


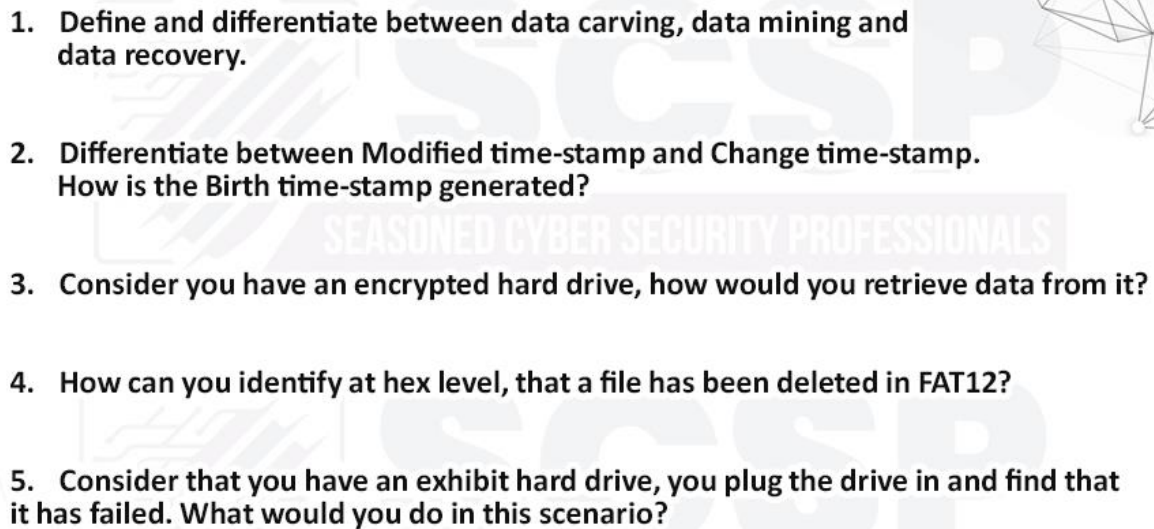


30 Questions Every Digital Forensics Investigator Must Know.




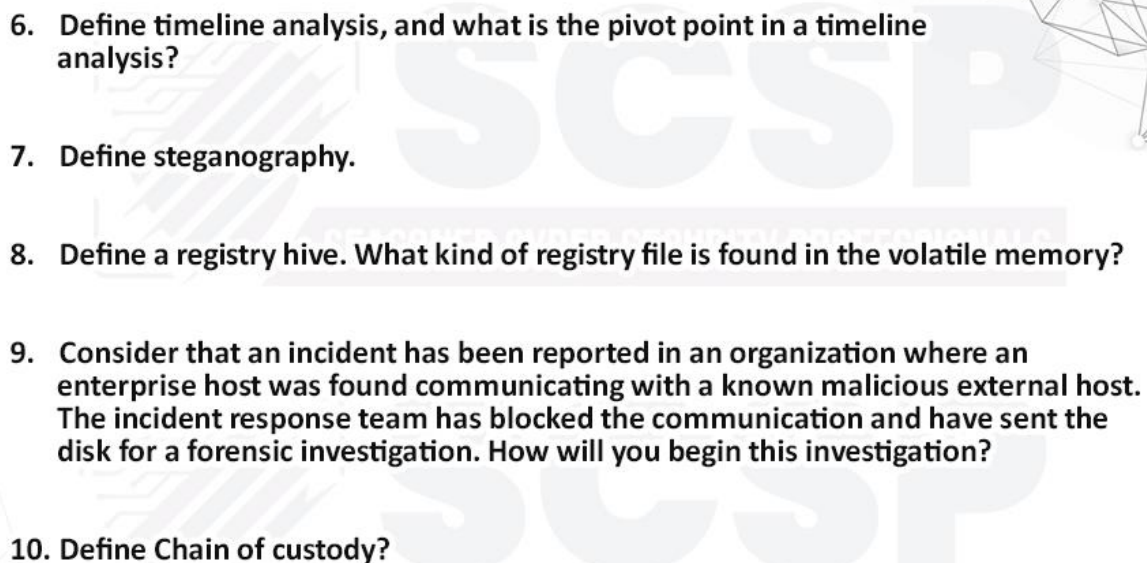
Follow us @scspcommunity



- 
- 
1. Define and differentiate between data carving, data mining and data recovery.
 2. Differentiate between Modified time-stamp and Change time-stamp. How is the Birth time-stamp generated?
 3. Consider you have an encrypted hard drive, how would you retrieve data from it?
 4. How can you identify at hex level, that a file has been deleted in FAT12?
 5. Consider that you have an exhibit hard drive, you plug the drive in and find that it has failed. What would you do in this scenario?


Follow us @scspcommunity




- 
- 
6. Define timeline analysis, and what is the pivot point in a timeline analysis?
 7. Define steganography.
 8. Define a registry hive. What kind of registry file is found in the volatile memory?
 9. Consider that an incident has been reported in an organization where an enterprise host was found communicating with a known malicious external host. The incident response team has blocked the communication and have sent the disk for a forensic investigation. How will you begin this investigation?
 10. Define Chain of custody?

Follow us @scspcommunity





- 
11. What steps are taken in a Digital Forensics process?
12. How would you differentiate between a raw/dd image and E01 image?
13. You have just received a report from an end-user of a suspicious looking email in their inbox, what steps will you take to investigate this scenario?
14. What are the differences between logical, file and physical extraction of a cellphone?
15. You have been asked to collect all location data of an airport from a mobile phone, what will be your approach towards this task?



Follow us @scspcommunity




- 
16. What is the primary reason of not uploading a targeted malware to VirusTotal?
17. While conducting a DFIR activity, what evidence do you find the most relevant? Explain why?
18. Is monitoring DNS queries important? Explain why?
19. Without considering atomic IoCs, Explain three cases of detecting malicious activities within your network.
20. In the 'identification' stage of IR, why scope needs to be considered? Explain.




Follow us @scspcommunity



- 
21. Name a way to partially recreate the bash history data during an investigation. As a forensic artifact, what is the primary problem with it?
22. Without execution, how can a malicious file be identified?
23. How would you investigate a DDoS attack on your company's LAMP site?
24. Botnet attack can be detected using which primary source?
25. A sample was observed making an HTTP get request in a segregated virtual environment for a text file, but because the machine was not connected to the internet the text file was not downloaded. As an investigator, how would you proceed?

Follow us @ scspcommunity



- 
26. Consider you are investigating a new APT, what would be your analysis methodology? Also explain the behavior of an APT.
27. Consider you are given a Binary, how would you identify if it is packed or not and how would you identify the type of packer used?
28. During forensics, define the process for memory analysis.
29. During a hard disk forensic, how would you define unallocated space?
30. During an investigation, how would you handle conflicts in the directions given by different stakeholders?

Follow us @ scspcommunity

