**Objectives and Directions:**

The objective of this assignment is for you to demonstrate your knowledge, skills, and abilities in examining and analyzing the Microsoft Windows 10 registry hives. You will be asked a series of questions based on the registry hive files provided with this assignment, which were created on a Windows 10 Enterprise virtual machine. You may use any software tools, but you are expected to validate your findings. Failure to validate your findings may result in incorrect answer based on the technical data you must provide in this assignment. Non-forensic tools (ie: Regedit.exe) may provide inaccurate results since these programs may alter the dates/times or other data. Be careful and validate your answers! Selection of tools may be derived from the lecture materials or other sources. Some level of research may be required in this assignment as not all of the procedures or data structures are discussed within the lecture material.

***NOTE: If you are asked to retrieve information from the registry hives provided for this practical, you are required to provide the name of the HIVE file, owner (if applicable), full qualified path, subkey or value name/data, as required. Failure to do so will result in no credit for the question.***

***NOTE: When requested to provide a date/time, the interpreted value must be translated based on an offset of GMT/UTC (-0000).***

1. List the software tools you used for this examination. Be sure to list the title of the software, version number or identifier, and the vendor/author.
2. What does BCD stand for, and what is the purpose of this registry hive?
3. True or False: The file system is currently updating the last accessed date and time field in the MFT or related file system files.
4. Decode the FILETIME value **3D 46 33 44 DD F6 CF 01** as Windows 64-bit Hex in UTC (-0000).
5. What is the SHA1 hash value of the file named SAM?
6. In a stand-alone installation of Windows 10 (not on a network domain), what is the name of the registry hive where user account passwords stored?
7. What is the “RID” of the user named Lizzy?
8. When is the last time the user “Harold” last logged in according to the data in the SAM hive?
9. What is the password hint provided for the “Red” profile?
10. What is the logical size of the user tile (graphic) for the Lizzy account?
11. What is MD5 hash value of the user tile (graphic) for the Lizzy account?
12. On a Windows 8 system, what is the parent folder name of all user profiles on the local machine, by default?
13. In Windows XP through Windows 10, each user account contains a registry hive file in the root of the user’s profile/folder. What is the name of this file?
14. In Windows 8 or 10, where are the SAM, SYSTEM, SOFTWARE, and SECURITY registry hives located? Provide the fully qualified directory path.
15. What is the name of the registered owner and organization?
16. Based on your analysis of the SYSTEM hive, what is the volume letter assigned to the operating system?
17. What is the date and time of installation for the operating system?
18. What is the current time zone name on the local machine?
19. What is the standard offset from GMT/UTC (number of minutes)?
20. Is automatic daylight savings enabled?
21. Is the last accessed date and time on files turned on based on your analysis of the registry hives?
22. Although you only have the registry hives from a Windows 10 system, assume that the volume contained a Recycle Bin folder with the folder name ending in “1004.” Assume the registry files you are examining were derived from the same system. What is the friendly name of the user that has a RID of 1004?
23. For Lizzy’s account, are files moved to the Recycle Bin or immediately deleted from the volume (volume with a GUID of {70e7c111-0000-0000-0000-f01500000000})?
24. What is the logical path of the last location that Lizzy opened in the Windows Registry?
25. For Lizzy’s account, is Remote Desktop enabled?
26. For Lizzy’s account, is the firewall enabled for private networks?
27. What is the name of the hive file and logical path for the subkey that stores user name and SID information for domain authenticated accounts?
28. Is User Account Control enabled for Red’s account?
29. What is the product name for the operating system?
30. Is there any evidence of Lizzy opening the BC Wipe Installer file? Where is this information stored and in which hive? How many times was the application executed?
31. What is the name of the financial software that ONLY Lizzy installed? What is the ROT13 encrypted value name?
32. How many times did Lizzy execute the Sticky Notes app?
33. What date and time did Lizzy access Skype?
34. Did Lizzy run any encryption software? If so what is the name of the program, and when was it executed?
35. What is the computer name as it would appear on a network?
36. What is the DHCP IP address?
37. What is the gateway IP address?
38. Is TrueCrypt a running service on the local machine?
39. Lizzy is suspected of visiting a website to view downloads for a program called GNU Cash. What is the full URL?
40. When did Lizzy access the URL related to question 39?
41. When a user logs in to Windows, what notice and caption appear on the screen?
42. When Lizzy views files in Windows (File) Explorer, will hidden files appear?
43. When Lizzy views files in Windows (File) Explorer, will file extensions appear?
44. What is the most recent typed URL for Lizzy’s account in Internet Explorer?
45. What is the main start page for Internet Explorer?
46. What are the URL’s for any other tabs that appear when Lizzy opens Internet Explorer?
47. What is the NTFS disk signature that is associated with the C: volume (provide hex values)? *NOTE: This topic is not covered in the lecture, and you need to research this issue.*
48. Based on question 47 and the associated data, in what hive file is this data located?
49. Based on question 47 and the associated data, what is the byte offset to the start of the volume?
50. In what physical sector does the volume boot record reside?