AN EVOLUTION IN LIVE FORENSICS

Helix3 Live CDROM will evolve April, 2009. *

What you can expect from Helix3 Pro:

- Brand new framework with a seamless User Interface across Mac OS X, Windows, and Linux
- Boots most intel x86 machines including Mac OS X
- No reliance on 3rd party tools for acquisition - completely self contained

- The most forensically sound memory imaging utility. with no external libraries required
- The easiest, quickest, smallest footprint volatile data acquisition available

- New forensically sound, system preview capability
  - Preview and recover deleted files
  - Locate, preview, store all graphic files
  - Acquire system log files

- Complete plug in to the H3 Enterprise environment
- Ability to use CDROM or USB device

- Built in RAM analysis
  - Ability to search through live RAM
  - Enumerate all running processes (including those hidden by rootkits)
  - Identify all drivers loaded in memory (including those hidden by rootkits)
  - Report device and driver layering
  - Identify all loaded kernel modules
  - Identify hooks (often used by rootkits)

e-fense®

CARPE DATUM

* Some items not available in initial release