LECTURE 11

DIGITAL EVIDENCE / ACQUISITION & PRESERVATION

1. What is nonvolatile information?

* This includes information, configuration settings, system files and registry settings that are available after reboot.

1. What is the Order of Volatility?

* CPU registers, CPU cache, RAM
* Network cache, Virtual Memory
* Hard drives and flash drives
* CDs, DVDs and printouts.

1. What are the types of data?

* Persistent: Data is stored so it is available from session to session.
* Volatile: Data is created within an application session.
* Residual: Data is unintentionally left behind on digital media and it’s not active on computer.
* Metadata: Data about data.

1. What are the different types of files?

* User-Created Files
* User-Protected Files
* Computer-Created Files
* Actively created by users and may contain important evidence of criminal activity.
* Users can hide evidence in a variety of ways
* Evidence can also be found in files and other data areas created as a routine function of the computer’s operating system.