Huron CONSULTING GROUP

User Panel

SANS WhatWorks in Forensics and IR Summit
July 7, 2009

Experience. Redefined.™

Background

Issue

- Employee resigned and suspected of going to competitor
- Another employee reported being solicited to follow suit
- Do we have a problem?

Technical

- Laptop-centric user base (Intel with WinXP)
- Full-disk encryption (WinMagic)
- Microsoft Exchange e-mail
- Users are local administrators

So what now…

Dead system forensics

- Live imaging (**FTK Imager**)
- Analysis database (**MS SQL Server**)
  - File system metadata (**EnCase**)
  - Link file decoding (**EnCase**)
  - INFO2 file decoding (**EnCase**)
  - Removable devices (**RegRipper**)
  - Internet History (**NetAnalysis)**
- TIF analysis (**EnCase**, **FTK**)
- UC analysis (**DataLifter**)

Live system forensics

- Remote connection (**F-Response**)
- Triage analysis (**Perl**)
  - Removable devices
  - File system metadata
- Live imaging (**EnCase**)
- E-mail analysis (**FTK**, **nuix**)
- Added to analysis database
  - Reporting
  - Correlation
  - Reconstruction
  - Timeline