Current Cyber Investigation Challenges in Digital Forensics

By

Ted Lindsey

Presented At

The Digital Forensic Research Conference

DFRWS 2006 USA Lafayette, IN (Aug 14th - 16th)

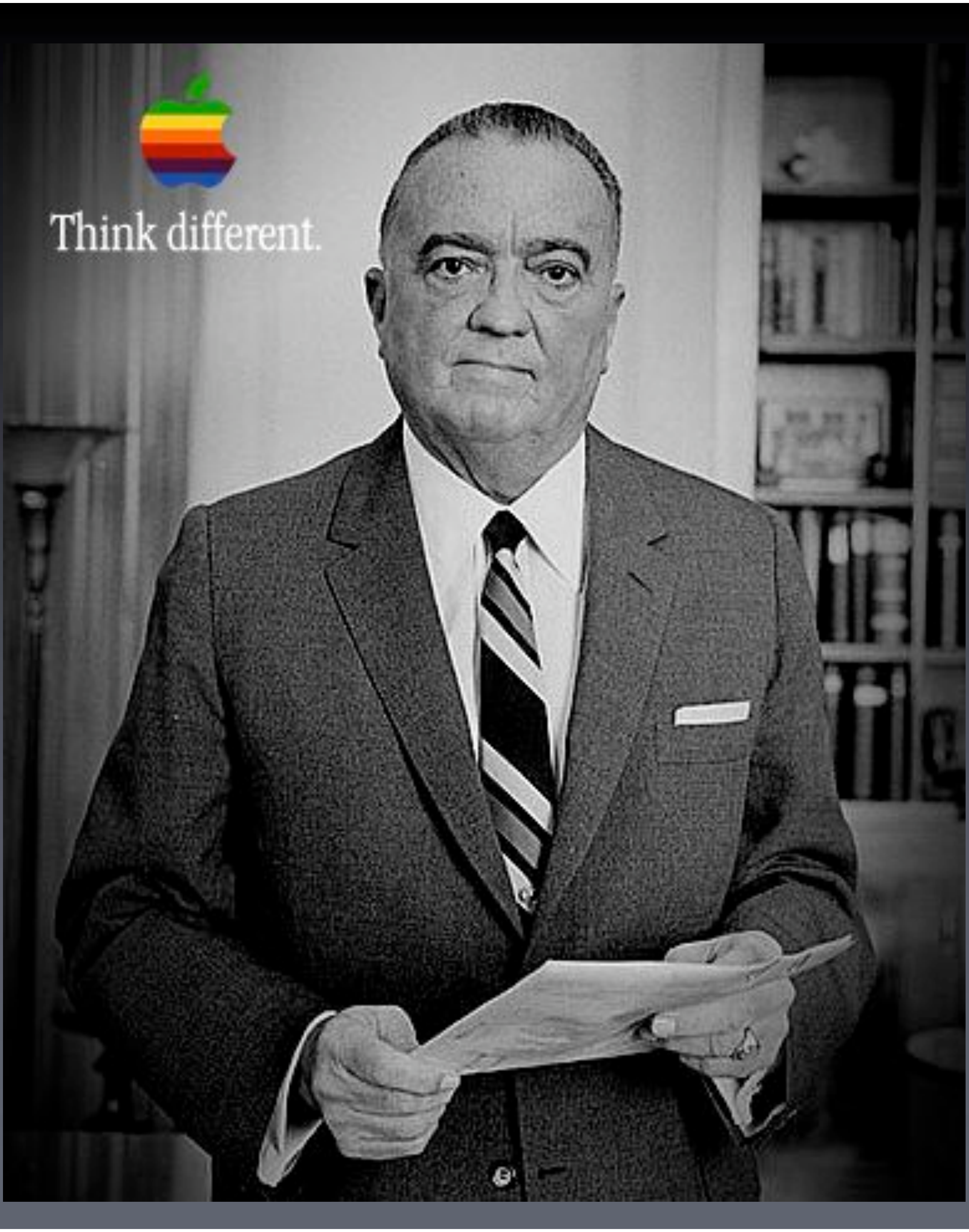
DFRWS 2006

Challenges in Digital Forensics

FBI Computer Scientist

LSR | Lindsey Systems Research

think solve accomplish


Think different.

Agenda

- Current Trends
- Top 10 Challenges

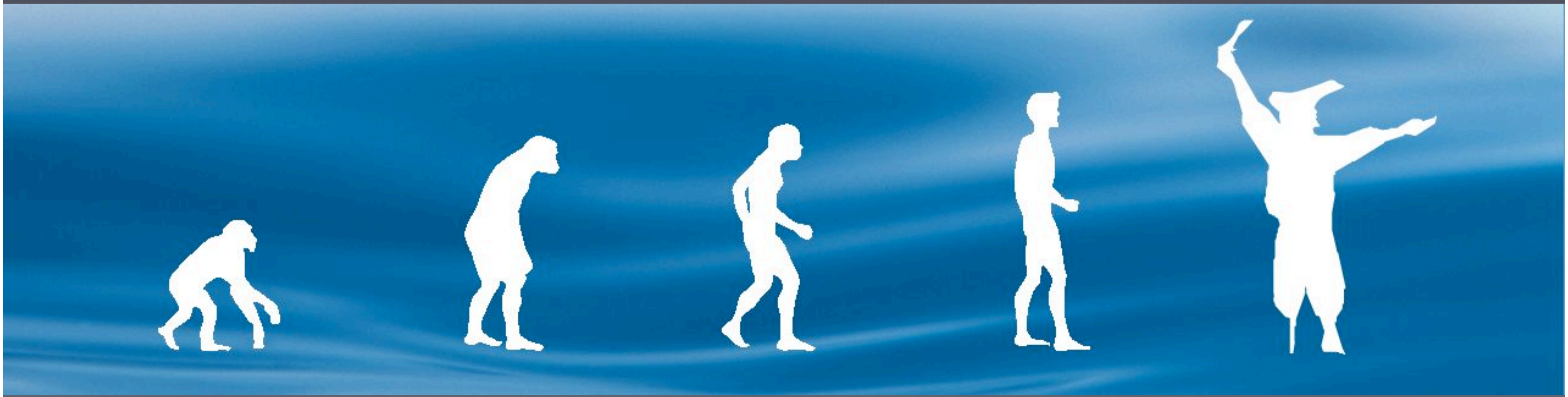
Crime is the problem, not hacking

Profit-driven criminal activity

2005 was the watershed year for organization

Underground market for crimeware

Evolution of the cyber criminal ecosystem

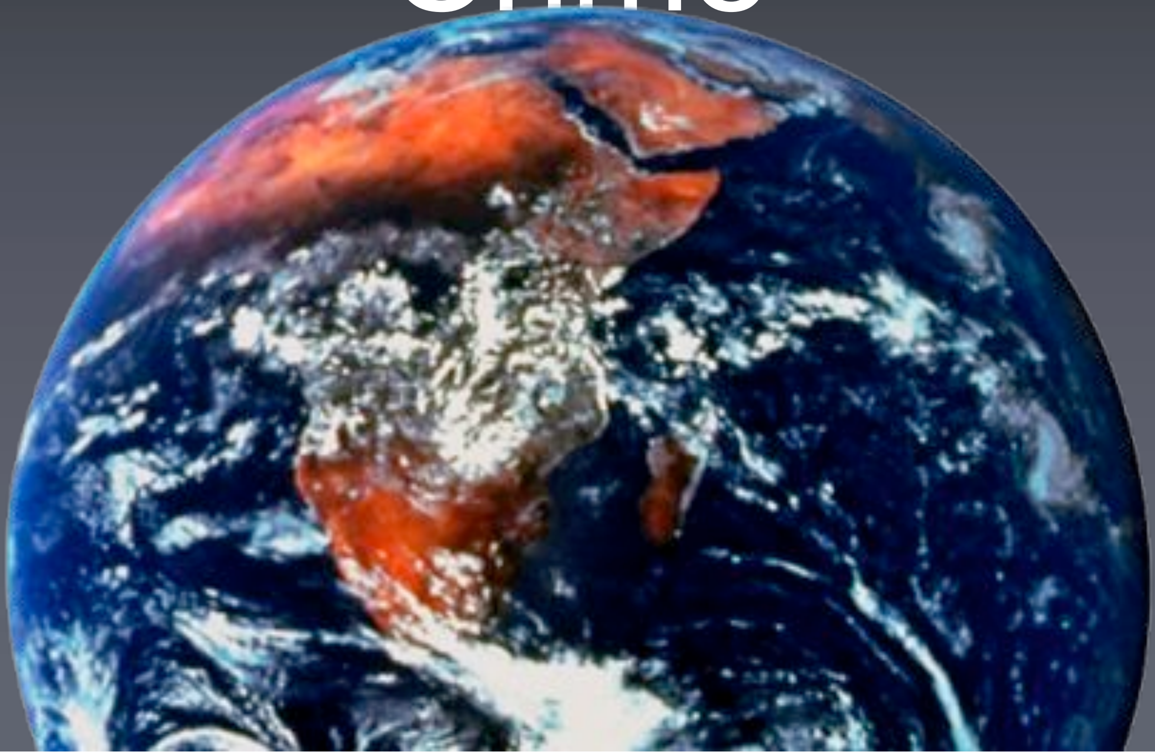


Malware development

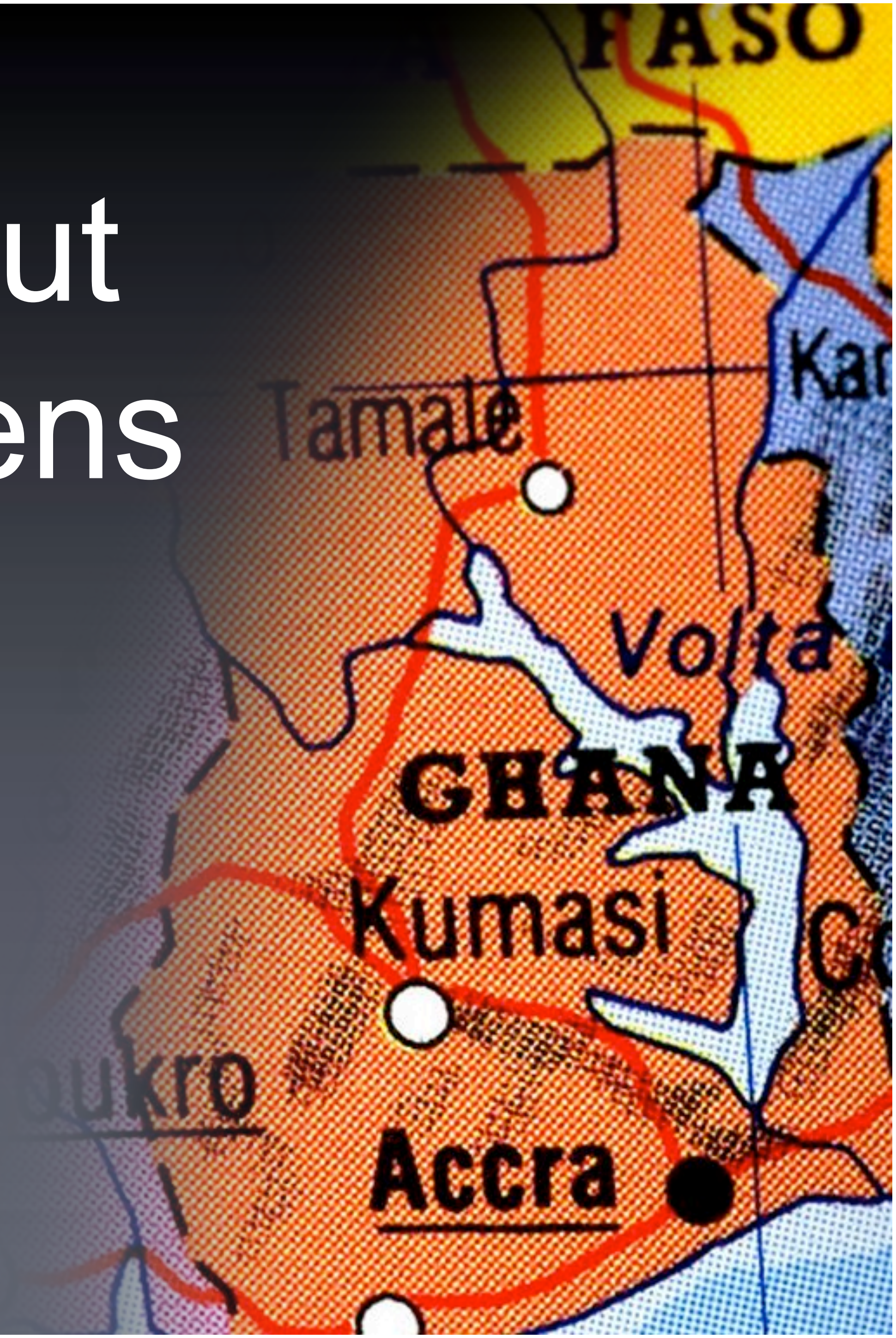
Malware distribution

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

60%

7%

47 Million

Challenges

Device Diversity

Volume of Evidence

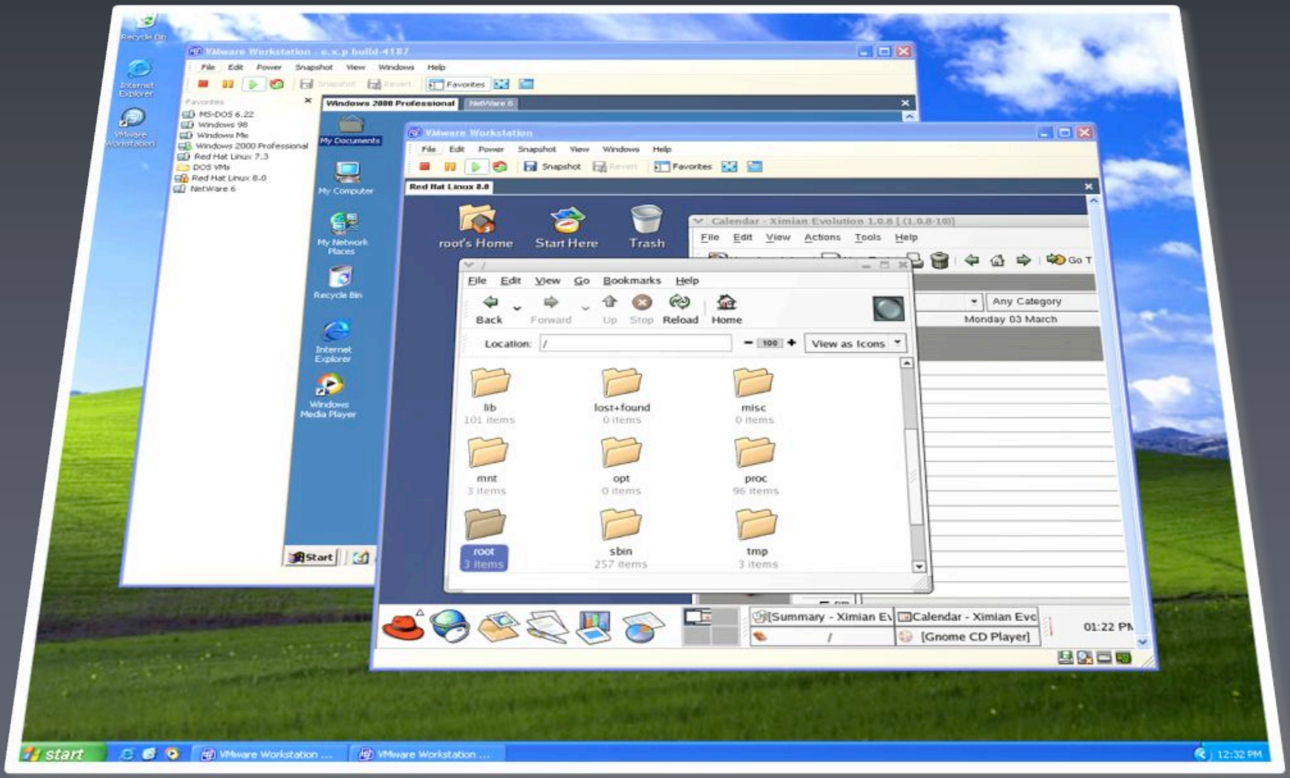
Video & Rich Media

Whole Drive Encryption

Wireless

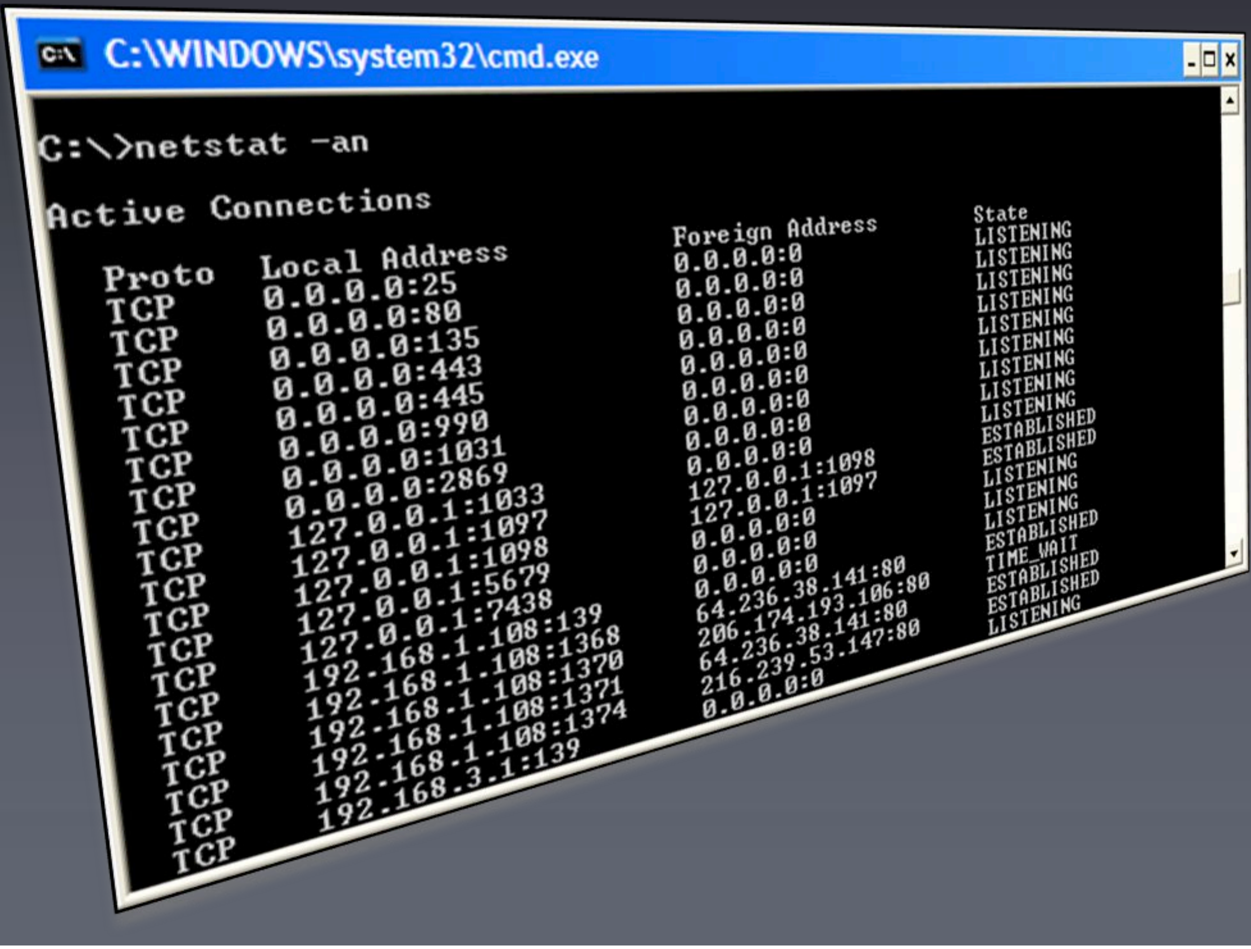
Wireless-G Broadband Router
2.4 GHz
LINKSYS
2.4 GHz
54g
Wireless-G Broadband Router
Cisco Systems
Power
DMZ
WLAN
Internet

Virtualization



Anti-Forensics

Live Response

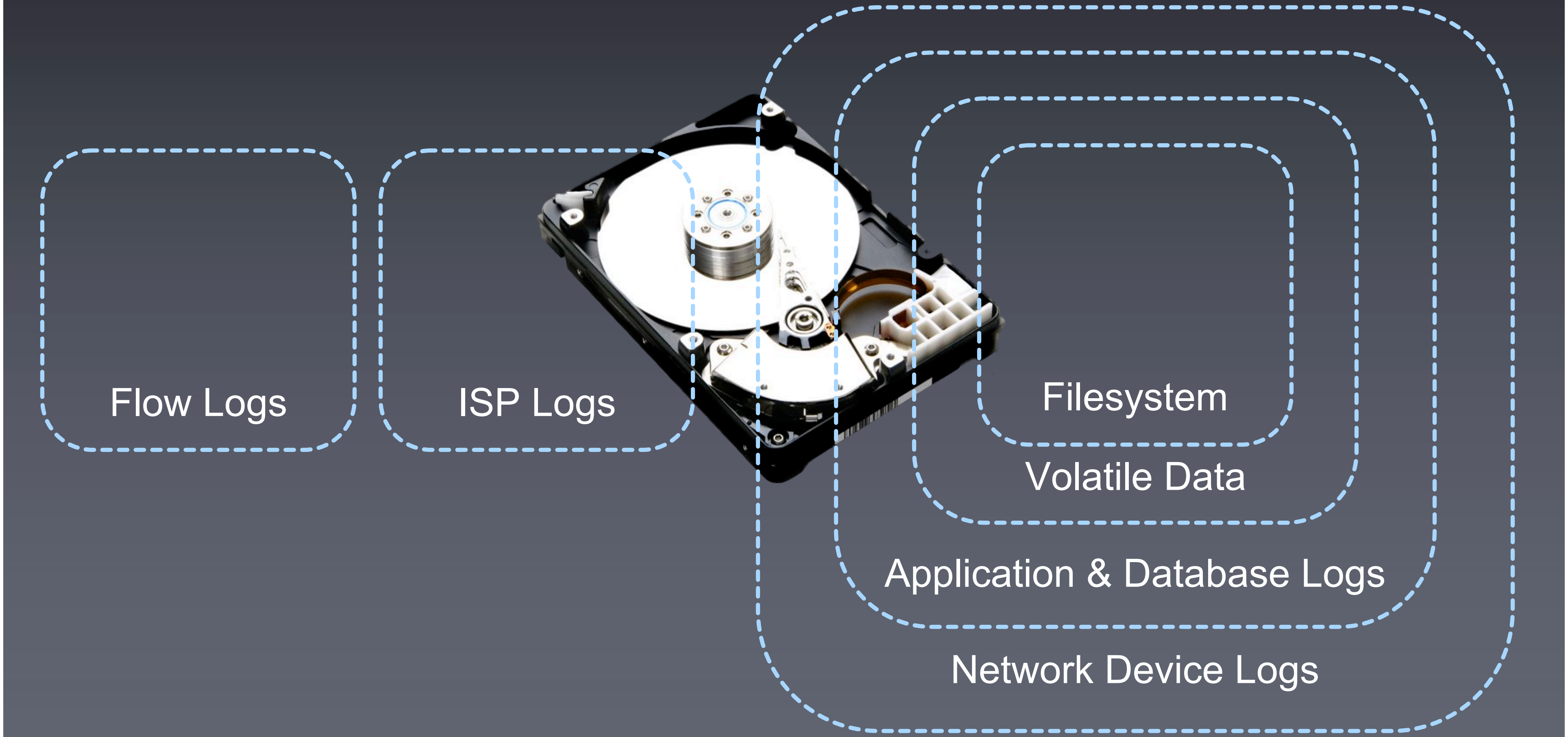


```
C:\>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:25             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:990            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1031           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2869           0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1033         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1097         127.0.0.1:1098         ESTABLISHED
  TCP    127.0.0.1:1098         127.0.0.1:1097         ESTABLISHED
  TCP    127.0.0.1:5679         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:7438         0.0.0.0:0              LISTENING
  TCP    192.168.1.108:139      0.0.0.0:0              LISTENING
  TCP    192.168.1.108:1368     64.236.38.141:80       ESTABLISHED
  TCP    192.168.1.108:1370     206.174.193.106:80     TIME_WAIT
  TCP    192.168.1.108:1371     64.236.38.141:80       ESTABLISHED
  TCP    192.168.1.108:1374     216.239.53.147:80      ESTABLISHED
  TCP    192.168.3.1:139        0.0.0.0:0              LISTENING
```

Distributed Evidence



Flow Logs

ISP Logs

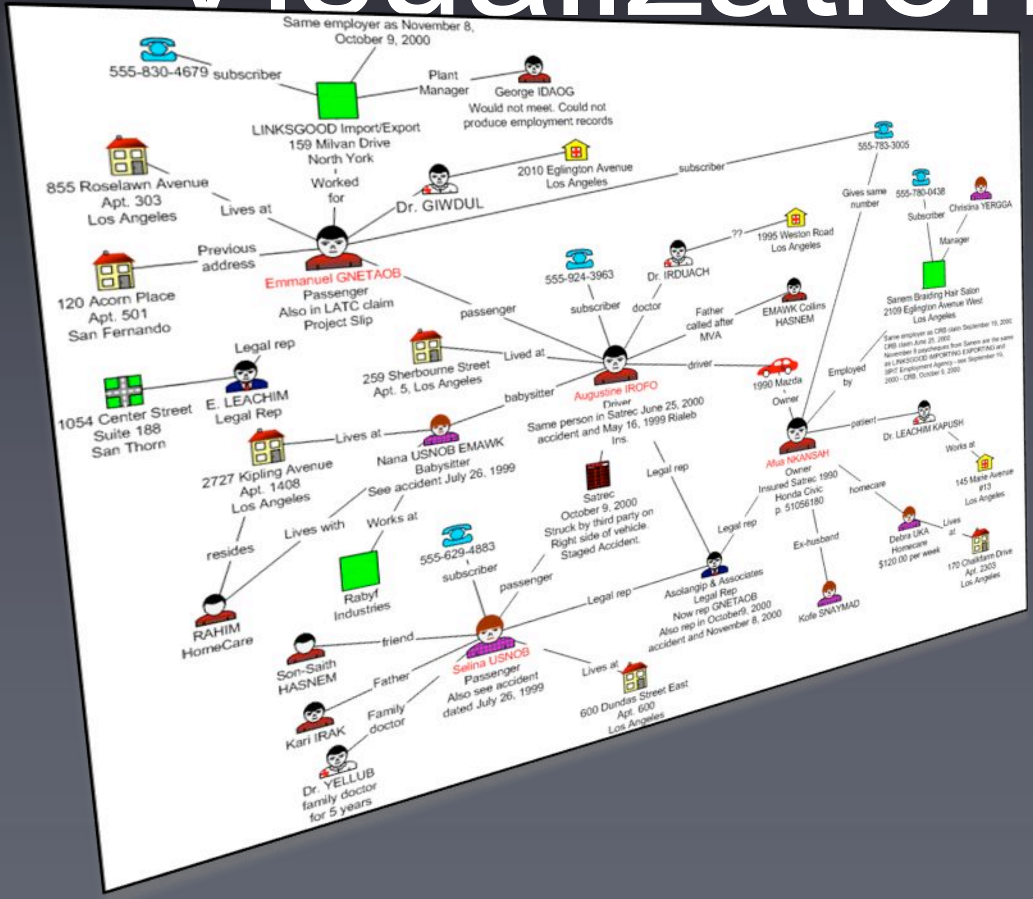
Filesystem

Volatile Data

Application & Database Logs

Network Device Logs

Usability & Visualization



“Do not go where the path may lead, go instead where there is no path and leave a trail.”

Ralph Waldo Emerson