Rapid Analysis of Live Response Data

July 2009

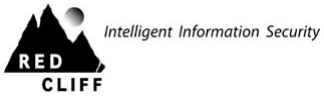
Kris Harms

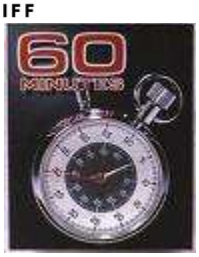
MANDIANT
INTELLIGENT INFORMATION SECURITY

Introductions

- Kris Harms
  - Incident Responder, Forensicator, Instructor, Crime Solver, Evil Finder

MANDIANT





ELSEVIER

MANDIANT Corporation

- Find evil. Solve crime.™
- Services, Software, Education
- Commercial and Federal Clients
- VISA Qualified Incident Response Assessor (QIRA)
- Washington, DC / New York / Los Angeles

MANDIANT

2

Agenda

- Live Response and Its Purpose
- Rapid Analysis Techniques For:
  - Autoruns
  - Process Listings
  - Handles
  - Event Logs
  - Timelines
  - Multiple LR Collections
- How to Cheat at Live Response Analysis
- Hail Marys of Analysis

MANDIANT

3

Demo

- Most of this presentation will be live demonstrations.

Tools Mentioned

- Sysinternals (Microsoft)
  - PSTool Suite

  (http://technet.microsoft.com/en-us/sysinternals/bb896649.aspx)
  - Logparser

  (http://www.microsoft.com/downloads/details.aspx?FamilyID=890cd06b-abf8-4c25-91b2-f8d975cf8c07&displaylang=en)
- Bit9 File Advisor

  (http://fileadvisor.bit9.com/services/search.aspx)
- Memoryze, RedCurtain, Highlighter

  (http://www.mandiant.com/software.htm)
- OpenPorts

  (http://tds.diamondcs.com.au/consoletools/openports.php)