

Edward L. Goings
Director, Forensic Technology



Tel 312 665 2551
Fax 312 665 5564

Email: egoings@kpmg.com

Employment:

KPMG LLP, Chicago

Manager, Forensic Technology Services
July 2001 - Present

Job Responsibilities: Develop and Manage Forensic Technology oriented engagements. Provided FTS services to other KPMG investigation and Dispute Advisory Services.

United States Air Force, Office of Special Investigation

Special Agent, Computer Crime Investigator

July 1999 - July 2001

Job responsibilities: Investigate intrusions into Department of Defense computer systems and networks and Conduct Computer Forensic Examinations in support of Federal Investigations.

Special Agent, Computer Forensic Field Examiner

September 1997 - July 1999

Job Responsibilities: Conduct computer forensics for the collection and preservation of electronic evidence.

United States Air Force

System Administrator

February 1996 - September 1997

Job Responsibilities: Operate and maintain Department of Defense secure communications systems and networks.

Security Police

Background

Currently a Director with Forensic Technology Services (FTS) for KPMG LLP, Chicago, IL. Ed develops and manages electronic investigations through digital evidence recovery and forensic data analysis. He oversees and conducts forensic examination of computer systems for the collection, preservation and admissibility of electronic evidence. I developed KPMG's Forensic Technology Service line in the Midwest.

Ed has thirteen years of active duty military service during which time he served as a Federal Agent in Computer Crime Investigations with the United States Air Force Office of Special Investigations. He has conducted computer intrusion investigations for the United States Air Force, conducted hundreds of Computer Forensic examinations on electronic stored data for the purpose of evidence preservation and admissibility in court, and have testified numerous times in Federal Court. He identified how and where intruders potentially access computer systems and then collected pertinent evidence to assist in prosecuting the perpetrator and provided valuable information to Air Force System Administrator on computer system's vulnerabilities and network security.

Selected Engagement Experience

- Major Natural Gas supplier had indication of internal fraud by top executives. Investigated allegations through downloading and searching over a million emails spanning over two years. The emails provided valuable evidence of executive cover-up and knowledge. Conducted computer forensic examination on computer systems located within the company that identified the level of involvement by each executive.

June 1988 - January 1996

Job Responsibilities: Enforce Federal and Department of Defense Laws on United States Air Force Installations.

Education/Certification/Training:

- Criminal Justice, North-East Louisiana University
- Industrial Security, University of the Air Force
- Graduate of the US Air Force Special Investigations Academy Special Agent Course
- Graduate of the Computer Crime Investigation Course
- Member of the Illinois Association of Computer Crime Investigators
- Member of the Association of Former OSI Special Agents
- Certified DOD Computer Forensic Field Examiner,
- MCSE 4.0
- Completed both the initial and advanced training in cyber hacking/incident response, Sytex, Inc.
- Completed computer investigation course, FBI Academy, Quantico, VA
- Certified NTFS File System Examiner, NTI Incorporated
- Certified DOD Computer Crime Investigator
- Certified System Administrator, Windows NT and Linux.
- Fluent in the Unix, Linux and Erix environment.
- Fluent on all platforms to include I386 and Dec Alpha.
- Holds current Top Secret / SCI security clearances.
- Certified MMPC (Emag

- Major automobile manufacturer had financial fraud in one of its foreign offices with approximately \$30 million dollars in unallocated funds. Recreated a database that allowed forensic investigators the capabilities to query and search four databases at once. Downloaded and searched over 350,000 emails spanning a six-month period. Conducted computer forensic examinations of key individuals personal computer systems. The examination identified knowledge that individuals had about the fraud.
- Major automobile parts manufacturer had financial fraud as a result of a top executive allegedly misusing corporate funds. Conducted an email download and searched of over 800,000 emails that identified how the executive was misusing funds for personal use. Conducted a computer forensic examination of multiple computer systems. The examination was vital in determining the total amount that was misappropriated resulting in \$10 million dollars being accounted for.
- Major titling agency had several top employees leave the company and allegedly stole over half of the companies' client base. Conducted computer forensic examinations of the former employees computer systems. It was identified through the examination that the employees had been planning the move for over a year and had been contacting clients before ever leaving and trying to convince them to come to their new company. Due to the evidence provided, the company filed a \$20 million dollar lawsuit against the former employees.
- Major food import company had two former employees leave to start their own business. Over half of the current client base followed the two employees to their new company. Conducted a computer forensic examination on both employees' computers. It was determined that

<p>Solutions)</p> <ul style="list-style-type: none"> ▪ Certified SMART (Forensic Software) ▪ Certified Encase ▪ Certified Email Examiner ▪ Certified ACL 	<p>both computers had been formatted in an attempt to destroy data. Recovered the data that provided valuable evidence of how the individuals had plotted for over nine months. Provided email from outside accounts i.e. yahoo email identified how the former employees lured clients to their new company. Based on the evidence provided, the company filed a \$15 Million dollar lawsuit against the former employees.</p> <ul style="list-style-type: none"> ➤ Top executive of a Fortune 500 Company was identified by IT personnel as possibly downloading child pornography from the Internet. Conducted a forensic examination of the executives computer system and determined that although the individual had downloaded over 35,000 pornographic images there were no images of child pornography. Determine the information the IT department saw was from pop-up created by adult pornographic web sites. ➤ Ex-CEO of a major credit card company was allegedly misusing corporate computer system for pornography and online gambling. Through a computer forensic examination, determined that the ex-CEO had downloaded thousands of pornographic images and had spent hundreds of hours at on-line casinos.
--	---