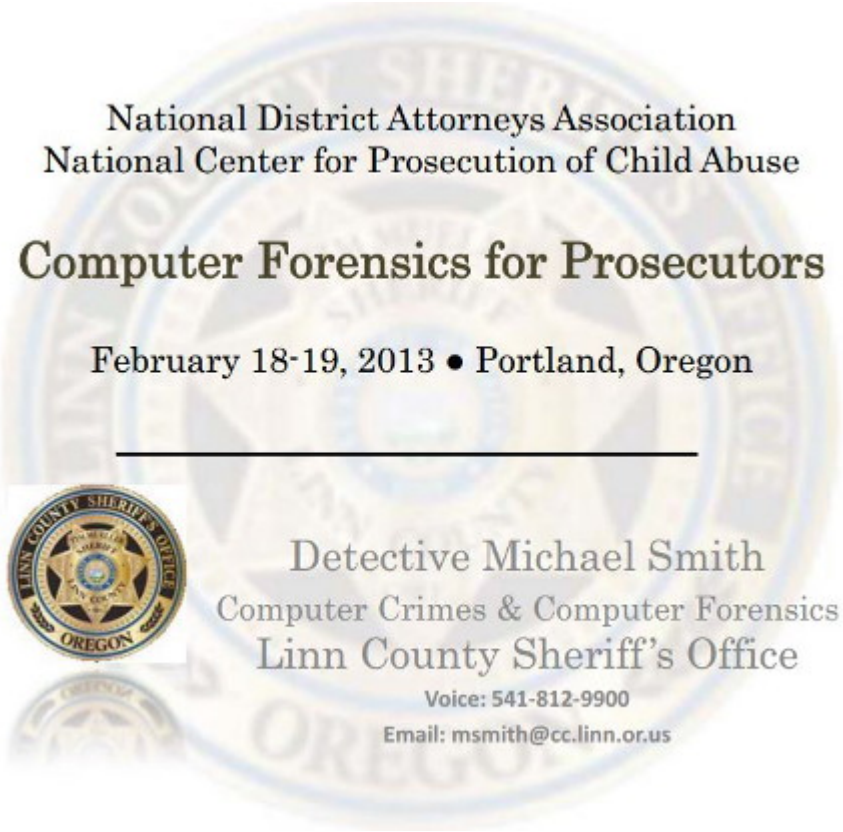
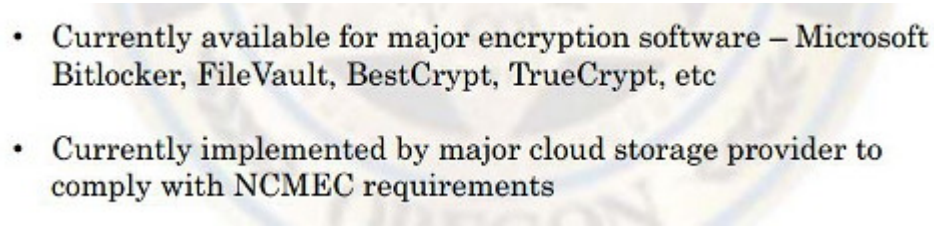
Computer Forensics for Prosecutors



Cryptome: Computer Forensics for Prosecutors 2013 und Computer Forensics for Prosecutors 2012 (via Fefe).

Ich finde es spannend, wenn die behaupten, sie könnten Truecrypt knacken. Es sei eine Hintertür vorhanden (S. 15). Wenn der oder die Betreffende keinen Fehler macht, gibt es kein realistisches Angriffsszenario gegen Truecrypt. Natürlich wird aber alles ausgehebelt, wenn das Opfer sich einen Keylogger unterjubeln lässt. Die Schwachstelle ist nicht Truecrypt, sondern das Passwort: „Seit Juli 2009 kursiert ein Bootkit für alle Windows-Versionen der x86-Architektur, welches die Eingabe des Kennworts für die TrueCrypt-Pre-Boot-Authentifizierung ausspähen kann.“ Das Rootkit muss aber erst auf den Rechner gelangen, und das geht nicht, wenn das Opfer nicht total bescheuert ist.



Ansonsten sind die Folien relativ „harmlos“ – nach der Devise: Schaut mal her, was wir schon alles können“ – und zum Teil Aufschneiderei wie schon die steilen Thesen der üblichen Verdächtigen, sie könnten einfach mal so „onlinedurchsuchen“.