Forensic Trends & Future

Shifting the Forensic Paradigm

DOJ Computer Crime and Intellectual Property Section
We are living in a Digital World

Future prosecutions depend on the ability to Identify, extract and analyze digital evidence.
It is estimated that 40 exabytes of new unique information will be generated worldwide this year.
That’s more than in the Previous 5,000 years.
The amount of technical Information is doubling Every 2 years
By 2010, it’s predicted to double... every 72 hours
Worldwide Online Population

824,400,000  (183,000,000 in North America)

Grew 10.4% from Jan 2007-Jan 2008

77.5 million more users than last year

Source: Comscore - www.comscore.com
185 Million registered users

45 Billion monthly page views

142 Terabytes of disk space

Source: Comscore - www.comscore.com
There were more than 2.7 billion searched performed on Google...

2,700,000,000

...this month
The number of text messages today
exceed the population of the planet
INFORMATION
The Good News
People Feel Anonymous Online
And They Create Evidence of Their Criminal Activity
Evidence is in Our Backyard
Top Ten Global Internet properties are in US

<table>
<thead>
<tr>
<th>Property</th>
<th>U.S. Audience</th>
<th>Non-US Audience</th>
<th>Total WW Unique Visitors (MM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Sites</td>
<td>80%</td>
<td></td>
<td>597.2</td>
</tr>
<tr>
<td>Microsoft Sites</td>
<td>80%</td>
<td></td>
<td>545.6</td>
</tr>
<tr>
<td>Yahoo! Sites</td>
<td>75%</td>
<td></td>
<td>495.3</td>
</tr>
<tr>
<td>eBay</td>
<td>71%</td>
<td></td>
<td>249.3</td>
</tr>
<tr>
<td>AOL LLC</td>
<td>60%</td>
<td></td>
<td>247.9</td>
</tr>
<tr>
<td>Wikipedia Sites</td>
<td>79%</td>
<td></td>
<td>242.6</td>
</tr>
<tr>
<td>Amazon Sites</td>
<td>67%</td>
<td></td>
<td>166.0</td>
</tr>
<tr>
<td>Fox Interactive Media</td>
<td>53%</td>
<td></td>
<td>160.6</td>
</tr>
<tr>
<td>Apple Inc.</td>
<td>69%</td>
<td></td>
<td>140.3</td>
</tr>
<tr>
<td>CNET Networks</td>
<td>74%</td>
<td></td>
<td>125.6</td>
</tr>
</tbody>
</table>
More Good News
Moore’s Law also holding true for hard drive capacity
$700 per MB
Seagate Barracuda 7200.11 ST31000340AS 1TB 7200 RPM 32MB

$139.99

Free 3 Business Day Shipping
(Not available in HI, AK and PR)

In Stock

ADD TO CART
ADD TO WISH LIST
EMAIL THIS PAGE
PRINT THIS PAGE
PRICE ALERT

Image Viewer

= 0.0001 per Megabyte
How Does This Effect Forensics
Significantly More Digital Evidence About Our Daily Activity

Digital Evidence Less Likely to be Overwritten
Now The Bad News
- Number of Computers Seized
- Types of Cases
- Complexity of OS/Applications
- Forensics Taking Longer
Current Forensic Methodologies do not SCALE
Forensic Backlog Increasing
Missing Volatile Data
Phased Approach
Volatile Data Collection

Investigative Mindset
Analysis vs Data Extraction

Data Correlation
Future – Phased Approach

- Triage
  - On Scene or
  - 1st Task at Lab (Pre-Imaging)

- Baseline Plus
  - Know Basically What You’re Looking For

- Full Forensics
  - Complex Cases
  - No Plea – Going to Court
Investigative Mindset

User Attribution
Who Pulled the Trigger?
• Professor Plum
• In the Study
• With the Candle Stick
Data Correlation
Data Correlation

- Computer
- Internet
  - Email
  - Blogs
  - Social Networking
  - Instant Messaging
- Cell Phone
  - Call logs
  - Texting
  - Location
• The **Amount** of Digital Information is Increasing Exponentially

• **Every Crime** involves digital evidence

• **Demand** for computer forensic support is exploding
Phased Approach to Forensic

Future prosecutions & national security depend on the ability to **Identify, extract** and **analyze** digital evidence.