

Personal Contact Information

- **Charles Shields, Jr., Ph.D., J.D.**
 - Research Associate at University of Texas at Dallas (UTD)
 - cshields@utdallas.edu
 - www.utdallas.edu/~cshields

Review of Two Papers

- **Richard T. Snodgrass, Stanley Yao and Christian Collberg**, "Tamper Detection in Audit Logs," In *Proceedings of the International Conference on Very Large Databases*, Toronto, Canada, August–September 2004, pp. 504–515.
- **Kyri Pavlou and Richard T. Snodgrass**, "Forensic Analysis of Database Tampering," in *Proceedings of the ACM SIGMOD International Conference on Management of Data (SIGMOD)*, pages 109-120, Chicago, June, 2006.

"Tamper Detection in Audit Logs"

Overview of Paper

- Emphasize the fact that audit logs be correct and verifiable
 - Required now by several US Federal laws (e.g. Sarbanes-Oxley, HIPAA, etc.)
- Review of existing audit log techniques
- Presentation of their basic idea (converting the audit log to a **transaction time database** with periodic validation and notarization)
- Give some performance enhancements (e.g. opportunistic hashing, linked hashing)
- Performance graphs and final summary