1. What does OSINT stand for, and why is it important in modern intelligence operations?
2. How does the "CYA" method protect an OSINT analyst?
3. Explain the C.R.A.W.L. method used in OSINT investigations.
4. What are the ethical considerations in OSINT investigations?
5. How do OSINT investigations differ from traditional intelligence gathering?
6. What are the main challenges faced by OSINT analysts?
7. What legal aspects must be considered when conducting OSINT investigations?
8. How does OSINT contribute to cybersecurity and threat intelligence?
9. Explain the role of OSINT in corporate security and risk assessment.
10. How does OSINT support law enforcement agencies?
11. What is the purpose of a sock puppet account in OSINT, and how does it relate to managed attribution?
12. What are the key components of computer hygiene when conducting online investigations?
13. What are some common types of virus and malware protection used in OSINT investigations?
14. What role did ransomware play in the 2017 WannaCry cyber attack?
15. What are some best practices for ensuring privacy while conducting OSINT investigations online?
16. How does operational security (OPSEC) affect OSINT investigations?
17. What are the risks of using public Wi-Fi when conducting OSINT research?\
18. Explain the importance of VPNs and encrypted communications in OSINT.
19. How do web browser extensions assist in OSINT investigations?
20. What precautions should an OSINT analyst take when accessing potentially harmful content?
21. What type of information can you find using Google's advanced search operators like "site:" or "intitle:"?
22. What is geo-tagging, and how is it used in OSINT investigations
23. Describe the best investigative approaches for gathering intelligence from deep platforms like Facebook, Twitter, and Telegram.
24. Explain how social media research can be used to obtain and leverage personal data in investigations.
25. Describe the use of web-based and proprietary open-source search tools for conducting online investigations.
26. What are the key advantages of using specialized username search tools in online investigations?
27. How does using advanced search operators on Google help improve search results for investigators?
28. What role do proprietary tools like Pipl or Shodan play in OSINT research?
29. How can OSINT be used to track cryptocurrency transactions and financial fraud?
30. Discuss a real-world case where OSINT played a crucial role in solving a cybercrime investigation.

31. You are tasked with locating the digital footprint of a suspect using only OSINT tools. Describe your approach using various search engines and keyword strategies.
32. Compare and contrast the features of deep platforms like Reddit, Telegram, and Gab with traditional platforms like Facebook and Twitter from an OSINT perspective.
33. Explain the process of reverse image search and how metadata in images (EXIF data) can aid in OSINT investigations. Provide an example of how image metadata led to actionable intelligence.
34. Describe the use of DNS lookups, WHOIS data, and traceroute in geolocating a suspect or asset. How does each contribute to the technical profiling process?
35. Briefly explain the difference between the Deep Web and the Surface Web, including their scope, content, and how they are accessed.
36. What is the significance of analyzing email headers in identifying the IP origin of a sender?
37. Define Google Dorking and explain its application in OSINT investigations. Provide two examples of Google search queries that can be used to identify vulnerabilities or sensitive information.
38. Describe how analyzing email headers can help in OSINT investigations. Discuss what information can be obtained from email headers and how it can be used to trace the origin of an email.
39. Explain how EXIF data in videos can help track the origin of digital content.
40. List any three advanced search engines or tools other than Google used in OSINT and their key capabilities.