Uhm…what's the question?

Rank a list of tools in order of importance that are in your incident response jump kit.

Who am I?

- Incident Responder/Forensic Analyst, in the corporate arena
- QSA (…but don't tell anyone…)
- Author of *Windows Forensics and Incident Recovery* (AWL, 2004)
- Author of *Windows Forensic Analysis 1/E* and *2/E*

The Answer

- Imagers (FTK, dd, etc.)
- Perl
- Various CDs (tools, bootable, blank)
- That grey goop between your ears
- …and of course, Cory Althiede

AccessData
A Pioneer in Digital Investigations

PRODISCOVER® Computer Forensics

Mike Poor ??