Scenario:

Upon hiring a new software developer, a company issued a Windows 10 based laptop to a new employee. Within four weeks of starting the new role, the employee was observed writing a social media post about purchasing a new high-end electric car that was inconsistent with their salary. In addition, the employee called in sick after just a few days on the job. The internal security team tasked with monitoring the social media accounts of their employees observed what appeared to be an attempt to sell intellectual property to someone within the Asian Pacific region. The security team retrieved the laptop and acquired an image of the disk drive to conduct a search for digital evidence.

Examine the resulting E01 File (Strongwill.E01x) and answer the questions below.

1. **What is the MD5 hash sum of "Strongwill.e01"?**
A: b5ae724f3c01a1daf94be64aa2cde231
B: b89989fd98f89d898a989d927346473
C: dbe1301e2d1345038db84a25d4f5718e
D: 9bacc29977891c009c3cea53c12cf93f
E: Skip

2. **What is the name of the examiner who created "Strongwill.e01"?**
A: Examiner (Blank no data input upon image creation)
B: Strongwill
C: R. C. Ahtac
D: J. D. Nicks
E: Skip

3. **What are the total number of sectors of the system?**
A: 265148416
B: 298989898
C: 203984938
D: 209839399
E: Skip

4. **What version of Microsoft Windows is installed?**

A: Windows 10 Personal (Home)
B: Windows 10 Enterprise Evaluation
C: Windows Server 2019 Themed as windows 10
D: Windows 7 Service Pack 2
E: Skip

5. **What is the build number of the Microsoft Windows installation?**
A: 18362
B: 5D356
C: 19H1
D: 1903
E: Skip

6. **What is the installation date of the Windows Operating system? Answer in UTC.**
A: 8/21/2019 5:22:04 AM
B: 7/22/2019 7:19:04 AM
C: 1/1/2001 00:00:00 AM
D: 6/10/1990 11:34:02 AM
E: Skip

7. **The application "SamsungPortableSSD.exe" may have been accessed through the Explorer GUI. If this event occurred, what is the volume serial number of the drive where the application run process originated from?**
A: C6783AB1
B: C9382CD2
C: C6783BA1
D: C8372DA9
E: Skip

8. **This operating system is currently set to what time zone?**
A: EST
B: EDT
C: PDT
D: CST
E: Skip

9. **What is the volume name of the Virtual Hard Drive that exists on the system?**
A: HIDDEN
B: PRIVATE
C: SECRET
D: VHD
E: Skip

10. **What is the filesystem of the Virtual Hard Drive located on the primary partition of the system?**
A: FAT32
B: APFS
C: NTFS
D: FAT16
E: Skip

11. **What is the name of the primary User Account of this system?**
A: user
B: test
C: users
D: windows
E: Skip

12**. A file may have been uploaded to HTTPS://www.virustotal.com. If this occurred, what is the SHA-256 hash sum of the uploaded file?**
A: acd946343893c33d15a1e82e6fe4c8d5f6518518bfb7d04f70b0b8bdb3775356
B: 60662a8971a0509ded01240408ffd21fb379ee13b4aff5a3fe79f16748b91f10
C: cc351446b9c1d9da3a6a8a676af961f55c7b00d1b8fe4b3ff9c851d1e39c3029
D: 38ec73a46e7a6a7171c91dc003d135f01134e2311a5e868c797a1c8eaeb62583
E: Skip

13**. The application C:\ProgramData\Samsung Apps\Portable SSD\SamsungPortableSSD.exe was accessed. How many times was it in "focus"?**
A: 1

B: 2
C: 3
D: 4
E: Skip

14**. Located on the primary users' desktop is a file with the name "file.exe". What is this specific file type?**
A: Portable Executable 32
B: Word Document Extended
C: Mach-0 X86_64
D: ELF Binary Executable
E: Skip

15. **Locate the file named "supersizeme.exe". What is the logical file size of this file in bytes?**
A: 35,696
B: 43,029
C: 25,756
D: 45,988
E: Skip

16. **A photograph depicting a black Labrador retriever can be found on the primary partition of the system. What, if any location information can be obtained from the EXIF data associated with the image.**
A: No location information can be ascertained
B: General location information can be ascertained
C: Direct Latitude and Longitude can be ascertained
D: Multiple Latitudes and Longitudes can be ascertained
E: Skip

17. **What is the installation size of "Microsoft One Drive" in bytes?**
A: 151119
B: 198312
C: 141449
D: 100000
E: Skip

18. **On what date did the first successful login utilizing RDP occur on this system?**
A: 11/27/2018
B:07/27/2019
C:10/09/2019
D:07/22/2019
E: Skip

19. **Does it appear that any of the following instances of malware are present on the system?**
A:Code-red
B: Locky
C: Magecart
D: No evidence of any potential malware
E: Skip

20. **What is the modified UTC time for "notimetosaygoodbye.docx"as listed by the metadata?**
A: 2019-10-09T20:05:00Z
B: 2013-03-22T19:34:00Z
C: 2019-03-09T09:44:00Z
D: 2019-03-22T19:44:00Z
E: Skip

21**. The computer user named "user" may have navigated to the "Downloads" directory using "Explorer". If this occurred, what is the date of the last access time?**
A: The user did not access this directory.
B: 10/7/2019
C: 10/1/2019
D: 10/19/2019
E: Skip

22**. The computer operator may have used the Windows terminal application to calculate the MD5 hashsum of the file. If this occurred, what is the name of the file as indicated by the Windows terminal Application?**
A: iis.png

B: desktop.ini
C: hashme.txt
D: notimetosaygoodbye.doc
E: Skip

23. **Are any Korean (Hangul) word processor documents stored on "Strongwill.E01"? If so, what is modified time of the last document accessed?**
A: No Hangul Word Processor Documents contained within "Strongwill.E01"
B: 7/22/2019
C: 7/21/2019
D: 10/19/19
E: Skip

24**.What is the last time the application "BASH.exe" was run?**
Answer in UTC-24hr format.
A: 10/06/2019 16:42:38
B: 10/07/2019 16:43:28
C: 10/07/2019 04:43:28
D: 10/10/2019 04:43:28
E: Skip