Computer Forensics Interview Questions

INFOSEC INSTITUTE

Computer forensic investigators are in high-demand. Often referred to as digital forensics engineers, computer forensic investigators are expected to know basic IT skills, understand computer architecture and networking, have the ability to collaborate with various teams and write detailed reports. A digital forensics professional must have analytical and investigative skills, as well as strong attention to detail.

Interview Questions

Below are 25 questions to help you prepare for a next computer forensics interview when applying for a job.

What is MD5 checksum?

MD5 checksum is a 128 bit value that helps identify the uniqueness of a file. You can have two file names, but each will have a different checksum. You use these checksums to compare two different files to identify if they are the same.

Name some common encryption algorithms that are used to encrypt data

Some common ones include triple DES, RSA, Blowfish, Twofish and AES.

What is an .ISO file?

An ISO file contains an application or CD image of several files and executables. Most app software can be made into an ISO that you then mount as a virtual drive and can browse files within the ISO. New Windows versions come with internal ISO mounting capabilities.

What is a SAM file?

A SAM, or Security Accounts Manager, file is a file specifically used in Windows computers to store user passwords. It’s used to authenticate both remote and local Windows users, and can be used to gain access to a user’s computer.

What is data mining?

Data mining is the process of recording as much data as possible to create reports and analysis on user input. For instance, you can mine data from various websites and then log user interactions with this data to evaluate which areas of a website are accessed by users when they are logged in.

What is data carving?

Data carving is different than data mining in that data carving searches through raw data on a hard drive without using a file system. Data carving is essential for computer forensics investigators to find data when a hard drive’s data is corrupted.

What operating systems do you use?

Most computer forensic experts know at least one operating system well. Be honest with this question, but you should know either Windows, Linux or Mac operating systems well. Your interviewer will probably go into more detailed questions based on your answer.

What type of email analysis experience do you have?

Computer forensics relies on email analysis. You should be experienced with email servers such as MS Exchange and free web-based platforms such as Gmail and Yahoo.

What is steganography?

Steganography conceals a message within a message. In other words, someone can send an email message with content that says one thing, but every third word comprises a second message that makes sense to a recipient.

What are some common port numbers?

TCP port numbers are the virtual connections created by computers and applications. Common port numbers are 21 for FTP, 80 for web services, 25 for SMTP and 53 for DNS.

Describe the SHA-1 hash

The secure hash algorithm 1 is a hash algorithm that creates a 160-bit or 20-byte message digest.

Describe your experience with virtualization

Do not lie here. Be honest about your experience with virtualizations, but be sure to describe the virtual infrastructures you are familiar with, i.e., Virtualbox, VMWare, etc. Make sure you identify the types of operating systems you have dealt with. You do not have to prove you were a system administrator, but you need to at least understand virtual storage, partitioning, how to log into a virtual box and the benefits — as well as the security issues — with virtualization. It can save a company money by combining the use of resources and minimizing the amount of hardware a company has to purchase. But if there are issues with VM sprawl, which is when an admin duplicates a machine and forgets about it, it creates a vulnerability because those machines are not patched or hardened. This is a prevalent issue.

How would you handle retrieving data from an encrypted hard drive?

First determine the encryption method used. For simple encryption types, try finding the configuration file. Use tools such as EaseUS Data Recovery, Advanced EFS Data Recovery or Elcomsoft Forensic Disk Decryptor. You can also use brute force methods.

What port does DNS run over?

53

What are some security issues related to the Cloud?

The biggest issue is the increased potential for data breaches or exfiltration as well as the potential for account hijacking. The Man in Cloud Attack is a new threat specific to Cloud usage. It is similar to the MitM attack, where an attacker steals the user token which is used to verify devices without requiring additional logins. Cloud computing introduces insecure API usage, which is discussed on the OWASP Top 10 Vulnerabilities list.

Describe some of the vulnerabilities listed on the OWASP Top 10 Vulnerabilities list?

This list is updated yearly with the current top 10 application security risks. Cross-site scripting is one item that has been on the list year after year. But others on the most current list include injections such as SQL, OS and LDAP, security misconfigurations, sensitive data exposure and under-protected APIs.

What is an ACL?

An access control list. It is a list used to grant users and processes access to system resources.

How would you be able to tell at the hex level that a file has been deleted in FAT12?

Run fsstat against the FAT partition to gather details. Run fls to get information about the image files. This will return information about deleted files and the metatdata information.

What are some tools used to recover deleted files?

Recuva, Pandora Recovery, ADRC data recovery, FreeUndelete, Active UNDELETE, Active partition or File recovery and more.

What is a form of simple encryption often used by an intruder or criminal?

XOR (exclusive OR)

How do you stay up to date on current cybersecurity trends?

This is a personal question; make sure you can share newsletters and websites you visit often. These could include InfoSec Institute, Cyberwire, IT whitepapers, and podcasts or webinars given by companies like Nessus, Metasploit and SANS.

How do you handle conflicting direction from different stakeholders?

This question is to see how you handle conflict. The best way to answer is you would first consult your direct supervisor, explain the conflict and ask for guidance on how to proceed.

If you needed to encrypt and compress data for transmission, which would you do first and why?

Compress then encrypt. Because encryption takes up resources and can be cumbersome to perform, it makes sense to compress the data first.

What is the difference between threat, vulnerability and risk?

A threat is what a potential attacker poses, by potentially using a system vulnerability that was never identified as a risk. Using this answer provides context for the three terms together, but you can define them separately.

- A threat is the possibility of an attack.
- A vulnerability is a weakness in the system.
- Risks are items that may cause harm to the system or organization.

Describe your home network

In cybersecurity-related positions, interviewers often want to know your interest in security spills over into your personal life as well. Make sure you know the security features of your router or your specific ISP. Be sure to mention any additional security measures you have added to your home network.

Conclusion

During the interview process, you may also be asked to describe your familiarity with various operating systems, your experience with Encase and/or FTK, or about other tools. Computer forensics is still a growing field; many applicants have educational experience, but no real-world experience. If you lack real-world experience, you can still discuss things you do in your spare time to stay up to date with current trends and what separates you from other candidates. This is an in-demand field with ample opportunity.

Good luck!