Week 2 Objectives

What is Forensic?

When do we do Forensic? Active Investigation vs Court Preparation

What information do we gather?

Harddrives and other storage devices, emails, documents, files, PDFs, executables, internet history, MetaData, system configuration information, IP addresses, host names, user names, system logs, last log-on, active time on-line, system status reports, text messages, phone logs,etc.

#1 to remember – is that what you are reviewing/working on could end up part of a case. Your research needs to be non-biased.

 Four main principals:

1. Do everything possible to ensure no data is modified when conducting your investigation
2. The individual doing the investigation must be competent and explain how and why of his/her actions.
3. Keep a clear log of exactly what you did. Make sure everyone understands.
4. The person in charge has overall responsibility for ensuring that the law and principles are adhered to.

Live Acquisition

Can’t shut the machine off…

* Due to processing
* Worried that something will change

Different Models

* Readiness, Evaluation, Collection, Analysis, Presentation and Review
* Mandate, Preliminary, Assessment, Execution, and Reporting
* Data Collection, Examination, Analysis, Reporting, and Recommendation

Issues

* Technical Issues
* Legal Issues
* Administrative