FF FF FF FF FF   xÝð.........ÿÿÿÿÿÿÿÿ
00000028  01 00 00 00 A0 E0 F0 00 D8 DD F0 00 FF FF FF FF 00 00 00 00   .... àð.ØÝð.ÿÿÿÿ....
0000003C  00 00 00 00 02 00 00 00 72 00 00 00 00 00 00 00 07 00 00 00   ........r...........
00000050  53 61 72 61 68 20 4D 00                                       Sarah M
```

C:\Users\burch\OneDrive\Desktop\Project2\Reg\SOFTWARE | Bytes selected: 4 | Offset: 0x30 (48) | ?

28) What is the Volume Serial Number (VSN), in decimal, associated with the SanDisk Cruzer Glide USB device that was connected to the system? 2159839650

29) What is the LastWrite time associated with the "Microsoft\DirectPlayNATHelp\DPNHPAST" subkey? o

30) What is the name of the "Foxit Software" application that is installed on the system? Foxit_ConvertToPDF

31) What version of operating system is installed? Windows 10 (Pro)

32) When was the operating system installed? Fri, 27 Jan 2017 02:58:47

Analyzing the SYSTEM Registry Hive

Parse the SYSTEM registry hive located in the "Reg" folder using RegRipper and/or view the hive contents using Registry Explorer to answer the following questions. NOTE: If you receive a prompt from Registry Explorer requesting to replay the transaction logs, select "No" to proceed without replaying the transaction logs, then "Yes" to load the 'dirty' registry hive.

33) Based on the USBSTOR subkey, how many USB devices appear to have been connected to this system? 2

34) What is the serial number of the SanDisk Cruzer Glide device? 20051739911AEEC1DE29&0

35) What is the computer name of this system? DESKTOP-KLOQJ0V

36) When does the computer name of this system appear to have been last changed or set? 1/27/2017 2:32:40 AM +00:00

37) Based on the ShimCache, what is the last modification time of "C:\WINDOWS\sysWOW64\wbem\wmiprvse.exe"? o

38) For the "Standard Profile" configuration of the Windows firewall, what is the default logging location for firewall logs? o

Analyzing the UsrClass.Dat Registry Hive

Parse the UsrClass.Dat registry hive located in the "Reg" folder using Shellbags Explorer and answer the following questions:

39) What is the name of the .zip file located in the user's Downloads directory? webbrowserpassview.zip

40) Based on the user's interaction with the Control Panel applet, what type of activity does it appear the user was conducting in the Control Panel? Due: 03/02/2021 11:59 PM Change an account?

41) What is the first interacted timestamp of the "C:\Python27\Lib\site-packages\requests2.18.4.dist-info" directory? First interacted with: 2018-03-13 18:12:26.178

42) Based on shellbags analysis, how many subdirectories are visible within the "C:\Projects" directory? 8

43) Based on shellbags analysis, what is the name of the last directory with which this user account interacted? Users