BTech-IV Subject-CLF Quiz 2

u19cs012@coed.svnit.ac.in (not shared) Switch account

Draft saved

* Required

QUIZ

Questions : 20
Marks : 20 Marks
Time : 20 mins

Which of the following is an example of volatile evidence? *

- (●) Running processes
- ( ) Download History
- ( ) Saved files
- ( ) Photos

Identify the correct option. *

- (●) Forensically Imaging is preferred because it gives access to system files which is not accessible in running system
- ( ) Data can not be recovered from Image file
- ( ) Data can not be recovered from cloned hard drive
- ( ) Forensically cloning is preferred becuase it is exact replica of image

Indian Information technology act does not apply to governors of Indian States and ambassadors of foreign countries *

- (●) True
- ( ) False
- ( ) Depends from state to state

Following state is True or False? *

1. With timestomp, anti-forensic technique, it is possible to change timestamp in $FN attribute but $SI can not be changed. $SI can only be manipulated at kernel level.

- ( ) True
- (●) False

Which of the following is not a property of faraday bag? *

- ( ) It protects evidence from electricity
- ( ) It protects evidence from magnetic effect
- (●) It protects evidence from heat
- ( ) It protects evidence from remote connection

Which of the following statement is not correct? *

- ○ From windows registry it is possible to identify USB devices connected to the system
- ◉ Prefetch can be used to identify the Microsoft office files that were executed in the system even if it were open from external drive
- ○ When a user customizes the folder, the details are stored in shellbags
- ○ Registry files can be acquired using FTK Imager and analysis can be done

Indian IT act applies to which of the following *

- ○ Will
- ○ Power of Attorney
- ◉ Cheque
- ○ Promissory Notes

Which of the following artifact gives program execution details? *

- ◉ Prefetch
- ○ Userassist
- ○ Jump Lists
- ○ LNK files

Which Section of Indian It act defines Protected System *

- ○ Sec 2(a)(1) of Indian IT act
- ○ Sec 69 of Indian IT act
- ○ Sec 69 B of Indian IT act
- ◉ Sec 70 of Indian IT act

Yellow dots can be examined in what type of evidence? *

- ○ Deleted documents
- ○ Scanned documents
- ○ Copied documents
- ◉ Printed documents

_____ of the IT Act , "Computer system " means device or collection of devices including input and output devices. *

- ○ Section 2(2)(I)
- ○ Section 2(1)(j)
- ◉ Section 2(1)(I)
- ○ None of the above

Which of the following statement is correct about write blocker? *

- ○ Write blocker does not allow to open a file from external hard drive
- ○ Write blocker does not allow to copy from work station to external hard drive
- ○ Write blocker does not allow to copy from external hard drive to work station
- ◉ Write blocker does not allow to rename file from external drive

Which of the following image file format does not store metadata? *

- ○ AFF
- ◉ Raw (dd)
- ○ SMART
- ○ E01

Which of the following evidence can not be found from windows registry? *

- ○ Name of the computer
- ○ USB devices attached to the system
- ◉ Timestamp of the file
- ○ Recently open files

Which of the following is protocol is used to transfer. mail from one mail server to other mail server? *

- [x] SMTP
- [ ] POP
- [ ] IMAP
- [ ] POP3

_____ means a document made by a person whereby he disposes of his property. *

- [ ] 1 . Trust
- [ ] 2. Will
- [ ] 3. Testament
- [x] Both 2 and 3

Which of the following is a measure to identify original website? *

- [ ] does not have any number in domain
- [ ] does not have sub-domain
- [x] Should have green lock symbol with https
- [ ] does not have green lock symbol with https

Indian Information Technology Act applies to cheque as well as the other negotiable instrument like bills of exchange and promissory noted etc. *

- ○ True
- ◉ False

Which of the following type of cybercrime describes gaining confidential information of the user through fake call. *

- ○ Hacking
- ○ Skimming
- ◉ Social engineering
- ○ Phishing

Which of the following is not a feature of Autopsy tool *

- ○ It can create timeline of the events
- ◉ It can identify original data stored behind steganography file
- ○ It can recover deleted data
- ○ It can generate report to be presented in the court of law

Back Submit Clear form

Never submit passwords through Google Forms.

This form was created outside of your domain. Report Abuse - Terms of Service - Privacy Policy

Google Forms