Forensically Sound Windows Boot Disk for Acquiring Network Storage

Problem – Acquiring Evidence

- More and more evidence is stored in network data centers
- Massive amounts of data means that investigators must perform triage – they can’t acquire it all
- A forensically sound boot disk allows the investigator to perform triage on a server without modifying its contents

Problem – Current Solutions

- Many currently use Linux or DOS boot disks
- Linux drivers for the newest hardware (e.g. RAID, SCSI and Fiber Channel controllers) not available until much later than they are for Windows
- Linux write blocking is “weak” mounting read-only.
- Current boot disks do not support “remote forensics” where investigator access evidence on “the cloud”.
- DOS and Linux interfaces and systems are not familiar to a vast majority of forensic examiners

Solution – Tool Development

- Create forensically sound Windows boot disk (SAFE)
  - Ensure truly forensically sound write-blocking using a driver-level software write blocker
- Allow investigator to add drivers for new server hardware.
- Allow investigator to use familiar, Windows-based tools while in the boot environment.
- Support investigating RAID – massive storage
- Support “remote forensics” where investigator can access remote servers in a forensically sound way

Windows Software Write Blocking

- SAFE uses a filter driver for write blocking
- Allow interception of commands in Windows driver stack
- Block level performs most write blocking
- Other levels of filter drivers needed for other cases
- Drivers are loaded before OS can write to the disk

Results to Date

- Added the ability to dynamically add server drivers to forensically sound Windows boot disk.
- Added to the boot disk the ability to acquire data from hardware RAID
- Transitioned to SAFE product – marketed commercially by ForensicSoft, Inc.
- Created SAFE VNC a tool that works with the forensically sound boot disk to allow remote forensics

Impact

- Created the only modern software write-blocker verified to be forensically sound using NIST Software Write Blocking Test Suite.
- Plans to make the boot disk the only environment to have ability to access Software RAID and Windows Dynamic Disks in a forensically sound way.
- This platform is now essential for acquiring mass storage on modern servers
- No other reasonable solution exists for triage and forensically sound acquisition of Software RAID and Windows Dynamic Disks

Research sponsored by the National Institute of Justice