Case 1:
In a cyber fraud trial, the prosecution presents a witness, Maria, who testifies that her neighbor told her that the accused, Juan, hacked into a local bank's system. Maria admits she never saw Juan commit the act, but insists "many people in the barangay already know about it." The defense objects, claiming it is hearsay.

Questions:

1. Is Maria's testimony admissible under the rules of evidence?
2. What is hearsay and why is it generally inadmissible?
3. Could Maria's testimony be saved if her neighbor is brought in to testify?

Case 2:
A financial firm accuses a former employee of insider trading using unauthorized logins. The prosecution presents automatically generated server logs showing repeated access from the accused's credentials. The defense objects, claiming the logs are hearsay.

Questions:

1. Do server logs fall under the hearsay rule?
2. Which rule allows their admission as evidence?
3. What must be established for them to be admissible?

Case 3:
In an election protest, the petitioner presents a series of emails allegedly showing vote manipulation instructions sent by the respondent to IT staff. The defense argues the emails are fake and inadmissible unless properly authenticated.

Questions:

1. Are emails considered electronic evidence?
2. What must the petitioner prove to have the emails admitted?
3. What methods can authenticate emails?
4. If the petitioner only submits screenshots of the emails, are they enough?

Case 4:
A mobile game company collects personal data from children aged 8–12 without parental consent. They store names, locations, and browsing history, then sell this data to advertisers. Parents sue under COPPA.

Questions:

1. Did the company violate COPPA?
2. Why does COPPA require parental consent?
3. What penalties can the company face?
4. How could the company comply with COPPA?

Case 5:
An accounting firm under investigation for securities fraud orders staff to delete thousands of financial emails and alter electronic ledgers. Whistleblowers report the deletion to regulators.

Questions:

1. What law was violated?
2. Why does the violated law prohibit document destruction?
3. Can employees who followed orders also be liable?

Case 6:
A hacker obtains Carlo's Social Security number and uses it to apply for a loan. Carlo only learns about it when a bank demands repayment. Investigators trace the false loan application to a cybercriminal operating in another city.

Questions:

1. What crime was committed?
2. What elements must be proven for identity theft?
3. How can digital forensics help investigators?
4. What remedies can Carlo pursue?

Case 7:
Anna receives hundreds of threatening messages daily from an anonymous Twitter account. The stalker also posts her private photos without consent. Police investigate and trace the account to her ex-boyfriend.

Questions:

1. What cybercrime applies?
2. How does cyberstalking differ from simple harassment?
3. What electronic evidence can be used against the suspect?
4. Can Anna get a restraining order?

Case 8:
A group of hackers launches a Distributed Denial of Service (DDoS) attack on a government website, crashing its servers and disrupting public services. They claim it was a protest.

Questions:

1. Is the act considered a crime even if no data was stolen?
2. What type of crime is this?
3. Can "hacktivism" be a legal defense?
4. What penalties may apply?

Case 9:
During an online extortion case, a victim received threatening emails demanding payment in cryptocurrency. Hours later, the victim was fatally shot in a robbery. Before dying, he told his wife: "It's the same man who threatened me in those emails." The wife testifies in court.

Questions:

1. Is the victim's statement admissible even though it is hearsay?
2. Under what rule does it qualify?
3. Why are dying declarations considered trustworthy?
4. What supporting electronic evidence should be presented?

Case 10:
A student accuses a professor of harassment, presenting screenshots of inappropriate messages from the professor's Messenger account. The defense claims the screenshots could have been fabricated.

Questions:

1. Are screenshots alone enough to admit the evidence?
2. What must the student prove under the Rules on Electronic Evidence?
3. What other sources can authenticate the chats?
4. If the professor deleted the chats on his phone, can they still be recovered?