FORENSICS PANEL:

Troy Larson – Microsoft Corp – troyla@microsoft.com

Question

- What software tool or capability needs to be created that hasn't been created yet?

Question Answered BY Troy Larson

- Senior Forensics Investigator with Microsoft for six years.
  - Internal investigations involving Microsoft corporate assets.
  - Forensics and network security research.
- Lawyer by training.
- Geology and aquaria.

Answer

- *A tool to perform intelligent network imaging of volume shadow copies.*

Why?

- *Static, not dynamic, source for a "forensic" image of a volume.*
- *Imaging could be restarted from where it stopped (or disconnected).*
- *Continuously.*
- *Thus, a laptop could be imaged in "chunks," over several days, even as the user moves about the enterprise, connecting, disconnecting, and changing IP addresses.*
- *Solves the problem of how corporations can image 100 GB+ laptop hard drives over standard corporate wireless networks.*

Answer

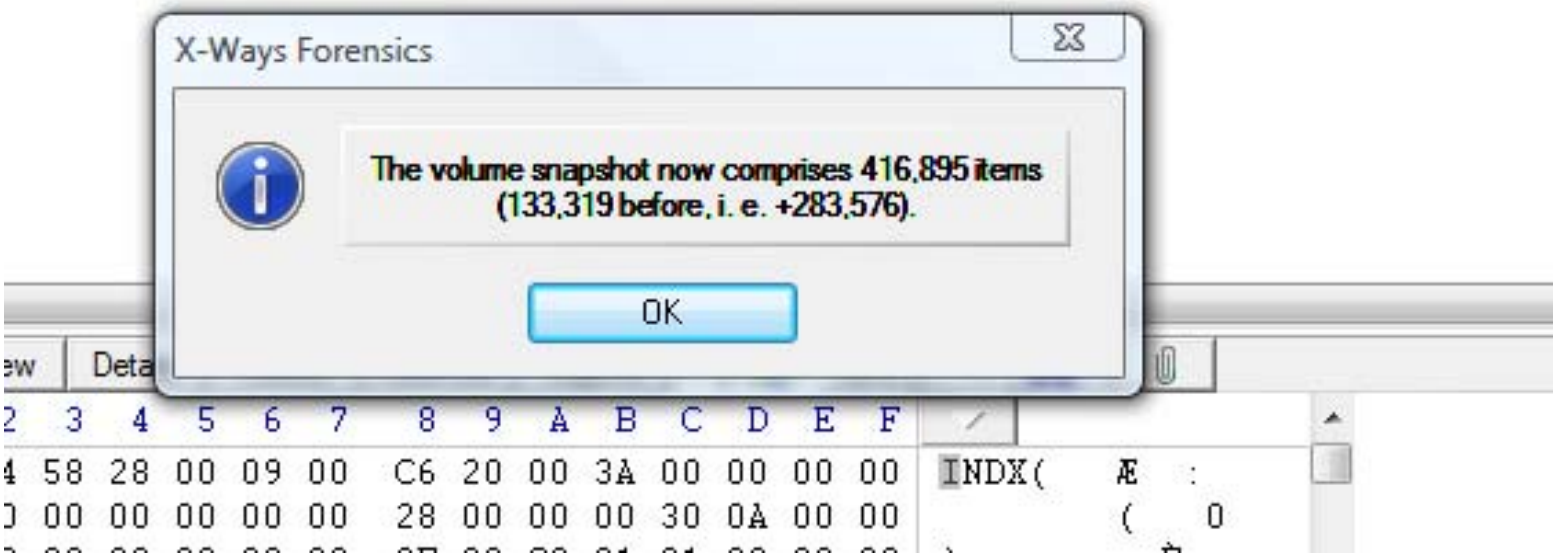
- Volume shadow copies are bit level differential backups of a volume.
  - 16 KB blocks.
- Shadow copies are the source data for Restore Points and the Restore Previous Versions features.
- Typically, shadow copies are created when a system boots up. Can be created at other times.
- The shadow copy service is enabled by default on Vista, but not on Windows 2008.
- Shadow copies reside in the *System Volume Information* folder.
- Shadow copies provide a “snapshot” of a volume at a particular time.
- Shadow copies can show how files have been altered.
- Shadow copies can retain data that has later been deleted, wiped, or encrypted.

Answer

Shadow copies can be imaged.

- Since shadows copies are **bit-level** differentials, imaged shadows will capture and reveal deleted data.

Answer



- Deleted data is captured by shadow copies, and is available for retrieval in shadow copy images.

Answer

- *We can image and process volume shadow copies as volumes.*

- *If an imaging tool could*
  - *image a shadow and |*
  - *know where it was in a shadow copy when it is disconnected and*
  - *start where it left off when reconnected:*
  - *Then, the imaging tool could image a volume, in parts, over time.*
  - *And network imaging will remain a viable procedure in a world where hard drive volume increases significantly faster than network bandwidth.*