Digital Forensics Research Workshop

Triage in Digital Forensics
Why Triage?

Right hand picture: http://forum.rollingstone.de/showthread.php?t=35030&page=29
Live Triage

• Mitigate risk to the acquisition process

• Identify next level artifacts

• Further suspect interview
Post Mortem Triage

- Interpret high pay-off artifacts without in depth forensic analysis
- Crowd source the analysis
- Identify next level artifacts
Remote Forensics

- Look at artifacts in a broader context
- Balance the work load
- Drop in expertise
Policy Considerations

• Competing legal standards

• Privacy considerations based on data type

• Exculpatory information
Triage in Digital Forensics

DISCUSSION