Q1.

According to the SecurityScorecard blog post "Looking for a Digital Forensics Expert Witness?", there are five attributes of an expert in digital investigations testimony:

1. **Experience:** The expert should have extensive experience in digital forensics and investigations, including experience testifying in court.
2. **Communication skills:** The expert should be able to clearly and concisely communicate complex technical concepts to a non-technical audience, including judges, juries, and opposing counsel.
3. **Ability to withstand pressure:** The expert should be able to remain calm and collected under pressure, especially during cross-examination.
4. **Objectivity:** The expert should be objective and unbiased in their testimony, and should only present facts and evidence, not opinions.
5. **Integrity:** The expert should be honest and ethical in their testimony, and should never intentionally mislead the court.

The SecurityScorecard blog post also identifies five attributes of effective testimony delivery:

1. **Clarity:** The expert should be able to clearly explain complex technical concepts to a non-technical audience in a way that is easy to understand.
2. **Conciseness:** The expert should be able to get to the point and avoid rambling.
3. **Credibility:** The expert should be credible and believable, and should present themselves in a professional manner.
4. **Professionalism:** The expert should be respectful of the court and all participants in the trial.
5. **Engagement:** The expert should be able to engage the audience and keep them interested in their testimony.

It is important to note that the attributes of an expert witness and the attributes of testimony delivery are not mutually exclusive. An expert witness should possess both sets of attributes in order to be effective in the courtroom.

Security scorecard. (2022). Looking for a digital forensics expert witness? guidelines and procedures for testimony. Security scorecard <https://securityscorecard.com/blog/looking-for-a-digital-forensics-expert-witness/>

Q2.

Ethics are key to being in the cybersecurity or even in other technology security fields. The CompTIA Candidate Code of Ethics provides a set of guidelines for certified individuals to follow. These guidelines cover a wide range of topics, including:

Honesty and integrity: Certified individuals must be honest and trustworthy in their dealings with clients, employers, and the public. They must not engage in any conduct involving dishonesty, fraud, deceit, or misrepresentation.

Confidentiality: Certified individuals must protect the confidentiality of their clients' information. They must not disclose any confidential information to unauthorized individuals or organizations.

Competence: Certified individuals must provide services competently and professionally. They must have the necessary skills and knowledge to perform their job duties effectively.

Responsibility: Certified individuals are accountable for their actions and decisions. They must take responsibility for any mistakes they make and work to correct them.

I believe that ethics are conditional in the sense that they may vary depending on the specific situation. For example, there may be times when a certified individual needs to break confidentiality in order to protect the public from harm. However, I believe that certified individuals should always strive to act ethically, even when it is difficult.

CompTIA. (2023). Professional code of ethics. Comptia. <https://www.comptia.org/testing/testing-policies-procedures/test-policies/continuing-education-policies/candidate-code-of-ethics>

Q3.

According to an article published in The Conversation, violating ethics could be a career-ender for digital forensics technicians. The article discusses the lack of a universal code of ethics for digital forensics technicians, but notes that there are a number of professional organizations and government agencies that have published ethical guidelines for the profession. These guidelines generally cover topics such as impartiality, objectivity, confidentiality, and integrity.

Cheating is an ethical violation. It is important for digital forensics technicians to be honest and transparent in their work. Cheating undermines the credibility of the technician and the evidence they collect.

The misuse of AI (Artificial Intelligence) can also be an ethical violation. If I were to use AI improperly for doing wrong things, such as altering evidence or hacking into systems, I would be violating the ethical standards of my profession.

If I were called to testify as an expert witness and my unethical behavior was brought up, it could have a number of negative consequences. I could be discredited as a witness, and my testimony could be given less weight by the judge and jury. In addition, I could be subject to disciplinary action from my employer or professional organization. I could also be held liable for my statements if they are found to be false or misleading.

I think here are the some ethical limits as a digital forensics technician:

I will not alter or destroy evidence.

I will not disclose confidential information.

I will not use my position for personal gain.

I will be honest and transparent in my work.

I will use AI responsibly and ethically.

Sloan III.J.John.(2015). There’s no code of ethics to govern digital forensics – and we need one. The conversation. <https://theconversation.com/theres-no-code-of-ethics-to-govern-digital-forensics-and-we-need-one-45755>