

# Universal, fast method for iPad forensics imaging via USB adapter

Gómez-Miralles, Luis & Arnedo-Moreno, Joan  
INCIDE - Investigación Digital, S.L.      Universitat Oberta de Catalunya  
Valencia (Spain)                              Barcelona (Spain)

Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS-2011)

July 1, 2011

Seoul, Korea

# Index

1. Intro: mobile devices, Apple.
2. iOS: forensic possibilities, partitioning.
3. Proposed method: process, results, issues.
4. Conclusions.

# Intro

- Mobile devices:
  - Exponential growth in the last decade.
  - Nowadays they are portable computers in our pockets, capable of nearly everything.

# Apple, iPhone, iOS

- 2007: iPhone and iPod Touch. Multi-touch interface, finger-based (no stylus).
- 2008: iPhone O.S. 2.0. App Store. Developers start coding applications extending the device capabilities.
- Revolution in the mobile market.
- 2010: iPad, the rebirth of tablets. iPhone O.S. goes “iOS”.
- iOS devices represent a huge part of the mobile market.
- *“Apple now gets about two-thirds of its revenue from iOS devices — a platform that didn’t exist 4 years ago”* (Source: Augustine Fou, mktsci.com)

# Motivation

- For many users, an iPad can replace their computer.
- iPad forensics, trending topic.
- Need for fast, open imaging methods.

# iOS partitioning

- Every iOS device is partitioned the same:
  - SYSTEM partition < 1 GB, containing the iOS package: basic firmware and bundled applications.
  - USER DATA partition (rest of the space).
- From a forensics point of view, all of the device's relevant information is contained in the USER DATA partition.

# iOS Forensics 1/2

- Without a full image:
  - Extract iTunes backups from the owner's computer (or force the device back up to another computer). Analyze data contained in these iTunes backups.
  - Simple, but misses many things including unallocated (deleted) data.

# iOS Forensics 2/2

- Obtaining a full image:
  - Zdziarski public method
    - Versatile, but wi-fi throughput is 1 MB/s.
  - Proprietary methods
    - Used by some software vendors
    - New iOS versions can take a while to be supported.
    - Paid, closed-source, and/or restricted to Law Enforcement agencies.



# Our proposal

Apple's Camera Connection Kit can be used to image a jailbroken iPad to a hard drive or SD card.



# Camera Connection Kit

- Cheap accessory (\$30).
- Set of 2 adapters that give the iPad a SD slot and a USB port.
- Apple: *“the iPad Camera Connection Kit gives you two ways to import photos and videos from a digital camera”*.
- Implementing the USB PTP protocol would have been enough, but the iPad implements the ***USB mass storage device class*** protocol. It can mount and use external storage drives.

# Step-by-step process

- Jailbreak the iPad.
- Use Cydia to install *openssh* and *coreutils*.
- Disable autolock.
- Connect the iPad to a network and use a nearby computer to SSH into it.
- Plug the CCK. Add some USB or SD storage formatted as HFS+.
- Mount the CCK media.
- Use “dd” to image `/dev/rdisk0s2` to external storage.
- Unmount media.
- Done.

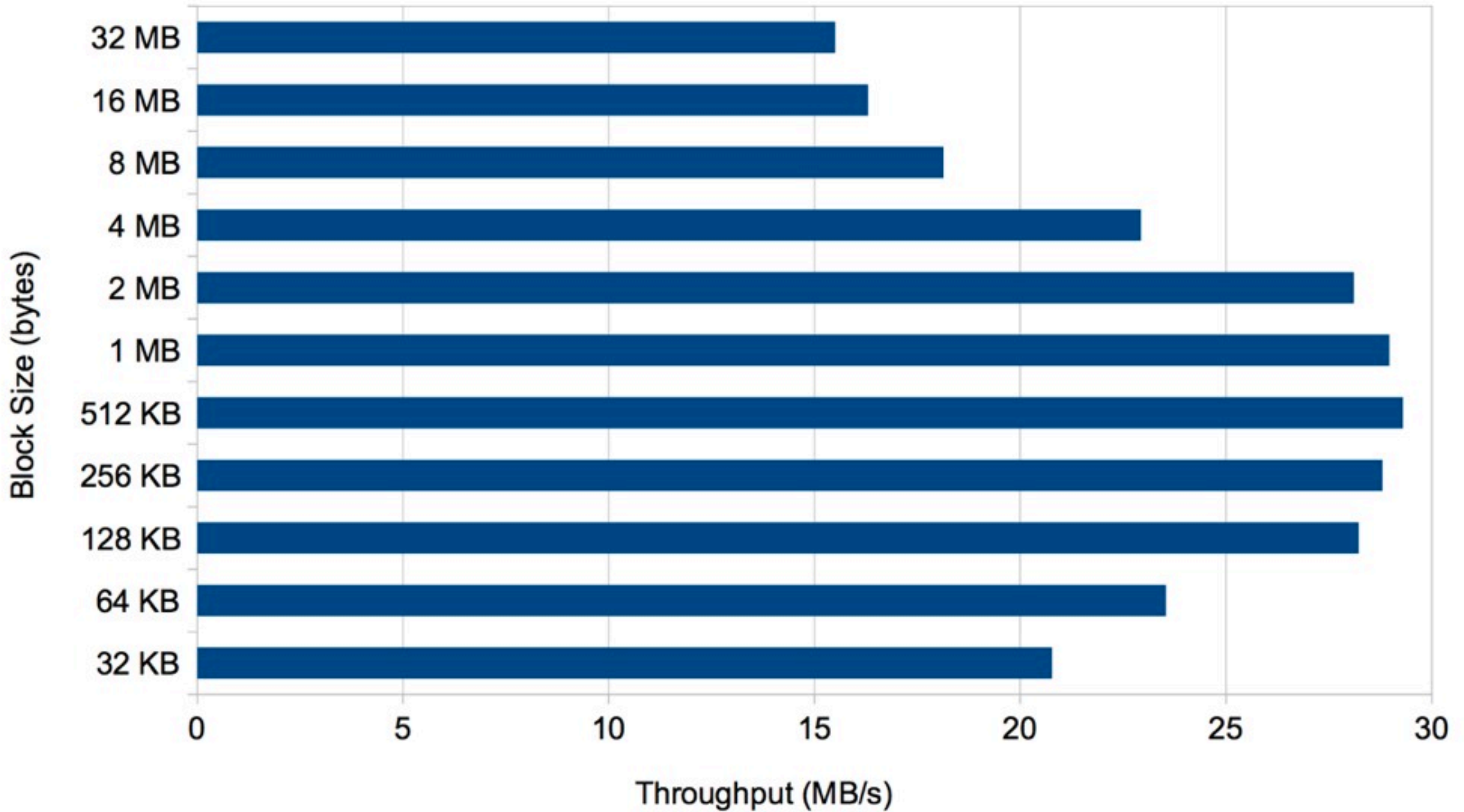
# Results

- Throughput:  
29 MB/s.
- For optimal results, use:  
`dd bs=512k`

Block Size [bs]	Speed (MB/s)			Av. speed (MB/s)
	Pass 1	Pass 2	Pass 3	
32 KB	20,7	20,8	20,8	20,77
64 KB	20,7	25,1	25,1	23,54
128 KB	29,5	27,6	27,6	28,22
256 KB	28,8	28,8	28,8	28,80
512 KB	28,8	29,5	29,6	29,30
1 MB	29,0	28,9	29,0	28,97
2 MB	28,1	28,1	28,1	28,10
4 MB	22,9	22,9	23,0	22,93
8 MB	18,1	18,1	18,2	18,13
16 MB	16,3	16,3	16,3	16,30
32 MB	15,5	15,5	15,5	15,50

# Imaging performance results

dd Block Size vs. Throughput



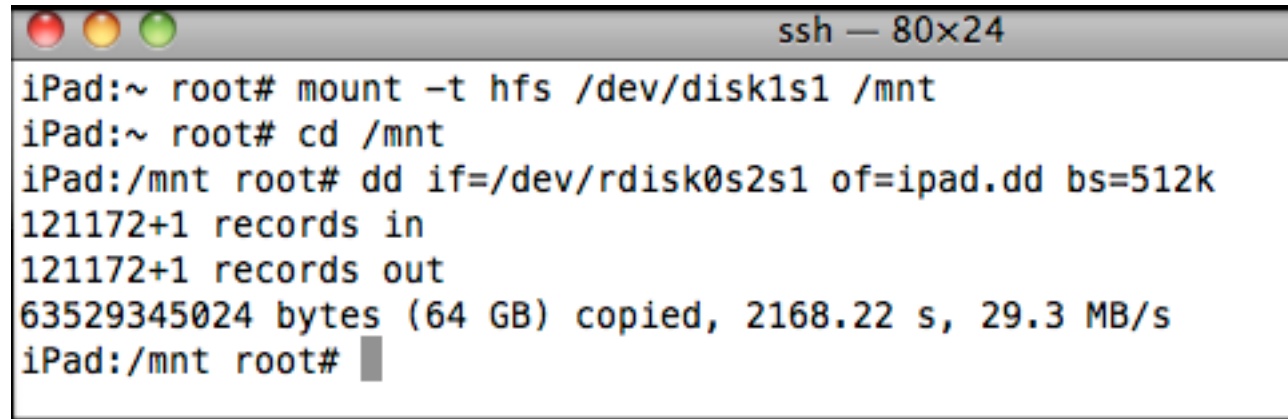
# Known issues

- Data protection: if activated, the image can be mounted but file contents are encrypted.
  - Common to all iOS forensics products, except Elcomsoft (for Law Enforcement only).
  - You can still see file names and dates.
- iOS 3.0+ does not allow to remount the partition read-only. It is recommended to keep the iPad activity to a minimum while imaging.
- It would be nice to do the same with an iPhone, but it does not support the CCK. No known hacks.

# Conclusions

- Cheap (\$30)
- Our method can be used with any iOS version as soon as there is a jailbreak for it (usually days after official release).
- Speed boost of  $\sim 30x$  over Zdziarski traditional (wi-fi) method.

# Questions?



```
ssh — 80x24
iPad:~ root# mount -t hfs /dev/disk1s1 /mnt
iPad:~ root# cd /mnt
iPad:/mnt root# dd if=/dev/rdisk0s2s1 of=ipad.dd bs=512k
121172+1 records in
121172+1 records out
63529345024 bytes (64 GB) copied, 2168.22 s, 29.3 MB/s
iPad:/mnt root# █
```

Gómez-Miralles, Luis & Arnedo-Moreno, Joan  
INCIDE - Investigación Digital, S.L.      Universitat Oberta de Catalunya  
Valencia (Spain)                              Barcelona (Spain)  
*pope@lgomez.es*                              *jarnedo@uoc.edu*