Legal Aspects of Digital Forensics (cont) Careers & Certifications

Chapters 4, 5, 20
Digital Archaeology, The Art & Science of Digital Forensics

Legislated Privacy Concerns

Chapter 4

Right to Privacy?

- □ Founding fathers did not openly recognize privacy as a right
- Our definitions of "privacy" go beyond the scope of the Fourth Amendment
- □ Numerous laws have been passed to provide these rights

Well-known Privacy Laws

- □ Graham-Leach-Bliley, 1999
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Family Educational Rights and Privacy Act of 2008 (FERPA)

Privileged Communications

- Must be between or involve:
 - attorney and client
 - doctor and patient
 - litigation work product
 - protected intellectual property

Admissibility of Evidence

Chapter 5

Admissibility - Relevance

- ☐ Is the evidence relevant?
 - Must be material (directly related to case)
 - Must be probative (will prove something)

Admissibility - Authenticity and Credibility

- ☐ Is the evidence authentic?
 - Must be fact not opinion (except expert witness)

- ☐ Is the evidence credible?
 - Proof of no tampering Chain of Custody!

Admissibility - Competency

- ☐ Is the evidence competent?
 - Cannot be prejudicial (e.g. prior criminal record)
 - Cannot be restrained by statute (e.g. privileged communication, violation of Constitutional rights)
 - Cannot be hearsay

Authenticity Considerations

- ☐ Plain View Doctrine
 - ■Approaches:
 - •Inadvertence (US v Carey)
 - Prophylactic (US v Comprehensive Drug Testing)
 - •Rule created by courts, e.g. Miranda Rule
 - Computers as containers
 - •Warrant for container applies to contents

Scope of Search

- Particularity must be specific in context of search
- □ Breadth limited to original probable cause

Private Searches

- Internal investigations
- Digital vigilantes
 - ■Cannot be authorized by the government
 - ■Purpose cannot be to help the government

Licensing & Certifications

Chapter 20

Certifications

- □ General certification standards focus:
 - Admissibility of evidence
 - Standards and certifications
 - Analysis and preservation
- □ Vendor-neutral
- □ Vendor-specific

Vendor-Neutral Certifications

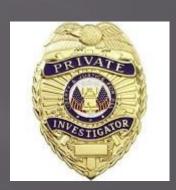
- Global Information Assurance Certification (GIAC)
 - SANS Institute
 - Associated with training course
 - Types:
 - GIAC Certified Forensic Analyst (GCFA)
 - GIAC Certified Forensic Examiner (GCFE)
- Certified Digital Forensic Examiner (CDFE)
- Digital Forensics Certification Board
 - Digital Forensics Certified Practitioner
 - Digital Forensics Certified Associate

Vendor-Specific Certifications

- ☐ Guidance Software
 - ■Encase Certified Examiner (ENCE)
 - ■Encase Certified eDiscovery Practitioner (ENCEP)
- ☐ AccessData
 - ■Summation Certified Enduser (SCE)
 - ■Summation Certified Case Manager (SCCM)
 - ■Summation Certified Administrator (SCA)
 - AccessData Certified Examiner (ACE)
 - AccessData Mobile Examiner (AME)
- □ Paraben
 - ■Paraben Certified Forensic Examiner
 - ■Paraben Certified Mobile Examiner

Licensing

- Requirements vary from state to state
 - In some states, vary from county to county
 - States rarely reciprocate on licensing requirements
 - Some states require you to get a PI license



QUESTIONS?