JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Forensic Investigation Process

CYBER INCIDENT RESPONSE

Forensic Investigation Process

1. Determine what you want to find out
2. Determine location to find that info
3. Document your plan
4. Acquire/preserve the evidence needed
5. Perform initial analysis (log actions)
6. Conduct deeper analysis (log actions)
7. Report on your findings

Order of Volatility (Data Collection Priorities)

- CPU Cache, Registers, Running Processes, and Memory
- Network Traffic
- Hard Disk Drives and USB Drives
- Backups, Printouts, Optical Media

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

What do you do when you find something you don't expect?

- There's always a risk you will find what you didn't want to find…

…Employee breaking the AUP

…Evidence of illegal activities

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE