

1. Of the various kinds of data described in Chapter 5 of Electronically Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search, and Retrieval, 2nd ed., select one and describe. How is this data generated and where does it reside? Is it easy or difficult to collect and why? What are any special considerations with collecting this data?
2. Describe a document/data/electronic evidence that you would want to avoid having to produce to the opposing party. What kind of information does this item contain and why do you want to protect it? Under what doctrine (attorney-client privilege, attorney work-product, another confidentiality doctrine)? If you were the lawyer, what arguments would you make and what would you have to show?
3. Have you used any of the techniques/tools/methods outlined in Chapter 5 to look for data (hidden, deleted, corrupted, encrypted, created using proprietary software, stored on obsolete media)? If so, what did you use and how did it work out? If not, I invite you to try some of the suggestions from the author using features of the software that you already have available to you. Were you surprised by how easy/difficult this was and what you were able to access?
4. What are some of the considerations for storing data? What should we do to be certain that our data is secure in the event of a disaster or threat? What are some of the issues with choosing a cloud computing vendor for storage versus using physical devices?
5. What other options would you suggest for controlling access to information/data? What else would you suggest that could add an extra measure of protection, particularly for truly sensitive information/data?
6. Any other surprising or interesting points from Module 10, Module 11 or the reading assignment.