# Digital Forensics

Dr. Bhavani Thuraisingham
The University of Texas at Dallas

## Intelligent Digital Forensics

October 8, 2008

# Reading for October 8 Lecture

- **http://dfrws.org/2006/proceedings/7-Alink.pdf**
- XIRAF – XML-based indexing and querying for digital forensics

http://dfrws.org/2006/proceedings/8-Turner.pdf

- Selective and intelligent imaging using digital evidence bags

- http://dfrws.org/2006/proceedings/9-Lee.pdf
- Detecting false captioning using common-sense reasoning

# Abstract of Paper 1

- This paper describes a novel, XML-based approach towards managing and querying forensic traces extracted from digital evidence. This approach has been implemented in XIRAF, a prototype system for forensic analysis. XIRAF systematically applies forensic analysis tools to evidence files (e.g., hard disk images). Each tool produces structured XML annotations that can refer to regions (byte ranges) in an evidence file. XIRAF stores such annotations in an XML database, which allows us to query the annotations using a single, powerful query language (XQuery). XIRAF provides the forensic investigator with a rich query environment in which browsing, searching, and predefined query templates are all expressed in terms of XML database queries