Week 6 Objectives

Digital Forensic Challenges

What are we trying to determine?

* Who did or/is doing what?
* When was it done?
* What was it changed from and to?
* Why? ... Being the most complicated Question

Programming

* 1st and foremost the application needs to have security in mind
* Identity management, Role separation, Logging
* Is the application designed to tell us who, when, what and why?

Company Investment in tracking technology

* Basic ability to pull logs
* Security Incident Event Monitor (SIEM) to correlate events

Encryption

Lack of Training

Lack of Resources

Volume of Data

Internet of Things/Device Proliferation

Cloud Computing

Legal Challenges

Number of Cases and Expectations for what’s possible