Untitled Section

Statement 1 : Section 65 of Information Technology act deals with tampering with *
computer source documents
Statement 2 : Section 66 of Information Technology Act deals with publishing
information which is obscene in electronic form
Which of the following option is correct ?

○ Both of the statements are true

○ Both of the statements are false

○ Statement 1 is true and Statement 2 is false

○ Statement 1 is false and Statement 2 is true

Which of the following is tool for passwords cracking *

○ ERDCommander

● Autopsy

○ AccessFTK Imager

○ None of the above

_____ is a process used in computer forensics to extract *
data from a disk drive or other storage device without the
assistance of the file system that originality created the file.

● File Carving

_____ is a process used in computer forensics to extract * data from a disk drive or other storage device without the assistance of the file system that originality created the file.

○ File Carving

○ File Imaging

○ Both of the above

○ None of the above

Which of the following is not the type of volatile evidence.

○ Routing table

○ Main Memory

○ Log files

○ Cached data

Clear selection

_____ is a method of hiding secret data, by embedding it into an audio, video, image, or text file.

○ Disk imaging

○ Cryptography

○ Steganography

_____ is a method of hiding secret data, by embedding it into an audio, video, image, or text file.

○ Disk imaging

○ Cryptography

● Steganography

○ Disk Cloning

Clear selection

_____ is the process of copying the entire contents of one hard drive to another including all the information that enables you to boot to the operating system from the drive.

○ Disk imaging

● Disk Cloning

○ Packaging

○ Transporting

Clear selection

USB devices connected can be found in the following registry hive ? *

○ HKEY_LOCAL_MACHINE\Sam\CurrentControlSet\Enum\USBSTOR

○ HKEY_LOCAL_MACHINE\System\Enum\USBSTOR

docs.google.com/forms/d/e/1FAIpQLSdLK_wKAq2Hj8mj9AoRQvERRlO1dz3iHFPKPdFKQCKEIQY1QQ/formResponse

USB devices connected can be found in the following registry hive ? *

○ HKEY_LOCAL_MACHINE\Sam\CurrentControlSet\Enum\USBSTOR

○ HKEY_LOCAL_MACHINE\System\Enum\USBSTOR

◉ HKEY_LOCAL_MACHINE\System\CurrentControlSet\Enum\USBSTOR

○ HKEY_LOCAL_MACHINE\System\CurrentControlSet\USBSTOR

Which of the following is a database file in Windows XP , Windows Vista and Window's 7 that stores user's passwords. *

○ Software

○ Windows event log

○ AD

◉ SAM

Select the proper order of Data Recovery
1.Repair damaged files that were retrieved
2. Logical recovery of files, partition, MBR and file system structures
3.Image the drive to a new drive or a disk image file.
4. Repair the hard disk drive. *

○ 1,2,3,4

◉ 4,3,2,1

The evidence and proof that can be obtained from the electronic source is called the_____.

- ◉ Digital Evidence
- ○ Explainable evidence
- ○ Either A or B
- ○ Both A and

Clear selection

Choose the correct option *

- ○ Psscan - Plugin used for listing the processes in the evidence
- ◉ pstree - Plugin used for listing the processes in a tree view
- ○ getsids - Plugin to get PID of the process
- ○ None of the above

Which of the following are password cracking methods *

- ○ Syllable attack
- ○ Rainbow attack
- ○ Rule based attack
- ◉ All of the above

docs.google.com/forms/d/e/1FAIpQLSdLK_wKAq2Hj8mj9AoRQvERRlO1dz3iHFPKPdFKQCKEIQY1QQ/formResponse

Digital evidences are used to establish a credible link between_____.

○ Attacker and the crime scene

○ Victim and the crime scene

◉ Attacker, Victim and the crime scene

○ Attacker and information

Clear selection

_____ is based on trying all the strings in a pre arranged listing, typically   *
derived from a list of words

◉ Dictionary attack

○ Brute force

○ Rainbow

○ Rule based Attack

Having a member of the search team trained to handle digital evidence:

○ Can reduce the number of people who handle the evidence

○ Can serve to streamline the presentation of the case

○ Can reduce the opportunity for opposing counsel to impugn the integrity of the
Evidence

◉ All of the above

Digital forensics is all of them except:

◉ Manipulation of computer data

○ Extraction of computer data

○ Preservation of computer data

○ Interpretation of computer data

Clear selection

What are not the characteristics of Digital Evidence?

○ Admissibility

○ Convincing to Judges

○ Completeness

◉ warrantless search

Clear selection

Recovery of _____ can be crucial in the investigation of electronic crimes.

○ non-electronic evidence

○ electronic evidence

◉ Both

○ none of them

○ non-electronic evidence

○ electronic evidence

◉ Both

○ none of them

Clear selection

Video surveillance can be a form of digital evidence

◉ True

○ False

Clear selection

What does FTK stands for? *

◉ Forensic Tool Kit

○ Format Tool Kit

○ Forensic Transfer Kit

○ Format Transfer Kit

Back   Submit   Clear form