

COMP 116 - Assignment 5

Forensics

Chris Piraino
Amadou Crookes

Hidden Data in Images

We ran diff on all the images and found out that a.jpg was not the same as the others. Knowing this we began to look into this image. We used steghide to find hidden data in a.jpg. There was no password so it was able to find out that there was another picture of Norman Ramsey hidden inside the picture of Norman Ramsey!



sdcard.dd Forensics

Downloaded sdcard.dd.zip, took the md5sum and checked to ensure it was the same as given on the course site, then unzipped the image file and took the md5sum of the uncompressed file to ensure that no data was lost.

```
$ md5sum sdcard.dd.zip
e651ac1429516c5fa63b7c526548b9bb *sdcard.dd.zip
```

```
$ md5sum sdcard.dd
c4d851d2e6e7d65739b92eb8723a3f3c *sdcard.dd
```

1. Vol 2 is formatted with FAT32 for Win95, and vol 3 is formatted as with the regular Linux

format ext3.

2. There does not seem to be any phone carrier involved. The two operating systems, Windows95 and Kali Linux, are not used as smartphone OSes, and there is nothing within either file system that would indicate a phone carrier's presence.
3. Windows95 - Autopsy reports vol 2 of the sdcard.dd is a Win95 partition. vol 3 is Kali GNU/Linux 1.0. Opened up sdcard.dd in Autopsy and looked in the /etc directory for files with *-release. Found a file named os-release with the following contents:

```
PRETTY_NAME="Kali GNU/Linux 1.0"
NAME="Kali GNU/Linux"
ID=kali
VERSION="1.0"
VERSION_ID="1.0"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG_REPORT_URL="http://bugs.kali.org/"
```

4. Sample of installed Applications:
 - Metasploit.
 - BlindElephant.py.
 - acccheck.pl - password guessing tool for Linux.
 - bluez-test-telephony - Python script trying to connect to bluetooth on a device.
 - the harvester and truecrack - deleted executables from the /usr/bin directory.
 - websploit.
 - cisco-torch.pl.
 - mrpkey.py - a script to calculate 3DES key for passports.
 - Burpsuite.
 - Blueranger.sh - finds nearby bluetooth devices.
 - Aircrack-ng - A WIFI password cracking executable, faked-tcp executable.
 - U3-Pwn.
 - Webslayer - a tool used for brute-forcing web applications.
 - Dumpzilla - a forensics tool.
 - TrueCrypt
 - recon-ng - a reconnaissance framework in Python.

To find this data, we looked through /usr/bin and either skimmed the source code of the scripts, or googled the executable's name in order to figure out what the purpose of












the program was.

5. The root password is toor. We found this by taking the /etc/passwd and /etc/shadow files and using John the Ripper to unshadow and crack the password against a word list.

```
defcon@ubuntu:~/john-1.8.0/run$ ./john --show unshadowed.txt
root:toor:0:0:root:/root:/bin/bash

1 password hash cracked, 0 left
```

6. There are no other user accounts on the disk. We checked the /etc/shadow file for user/password combinations and only root was enabled. All of the rest of the “users” in /etc/shadow were used for different programs installed on the machine, e.g. www-data for nginx and mysql for mysql.
7. Photos of Celine Dion, tour dates, and set lists in root directory. The suspect also bought a ticket to see Celine in Vegas. After sorting all the files by extension we searched through the JPG files and found the ticketmaster confirmation email.
8. The suspect deleted files named new1.jpg, new2.jpg, and new3.jpg from the /root directory at some point. Under the /root/Pictures directory there are pictures named old*.jpg, so we assume that the new*.jpg pictures are new Celine Dion pictures, perhaps with data embedded within.

 new1.jpg	1970-01-02 20:33:59 EST	1970-01-02 20:33:59 EST	1970-01-02 20:33:17 EST	1970-01-02 20:32:53 EST	0	Unallocated
 .Dropbox.zip	1970-01-02 20:21:07 EST	1970-01-02 20:21:07 EST	1970-01-02 20:21:06 EST	1970-01-02 20:21:06 EST	20971520	Allocated
 new2.jpg	1970-01-02 20:34:00 EST	1970-01-02 20:34:00 EST	1970-01-02 20:33:22 EST	1970-01-02 20:32:53 EST	0	Unallocated
 .local	1969-12-31 21:14:32 EST	1969-12-31 21:14:32 EST	1969-12-31 21:14:32 EST	1969-12-31 21:14:32 EST	4096	Allocated
 .ICEauthority	1969-12-31 21:20:26 EST	1969-12-31 21:20:26 EST	1969-12-31 21:20:26 EST	1969-12-31 21:20:26 EST	0	Allocated
 .pulse-cookie	1969-12-31 21:14:37 EST	1969-12-31 21:14:37 EST	1969-12-31 21:14:37 EST	1969-12-31 21:14:37 EST	256	Allocated
 .pulse	1969-12-31 21:14:43 EST	1970-01-02 20:34:23 EST	1969-12-31 21:14:37 EST	1969-12-31 21:14:37 EST	4096	Allocated
 .gvfs	1969-12-31 21:14:37 EST	1969-12-31 21:14:37 EST	1969-12-31 21:14:37 EST	1969-12-31 21:14:37 EST	4096	Allocated
 .gstreamer-0.10	1969-12-31 21:15:22 EST	1969-12-31 21:15:22 EST	1969-12-31 21:15:20 EST	1969-12-31 21:15:20 EST	4096	Allocated
 new3.jpg	1970-01-02 20:34:03 EST	1970-01-02 20:34:03 EST	1970-01-02 20:33:38 EST	1970-01-02 20:32:53 EST	0	Unallocated
 .TrueCrypt	1969-12-31 21:19:42 EST	1969-12-31 21:19:42 EST	1969-12-31 21:19:37 EST	1969-12-31 21:19:37 EST	4096	Allocated

9. We believe that the .Dropbox.zip file is encrypted using TrueCrypt. When trying to extract the .Dropbox zip file, an error is produced stating that the file is corrupt, and using the file command on the .Dropbox.zip file results in a file type of data. We have not been able to decrypt the file as of yet.
10. Bought a ticket to see Celine Dion on Jul. 28th, 2012 in Las Vegas. Found this by noticing

a deleted receipt.pdf file in the /root directory. Then, using PhotoRec, we sorted the files by type and looked through the pdfs to find the ticketmaster receipt.

11. There are a number of very weird pictures on the disk, including a picture of a woman with a ballgag, a picture of raw meat, a picture of a creepy man with white facepaint, and of course a number of pictures of Celine Dion. On vol 2 there was also evidence of a iPhone photo being taken and stored, but we could not find it.

12. The suspect was stalking Celine Dion.