



IR Process & Smart Phones

Terrance Maguire

tmaguire@cmdlabs.com

443-451-7330

Overview

cmdLabs>
Forensics | Response | Training

- Smart phones
 - Android, iPhone, Blackberry
- Volatile data
 - Running processes
 - Malware / spyware
- File system examination
 - Installed applications



Bank Robbery

cmdLabs>
Forensics | Response | Training

- Fake banking applications for Android
- ZeuS in the mobile (Zitmo)
 - Symbian and possibly Blackberry
- Starts by compromising computers
 - Captures online banking details
 - Asks users for cell phone number and model
- Intercepts SMS associated with online banking
 - Mobile transaction authentication numbers
 - Approve unauthorized bank transactions



Copyright 2010 cmdLabs LLC. All rights reserved.

DroidDream

cmdLabs>
Forensics | Response | Training

- Targeting legitimate application developers
 - Embed malicious code within their applications
 - Trojaned apps put on Android market place
- Broad capabilities
 - Root the operating system
 - Exfiltrate IMEI and IMSI



```
d = |write |IMSI|V
t u
d = |access2D $(Lcom/android/robot/adbRoot;)
Landroid/content/Context; |access2I $(Lcom/android/robot/adbRoot;)
Landroid/os/Handler; |write |IMSI|V getIMEI -
(Landroid/content/Context;|Ljava/lang/String; |phone|
# |getSystemService $(Ljava/lang/String;|Ljava/lang/Object;
: F
# = "android/telephony/TelephonyManager; |
getDeviceId: $(|Ljava/lang/String;
: %
: $ | | getIMSI |getSubscriberId
```

Mobile Incident Response

cmdLabs>
Forensics | Response | Training

- Closely monitor access to sensitive data
- Mobile Forensic Preparedness
 - forensic preservation of volatile data
 - Forensic examination of mobile device
- Limited network visibility
 - Banks with mobile applications
 - Organizations with company mobile devices

Copyright 2010 cmdLabs LLC. All rights reserved.

UNIX IR Refresher

cmdLabs>
Forensics | Response | Training

- Network traffic shows intruder connecting

```
Snort: 18:39:02 victim.3800 > attacker.3096: P
3707982354:3707982447(93) ack 220800367
```
- Network connections show intruder

```
# netstat -a
victim.3800      attackerIP.3096ESTABLISHED
victim.32828    irc-server.6667 ESTABLISHED
victim.telnet   investigator.2666  ESTABLISHED
```
- Processes show intruder activities

```
# ps -ef
hacked 11749  1 0  Mar 30 ?    0:13 irc-client
```

6

Copyright 2010 cmdLabs LLC. All rights reserved.

Incident Response Data

cmdLabs>
Forensics | Response | Training

- Full memory dump
- Volatile Data
- Non Volatile Data
- Network Logs

Copyright 2010 cmdLabs LLC. All rights reserved.

Android Systems

cmdLabs>
Forensics | Response | Training

- Remember it's UNIX
- Linux based OS
 - Droid x
 - G1/MyTouch
- File systems
 - YAFFS2
 - ext4



Copyright 2010 cmdLabs LLC.

Android Memory Forensics

cmdLabs>
Forensics | Response | Training

- Physical memory dump
 - DMD module developed by Joe Sylve
- Insert module on device (insmod dmd)
 - Creates /dev/dmd device
- Get start and end memory address(es)
 - `grep -i "system ram" /proc/iomem`
- Dump memory to removable media
 - `echo "0x80c00000 0x9fdffff /sdcard/mem.dump" > /dev/dmd`

Copyright 2010 cmdLabs LLC. All rights reserved.

Android Memory Forensics

cmdLabs>
Forensics | Response | Training

- Examination of Android physical memory
 - Volatility plugin for Android memory
 - Developed by Andrew Case, Digital Forensics Solutions

```

root@newbuntu:~/volatility# python volatility.py --profile=android -f /mnt/media/vollogs/android-dm1.dump --disk_lime_pt
Volatile Systems Volatility Framework 1.4_rc1
Name            Start         End
----            -
1004            0x00000000    0x00000000
sdmmcblk1p1     0x00000000    0x00000000
sdmmcblk1p2     0x00000000    0x00000000
sdmmcblk1p3     0x00000000    0x00000000
sdmmcblk1p4     0x00000000    0x00000000
sdmmcblk1p5     0x00000000    0x00000000
sdmmcblk1p6     0x00000000    0x00000000
sdmmcblk1p7     0x00000000    0x00000000
sdmmcblk1p8     0x00000000    0x00000000
sdmmcblk1p9     0x00000000    0x00000000
sdmmcblk1p10    0x00000000    0x00000000
sdmmcblk1p11    0x00000000    0x00000000
sdmmcblk1p12    0x00000000    0x00000000
sdmmcblk1p13    0x00000000    0x00000000
sdmmcblk1p14    0x00000000    0x00000000
sdmmcblk1p15    0x00000000    0x00000000
sdmmcblk1p16    0x00000000    0x00000000

root@newbuntu:~/volatility# python volatility.py --profile=android -f /mnt/media/vollogs/android-dm1.dump --disk_lime_pt
Volatile Systems Volatility Framework 1.4_rc1
Name            Start         End         Type
----            -
/dev/block/sdmmcblk1p4  /system
sysfs            /sys
devpts           /dev/pts
/dev/block/dm-1   /mnt/aesd/ocm.sovim.sngrybirds-1
proc             /proc
BIOS             /dev/cdrom0
sysfs            /mnt/sdcard/.android_secure
tmpfs

```

Copyright 2010 cmdLabs LLC. All rights reserved.

Android Volatile Data

cmdLabs>
Forensics | Response | Training

- Running processes through adb shell

```
$ ps
USER      PID  PPID  VSIZE  RSS      WCHAN    PC         NAME
root      1    0     284    196      c00belac 0000c86c S /init
root      2    0      0      0      c006687c 00000000 S kthreadd
<edited for length>
system    75   50    164160 23888    ffffffff afe0c51c S system_server
radio     119  50    100864 16812    ffffffff afe0d4a4 S com.android.phone
app_8     122  50    111900 19192    ffffffff afe0d4a4 S android.process.acore
app_14    151  50    102920 17548    ffffffff afe0d4a4 S com.google.process.gapps
app_16    187  50    89808  14116    ffffffff afe0d4a4 S android.process.media
root      217  2     0      0      c00334c0 00000000 D audmgr_rpc
app_2     246  50    93852  16520    ffffffff afe0d4a4 S com.android.calendar
app_19    289  50    88648  13088    ffffffff afe0d4a4 S com.android.alarmclock
app_8     297  50    96736  14584    ffffffff afe0d4a4 S com.tmobile.myfaves
app_6     304  50    94356  13656    ffffffff afe0d4a4 S com.android.mms
app_24    317  50    89356  13076    ffffffff afe0d4a4 S
com.google.android.apps.uploader
app_37    327  50    97320  13932    ffffffff afe0d4a4 S com.vonagemobile.fbphone
app_17    333  50    88288  12176    ffffffff afe0d4a4 S com.android.voicedialer
app_22    342  50    90068  13820    ffffffff afe0d4a4 S com.google.android.gm
shell     375  57    740    316      c0054578 afe0d14c S /system/bin/sh
shell     381  375   884    316      00000000 afe0c27c R ps
```

Android Volatile Data

cmdLabs>
Forensics | Response | Training

- top

```
User 2%, System 2%, IOW 0%, IRQ 0%
User 9 + Nice 0 + Sys 7 + Idle 295 + IOW 0 + IRQ 0 + SIRQ 0 = 311
  PID CPU% S  #THR   VSS   RSS PCY UID      Name
2161  2% R    1    860K   432K fg root    top
1259  0% S   63 259604K 62492K fg system  system_server
2141  0% S    8 153252K 24456K fg app_99  jackpal.androidterm
  715  0% S    1     0K     0K fg root    pvrflip/0
```

- /system/xbin/busybox netstat

Forensic Acquisition

cmdLabs>
Forensics | Response | Training

- mre\$./adb shell
\$ su
- # dd if=/dev/block/userdata bs=1024 |
/system/bin/busybox nc 192.168.2.2 755
7028736+0 records in
7028736+0 records out
7197425664 bytes transferred in 24211.203 secs

Copyright 2010 cmdLabs LLC. All rights reserved.

Remote Acquisition

cmdLabs>
Forensics | Response | Training

- F-Response
 - ARM agent
 - On SDCard
- Expanding
Android
device support
 - Segmentation
Faults on
some devices

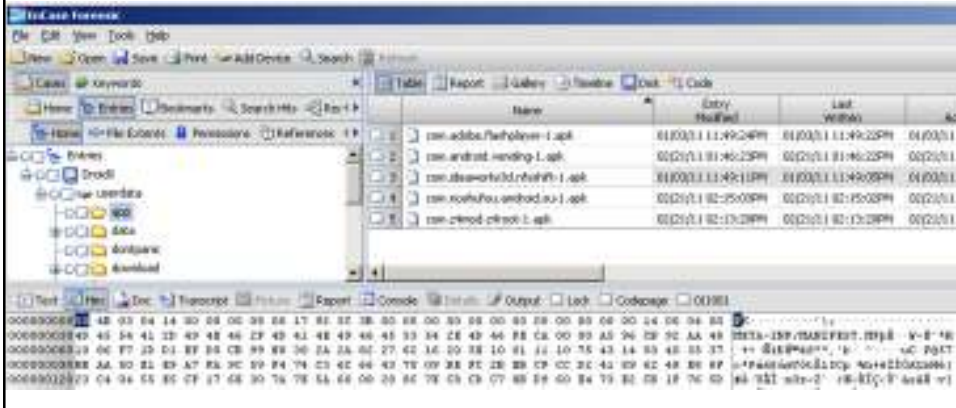
```
# ./f-response-ce-e-android -c ./fresponse.ini
F-Response Consultant/Enterprise(Android/ARM Edition) Version 3.09.08
F-Response Disk: /dev/mtd/mtd0 (26624 sectors, 512 sector size)
13 MB write blocked storage on F-Response Disk:mtd0
F-Response Disk: /dev/mtd/mtd1 (5120 sectors, 512 sector size)
2 MB write blocked storage on F-Response Disk:mtd1
F-Response Disk: /dev/mtd/mtd2 (640 sectors, 512 sector size)
0 MB write blocked storage on F-Response Disk:mtd2
F-Response Disk: /dev/mtd/mtd3 (128 sectors, 512 sector size)
0 MB write blocked storage on F-Response Disk:mtd3
F-Response Disk: /dev/mtd/mtd4 (128 sectors, 512 sector size)
0 MB write blocked storage on F-Response Disk:mtd4
F-Response Disk: /dev/mtd/mtd5 (128 sectors, 512 sector size)
0 MB write blocked storage on F-Response Disk:mtd5
F-Response Disk: /dev/mtd/mtd6 (6144 sectors, 512 sector size)
3 MB write blocked storage on F-Response Disk:mtd6
F-Response Disk: /dev/mtd/mtd7 (614400 sectors, 512 sector size)
300 MB write blocked storage on F-Response Disk:mtd7
F-Response Disk: /dev/mtd/mtd8 (12288 sectors, 512 sector size)
6 MB write blocked storage on F-Response Disk:mtd8
F-Response Disk: /dev/mtd/mtd9 (3561472 sectors, 512 sector size)
1739 MB write blocked storage on F-Response Disk:mtd9
```

Copyright 2010 cmdLabs LLC. All rights reserved.

File System Examination

cmdLabs>
Forensics | Response | Training

- Android file system forensics

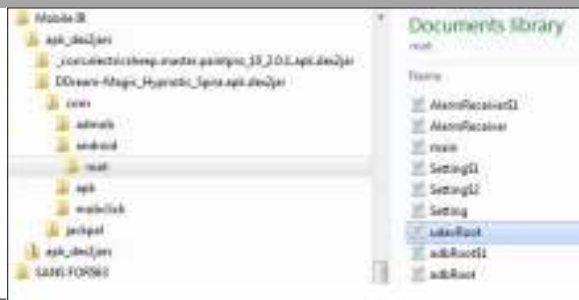


Copyright 2010 cmdLabs LLC. All rights reserved.

Malware Analysis

cmdLabs>
Forensics | Response | Training

- DroidDream
 - Root exploit
 - Data theft
 - Updates



```

$P*4 2 ^ /com/android/root/udevRoot  {}java/lang/Object  ^
udevRoot.java
BUFFER_SIZE  1^ 1
FRAME_EXPLOIT  {}java/lang/String;  exploit@
^FRAME_REMOTE_DATA_RD  {}remote_data.sd  @  {}FRAME_REMOTE_WEP_RD  {}remote_www_sd.sd
@  ^  {}FRAME_REMOTE_WYS_SD  {}remote_www_sd.sd  @
FRAME_SD_BIN
profile@  {}REMOTE_EXEC_PATH  {}/system/bin/mount@  =  {}ROOT_SHELL_PATH  {}/data/local/tmp/
rootshell@
SU_EXEC_PATH  {}/system/bin/profile@  {}TAG  {}UdevRoot  @
{}DisableWifi  2  ^ctk  {}Landroid/content/Context;
remote@system
wifiManager  Landroid/net/wifi/WifiManager;  =<init>  (Landroid/content/Context;)V  ^
ITV
    
```

Copyright 2010 cmdLabs LLC. All rights reserved.

Live Response Lessons

cmdLabs>
Forensics | Response | Training

- Don't trust the operating system
 - May give false information
 - Seek corroborating sources of evidence
- No extensive examination and searching
 - If it is that interesting, acquire memory and disk
- Don't copy large amounts of data remotely
 - Slow and prone to failure
 - Get physical access if possible

17

Copyright 2010 cmdLabs LLC. All rights reserved.

Android Challenges

cmdLabs>
Forensics | Response | Training

- Root access
 - alters the system
- YAFFS2 file system
 - File carving as an alternative

Hope for the future:

- Recovery partition and boot loader acquisition
 - Does not require rooting the device
- File system moving to ext4
 - Similar to common Linux file systems

Copyright 2010 cmdLabs LLC. All rights reserved.

iPhone Overview

cmdLabs>
Forensics | Response | Training

- Remember it's UNIX!
- Volatile data
 - Jailbreak (redsn0w)
 - Terminal, adv-cmds, and top
- File System
 - Physical acquisition



Copyright 2010 cmdLabs LLC. All rights reserved.

iPhone Volatile Data

cmdLabs>
Forensics | Response | Training

- Process list
 - ps and top
- Network connections

```
Processes: 37 total, 1 running, 36 sleeping... 215 threads... 13:08:38
Load Avg: 0.85, 0.80, 0.63 CPU usage: 2.40% user, 17.09% sys, 73.50% idl
SharedLibs: num = 0, resident = 0 code, 0 data, 0 linkedit.
MemRegions: num = 10536, resident = 137M + 0 private, 51M shared.
PhysMem: 64M wired, 14M active, 8504K inactive, 249M used, 4224K free.
VM: 1986M + 0 936464(0) pageins, 5924(0) pageouts
```

PID	COMMAND	%CPU	TIME	#TH	#PRTS	#MREGS	RPRVT	RSHRD	RSIZE	VSIZE
2987	assetsd	0.0%	0:00.53	3	81	99	1752K	2296K	3132K	70M
2985	top	13.7%	0:04.10	1	23	39	432K	1448K	908K	14M
2977	bash	0.0%	0:00.07	1	14	50	292K	1964K	904K	14M
2976	bash	0.0%	0:00.05	1	14	50	276K	1964K	908K	14M
2975	login	0.0%	0:00.06	1	19	59	248K	1344K	548K	15M
2974	login	0.0%	0:00.08	1	19	59	248K	1344K	548K	15M
2973	Terminal	6.0%	0:12.56	4	116	470	5276K	10M	11M	85M
2931	Twitter	0.0%	0:56.37	8	143	228	6984K	2816K	32M	80M
2907	Preference	0.0%	0:02.31	5	139	248	3096K	2736K	4264K	75M
2901	Maps-iPhon	0.0%	0:12.06	9	166	235	4420K	2736K	6900K	76M
2824	AppStore	0.0%	0:10.95	7	145	256	8660K	3132K	10M	88M
2823	MobileTime	0.0%	0:00.96	5	94	182	2460K	2736K	3180K	61M
2779	MobileSaf	0.0%	0:01.13	5	103	219	2008K	2736K	2720K	70M
2756	MobileSafa	0.0%	1:40.11	11	186	457	19072K	3544K	21M	148M
913	iapd	0.0%	1:01.51	5	151	113	1156K	1824K	1680K	39M
415	MobileMusi	0.0%	1:08.39	5	147	211	3892K	2756K	5540K	74M
376	Schelper	0.0%	5:19.22	4	52	58	360K	1224K	476K	18M
356	MobileMail	0.0%	15:22.56	13	324	637	13932K	3628K	19M	118M
355	MobilePhon	0.0%	1:41.14	6	164	473	5480K	2832K	7272K	85M

```
ip link show
ip netns exec redsn0w bash
ip netns exec redsn0w ps
ip netns exec redsn0w top
ip netns exec redsn0w netstat -tln
```

Non Jailbroken iPad2

cmdLabs>
Forensics | Response | Training



Copyright 2010 cmdLabs LLC. All rights reserved.

Physical Acquisition

cmdLabs>
Forensics | Response | Training



Copyright 2010 cmdLabs LLC. All rights reserved.

Encryption Barriers

cmdLabs>
Forensics | Response | Training

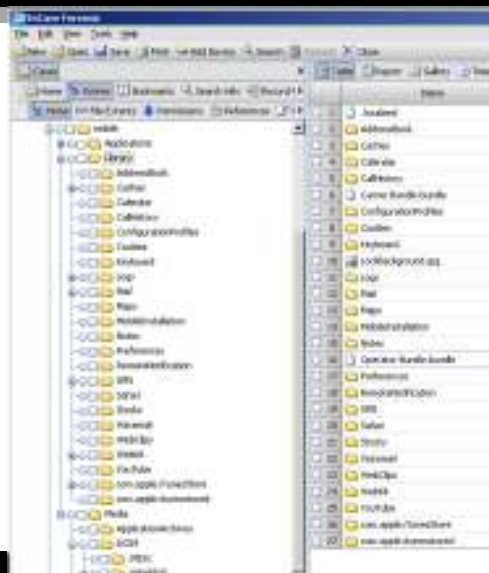


Copyright 2010 cmdLabs LLC. All rights reserved.

File System Examination

cmdLabs>
Forensics | Response | Training

- Apple HFSX / HFS+
- Keyword searches
- File carving
 - Screen captures



Copyright 2010 cmdLabs LLC. All rights reserved.

Keychains

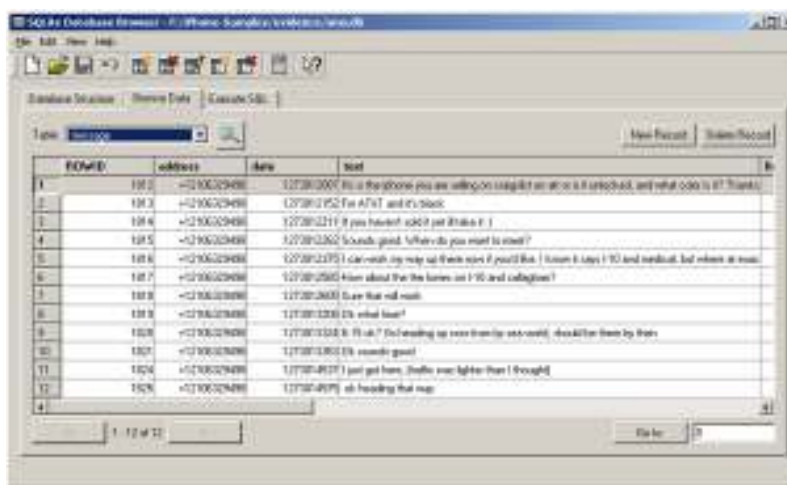
cmdLabs>
Forensics | Response | Training

- F:\MacSamples>sqlite3.exe
"iPhone2\Keychains\keychain-2.db"
- SQLite version 3.6.16
- Enter ".help" for instructions
- Enter SQL statements terminated with a ";"
- sqlite> select labl,acct,svce from genp;
- |eric.rooster@yahoo.com|Yahoo-token
- |erooster@live.com|
- |erikroost@hotmail.com|
- |therooster@hotmail.com|
- |therooster@hotmail.com|com.apple.itunesstored.keychain
- erooster|MMODBracketsAccount|
- LumosityBrainTrainer|erooster|LumosityBrainTrainer

Copyright 2010 cmdLabs LLC. All rights reserved.

Text Messages

cmdLabs>
Forensics | Response | Training



ID	IDNUM	address	date	text
1	1313	+1200329486	12/28/2007	Is it the phone you are calling on tonight or at or is it unpatched, and what code is it? Thanks!
2	1313	+1200329486	12/28/2007	PS: For AT&T and it's stock.
3	1314	+1200329486	12/28/2007	If you haven't called yet thank u!
4	1315	+1200329486	12/28/2007	Sounds good. I'll be in the area if you need to meet?
5	1316	+1200329486	12/28/2007	I can't wait to see you all from next year! I'll be in the area if you need to meet. I'll be in the area if you need to meet.
6	1317	+1200329486	12/28/2007	How about the the lines on I-90 and California?
7	1318	+1200329486	12/28/2007	How about the the lines on I-90 and California?
8	1319	+1200329486	12/28/2007	How about the the lines on I-90 and California?
9	1320	+1200329486	12/28/2007	How about the the lines on I-90 and California?
10	1321	+1200329486	12/28/2007	How about the the lines on I-90 and California?
11	1322	+1200329486	12/28/2007	How about the the lines on I-90 and California?
12	1323	+1200329486	12/28/2007	How about the the lines on I-90 and California?

Copyright 2010 cmdLabs LLC. All rights reserved.

Epilog

cmdLabs>
Forensics | Response | Training

- Deleted SQLite entries

Name	Page Number	Deleted Date/Time	Deleted Bytes	Deleted	File Name	File Content	File Content	File Content	File Content
Message Analysis	37	0.07.10.07.1	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.2	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.3	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.4	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.5	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.6	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.7	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.8	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.9	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.10	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.11	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.12	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.13	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.14	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.15	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.16	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.17	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.18	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.19	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.20	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.21	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.22	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.23	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.24	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.25	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.26	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.27	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.28	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.29	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.30	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14
Message Analysis	37	0.07.10.07.31	Message 32.01.14	YES	Message Analysis	Message 32.01.14	Message 32.01.14	Message 32.01.14	Message 32.01.14

Keylogger

cmdLabs>
Forensics | Response | Training

- User entered strings

```

dynamic: test 00
Offset
00000000 DynamicDictionary-4  A single event at home daily event weekly
00000001 event biweekly event monthly event yearly event yearly this just
00000002 for short note this is note this is the second line this is the
00000003 third line this is the fifth line another note just for testing
00000004 things some more this is going into the clipboard airplane hoah
00000005 detroit someometers lbe aw state building empire state hotel
00000006 d square new york grand central new york penn new york station a
00000007 y all day event home lockdown password password password passowrd
00000008 d password password number number changing aid changed old chang
00000009 ed office association http eww association local iphone yahoo dr
0000000a not such just playing with my iphone testing in lite on my ipho
0000000b ne now the regular yahoo app yeah dr i'm using the official sia
0000000c app on my that's the plan now from is think it is getting good d
0000000d ata sending an text recording cd cd root alpine cd root cd libra
0000000e ry cd ocher cd cd cells cat cells less more quit quit exit exit
0000000f alpine cd text on the road can you tell where was it's puzzle b
00000010 est testing ping did you see this diego yahoo com com what up ht
00000011 tp com auxiline apphonerson icankascheeburger esip
00000012 ve my gmail pphonewo pphonewo ped plist eu si le lo ce
00000013 file vnicain dave
  
```

Copyright 2010 cmdLabs LLC. All rights reserved.

Locations

cmdLabs>
Forensics | Response | Training

- cells.plist
- cells-local.plist

```

kali@kali: ~$ cat /usr/share/doc/forensic-toolkit/cells.plist
Offset:
00000000 bplsm090  318 410 8a4264 0e6bd 310 818 8a5e07 2e5e77e
00000040 a_ 319 418 0a06d5 8a5e77cab 72 429 8e722227 -98 40765818 1800
00000080 800000 1 292612672 942 72 +29 46634892 -98 40997465 3000 888000
000000c0 1 292743263 725 72 +29 40888803 -98 58287209 3888 400000 1 292
00000100 871065 888 8 4 7 8 8
  
```



Copyright 2010 cmdLabs LLC

Blackberry

cmdLabs>
Forensics | Response | Training

- Loaded modules and dependencies
 - javaloader
- File System
 - Blackberry Desktop Manager
 - Mounted logically



Copyright 2010 cmdLabs LLC. All rights reserved.

Compromised Blackberry

cmdLabs>
Forensics | Response | Training

- Malicious program running on Blackberry

Name	Version	Size	Created
net_rim_platform_resource_en_US	4.0.2.49	2288	Thu Sep 01 15:20:30 2005
net_rim_platform_im_resource_en_US	4.0.2.49	1824	Thu Sep 01 15:20:24 2005
net_rim_app_manager	4.0.2.49	1796	Thu Sep 01 15:20:32 2005
net_rim_app_manager_console	4.0.2.49	3364	Thu Sep 01 15:20:33 2005
<edited for length>			
net_rim_bb_phone_app	4.0.2.49	79768	Thu Sep 01 15:23:38 2005
net_rim_bb_task_app	4.0.2.49	38732	Thu Sep 01 15:35:35 2005
InstantMessaging	4.1.7	329920	Fri Aug 12 13:54:17 2005
Smartphone	0.0	28988	Sat Jan 30 09:54:08 2010

167 modules; 9282804 bytes total

Copyright 2010 cmdLabs LLC. All rights reserved.

MobileSpy

cmdLabs>
Forensics | Response | Training

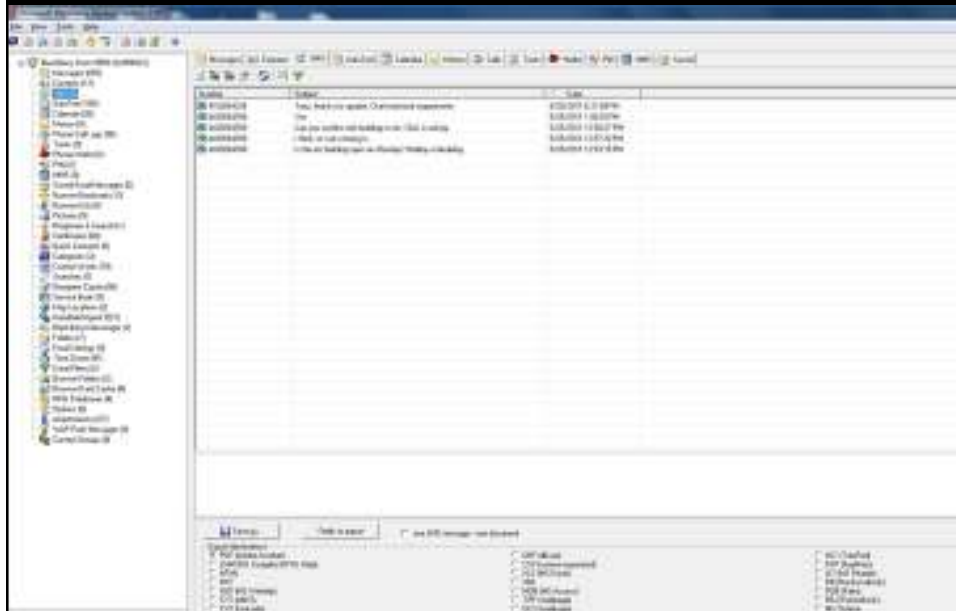
The screenshot displays the MobileSpy web interface. At the top, there is a banner for "MOBILE SPY" with the tagline "Spy Software for Mobile Phones" and a list of features: "Monitor BlackBerry, iPhone, Android, more!", "Silently Record Text Messages", and "GPS Locations and Call Details!". Below the banner is a navigation menu with links for HOME, SMS LOGS, CALL LOGS, GPS LOGS, SUPPORT, and LOGOUT. The main content area is titled "SMS LOGS MOBILE SPY" and "SMS Messages Sent and Received". It shows a table of logs with columns for TIME, SENDER, RECEIVER, DIRECTION, and TEXT MESSAGE. The table contains three rows of data. On the left side, there are two panels: "LOG VIEWERS" with options like "View SMS Logs", "View Call Logs", "View GPS Logs", "View URL Logs", "Logs Summary", and "CSV Format"; and "USER TOOLS" with options like "Search Logs", "Clear All Logs", "Change Password", "User Settings", and "Logout Account".

TIME	SENDER	RECEIVER	DIRECTION	TEXT MESSAGE
2010-01-07 15:08:59	12836452774	Monitored Device	Incoming	Delivered
2010-01-07 11:58:51	Monitored Device	2036452774	Outgoing	Transfer complete. Awaiting delivery.
2010-01-05 12:17:20	Monitored Device	2036452774	Outgoing	Meet me in 2 at the usual

Copyright 2010 cmdLabs LLC. All rights reserved.

Blackberry Backup (IPD)

cmdLabs>
Forensics | Response | Training



Blackberry Options

cmdLabs>
Forensics | Response | Training

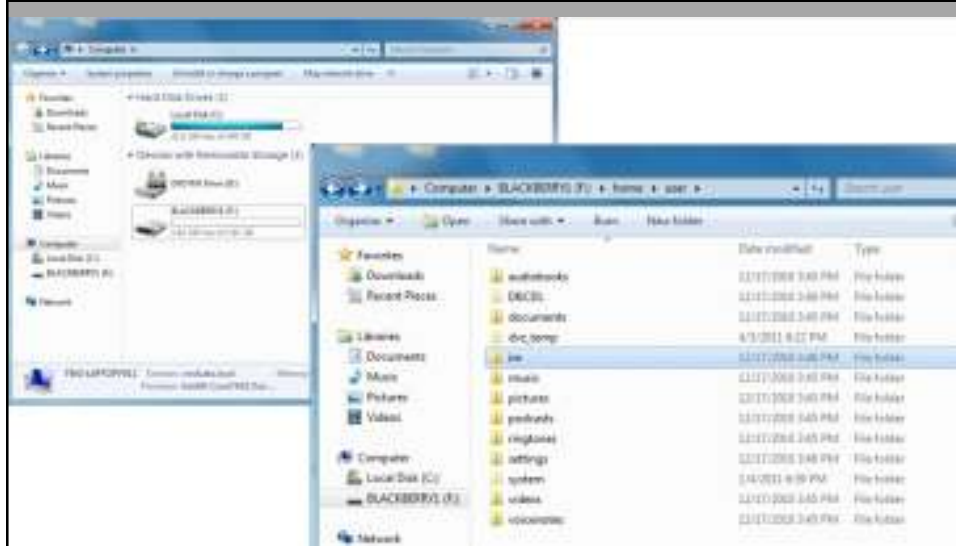
- Mass Storage Mode
 - Access device via desktop OS
 - Enabled by default
 - Requires password access
- Access items in file system
 - Saved BBIM chats
 - Malware artifacts



Copyright 2010 cmdLabs LLC. All rights reserved.

Blackberry File System

cmdLabs>
Forensics | Response | Training



Copyright 2010 cmdLabs LLC. All rights reserved.

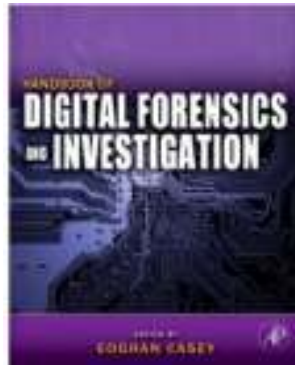
Questions & Contact

cmdLabs>
Forensics | Response | Training

SANS FOR563

Mobile Device Forensics

Criminals be Warned: Anything you text will be used against you.



Copyright 2010 cmdLabs LLC. All rights reserved.