

# PFIC



**Paraben's Forensic Innovations Conference**

Park City, Utah

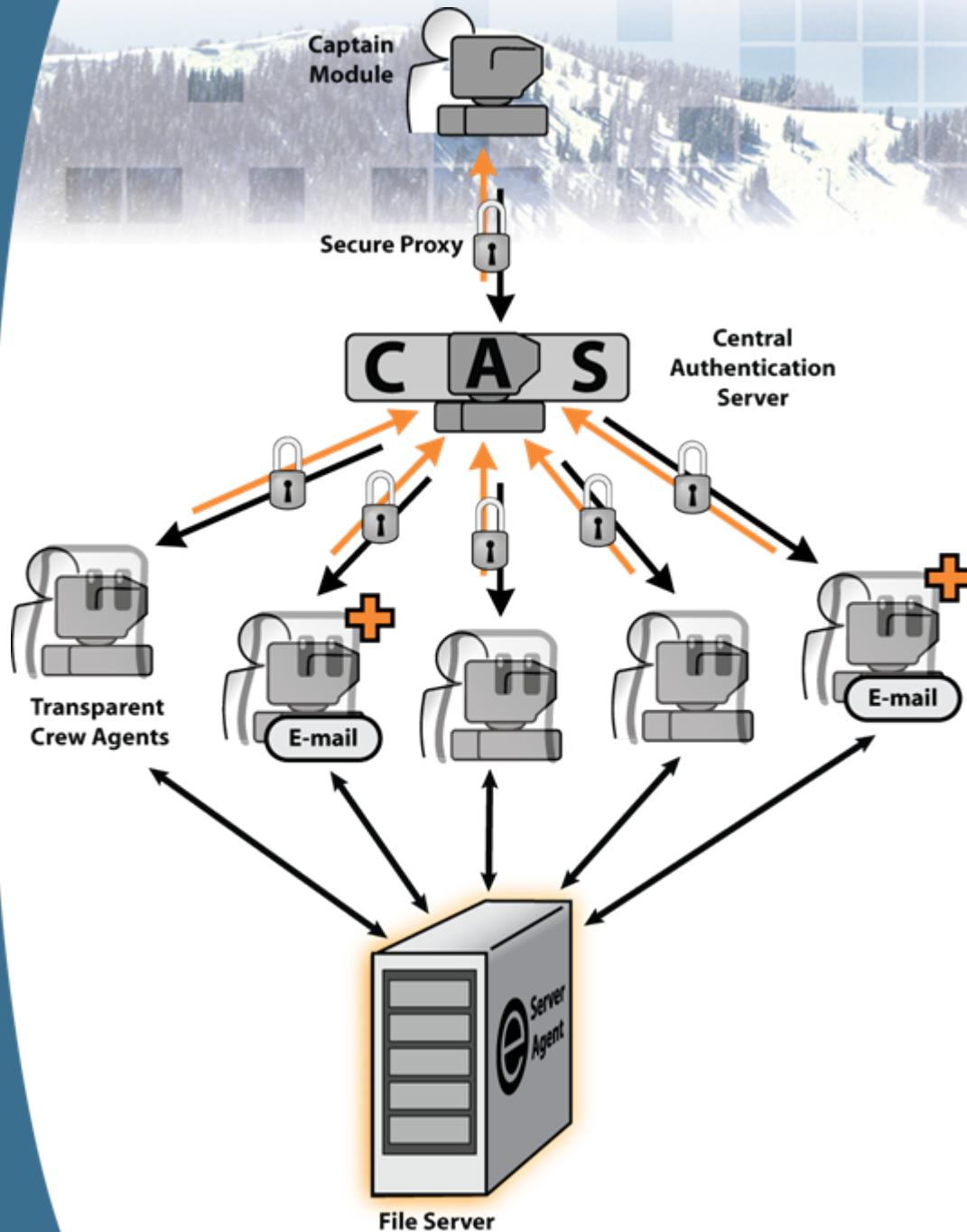
November 8<sup>th</sup>-11<sup>th</sup> 2009

## Live Email Forensics

### P2 Enterprise Acquisitions

# P2 Enterprise System

General Structure



# P2 Enterprise Agents



- Three Agent Types
  - Standard Agent
  - Plus Agent
  - Server Agent
  
- Common Features (Shuttle/Full)
  - Stealth
  - Acquisitions (File/Drive)
  - Memory Acquisitions
  - Cross Agent Searching

# P2 Enterprise Points

*Stopping risk to your information data.*

- File Tracking
  - Data Classification Example
  - Instead of picking up the pieces you are watching the pieces fall
- Cross Agent Searching
  - Search many machines all at once with full language support
- Acquire Data
  - Active mailstore data access
  - Acquire logical single files or directories
  - Acquire full logical drives
  - Acquire full physical drives
- Active Malware Search
  - Integrated WetStone Gargoyle Engine
- Multi-threaded
- Automated Scheduling of All Activities



*More Features & Capabilities Exist in Tool.*

# Email Types Supported

- Microsoft Outlook (PST)
- Microsoft Exchange (EDB)



# PRACTICAL

