Excercises

1. Name the two main objectives of forensic readiness. Why are these objectives important for digital investigations?

2. What should you consider when identifying potential sources of the evidence?

3. What is the purpose of forensic tool testing? Describe the advantages and disadvantages of function-driven testing methodology.

4. You are hired as a network security architect at an enterprise. Your task is to implement a set of controls to get the infrastructure *digital forensics ready*. Describe what steps you would take.

5. Give examples of procedures to support a digital investigation process.

6. A security breach was identified in a system supporting a critical business process. The system has a 99.97% availability requirement. Describe the challenges in performing a forensic investigation under these conditions. Consider how you would resolve these challenges.