Forensic Analysis of Wireless Networking Evidence of Android Smartphones

Panagiotis Andriotis, George Oikonomou, Theo Tryfonas

Introduction

Despite the rapid evolution of mobile devices over the recent past years, mobile phone forensics as a field within forensic science is at an early stage, when compared to traditional computer forensics.

Problem definition

According to industrial research findings (IDC) on the worldwide smartphone operating system (OS) market share, sales indicate that Android is the leading OS. Thus, it is more likely to seize an Android phone from a crime scene for investigation, than a device running under any other OS. The use of wireless communications became an easy task for modern smartphones and criminal activity takes advantage of these utilities.

Aim of Research

To introduce a method for acquiring evidence from an Android smartphone in a proper and acceptable forensic manner and also help the investigators to prove the use of the Bluetooth technology and wireless communications by a suspect in the course of a crime investigation.

Implementation

We used three devices with specs:	**Samsung Galaxy Europa**	**HTC Desire**	**LG Optimus E400**
CPU	600 MHz	1 GHz	800 MHz
Memory (MB)	170	576 RAM 512 ROM	1 GB 384 RAM
OS	2.1-update	2.2.2	2.3.6

- Open source software (Unix utilities)
- *SuperOneClick* for rooting the device
- *Busybox* (Unix utilities for the device)

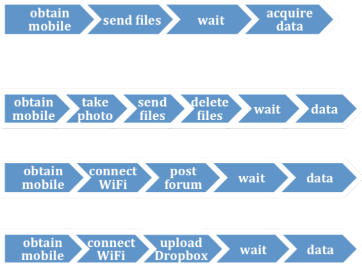
ACPO Guidelines (principles)

- No action taken should change data held on a computer or storage media.
- If an investigator access original data he/she must be competent to do so.
- An audit trail should be created and preserved.
- The person in charge of the investigation has overall responsibility for ensuring that these principles are adhered to.

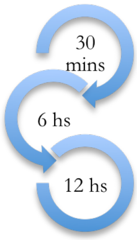
Scenarios

- Child pornography photos were found in a laptop. The Police believe photos were transferred over a Bluetooth connection.
- A man was arrested after witnesses saw him holding a smartphone below a girl's skirt line. Authorities are looking for Bluetooth activity.
- A student has posted questions from a test to an online forum via Wi-Fi and requested the answers from other users.
- A suspect is believed to be uploading inappropriate images using an unsecured Wi-Fi network via his smartphone using his Dropbox application installation.

Methodology



Experiment Lifecycle



In order to investigate the impact of *time* to the results.

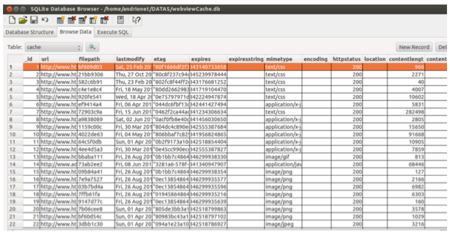
Methodology

- Activate 'airplane mode', 'USB debugging mode', then connect.
- Start ADB server, acquire logs with *logcat*.
- Send SIM, SD card for investigation, gain root access.
- Use *dd* or *nanddump* to perform physical acquisition of user data.
- *Pull* images from SD to the examination machine (we used an Ubuntu 12.04 64bit machine).
- *Mount* images to machine, use Table 1 to investigate.
- Unmount (*umount*) properly.
- Use a checksum to mark images.

Information Sources

Path	File name
/misc/bluetooth/MAC (MAC: device dependant)	classes, config, lastseen, linkkeys, names, profiles
/data/com.android.bluetooth/databases	btopp.db
/misc/wifi	wpa_config.conf
/data/com.google.android.server.checkin/databases	checkin.db
/data/com.google.android.gsf/databases	htcCheckin.db
/data/com.google.android.location/files	cache.wifi, cache.cell
/data/com.android.browser/databases	browser.db, webview.db, webviewCache.db
logcat files	main and events buffer
Databases related to applications e.g. Dropbox	e.g. db.db

Table 1: Paths and file names where an investigator can find relative information to wireless activity.



	_id	url	filepath	lastmodify	etag	expires	expiresstring	mimetype	encoding	httpstatus	location	contentlengt	content
1	1	http://www.ht	bf609d03	Sat, 25 Feb 20	"80f1666df2f3	343140733658		text/css		200		966	
2	2	http://www.ht	21bb9306	Thu, 27 Oct 20	"80c8f237c94d	345239978444		text/css		200		2271	
3	3	http://www.ht	582c6b91	Thu, 23 Feb 20	"802fc8f44ff2	343176681252		text/css		200		40	
4	4	http://www.ht	c4e1e8c4	Fri, 18 May 20	"80dd2662983	341719104470		text/css		200		4007	
5	5	http://www.ht	920fe541	Wed, 18 Apr 2	"0e75797971d	342224947874		text/css		200		10602	
6	6	http://www.ht	ef9414a4	Fri, 06 Apr 20	"044dc6fbf13c	342441427494		application/x-j		200		5831	
7	7	http://www.ht	72903c9a	Fri, 15 Jun 20	"0462f2ca44a	341234306634		text/css		200		282498	
8	8	http://www.ht	a9838089	Sat, 02 Jun 20	"0acf0fb8e40c	341456030650		application/x-j		200		2805	
9	9	http://www.ht	1159c00c	Fri, 30 Mar 20	"804dc4c890e	342555387684		application/x-j		200		15650	
10	10	http://www.ht	4022de63	Fri, 04 May 20	"806bbaf7c82	341956824865		application/x-j		200		91668	
11	11	http://www.ht	64c5f0db	Sun, 01 Apr 20	"0b2f9173a10	342518854404		application/x-j		200		10905	
12	12	http://www.ht	4ee4d5a3	Fri, 30 Mar 20	"0e45cc990ec	342555387827		application/x-j		200		7859	
13	13	http://www.ht	bbaba111	Fri, 26 Aug 20	"0b1bb7c4864	346299938330		image/gif		200		813	
14	14	http://www.ad	73ab2ee2	Fri, 08 Jun 20	"3281a6-578f-	341340947907		application/jav		200		68446	
15	15	http://www.ht	09b84a41	Fri, 26 Aug 20	"0b1bb7c4864	346299938354		image/png		200		127	
16	16	http://www.ht	7e9a7527	Fri, 26 Aug 20	"0ec13854864	346299935577		image/png		200		2166	
17	17	http://www.ht	03b7bd4a	Fri, 26 Aug 20	"0ec13854864	346299935596		image/png		200		6982	
18	18	http://www.ht	7ffb61fa	Fri, 26 Aug 20	"01945864864	346299935216		image/png		200		6303	
19	19	http://www.ht	9147d77c	Fri, 26 Aug 20	"0ec13854864	346299935639		image/png		200		160	
20	20	http://www.ht	7b06cee8	Sun, 01 Apr 20	"805de3bb3a1	342518799863		image/png		200		3578	
21	21	http://www.ht	bf60d54c	Sun, 01 Apr 20	"80983bc43a1	342518797102		image/png		200		1029	
22	22	http://www.ht	3dbb1c30	Sun, 01 Apr 20	"094a1e23a10	342518786927		image/jpeg		200		3216	

Screenshot from the webviewCache.db

This work has been supported by the "Prevention of and Fight against Crime" Programme of the European Union.

Evaluation

The log files are not always very informative about Bluetooth and Wi-Fi usage details and they depend on the time of seizure, the phone's storage capacity and its usage before the seizure. However, Table's 1 contents contain precious data that can enhance an investigator's work according to the ACPO principles.

Contribution

Our research demonstrated that during the forensic examination of an Android smartphone an investigator is able to obtain information regarding the use of the Bluetooth technology and Wi-Fi networks. We indicated the files and folders the investigator should target and also presented a methodology for evidence acquisition focused around the use of the wireless facilities of the phone. Finally, we highlighted some security problems that occur by the exposure of the user's passwords in certain cases by the Android system.

Future work

- Confirm findings with Android's v3 & v4
- Investigate security problems (non encrypted passwords).

Annual Symposium 2012

IAAC Sponsors