# Digital Forensic Evidence Examination

**4th edition**
**by Dr. Fred Cohen**

## About the Book

Digital Forensic Evidence Examination focuses on the scientific basis for analysis, interpretation, attribution, and reconstruction of digital forensic evidence in a legal context.

It defines the bounds of "Information Physics" as it affects digital forensics, describes a model of the overall processes associated with the use of such evidence in legal matters, and provides the detailed basis for the science of digital forensic evidence examination. It reviews and discusses digital forensic evidence analysis, interpretation, attribution, and reconstruction and their scientific bases, discusses tools and methodologies and their limits, and reviews the state of the science and its future outlook.

## About the Author

Dr. Fred Cohen is well known for his seminal work on computer viruses and defenses, critical infrastructure protection, security governance, and the use of deception and counter-deception in information security. As an educator, he has taught graduate courses in digital forensics for more than ten years, taught California POST certified courses, lectured at the Federal Law Enforcement Training Center, and given talks and guest lectures in digital forensics and related topics all over the world. As an expert witness, he has testified in cases at all levels, ranging from Federal criminal cases to civil disciplinary boards. He has created digital forensics tools including the *White Glove Linux* operating environment, the Unix-based *ForensiX* toolkit, and *ForWord;* built special purpose network forensics devices used by law enforcement and private investigations, published refereed journal articles and conference papers in digital forensics, is on editorial boards for publications in digital forensics and related areas, and is President and University Professor at California Sciences Institute.

For more information and to try out some of the more interesting analytical tools created by Dr. Cohen, call him up, visit his Web site at http://all.net/, or contact him via email.

Digital Forensic Evidence Examination

Fred Cohen

| Legal theory | Application | Legal context | | Calendar | Strategies |
|---|---|---|---|---|---|
| Methodology | Jurisdiction | Case type | Proof standard | Costs | |

| Evidence | Tools | People | Challenges | Legal process |
|---|---|---|---|---|
| Identify | Methodology | *Scientific* | Make/Miss | Pre-legal |
| Collect | History | Knowledge | Content | First filing |
| Preserve | Pedigree | Skills | Context | Notice |
| Transport | Reliability | Experience | Meaning | Preservation |
| Store | Testing | Training | Process | Productions |
| Analyze | Calibration | Education | Relationship | Disclosures |
| Interpret | Function | *Non-scientific* | Ordering | Depositions |
| Attribute | Limitations | Clarifying | Time | Motions |
| Reconstruct | | Observation | Location | Sanctions |
| Present | Litigants | Honesty | Corroboration | Admissibility |
| | Due care | Integrity | Consistency | Pre-trial |
| Destroy | Retention | Competence | Accident/intent | Testimony |
| | | | False positive | Disposition |
| | | | False negative | |

| Relevance | Admissibility | | Original writing |
|---|---|---|---|
| Authenticity | Probative > Prejudicial | Hearsay | |