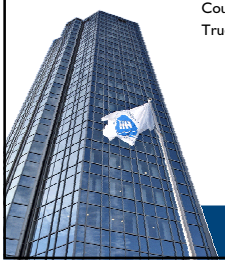
Antiforensics



Counter forensics
True crypt

Wecksten, Mattias
2009

True Crypt

- True Crypt baseras på tanken om ”rimlig tvivel”.
- Krypterat data ser ut som slumpmässig data eller oallokerat utrymme.
- Hävdar du med andra ord att det inte finns krypterat data så kan man inte visa på motsatsen.

Wecksten, Mattias
2009

Gömda enheter

- En lämplig strategi för att motivera eventuella spår av true crypt kan vara att nästla krypterade partitioner i varandra.
- Först en krypterad enhet som du anpassar så att den ser ut att innehålla hemlig eller kryptovärdig information. Till denna enhet kan du lämna ut lösenordet.
  - ”Decoy”
- I den första krypterade enhetens oallokerade utrymme kan du kapsla ytterligare en krypterad enhet som du håller hemlig.

Wecksten, Mattias
2009

Gömda operativsystem

- På samma vis som man kan ha gömda enheter kan man ha gömda operativsystem.
- Tänk på att använda ditt decoyoperativ så mycket som möjligt.
  - Annars ser det vid en granskning ut som om du inte använt datorn.
- Olika lösenord öppnar upp olika operativsystem.
- Decoyoperativet motiverar true crypt boot loadern.

Wecksten, Mattias
2009

Strategier

- Kan man göra dolda avbildningar av systemet över tiden så kan man analysera vart på diskarna data ändras.
- På så sätt kan man identifiera dolda enheter.

Wecksten, Mattias
2009

Antiforensics

- Kryptering
- Stenografi
- Self splitting
- Time stamping
- Wipe
- Hiding
- Atack på verktyget
  - Zip-bomb
- MD5 collisions
- BIOS Rootkit

Wecksten, Mattias
2009