What Windows Area Needs Additional Research and Development?

Jesse Kornblum
Introduction

- Computer Forensics Research Guru
  - md5deep/hashdeep
  - fuzzy hashing (ssdeep)
  - foremost

- Now with Kyrus Technology
  - Previously AFOSI, USNA, DoJ, ManTech
The Lobby 7 Theory
The Lobby 7 Theory
What is Normal?

• We need a definition of what’s “normal”
  – Or at least a way to compute one
• What’s supposed to be running and on the disk

• Good start with Peter Silberman’s Least Frequency of Occurrence

• Can such a profile be generated
  – A priori?
  – From a clean image?
  – From a standard load?
  – From a potentially compromised machine?
Questions?

Jesse Kornblum
jesse.kornblum@kyrus-tech.com