

There were more than 2.7 billion searches performed on Google...

2,700,000,000

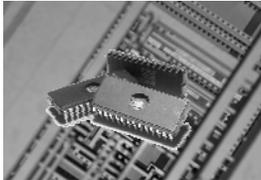
...last month

source: Karl Fack - @thefutureofit.blogspot.com



Moore's Law

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





- **Number of Computers Seized**
- **Types of Cases**
- **Complexity of OS / Applications**
- **Forensics Taking L o n g e r**

**More
Bad
News**



Step 1

Finding Potential Digital Evidence

Types of Electronic Media

Desktops to Servers

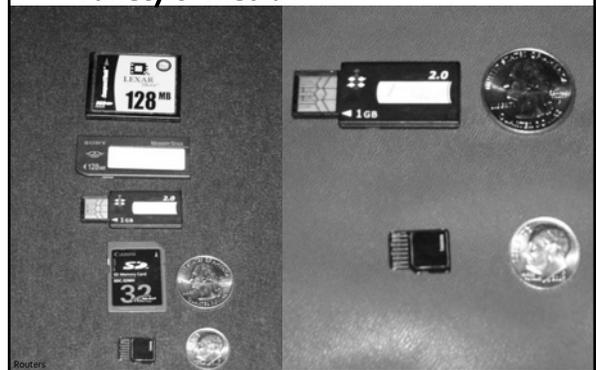


Variety

Variety of Media



Variety of Media



Routers

But Wait, There's More

Wi-Fi - 700g

ASUS

ipods, Cell

CellPhones, PDA's &iPods

- **Cell Phones now do more than just make phone calls**

What can be stored on iPods

Cell Phones, PDA's &iPods

- **iPods are very popular.**
- **They're more than music players, they are storage devices.**

What can be stored on iPods

What can be on Those iPods?

- Music
- Videos
- Contact List
- Porn
- Calendars
- Porn
- Operating Sys
- Porn

Other-Ptr, Fx, VoIP

Other Digital Storage Devices

- Printers
- Faxes
- VoIP phones

#	Job Name	Owner	Status	Completed	Other Options
1	Microsoft Word - 2006 NPLCComerian	Local User	Completed	6:19:54PM	
2	Copy Job 125	Local User	Completed	5:13:54PM	
3	Copy Job 124	Local User	Completed	4:59:37PM	
4	Copy Job 123	Local User	Completed	3:53:29PM	

Quick test

Where's the evidence?

PDA

USB

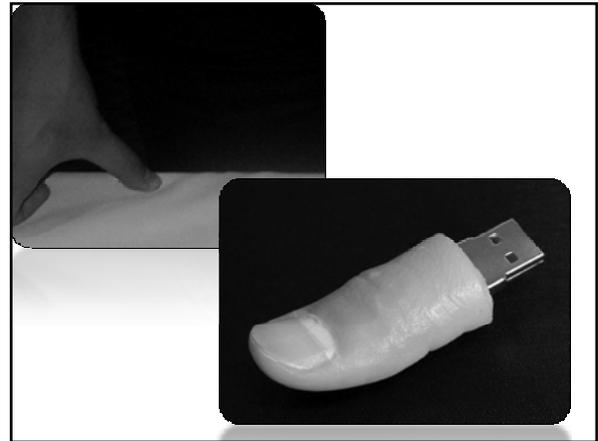
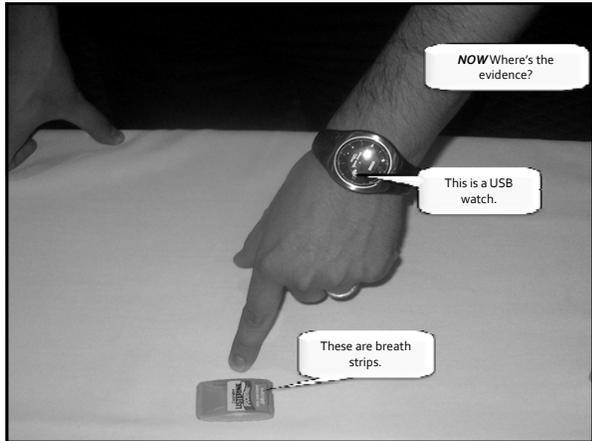
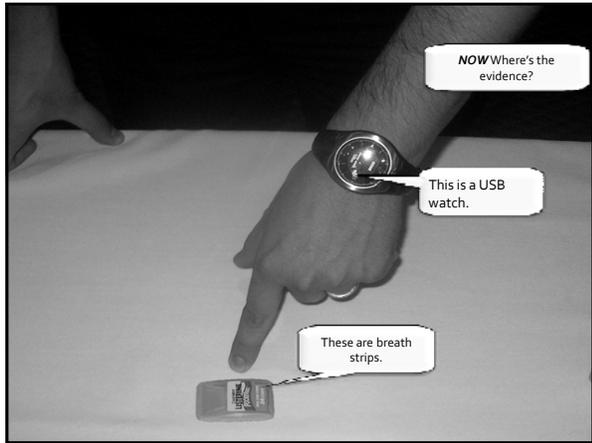
USB

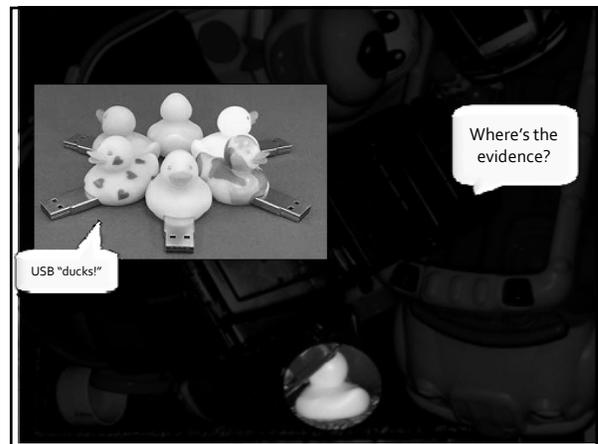
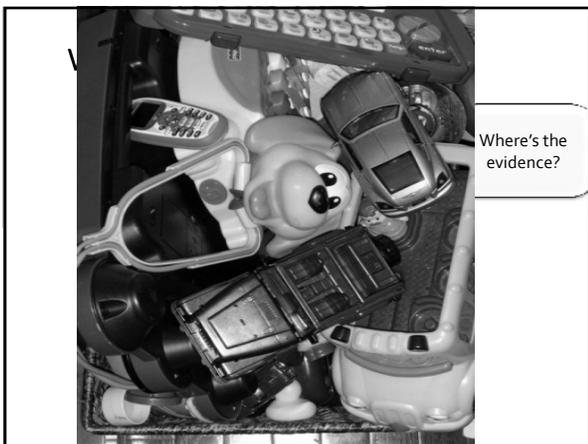
Hard Drive

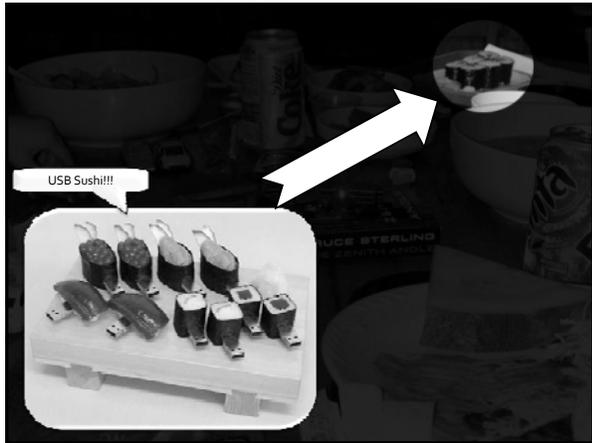
USB

CELL

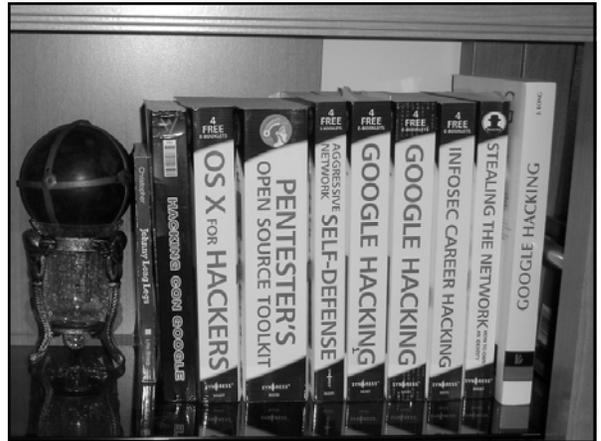
CF CARD

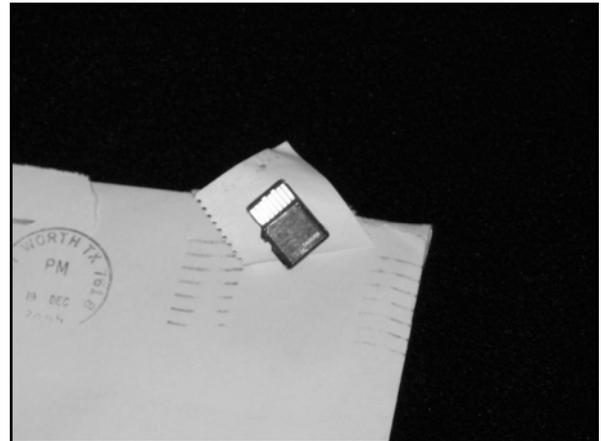






Just Kidding





||| **Phased Approach**
Volatile Data Collection

Pre-Search Reconnaissance

Multiple Data Source Correlation

Triage - On Scene

- Volatile Data Collection
- Collection quickly becoming a must
- RAM Analysis

||| **Triage – On Scene**

- Volatile Data Collection
 - Collection quickly becoming a must
- Aid in Interview/Interrogation

||| **Triage – On Scene**

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

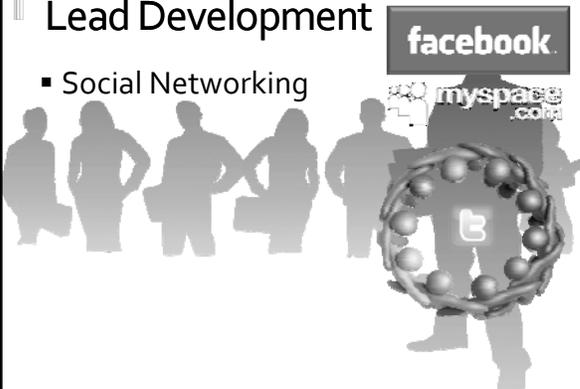
||| **Lead Development**

- Web Based Email



||| **Lead Development**

- Social Networking



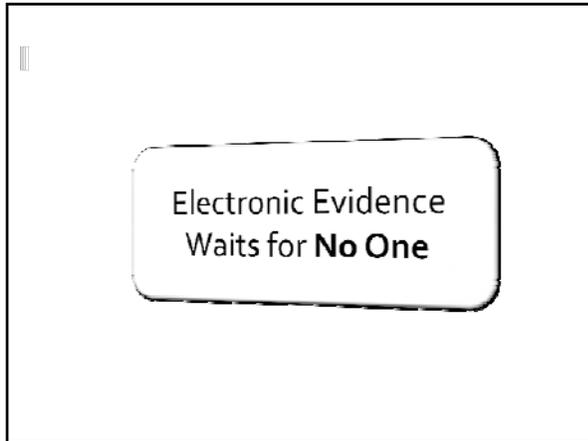
||| **Triage – On Scene**

- Volatile Data Collection
 - Analysis not necessary for traditional crimes
- Aid in Interview/Interrogation
- Lead Development
- Evidence Preservation
- **Additional Evidence Identification**

||| **Lead Development**

- Online File Storage





Summary

- Digital Evidence Comes in Many Shapes and Sizes
- Investigators must know What and Where to look

Educated Prosecutors and Judges understand SCOPE of Search

This is what it looks like

