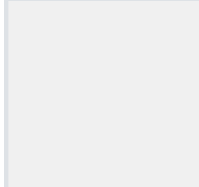

USE Forensics Image to answer question 1-25

Question 1

Not yet answered

Points out of 1.00



Flag question

Question text

What is the destination time zone offset in from UTC for the following email received by Jimmy Wilson "447018D5-00000006.eml"

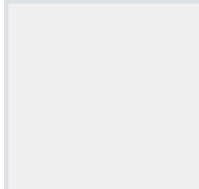
Select one:

- ☐ a. +04:00 E-Mail öffnen, Texttab öffnen
- ☐ b. -07:00 Message:Raw-Header:X-Received: ...Sun, 16 Feb 2014 09:55:13 -0800 (PST)
- ☐ c. -08:00
- ☒ d. -05:00
- ☐ e. -09:00

Question 2

Not yet answered

Points out of 1.00



Flag question

Question text

What is the total capacity in bytes (decimal) of the partition labeled "J. Wilson" found in the System.vhd file?

Select one:

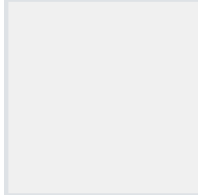
- ☐ a. 253,755,392

- ☐ b. 209,715,200
- ☐ c. 230,686,720
- ☒ d. 681,574,400
- ☐ e. 734,003,200

Question **3**

Not yet answered

Points out of 1.00



Flag question

Question text

What was the date and time the following email received by Jimmy Wilson "447018D5-00000006.eml" was originally sent?

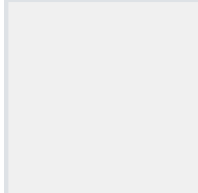
Select one:

- ☐ a. Sun, 16 February 2014 10:55:09 -05:00
- ☐ b. Sun, 16 February 2014 07:55:09 -05:00
- ☒ c. Sun, 16 February 2014 12:55:09 -05:00
- ☐ d. Sun, 16 February 2014 11:55:09 -05:00
- ☐ e. Sun, 16 February 2014 13:55:09 -05:00

Question **4**

Not yet answered

Points out of 1.00



Flag question

Question text

The physical disk contains a Virtual Hard Drive which is greater than 10MB in size, the full name of the file is: system.vhd

Select one:



True

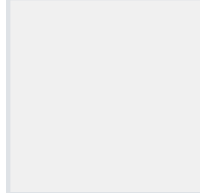


False

Question **4**

Not yet answered

Points out of 1.00



Flag question

Question text

The disk GUID (in hex) of the physical disk is: 6FAE8D386C441743AE3298C4BDE04830

Select one:



True



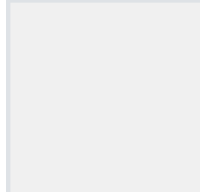
False

[Previous page](#)

Question **5**

Not yet answered

Points out of 1.00



Flag question

Question text

What is the cluster size in bytes within the second partition of the physical disk?

Select one:



a. 4,096



b. 512



c. 8,192



d. 2,048

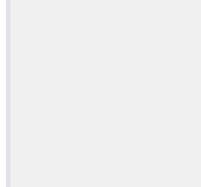


e. 1,024

Question **6**

Not yet answered

Points out of 1.00



Flag question

Question text

On February 20, 2014 @ 17:02:35 UTC -00:00, what was the system up time in seconds is: 9,634

Select one:



True

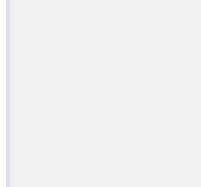


False

Question **7**

Not yet answered

Points out of 1.00



Flag question

Question text

The MD5 hash value of the pdf.pdf file is:
C1F95108A34228535A9262085E784D7C3E27FC68

Select one:



True



False

Question **8**

Not yet answered

Points out of 1.00

Flag question

Question text

The user account Jimmy Wilson has his logon password enabled and the password hint is safeone.

Select one:



True



False

[Previous page](#)

Question 9

Not yet answered

Points out of 1.00

Flag question

Question text

What is the partitioning format (Schema) of the physical disk?

Select one:



a. None of the other answers are correct



b. GPT



c. The Physical disk is not partitioned



d. MBE

Question 10

Not yet answered

Points out of 1.00

Flag question

Question text

The final destination IP Address for the following email received by Jimmy Wilson "447018D5-00000006.eml" is: 10.221.48.196

Select one:

- ☐ True
- ☐ False

Question 11

Not yet answered

Points out of 1.00

Flag question

Question text

The 2nd partitions unique GUID (in hex) of the physical disk is:
423FDC8AA701EE46AF5A70C06738E819

Select one:

- ☐ True
- ☐ False

Question 12

Not yet answered

Points out of 1.00

Flag question

Question text

What is the logical size in bytes (decimal) of the pdf.pdf file?

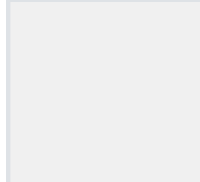
Select one:

- ☐ a. 444,332
- ☐ b. 433,994
- ☐ c. 395,232
- ☐ d. 253,283

Question **13**

Not yet answered

Points out of 1.00



Flag question

Question text

The User account BillyBob sent the following files to the \$recyclebin: New Price List.txt and New Price List Encoded.

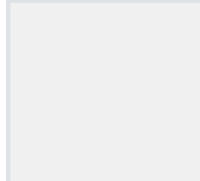
Select one:

- ☐ True
- ☐ False

Question **14**

Not yet answered

Points out of 1.00




Flag question

Question text

What is the logical file size in bytes (decimal) of the PLEAS.txt file?

Select one:

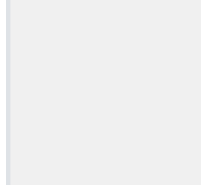
- ☐ a. 110,592
- ☐ b. 122,336
- ☐ c. 122,880

 d. 108,227

Question **15**

Not yet answered

Points out of 1.00



Flag question

Question text

Provide the full name of the User that has the RID number 0x3EB:

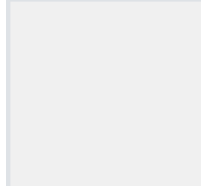
Select one:

- ☐ a. Administrator
- ☐ b. Betty Boop
- ☐ c. Joe T. Nameless
- ☐ d. BillyBob
- ☐ e. Guest

Question **16**

Not yet answered

Points out of 1.00



Flag question

Question text

When was the last log-in date and time for the User "Jimmy Wilson"?

Select one:

- ☐ a. February 18, 2014 12:38:16 UTC -00:00
- ☐ b. January 19, 2014 06:22:12 UTC -00:00
- ☐ c. March 03, 2014 11:11:11 UTC -00:00
- ☐ d. None of these times are correct
- ☐ e. February 19, 2014 13:30:58 UTC -00:00
- ☐ f. April 01, 2014 00:00:01 UTC -00:00



g. February 17, 2014 17:38:22 UTC -00:00

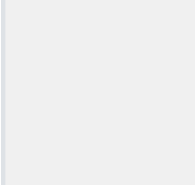


[Previous page](#)

Question **17**

Not yet answered

Points out of 1.00



[Flag question](#)

Question text

The following individuals: jose.Badguy@hushmail.com, robert.ripoff@gmx.com sent emails to the User Jimmy Wilson?

Select one:



True

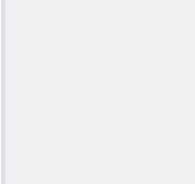


False

Question **18**

Not yet answered

Points out of 1.00



[Flag question](#)

Question text

What program did the User Jimmy Wilson have set to run when he logged on to the computer?

Select one:



a. None of the other answers are correct



b. Notepad.exe



c. StinkyNot.exe



d. MSAccess.exe

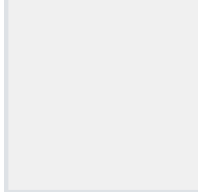


e. MSWord.exe

Question **19**

Not yet answered

Points out of 1.00



Flag question

Question text

The SHA1 hash value for the AISB08.pdf file is:
BDEBF09E8B2D404D1C483C3EBFB8AD37C780D909

Select one:



True

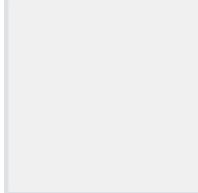


False

Question **20**

Not yet answered

Points out of 1.00



Flag question

Question text

What encryption programs were used on this computer?

Select one:



a. Veracrypt/BitLocker



b. BitLocker/Veracrypt



c. File Vault/Truecrypt



d. BCTextEncoder/Veracrypt



e. No encryption programs were used



f. Truecrypt/BCTextEncoder

Question **22**

Not yet answered

Points out of 1.00

Flag question

Question text

The SHA1 hash value for the Card Printers.htm file is:
F6CF04DB3D1BA828E375BBFE988876CE06164126

Select one:

- ☐ True
☐ False

Question **23**

Not yet answered
Points out of 1.00

Flag question

Question text

What search engine did the User "Jimmy Wilson" use to search for: how to steal identities?

Select one:

- ☐ a. Yahoo
☐ b. Bing
☐ c. DuckDuckGo
☐ d. Dogpile
☐ e. Google

Question **24**

Not yet answered
Points out of 1.00

Flag question

Question text

What is the last Date/Time the User "Jimmy Wilson" last ran the Windows Mail Application?

Select one:

- ☐ a. Sat, 25 January 2014 15:27:51 -00:00 UTC
- ☐ b. Sat, 25 January 2014 19:27:51 -00:00 UTC
- ☐ c. Sat, 25 January 2014 18:27:51 -00:00 UTC
- ☐ d. Sat, 25 January 2014 17:27:51 -00:00 UTC
- ☐ e. Sat, 25 January 2014 16:27:51 -00:00 UTC

[Previous page](#)

Question **25**

Not yet answered
Points out of 1.00

Flag question

Question text

What is the SHA1 hash value of the Physical Disk?

Select one:

- ☐ a. a1102c70a50768b588225fdcad6efa5d5d57341b
- ☐ b. None of the other answers are correct
- ☐ c. 5fdcad6efa5d5d57341ba1102c70a50768b58833
- ☐ d. 68b588225fdcad6efa5d5d5734b1a1102c70a507

[Previous page](#)

