Preserving Electronic Evidence on OpenVMS

Wednesday, October 23, 2024

2024 OpenVMS Bootcamp
Marriott Long Wharf
Boston, Massachusetts

Introduction

- Differences between Technical & Legal
- Legal Needs
- Technical Measures
- Summary

Disclaimer

- I am not an attorney
- I do not play an attorney on TV
- Speak with legal counsel, they will be justifying your approach. You need to fully understand their needs; they need to understand technical limitations.

However

- I have consulted on digital evidence issues since 1987
- I have testified, in depositions and court
- Spoken since 1990 on digital evidence
- Contributor to the Computer Security Handbook (1995-2014)

Background

This presentation is law enforcement neutral. Rather, it is about “fair play.”

The “Boston Massacre” happened not far from this room room. John Adams, then a Boston attorney and the eventual second President of the United States successfully defended the British Officer and soldiers accused in that incident. That episode is one of the reasons for the the rights to counsel and a jury trial enshrined in the US Bill of Rights

Legal Contexts are different from Technical

- No “do overs”
- Finality
- One must respect the rules
- Precision is important

Agreeing on wording is not an agreement

- Definitions of “reasonable” vary
- You and your counsel are a team
- Listen to your counsel
- Proceedings are adversarial

Examples:

- Carolyn Warmous “Fatal Attraction” case
- Morgan Stanley v Sunbeam
- Discovery formats “Reasonable, Machine-readible”
- Sanctions; Directed verdicts; Exclusion

Exercise

- Graduate school “murder boards”
- Ask your counsel to put you through mock testimony and/or deposition – extra hostile

Authenticity and Provenance

- Alteration
- Accuracy
- Contemporaneous
- Knowing and proving are different

Routine Backups

- see “Murder board”
- Individuals leave; get sick; fuzzy memories
- Litigation over provenance is time consuming, costly
- Solution: Address provenance at artifact/backup creation

Documentation Costs

- Once organized; minutes per backup
- Discovery litigation: Often more than US$ 10,000
- Litigation is distracting to both technical and legal
- Provenance documentation is not in and of itself a privacy hazard.

Documenting Provenance

- CHECKSUM save set; Notarized affidavit
- CHECKSUM/FILE/ALGORITHM=SHA256
- Affidavit: Who; When; Filename; File length; SHA-256
- Notarize affidavit!!!!!
- Notarized affidavits are generally accepted; even if the signer is unavailable
- Large organizations often have notaries in-house

OpenVMS Systems and Forensics

- Almost all “forensic” training is PC-centric
- Relatively few forensic technicians know linux
- Almost all have never heard of OpenVMS

PC Forensics “Doctrine”

- Generally pull plug; “Tag and Bag”
- IDE, SATA, SAS, USB interfaces
- NTFS, FAT, extN file systems
- Heavily utilities/tools focused

OpenVMS does not match the frame

- Cannot generally just “pull the plug”
- Often uses Fast and Fast Wide SCSI
- Forensic Toolkits do not recognize FILES-11
- “tag and bag” often causes damage to data on enterprise storage arrays

Speaking of storage arrays

- oldest, e.g., HSxx: Volumes; possible RAID 0/1/5 support on a physical volume basis
- second oldest, e.g. P2000: partitioned tranches of drives
- Recent, e.g., MSA2052: Demand allocated “pages”
- inexperienced eyes can often not discriminate
- OS-hosted logical volumes: VMware, VirtualBox, Hyper-V, LD

Speaking of storage arrays – Potentially Nested

- an MSA2052 host logical NTFS volume which itself contains a VirtualBox logical disk for an OpenVMS-x86 instance, which itself contains an OpenVMS LD logical disk

Law enforcement bangs on the door without notice

- Have a plan
- Understand your system
- Document what transpires
- Planned response – call legal
- SEPERATELY Debrief all personnel afterwards; Keep notes
- Planned response – call legal

Summary

- Enhance procdedures to ensure documented provenance
- Document provenance of change logs; sources, etc.
- Increase scope of planning
- Ad hoc reactions are risky and challenging
- Being prepared is not costly

Questions?

Robert Gezelter Software Consultant
35 – 20 167th Street, Suite 215
Flushing, New York 11358 – 1731
United States of America

+1 (718) 463 1079
gezelter@rlgsc.com
http://www.rlgsc.com

Session Notes & Materials:
http://www.rlgsc.com/openvms-bootcamp/2024/index.html