GENERAL DYNAMICS
Advanced Information Systems

Vendor Solutions Panel
SANS Forensic Summit 2010

David Nardoni

Remote Collection Challenge

- What we need
  - All examiners to be able to collect relevant evidence (Disk, memory, logs, packet captures)
  - Support for multiple platforms
  - Cost effective solution

Capabilities Developed

- Develop a tactical approach
  - Agent deployment and triage
  - Feedback to lead incident handler
  - Hand off to data preservation team
- Use laptops as jump points
- Ability to automate triage/collections processes (COM Object)
- Vendor response
  - When I call they respond quickly

Examples

- Leverage remote collection points into data centers
- Simplicity and price allowed more examiners to perform remote collections
- Automate triage collections through leveraging COM object

Questions

David Nardoni EnCE, CISSP, GCIH
Sr. Forensic Specialist
General Dynamics Advanced Information Systems
Network Defense and Digital Forensics
david.nardoni@gd-ais.com

GENERAL DYNAMICS