(Encrypted) iPhone Backups

Hal Pomeranz

Deer Run Associates

Installed Apps

Serial #

IMEI

Device Type

Phone #

Synched hosts

Metadata is Never Encrypted

Timestamps

File Names/Paths

OS Version

ICCID

Last Backup Date

~/Library/Application Support/
MobileSync/Backup

…\AppData\Roaming\Apple Computer
\MobileSync\Backup

```
$ cd ~/Library/Application\ Support/MobileSync/Backup/
$ file *
5d161b921298d21c4f4f5342a60a360e4723bd35: directory
6e2ea2a3cf1f0c76fa605210aea414a54b9c79af: directory
73ab81450db652c29881d9cd443e0a3fd8ecc2d0: directory
87981ddf6201413f1a505b9b279a77c39d1e4bc8: directory
e7149547b7eb33483182bf70378c329d8fe90d59: directory
```

- One directory for each device
- First backup is “full”, incrementals thereafter

```
$ cd 6e2ea2a3cf1f0c76fa605210aea414a54b9c79af
$ ls
00341074795f5c41178aac528d6d2cbe4bfb9873
004f6a5a1edf5f9caefa6c88f8c62b4612f2d3fa
00bb30a010ecb33bf54e6e9267d8a6945d9ca6aa
…
$ ls | wc -l
    4033
```

SHA1NAME = SHA1(Domain + ‘-’ + Filename)

```
$ ls *.*
Info.plist          Manifest.plist
Manifest.mbdb       Status.plist
```

Info.plist *– Device IDs, Phone #, OS vers, Apps*

Manifest.plist *– Encryption status & keybag, App versions*

Status.plist *– Backup status and date*

https://github.com/halpomeranz/mbdbls

```
usage: mbdbls.py [-f FILE] [--tab] [-T {l,e,u}] [-l | -s]
                 [-t {m,a,c} | -S] [-r]

Parse Manifest.mbdb files from iTunes backup directories

optional arguments:
  -h, --help            show this help message and exit
  -f FILE, --file FILE  File to parse (default Manifest.mbdb)
  --tab                 tab-delimited output (implies -l)
  -T {l,e,u}, --time_fmt {l,e,u}
                        Output (l)ocaltime, (u)tc, (e)poch
  -l                    detailed listing
  -s                    display file paths only
  -t {m,a,c}            Sort by m/a/c time
  -S                    Sort by file size
  -r                    Reverse sort order
```

Any final questions?

hal@deer-run.com

@hal_pomeranz

http://deer-run.com/~hal/ ← *slides here*

Sarah's Mac Forensic Analysis course –

http://www.sans.org/course/FOR518

SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

Website

digital-forensics.sans.org

SIFT Workstation

dfir.to/SANS-SIFT

Join The SANS DFIR Community

- Blog: dfir.to/DFIRBlog
- Twitter: @sansforensics
- Facebook: sansforensics
- Google+: gplus.to/sansforensics
- Mailing list: dfir.to/MAIL-LIST
- YouTube: dfir.to/DFIRCast

DFIR CURRICULUM

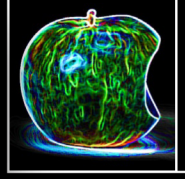
CORE

FOR408
Windows Forensics
GCFE

SEC504
Hacker Tools, Techniques, Exploits & Incident Handling
GCIH

OPERATING SYSTEM & DEVICE IN-DEPTH

FOR585
Advanced Smartphone Forensics



FOR518
Mac Forensics

FOR526
Memory Forensics In-Depth

INCIDENT RESPONSE & ADVERSARY HUNTING

FOR508
Advanced Incident Response
GCFA

FOR572
Advanced Network Forensics and Analysis
GNFA

FOR578
Cyber Threat Intelligence

LEARN REM

FOR610
REM: Malware Analysis
GREM

MGT535
Incident Response Team Management