REQUIREMENTS FOR EFFECTIVE COMPUTER CRIME INVESTIGATIONS
We are living in a Digital World

Future investigations depend on the ability to quickly **Identify**, **Extract** and **Analyze** digital evidence.
CyberCrime
Investigative Skills
Rapidly Evolving
Estimated 40 Exabyte of new unique information generated worldwide this year

Source: Karl Fisch - thefischbowle.blogspot.com

Monday, January 17, 2011
That’s more than in the Previous 5,000 years.
The amount of technical information is doubling every 2 years.

Source: Karl Fisch - thefischbowle.blogspot.com

Monday, January 17, 2011
1.97 Billion
Internet Users


Monday, January 17, 2011
Live Different


Monday, January 17, 2011
Communicate
Different


Monday, January 17, 2011
107 Trillion e-mails sent in 2010
107 Trillion e-mails sent in 2010

That is 293 Billion email a day


Monday, January 17, 2011
107 Trillion e-mails sent in 2010

That is 293 Billion email a day


Monday, January 17, 2011
Social
Social Networking
600 Million
7 Hours a Month
70% Outside the U.S.
68.5 Million per day

And They Create Evidence of Their Criminal Activity
Searches Per Month...

15,000,000

Source: Karl Fisch - thefischbowle.blogspot.com

Monday, January 17, 2011
Searches Per Month...

15,000,000

in 1999

Source: Karl Fisch - thefischbowle.blogspot.com

Monday, January 17, 2011
2,701,500,000 in 2006
10,975,000,000

10,975,000,000

...last month

Monday, January 17, 2011

More Good News
Moore’s Law (1965)

Number of transistors that can be placed on an integrated circuit will increased exponentially, doubling approximately every two years.
Moore’s Law (1965)

Number of transistors that can be placed on an integrated circuit will increased exponentially, doubling approximately every two years.
Moore’s Law (1965)

Number of transistors that can be placed on an integrated circuit will increased exponentially, doubling approximately every two years.

Capacity of hard drives have more than doubled every two years for the past 7 years.
$700 per MB
$700 per MB
How
Does
This
Affect
You

Monday, January 17, 2011
Significantly More Digital Evidence About Our Daily Activity
Significantly More Digital Evidence About Our Daily Activity

Digital Evidence Less Likely to be Overwritten
Now The Bad News
DRIVE CAPACITY HAS EXCEEDED HUMAN DIGESTIBILITY
Number of Computers Seized

Monday, January 17, 2011
Types of Cases
Complexity of OS
Forensic Taking LONGER
Missing Potential Evidence
What Do You Do?

You loose what's open, apps, etc?

Monday, January 17, 2011
Triage – On Scene

- Volatile Data Collection
  - Collection quickly becoming a must
Web Based Email
Web Based Email
Online File Storage
Online File Storage

Monday, January 17, 2011
Triage – On Scene

- Volatile Data Collection
  - Collection quickly becoming a must
  - Aid in Interview
Triage – On Scene

- **Volatile Data Collection**
  - Collection quickly becoming a must
  - Aid in Interview
  - Lead Development
  - Evidence Preservation

Monday, January 17, 2011
Electronic Evidence Waits for No One
Overwhelmed with Digital Evidence
Taught Tools Not Methodology
When faced with overwhelming information we have great difficulty making a decision
Locard’s Evidence Transfer Principal
Data Visualization
Data Correlation
Future of CyberCrime Investigations

- Collaborative Approach
- One Hard drive - Multiple Examiner
- Server Based Forensics
Server Based Environment

- Large Data Volumes
- Load Balancing
- Special Use Equipment
Server Based Environment

- Large Data Volumes
- Load Balancing
- Special Use Equipment
Digital Evidence a Part of Every Crime
Phased Approach
Triage is Critical
Collaborative Investigative Approach

Monday, January 17, 2011
Better Training

FOR408 Computer Forensic Essentials
GCFE

FOR508 Computer Forensic Investigations and Incident Response
GCFIA

FOR558 Network Forensics

FOR563 Mobile Device Forensics

FOR610 REM: Malware Analysis Tools & Techniques
GREM

Additional Forensics Courses

FOR526 Advanced Filesystem Recovery and Memory Forensics
COMPUTER CRIME AND
INTELLECTUAL PROPERTY SECTION

OVIE L. CARROLL
DIRECTOR, CYBERCRIME LABORATORY

U.S. DEPARTMENT OF JUSTICE
1301 NEW YORK AVE. NW, SUITE 600
WASHINGTON, DC 20005

TEL: (202) 307-3955
(202) 355-5632
FAX: (202) 514-6113
OVIE.CARROLL@USDOJ.GOV

Monday, January 17, 2011