FBI Computer Scientist
Agenda

• Current Trends
• Top 10 Challenges
Crime is the problem, not hacking
Profit-driven criminal activity
2005 was the watershed year for organization
Underground market for crimeware
Evolution of the cyber criminal ecosystem
Malware development
Malware distribution
Money laundering
Multi-national groups backed by Organized Crime
Operating out of safe havens
Botnets

“A botnet is comparable to compulsory military service for windows boxes.”

Stromberg
7%
47 Million
Challenges
Device Diversity
Volume of Evidence
Video & Rich Media
Whole Drive Encryption
Wireless
Virtualization
Anti-Forensics
Live Response
Distributed Evidence

Flow Logs
ISP Logs
Filesystem
Volatile Data
Application & Database Logs
Network Device Logs
“Do not go where the path may lead, go instead where there is no path and leave a trail.”

Ralph Waldo Emerson