Anti-Forensics: The Coming Wave in Digital Forensics

Marcus K. Rogers PhD, CISSP, CCCI

Definition

Attempts to negatively effect the existence, amount and/or quality of evidence from a crime scene, or make the analysis and examination of evidence difficult or impossible to conduct.

Categories

Data hiding

Artifact wiping

Trail obfuscation

Attacks against the CF process/tools

Already being discussed by the "Underground"

BlackHat USA • EUROPE • ASIA Briefings

CF Process

Multiphase approach

Crime scene identification/control

Evidence identification

Evidence preservation & collection

Evidence transportation

Examination and Analysis

Interpretation

Report and Presentation

Evidence Preservation & Collection

Hiding data from the acquisition tools:

•Altering the HDA or DCO at the drive level.

Attacks seek to prevent the creation of bitstream images or prevent integrity checking.

For the most part it is obvious that something is amiss.

Examination & Analysis

Documented attacks against

FTK, EnCase, iLook, WinHex, TCT, Sleuthkit, etc.

Compression bombs

Nested directories

Altering the MFT and inodes

File signature altering, hash fooling

The more automated the tool the more susceptible it is to attack!

Anti-Anti-Forensics

Understand what the tools are doing or supposed to do:

•Error logging on tools

•Don't automate everything by default.

•Funded research on AF

•Most research to date is grass roots and ad hoc.