



Mobile Forensics: A Path Forward

May 28, 2009

Unclassified/FOUO

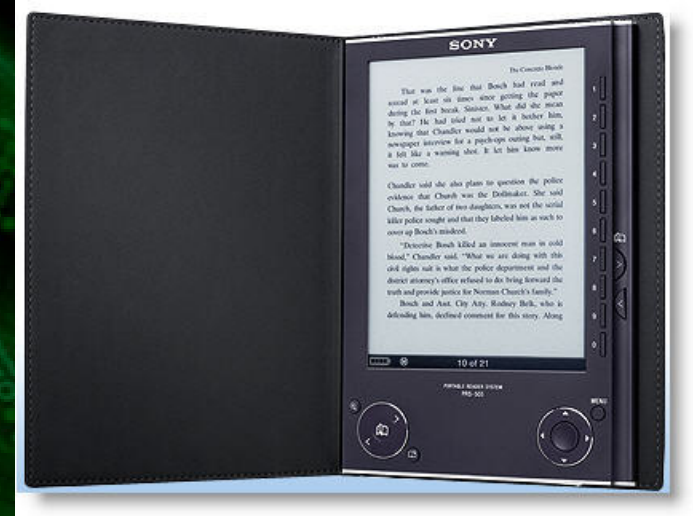
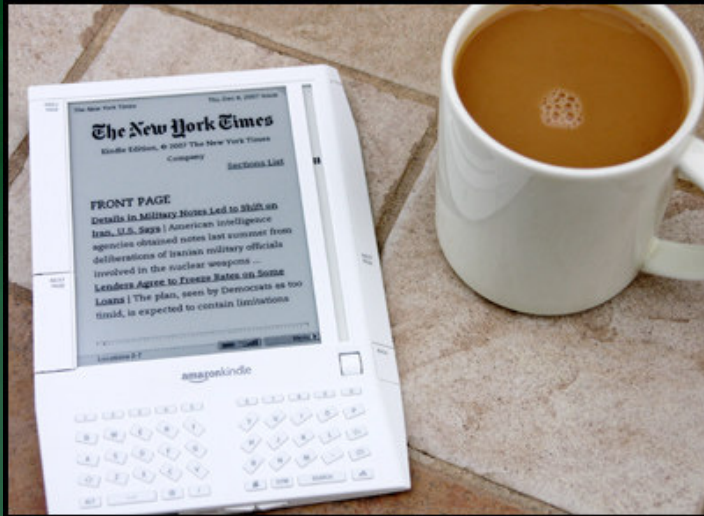


Outline

- **Trends & challenges in mobile forensics**
- **Developments in digital evidence that will change mobile forensics**
- **Responses & suggestions for moving forward**
- **Questions & comments**



A Plethora of Devices



flipshare

- View & organize videos
- Email videos
- Publish clips online
- Make movie mixes with music
- Capture photos from videos

© 2002-2008 Pure Digital Technologies, Inc.





Dozens of Tools





Demand for Services Is Up





Storage Capacity is Increasing

SOLAR FLYER p.78 Around the World without a Drop of Jet Fuel

STEM CELLS: A USER'S MANUAL p.80

POPULAR SCIENCE

23 HOT PRODUCTS

THE FUTURE NOW

The First Color E-Reader p.16

3RD ANNUAL INVENTION AWARDS

TOMORROW'S TANK

The Unmanned Beast That Tops 60 mph—and Was Built in a Garage p.38

PLUS

- ▶ A Skyscraper-Escape Harness
- ▶ The Wearable Web
- ▶ Robotic Legs
- And More Incredible Backyard Creations

NEW! CLONING CURES BALDNESS p.32

DEAN KAMEN WANTS TO REINVENT YOU p.57

NEWS ON SOLE TRIP

7482016880

HEADLINES

SHRINKAGE

ENDLESS MEMORY

COMING SOON: THE TWO-TERABYTE FLASH CARD

Cameras run out of memory at the worst times—like when you catch cow Michael Jordan at the poker table in Vegas. But a new flash-memory system can fit up to two terabytes of storage, or 480 hours of high-definition video, into this average memory card.

Durand CD memory cards also file using the 10-year-old FAT32 standard filing program. FAT32 effects video photos or videos into small pieces, which it saves in random locations on the card. This slows down the flash drive as it saves and retrieves files, causing sludge at 32-gigabyte—any more would make the card impractically sluggish. So new SD extended capacity (SDXC) cards will feature a Microsoft's FAT system, which opens the door to bigger storage by saving files in one place in an organized way that makes them easier to find.

The first SDXC cards, due out from Panasonic's shop, will offer a gigabyte—space for 3,500 12-megapixel photos on a 50-gigabyte memory card—and load 'em up speeds 10 times as fast as current cards. As yet, movies occlude down transistors (the circuits that physically store data), standard cards read the electrically stored memories. Although the cards won't work in 10-year-old reading devices, SDXC cameras, if a pipeline will prove you wild stories—as long as your battery doesn't die.—MARRHA L. L. J. REAVES

TOTAL RECALL Revamped flash cards won't store all Blu-ray movies.

30-SECOND SCIENCE

ANIMAL ATTACK

VERMIN AND FARM CRITTERS STIR UP HEALTH SCARES

THIS LITTLE PIGGIE HAD EBOLA

In January, the Ebola virus kept ten piglets farmers in the Philippines. But don't panic. Despite being a cousin of the deadly African disease, Ebola-Reston, mainly causes flu-like symptoms in humans, says Pierre Rollin, a biologist at the Centers for Disease Control and Prevention. To be safe, the Philippine government ordered farmers to cull about 6,500 pigs from infected farms. Ebola-Reston first seemed to infect Philippine monkeys in 1996 and has since passed to other species. Scientists think contagion best occurred in pigs' water supply, and the swine then copied the virus onto humans.—KATHY RINEY RAYMOND

SUPERBIRDS Flies feed on bacteria hidden in chicken feces and spread them in a plume.

YIKES! Rats' genetic mutations let them survive poison.

CALL IN THE SWAT TEAM

Roughly 70 percent of all the antibiotics used in the U.S. are for warding off bacterial infection in farm animals so they can grow bigger. The trouble is, these bacteria eventually develop resistance to the drugs and, researcher Jay Graham of Johns Hopkins University has recently shown, flies are spreading the resistant bacteria around. The flies can pick up strains from chicken droppings that cause human illnesses such as meningitis and carry them as far as 20 miles. Graham's team is mandating animal waste with the same techniques used for human sewage.

UNSTOPPABLE MUTANT RATS

Sixty years of killing rats with poison might be making them stronger, according to new research. A series of small mutations in some rats' genetic codes allows them to survive high doses of warfarin, the most commonly used rodenticide. Warfarin inhibits blood clotting, causing fatal internal bleeding. Although "super-warfarin" poisons are available, study leader Lumasa Most of the University of Würzburg in Germany warns that the rodents might develop immunity to those chemicals as well.

SDXC 2TB

© 2008 TIME INC. ALL RIGHTS RESERVED. PHOTO: JEFFREY M. HARRIS

SD 2TB



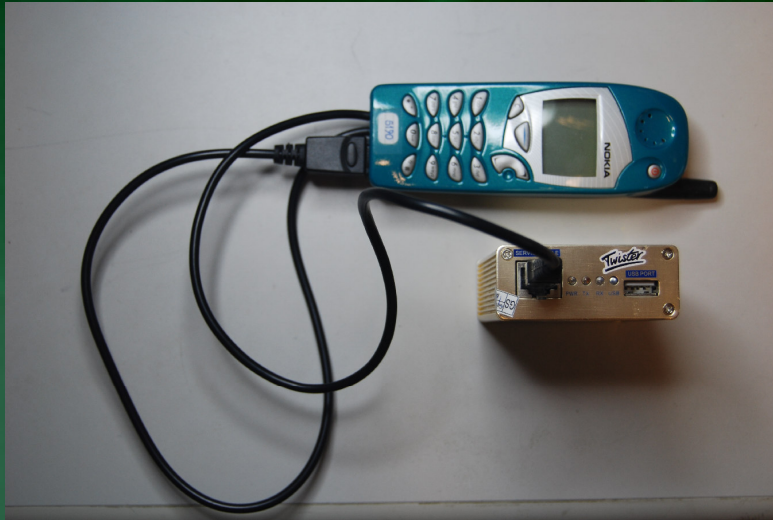
Increased Security

- + More data stored as plain text
- Increases in computing power and memory
- Easier to implement good security





Traditional Access Methods Becoming More Difficult



- **Bootloaders**
 - Manufacturers implementing security in boot ROM
- **JTAG Ports**
 - Manufacturers not connecting JTAG pins to accessible test pads
- **Chip Removal**
 - Increased use of custom/proprietary IC processor and memory chips



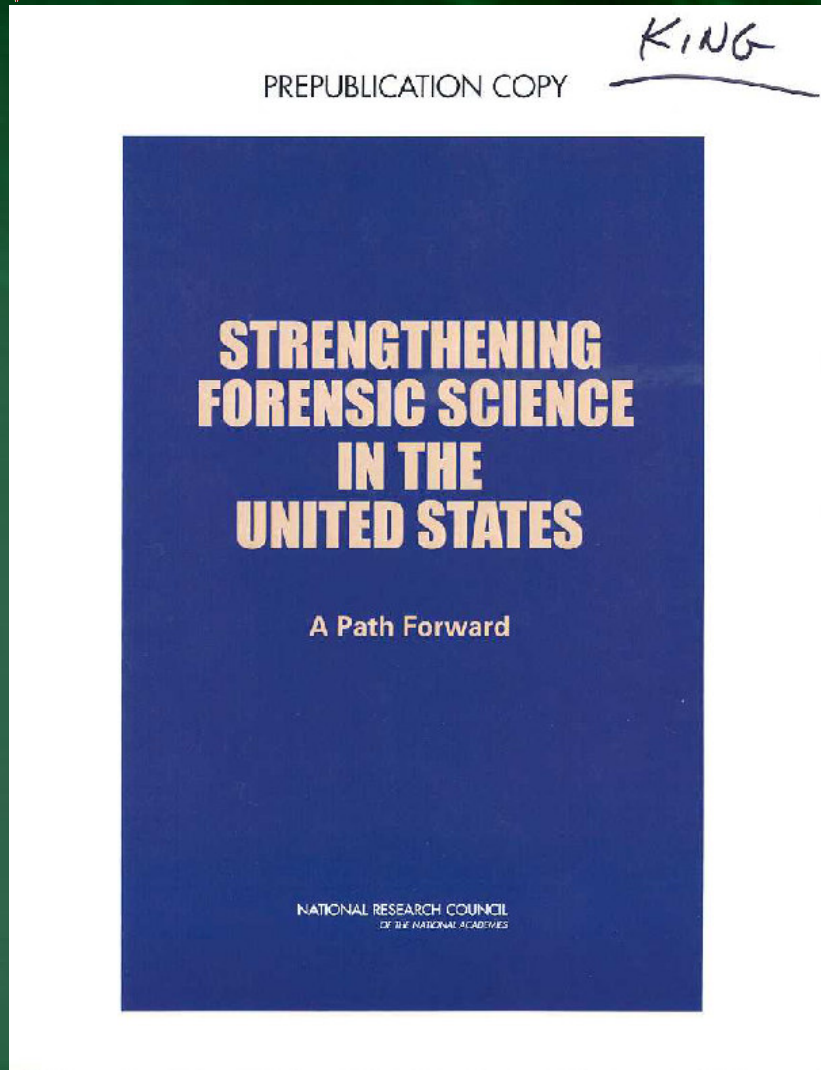
Significant Developments in Digital Evidence

- **Investigative Based Model**
 - Non-forensic
 - Non-examiner
 - Timely/rapid
 - On-scene
 - Live capture
 - Preview/triage
 - Low cost/COTS
 - Further the investigation

- **Laboratory Based Model**
 - Forensic
 - Highly skilled
 - Methodical
 - Comprehensive
 - Static
 - Robust QA Program
 - High cost
 - Fair, impartial & scientific



Significant Developments in Digital Evidence

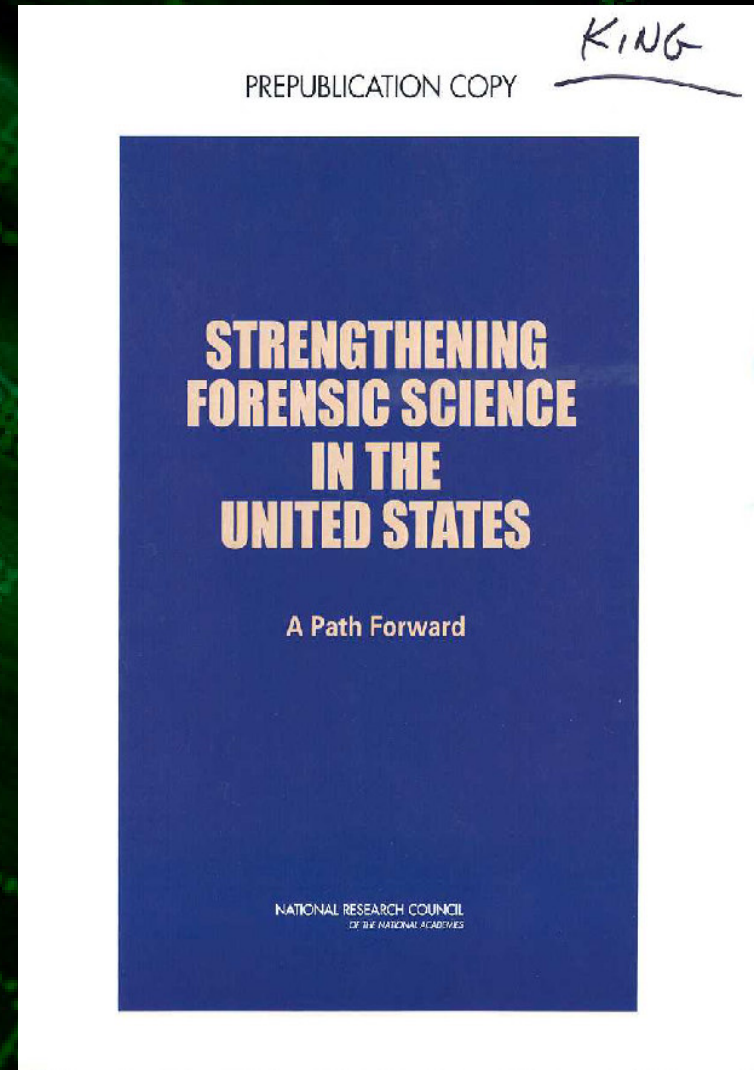


- **The Perfect Storm**
 - DNA becomes new standard
 - West Virginia State Police Crime Lab
 - Houston Crime Lab
 - Baltimore County Circuit Court Judge rules against latent prints
 - FBI Madrid Train Bombing
 - The Innocence Project



Significant Developments in Digital Evidence

- **13 Recommendations, including:**
 - NIFS
 - Remove control from law enforcement
 - Mandatory accreditation
 - Mandatory certification
 - Licensing??
 - Mandatory QA
 - National Code of Ethics





A Path Forward...

- **Minimum Quality Assurance Standards**
- **Leveraging off of Non-Examiners**
- **Aggressive use of preview**
- **More robust tools**
- **Increased sharing of resources**
- **Increased standardization for mobile devices**
- **Increased participation**

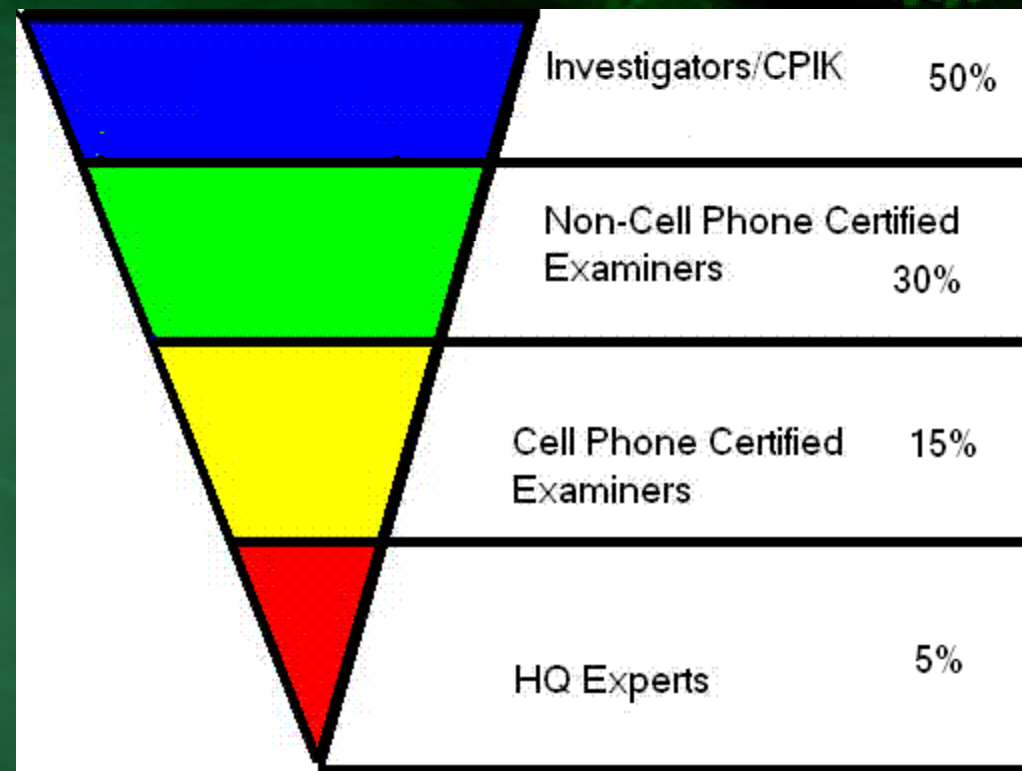


Minimum Quality Assurance Standards?

- Write protection OR copy
- Chain of custody
- Known tools
- Peer review
- Contemporaneous notes
- Written report
- ???



Leverage off of Non-examiners





Example: CPIK

- **Making available two easy to use cell phone tools to special agents and investigators for previewing at least a portion of data.**
- **Cell Phone Investigative Kiosks are being set up at FBI Field Offices and Regional Computer Forensic**



Aggressive Use of Previews

- **New Zealand Police Model**
 - **80 percent reduction in submitted matters**
 - **100 percent of resources on 20 percent of cases**



More Robust Tools

- Results are always different for different Manufacturers
- Each product does well in some areas and not so well in other areas
- Don't focus on low hanging fruit

Product	Contacts	Call Logs	Calendar	Message	Photos	Audio
A	Yes	Partial	Yes	No	Yes	Yes
B	Yes	Partial	No	No	Yes	No
C	Yes	Partial	No	No	Yes	No
D	Partial	Partial	No	No	No	No



Example: Increased Sharing of Resources

Scientific Working Group on Digital Evidence (SWGDE)

Scientific Working Group on Imaging Technology (SWGIT)

American Academy of Forensic Sciences

High Tech Crime Investigators Association (HTCIA)

International Association of Computer Investigative Specialists (IACIS)

International Association of Chiefs of Police, Sub-committees on Public Private Liaison and Cyber Crime-Digital Evidence

Others...



Example: Increased Sharing of Resources

- www.cftt.nist.gov/mobile_devices.htm



CFTT Overview

- CFTT – Computer Forensics Tool Testing Program provides a measure of assurance that the tools used in the investigations of computer-related crimes produce valid results.
- Directed by a steering committee composed of representatives of the law enforcement community.
- The steering committee selects tool categories for investigation and testing by CFTT staff. A vendor may request testing of a tool, however the steering committee makes the decision about which tools to test.
- CFTT is a joint project of: NIJ, OLES, FBI, DoD, Secret Service and other agencies.



Increased Standardization of Devices



- **Open Mobile Terminal Platform (OMTP)**

- **September 2007 announced Micro USB is future common connector**

- **BONDI Initiative addressing the Mobile Platform Fragmentation Problem**



Increased Participation

- **Get involved in the policy side not just the technical side.**
 - **Take a position on the NAS Report and its recommendations.**
 - **Take a position on PI licenses for forensic examiners.**
 - **Write letters, e-mails, and articles.**
 - **E.g. Forensic Magazine; International Journal of Digital Evidence, etc.**



54 68 61 6e 6b 20 59 6f
75



Thank You...



Questions & Comments