NTFS is one of the most common file system for computers.

1) (4 pt) Describe in your own words how the Master File Table in NTFS is structured.
2) (4 pt) What happens on disk when a file is deleted (without it going to the recycle bin)? What methods do you know that can be used to still retrieve the file content?
3) (2 pt) You are looking for a file with a specific known string (something distinct, like "AAAAAAAAAAAAAAAAAAAA") in it. How can you a) identify and b) retrieve all files that contain that string?

You are a court certified expert witness ("Sachverständige/r") and the prosecutor ("Staatsanwalt/in") asks you to join a police raid the next morning - something about an online bitcoin scam. They estimate to confiscate something like 3 servers and 10 workstations, plus the smartphones of the people there.

1) (4 pt) How do you prepare yourself for the raid, what do you plan to take with you?
2) (4 pt) In the basement you discover it is rather 100 servers, spread over multiple 19" racks, and more then 50 mobile phones. How do you proceed?
3) (2 pt) Describe in your own words the role of the expert witness in court cases and investigations by the police.

Different questions which do not justify a separate question on their own:

1) (2 pt) Why do SSDs and magnetic hard drives behave differently during analysis? What do you need to consider during analysis?
2) (2 pt) Describe in your own words the "order of volatility".
3) (2 pt) Why do investigators put smartphones into faraday cages? What could happen otherwise?
4) (2 pt) Why can it be useful to use psscan in addition to pslist in volatility?
5) (2 pt) What information can you retrieve from a windows registry regarding wifi networks, and where is it stored?

1) (4 pt) Where (and how) is encryption used on modern smartphones, PCs and in digital communication?
2) (2 pt) Describe use cases for both symmetric and asymmetric cryptography (in the context of digital forensics).
3) (4 pt) What different methods do you know to break/bypass encryption?

During an investigation you are tasked to analyze a modern Pixel phone running Android 12.0. The owner is not giving you the password/unlocking code.

1) (4 pt) Describe different methods to get access to the data nonetheless.
2) (3 pt) Describe **in your own words** what a "jailbreak" is, and why it can be useful during analysis. Can you bypass a user password with a jailbreak?
3) (3 pt) You obtain different access tokens and passwords for online services during analysis, and are allowed to use the to retrieve data. How do you proceed?