DFRWS
DIGITAL FORENSIC RESEARCH CONFERENCE

Social Networking Applications on Mobile Devices

By

Noora Al Mutawa, Ibrahim Baggili and Andrew Marrington

Presented At

The Digital Forensic Research Conference

DFRWS 2012 USA Washington, DC (Aug 6th - 8th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org

Social Networking Applications on Mobile Devices

Noora Al Mutawa (MSc)

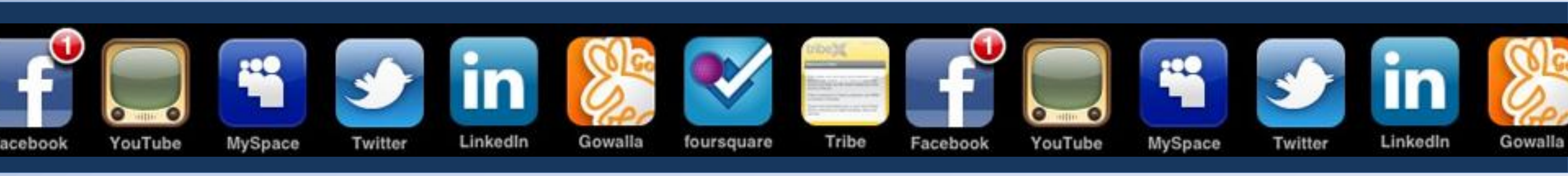
Ibrahim Baggili (PhD)

Andrew Marrington (PhD)

DFRWS 2012

Advanced Cyber Forensics Research Laboratory

Zayed University, College of Technology



Outline

- Problem Statement
- Goal of research
- Related Work
- Limitation
- Methodology
- Primary results
- Conclusion

Problem Statement

- The use of social networking applications on smartphones is on the rise.
- 91% of smartphone users go online to socialize (Smart Intent Index, 2010).
- Potential evidence could be held on these devices.
- Previous research has been limited to the recovery of very basic information related to the use of SN applications on smartphones.

Problem Statement

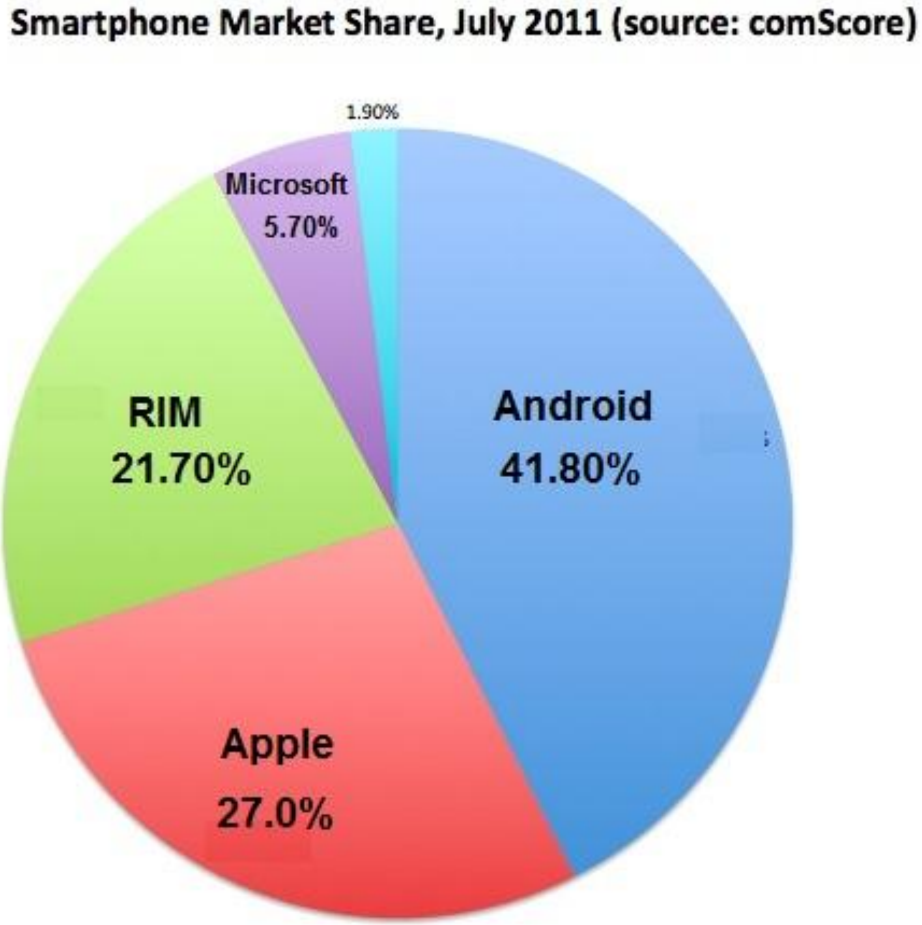


Figure 1. Most widely used smartphones.

Problem Statement

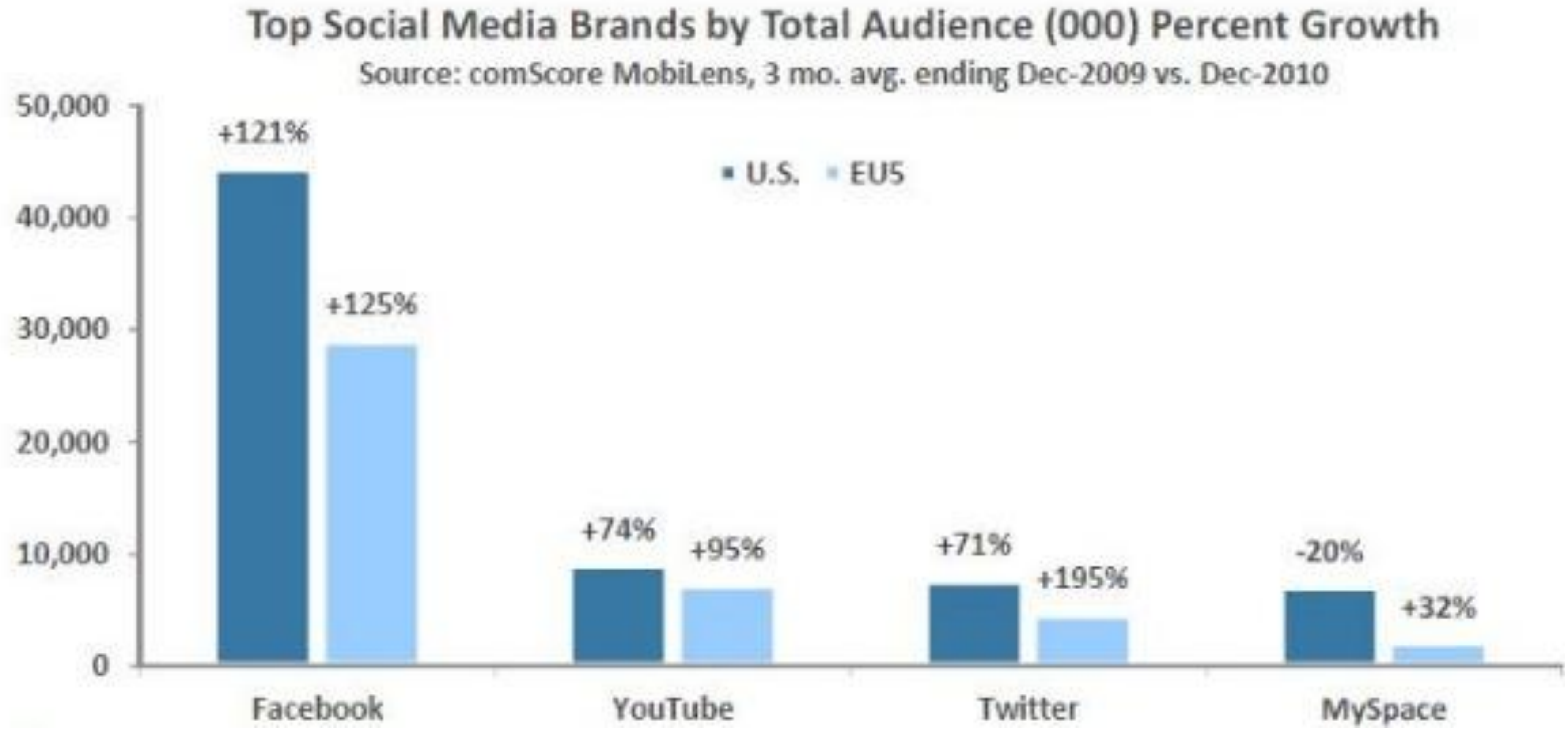


Figure 2. The rise in using SN applications on smartphones.

Problem Statement

This research focused on conducting forensic analysis on three widely used social networking applications on smartphones:

- **Facebook**
- **Twitter**
- **MySpace**

The tests were conducted on three popular smartphones:

- **BlackBerrys**
- **iPhones**
- **Android phones**

Goal of Research

Investigate whether activities performed through SN applications were stored on the smartphone's internal memory. If so, the amount, significance, and location of the data that could be found and retrieved from the logical image (backup) of each device were determined.

Goal of Research

- The results of this study can be of great assistance to smartphone forensic examiners in locating significant data in cases involving social networks.
- It can also provide the basis for creating digital forensics tools to extract and reconstruct social networking data from a variety of modern smartphones.

Related Work

- Burnette (2002) discussed the forensic examination of older versions of BlackBerrys and covered the hardware and software used for acquisition.
- Later research provided foundational concepts on forensic analyses of the new generations of smart phones (e.g., BlackBerry and iPhone) (Punja & Mislan, 2008).
- A forensic examination of iPhone 3GS's logical image showed that a database related to the Facebook application is stored on the phone's memory. The database stores data for each friend in the list, including their names, ID numbers, and phone number (Bader & Baggili, 2010).

Related Work

- A forensic examination of an Android's logical image showed that basic Facebook friend information is stored in the contacts database (contacts.db) (Lessard & Kessler, 2010).
- It also showed that the device stores Twitter passwords and Twitter updates performed through the Twitter application in plain text (Lessard & Kessler, 2010).
- Forensic research papers on BlackBerry phones and Windows smartphones, did not mention finding or recovering any data related to the use of social networking applications.

Limitation

- Logical backup and analysis.
- iPhone, BlackBerry and Android.
- Facebook, Twitter, Myspace.

Methodology

- Manual forensic examinations and analysis were performed on three commonly used social networking applications on three popular smartphones.
- The experiments were conducted using forensically sound approaches and under forensically acceptable conditions.
- The test and examination procedure was derived from the Computer Forensics Tool Testing program guidelines established by NIST to ensure the quality of the testing methods and the reliability and validity of the results.
- The research aimed to work with realistic data similar to that found in an actual investigation.

Methodology

Instruments:

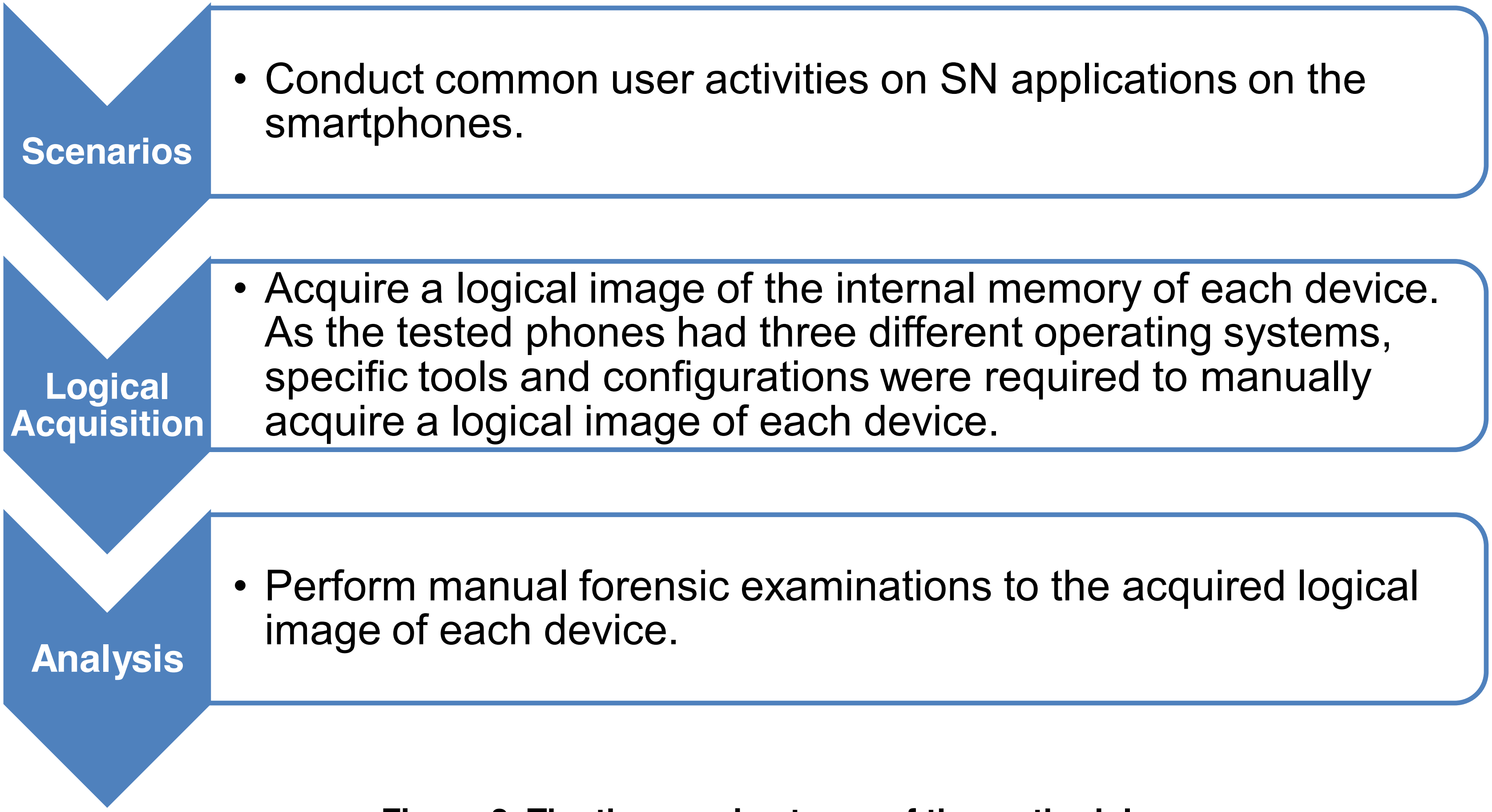
- Two Blackberry Torch 9800 phones (software version: 6.0 Bundle 862).
- Two iPhone 4 devices, 32GB (version 4.3.3 8J2).
- One Android phone (Samsung GT-i9000 Galaxy S - Firmware version 2.3.3).
- Facebook, Twitter, and MySpace applications for each tested phones.
- BlackBerry Desktop Software (version 6.1.0 B34).
- Apple iTunes Application (version 10.4.0.80).
- TextPad (version 4.5.2).
- Plist Editor for Windows (version 1.0.1).
- SQLite Database Browser (version 1.3).

Methodology

Instruments

- DCode (version 4.02a).
- EnCase (version 6.5).
- A software USB write-blocker (Thumbscrew).
- USB data cables.
- A Micro SD card.
- A Micro SD card reader
- Odin3 (version 1.3).
- MyBackup Rerware, LLC (version 2.7.7).

Methodology



Scenarios

- Conduct common user activities on SN applications on the smartphones.

Logical Acquisition

- Acquire a logical image of the internal memory of each device. As the tested phones had three different operating systems, specific tools and configurations were required to manually acquire a logical image of each device.

Analysis

- Perform manual forensic examinations to the acquired logical image of each device.

Figure 3. The three main stages of the methodology.

Scenarios

Application	Performed Activities	Comments
Facebook	Login with username: infected.mushroom2011@hotmail.com and password: mushroom77	
	Post in news feed	
	Upload photos + captions	
	Send email messages	
	Post on friend’s wall	
	Instant messaging (chat)	
	View profiles of friends	
Twitter	Login with username: infected.mushroom2011@hotmail.com and password: mushroom246	
	Follow people	
	Post tweets	
	Upload photos	
MySpace	Login with username: infected.mushroom2011@hotmail.com and password: mushroom888	
	Upload pictures	Did not function for Android
	Add friends	
	Change status	
	Check emails	
	Send emails	
	Post comments	
	View profiles	

Table 1. Activities performed on each application of each tested device

Logical Acquisition

Logical Acquisition

- **Blackberry**

1. Performed using BlackBerry Desktop Software.
2. A USB software write-blocker was utilized to preserve the integrity of the device's data and prevent any alteration or contamination to the original data stored on the device.
3. Automatic Synchronization was disabled.
4. The logical bit-by-bit image was created manually by performing a full backup of the device. An IPD file was created, and the default file location was *~\My Documents\BlackBerry\Backup*

Logical Acquisition

- iPhone

1. Performed using Apple iTunes application.
2. A USB software write-blocker could not be used.
3. Automatic Synchronization was disabled.
4. The logical bit-by-bit image was created manually by performing a full backup of the device. A backup directory was created and placed at: *C:\Users\[user]\AppData\Roaming\Apple Computer\MobileSync\Backup\[unique identifier]*

Logical Acquisition

- **Android**
  1. Device had to be rooted.
  2. Acquisition performed using MyBackup Rerware, LLC.
  3. Backup files (data files) were stored on an external Micro SD card.

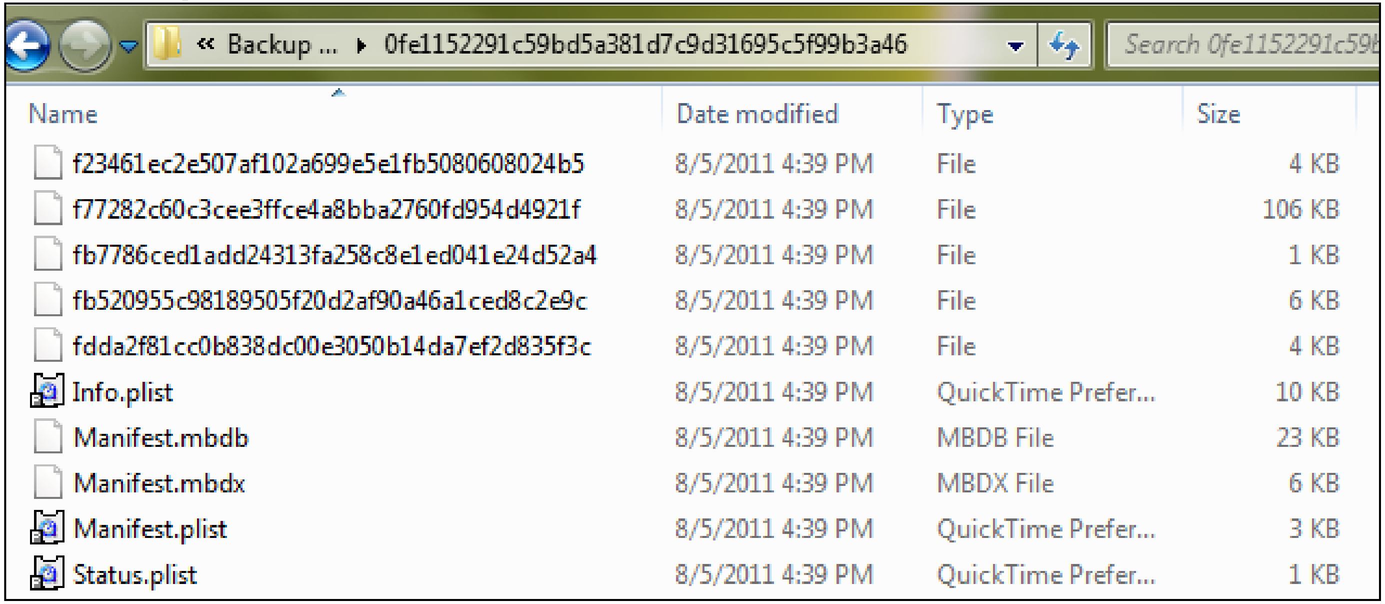
Examination and Analysis

Examination and Analysis - BlackBerry

- Acquisition resulted in the creation of a single proprietary IPD file.
- The file had a unique header “Inter@ctive Pager Backup/Restore File”.
- The file contained databases of user data and configurations.
- No traces of social networking activities performed during the test were found.

Examination and Analysis - iPhone

- Acquisition resulted in the creation of a folder with a unique alphanumeric name, which contained hundreds of backed up files.



« Backup ... ▸ 0fe1152291c59bd5a381d7c9d31695c5f99b3a46

Name	Date modified	Type	Size
f23461ec2e507af102a699e5e1fb5080608024b5	8/5/2011 4:39 PM	File	4 KB
f77282c60c3cee3ffce4a8bba2760fd954d4921f	8/5/2011 4:39 PM	File	106 KB
fb7786ced1add24313fa258c8e1ed041e24d52a4	8/5/2011 4:39 PM	File	1 KB
fb520955c98189505f20d2af90a46a1ced8c2e9c	8/5/2011 4:39 PM	File	6 KB
fdda2f81cc0b838dc00e3050b14da7ef2d835f3c	8/5/2011 4:39 PM	File	4 KB
Info.plist	8/5/2011 4:39 PM	QuickTime Prefer...	10 KB
Manifest.mbdb	8/5/2011 4:39 PM	MBDB File	23 KB
Manifest.mbdx	8/5/2011 4:39 PM	MBDX File	6 KB
Manifest.plist	8/5/2011 4:39 PM	QuickTime Prefer...	3 KB
Status.plist	8/5/2011 4:39 PM	QuickTime Prefer...	1 KB

Figure 4. iPhone backup files.

Examination and Analysis - iPhone

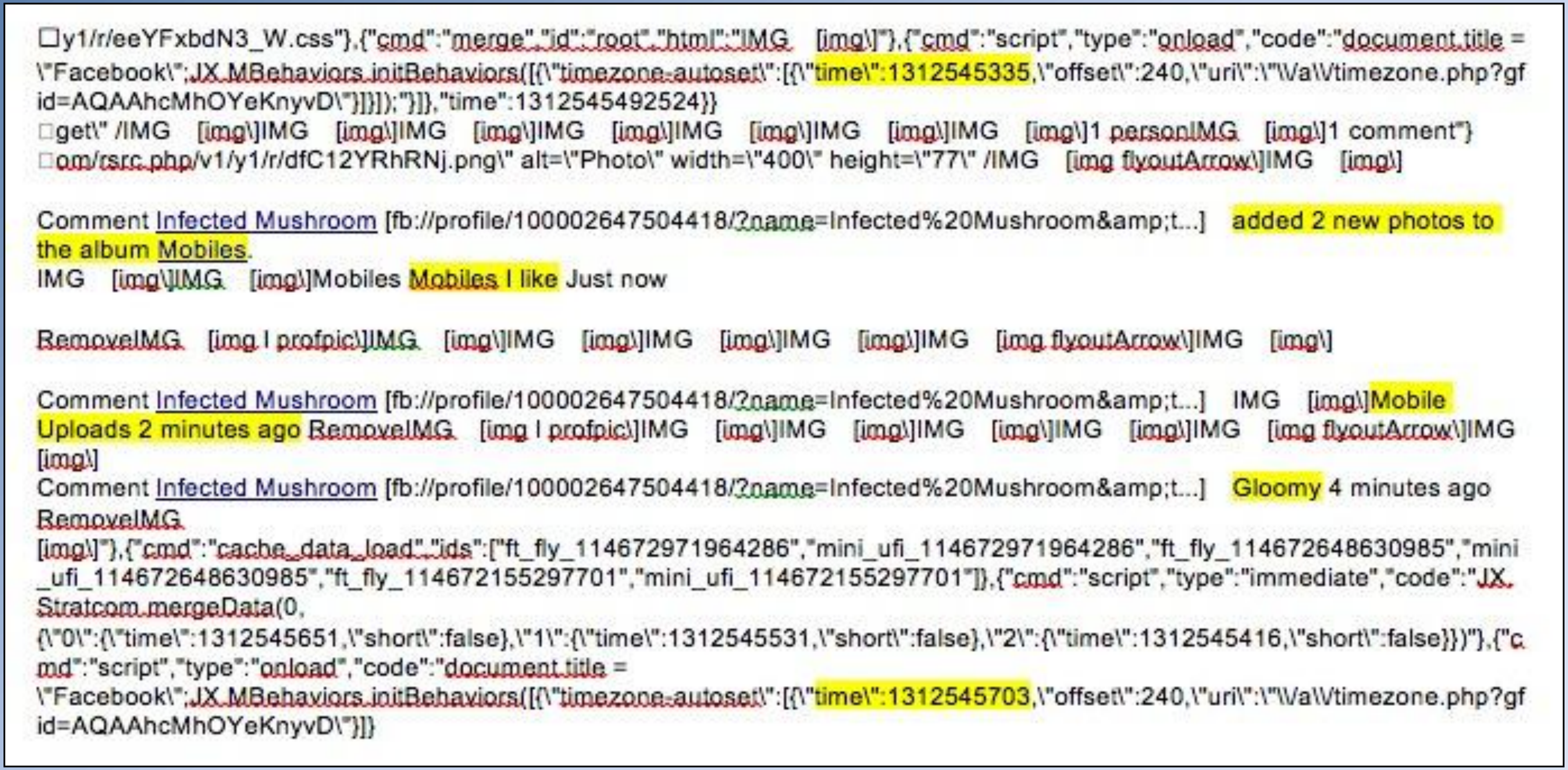
- Examining the backup files in a text editor showed that they are in binary format or plain text that may contain encapsulated images, SQLite database files, or other plist files.
- Files were viewed and examined according to their headers (e.g., “SQLite format 3”, “bplist00”).
- Tools used: Plist Editor for Windows, SQLite Database Browser, Text Editor, and EnCase.

Facebook Artifacts- iPhone

Type of evidence file	Location of evidence within the backup files	Type of evidence
SQLite Database	*6639cb6a02f32e020385 1f25465ffb89ca8ae3fa*	**Data of Facebook Friends:** Profile IDs First/Last names URL of profile pictures Phone numbers Email addresses
SQLite Database	*9f2140d8e87b45a9bb5d fc813fd2299c02851e6b*	**Traces of previous activities:** Uploading photos Posting comments User name Profile ID Nature of activity Timestamps (UNIX)
Plist	*384eb9e62ba50d7f3a21 d9224123db62879ef423*	**User details:** Last email used to login Profile ID User name URL of profile picture **Details of all users that have previously logged into FB.** **Details of friends with active chat session + Timestamps.**

Table 2. Facebook artifacts found in the iPhone logical backup files.

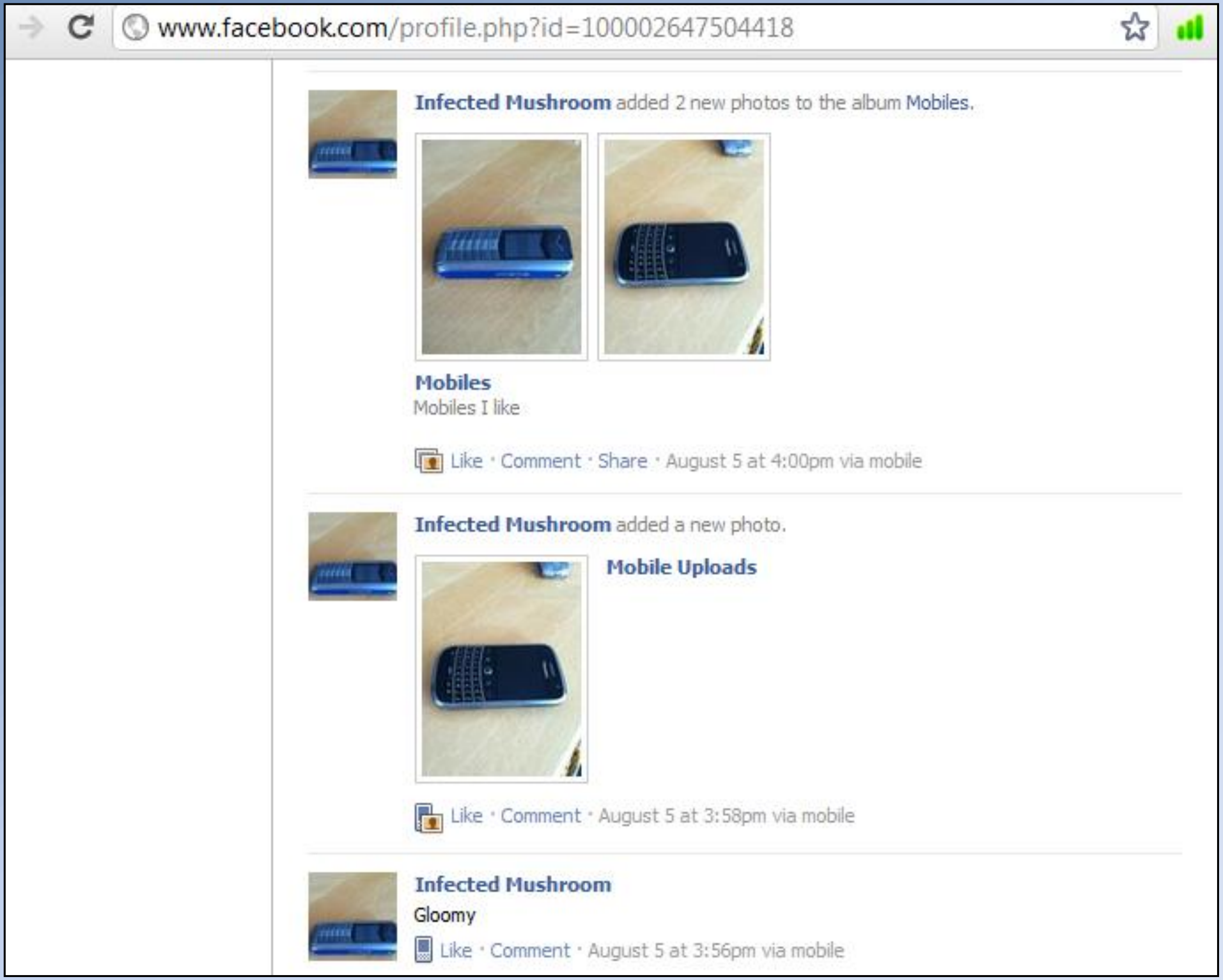
Facebook Artifacts- iPhone



```
□y1/r/eeYFxbdN3_W.css"},{"cmd":"merge","id":"root","html":"IMG   [img\]"},{"cmd":"script","type":"onload","code":"document.title =
\"Facebook\";JX.MBehaviors.initBehaviors([{\"timezone-autoset\":[{\"time\":1312545335,\"offset\":240,\"uri\":\"\/a\/timezone.php?gf
id=AQAAhcMhOYeKnyvD\"}]}]);"}]},"time":1312545492524}}
□get\" /IMG   [img\]IMG   [img\]IMG   [img\]IMG   [img\]IMG   [img\]IMG   [img\]IMG   [img\]1 personIMG   [img\]1 comment"}
□om/rsrc.php/v1/y1/r/dfC12YRhRNj.png\" alt=\"Photo\" width=\"400\" height=\"77\" /IMG   [img flyoutArrow\]IMG   [img\]

Comment Infected Mushroom [fb://profile/100002647504418/?name=Infected%20Mushroom&amp;t...]   added 2 new photos to
the album Mobiles.
IMG   [img\]IMG   [img\]Mobiles Mobiles I like Just now

RemoveIMG   [img I profpic\]IMG   [img\]IMG   [img\]IMG   [img\]IMG   [img\]IMG   [img flyoutArrow\]IMG   [img\]

Comment Infected Mushroom [fb://profile/100002647504418/?name=Infected%20Mushroom&amp;t...]   IMG   [img\]Mobile
Uploads 2 minutes ago RemoveIMG   [img I profpic\]IMG   [img\]IMG   [img\]IMG   [img\]IMG   [img\]IMG   [img flyoutArrow\]IMG
[img\]
Comment Infected Mushroom [fb://profile/100002647504418/?name=Infected%20Mushroom&amp;t...]   Gloomy 4 minutes ago
RemoveIMG
[img\]"},{"cmd":"cache_data_load","ids":["ft_fly_114672971964286","mini_ufi_114672971964286","ft_fly_114672648630985","mini
_ufi_114672648630985","ft_fly_114672155297701","mini_ufi_114672155297701"]},{"cmd":"script","type":"immediate","code":"JX.
Stratcom.mergeData(0,
{\"0\":{\"time\":1312545651,\"short\":false},\"1\":{\"time\":1312545531,\"short\":false},\"2\":{\"time\":1312545416,\"short\":false}})"},{"c
md":"script","type":"onload","code":"document.title =
\"Facebook\";JX.MBehaviors.initBehaviors([{\"timezone-autoset\":[{\"time\":1312545703,\"offset\":240,\"uri\":\"\/a\/timezone.php?gf
id=AQAAhcMhOYeKnyvD\"}]}
```

Figure 5. Traces of uploading photos and posting comments using the iPhone Facebook application.

Facebook Artifacts- iPhone



www.facebook.com/profile.php?id=100002647504418

Infected Mushroom added 2 new photos to the album Mobiles.

Mobiles
Mobiles I like

Like · Comment · Share · August 5 at 4:00pm via mobile

Infected Mushroom added a new photo.

Mobile Uploads

Like · Comment · August 5 at 3:58pm via mobile

Infected Mushroom
Gloomy
Like · Comment · August 5 at 3:56pm via mobile

Figure 6. The actual photos and comments as presented on the Facebook website.

Twitter Artifacts- iPhone

Type of evidence file	Location of evidence within the backup files	Type of evidence
Plist	*eb8899d553cf56308 0453f9a366600de1d cf6286*	**User information:** User name URL of profile picture Tweets posted by the user Timestamps (absolute time value)
Plist	*f77282c60c3cee3ffce 4a8bba2760fd954d4 921f*	**User information** **Data of people followed by the user:** Usernames Details from their profile pages URL of profile pictures Posted tweets Timestamps

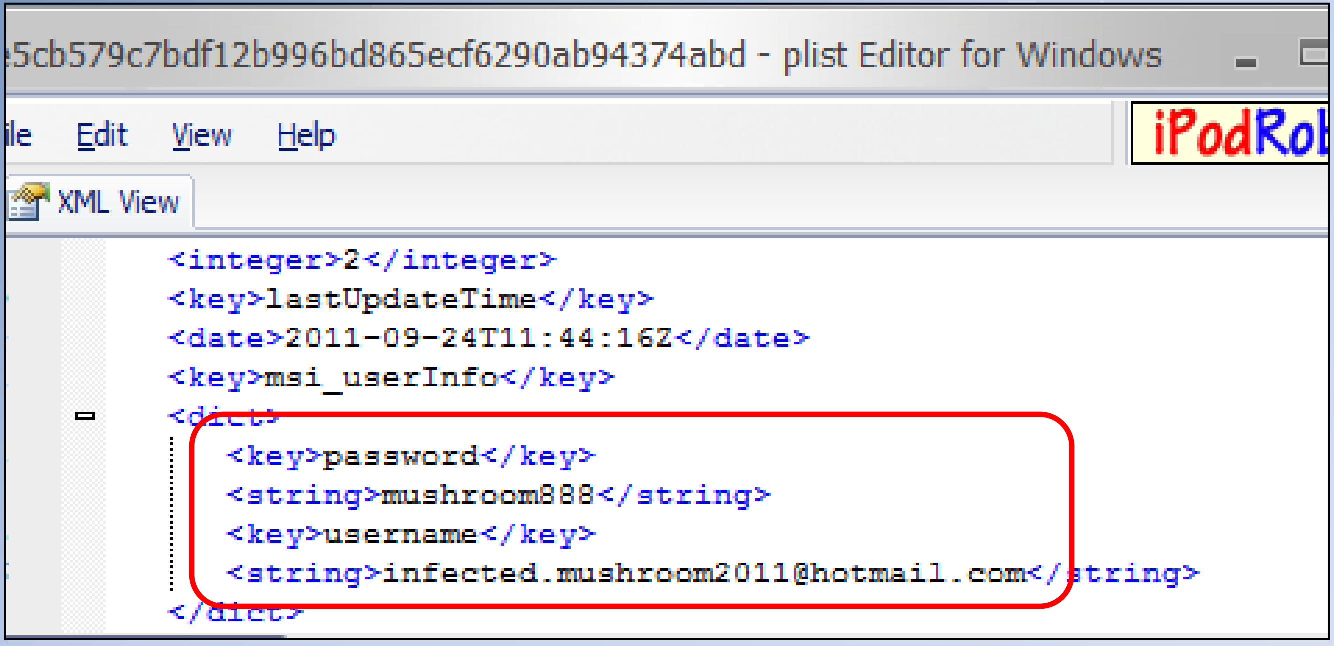
Table 3. Twitter artifacts found in the iPhone logical backup files.

MySpace Artifacts- iPhone

Type of evidence file	Location of evidence within the backup files	Type of evidence
SQLite Database	*48598f280bb577d1e68aaddadccba35c54acbb48*	**User information:** User name Posted comments Timestamps (absolute time value)
Plist	*e5cb579c7bdf12b996bd865ecf6290ab94374abd*	**User information:** Username + password (in clear text)

Table 4. MySpace artifacts found in the iPhone logical backup files.

MySpace Artifacts- iPhone

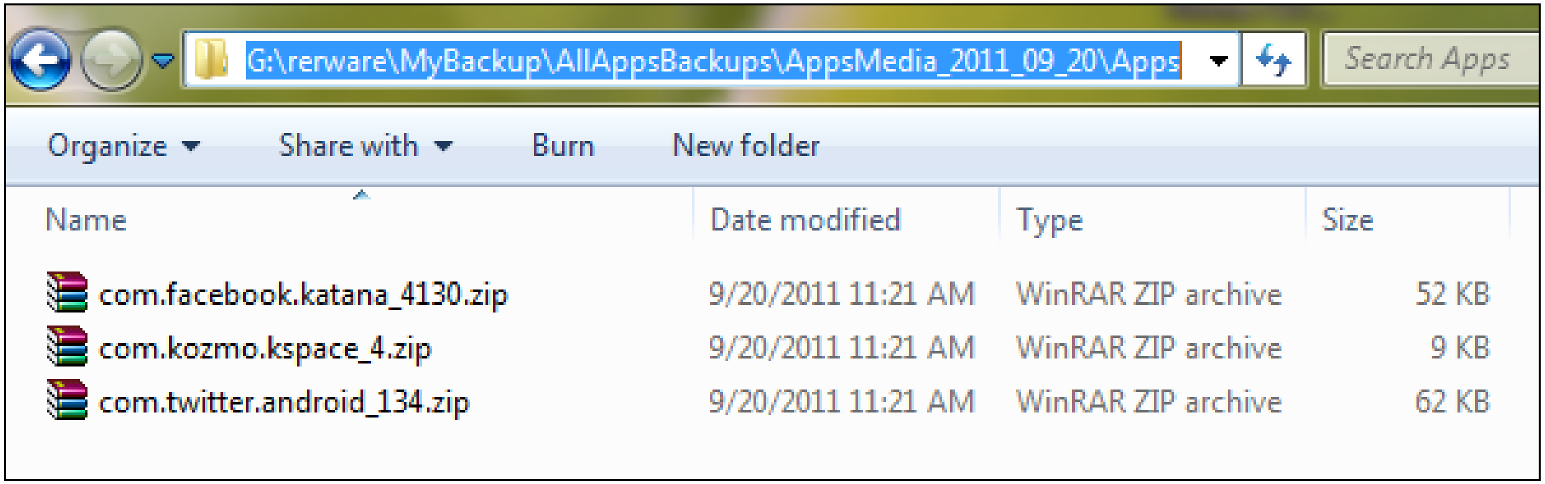

5cb579c7bdf12b996bd865ecf6290ab94374abd - plist Editor for Windows
ile
Edit
View
Help
iPodRob
XML View

```
<integer>2</integer>
<key>lastUpdateTime</key>
<date>2011-09-24T11:44:16Z</date>
<key>msi_userInfo</key>
<dict>
   <key>password</key>
   <string>mushroom888</string>
   <key>username</key>
   <string>infected.mushroom2011@hotmail.com</string>
</dict>
```

Figure 7. MySpace username and password.

Examination and Analysis - Android

- Acquisition resulted in the creation of a folder with three archive files, one for each SN application.



G:\rerware\MyBackup\AllAppsBackups\AppsMedia_2011_09_20\Apps

Name	Date modified	Type	Size
com.facebook.katana_4130.zip	9/20/2011 11:21 AM	WinRAR ZIP archive	52 KB
com.kozmo.kspace_4.zip	9/20/2011 11:21 AM	WinRAR ZIP archive	9 KB
com.twitter.android_134.zip	9/20/2011 11:21 AM	WinRAR ZIP archive	62 KB

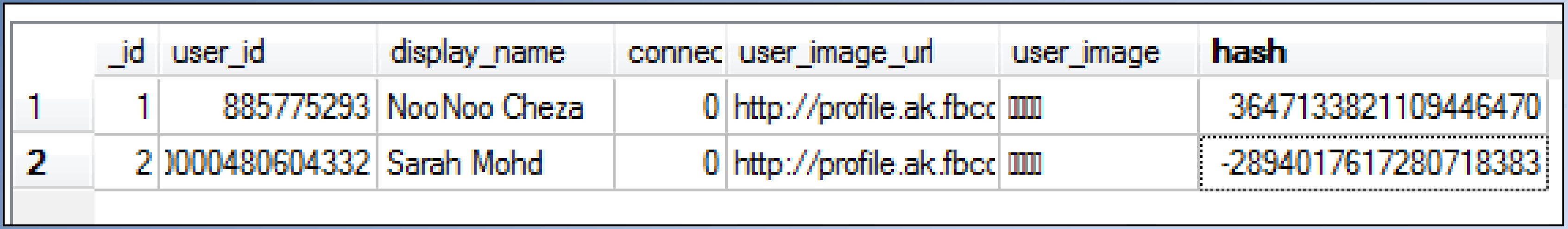
Figure 8. Android backup files.

Facebook Artifacts- Android

Type of evidence file	Location of evidence within the backup files	Type of evidence
SQLite Database	*fb.db*	**Tables that held records of:** Created albums Chat messages Friends Friends data Mailbox messages Uploaded photos
Image Files	*files* folder	Pictures that the user had viewed within the FB Android application Uploaded pictures

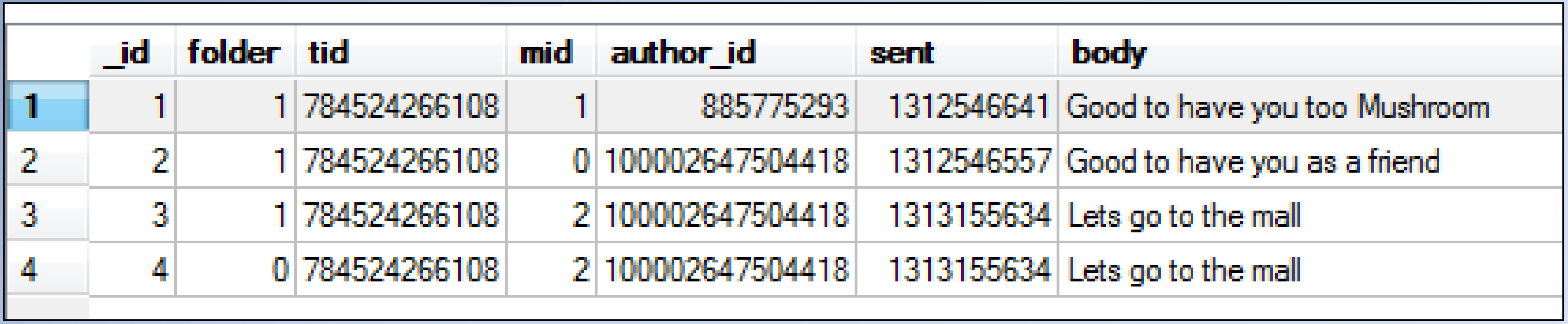
Table 5. Facebook artifacts found in the Android logical backup files.

Facebook Artifacts- Android



	_id	user_id	display_name	connec	user_image_url	user_image	hash
1	1	885775293	NooNoo Cheza	0	http://profile.ak.fbcc	□□□□	3647133821109446470
2	2	)000480604332	Sarah Mohd	0	http://profile.ak.fbcc	□□□□	-2894017617280718383

Figure 9. Records of Facebook friends.



	_id	folder	tid	mid	author_id	sent	body
1	1	1	784524266108	1	885775293	1312546641	Good to have you too Mushroom
2	2	1	784524266108	0	100002647504418	1312546557	Good to have you as a friend
3	3	1	784524266108	2	100002647504418	1313155634	Lets go to the mall
4	4	0	784524266108	2	100002647504418	1313155634	Lets go to the mall

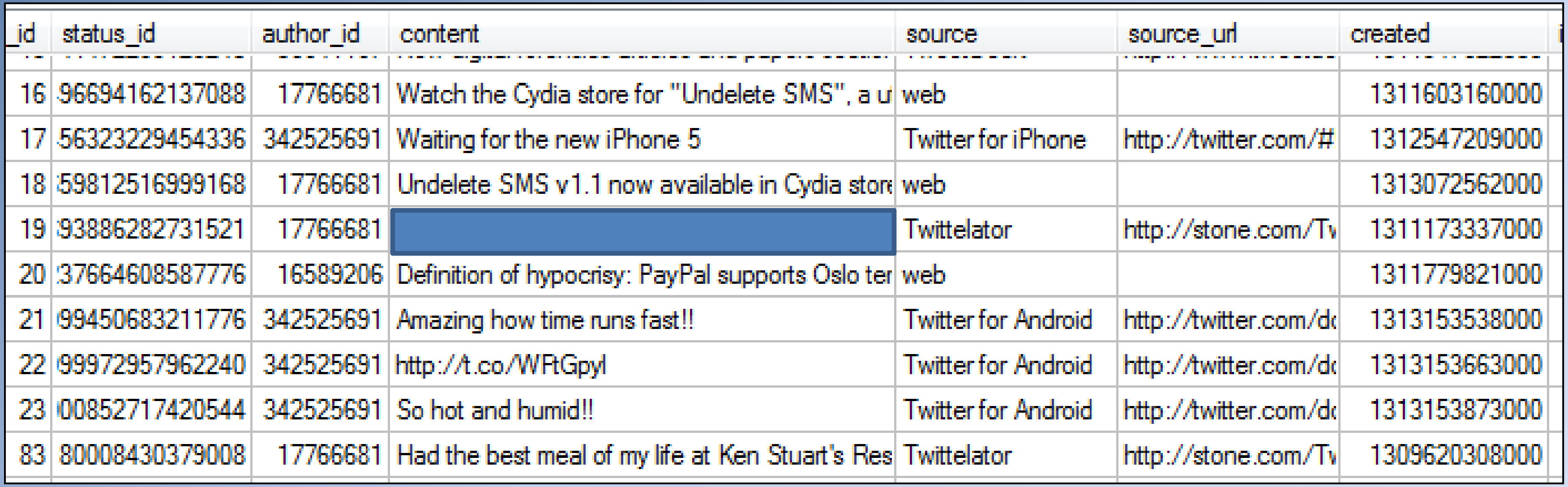
Figure 10. Records of Facebook mailbox messages.

Twitter Artifacts- Android

Type of evidence file	Location of evidence within the backup files	Type of evidence
SQLite Database	*342525691.db*	**Tables that held records of:** Posted tweets Photos Friends Users Other activities

Table 6. Twitter artifacts found in the Android logical backup files.

Twitter Artifacts- Android



_id	status_id	author_id	content	source	source_url	created
16	96694162137088	17766681	Watch the Cydia store for "Undelete SMS", a u	web		1311603160000
17	56323229454336	342525691	Waiting for the new iPhone 5	Twitter for iPhone	http://twitter.com/#	1312547209000
18	59812516999168	17766681	Undelete SMS v1.1 now available in Cydia store	web		1313072562000
19	93886282731521	17766681		Twittelator	http://stone.com/Tv	1311173337000
20	37664608587776	16589206	Definition of hypocrisy: PayPal supports Oslo ter	web		1311779821000
21	99450683211776	342525691	Amazing how time runs fast!!	Twitter for Android	http://twitter.com/dc	1313153538000
22	99972957962240	342525691	http://t.co/WRtGpyl	Twitter for Android	http://twitter.com/dc	1313153663000
23	00852717420544	342525691	So hot and humid!!	Twitter for Android	http://twitter.com/dc	1313153873000
83	80008430379008	17766681	Had the best meal of my life at Ken Stuart's Res	Twittelator	http://stone.com/Tv	1309620308000

Figure 11. Records of posted tweets.

MySpace Artifacts- Android

Type of evidence file	Location of evidence within the backup files	Type of evidence
SQLite Database	*webview.db*	**Username + password of MySpace user.**
SQLite Database	*webviewCache.db*	**Cookies + cache files**

Table 7. MySpace artifacts found in the Android logical backup files.

Twitter Artifacts- Android

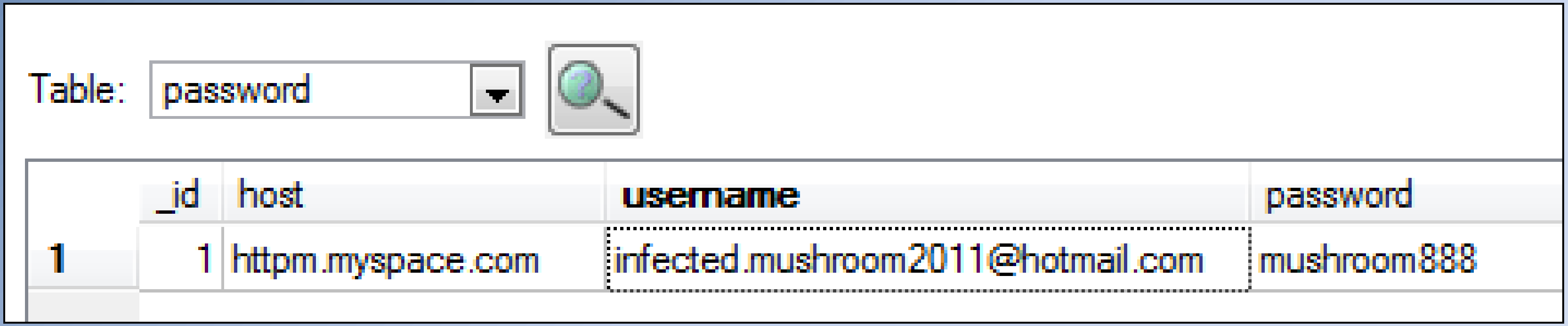


Table: password

	_id	host	username	password
1	1	httpm.myspace.com	infected.mushroom2011@hotmail.com	mushroom888

Figure 12. MySpace username and password stored in the *webview.db* file.

Conclusion and Future Work

- Recovered artifacts and traces related to the use of social networking applications on a variety of smartphones using different operating systems.
  - Logical Acquistion
  - The tested social networking applications were Facebook, Twitter, and MySpace, which were used on BlackBerrys, iPhones, and Androids.
- The forensic analysis determined the:
  - Amount
  - Significance
  - Location

Conclusion and Future Work

- No traces of social networking activities could be recovered from BlackBerrys.
- iPhones and Android phones stored a significant amount of valuable data that could be recovered and used by the forensic investigator.
- Results should help examiners/practioners
- Study provides the basis for creating digital forensics tools to extract and reconstruct social networking data from a variety of modern smartphones.

References

Al Mutawa, N., Al Awadhi, I., Baggili, I., & Marrington, A. (2011). *Forensic artifacts of Facebook's instant messaging service*. Unpublished manuscript submitted for publication.

Al--Zarouni, M. (2006). Smart handset forensic evidence: a challenge for law enforcement. *Edith Cowan University*. Retrieved May 31, 2011, from citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.85.4441&rep=rep1&type=pdf

Bader, M., & Baggili, I. (2010, September). iPhone 3GS forensics: logical analysis using apple itunes backup utility. *Small scale digital device forensics journal*. Retrieved June 2, 2011, from www.ssddfj.org/papers/SSDDFJ_V4_1_Bader_Bagilli.pdf

Burnette, M. (2002). Forensic examination of a rim (blackberry) wireless device. Retrieved June 2, 2011, from http://www.mandarino70.it/Documents/Blackberry%20Forensics.pdf

Dellutri, F., Ottaviani, V., & Me, G. (n.d.). MIAT-WM5: Forensic acquisition for windows smart pocketpc. *European council for modelling and simulation*. Retrieved June 3, 2011, from http://www.scs-europe.net/conf/ecms2008/ecms2008%20CD/hpcs2008%20pdf/hpcs08w1-5.pdf

General Test Methodology for Computer Forensic Tools. (2001). National Institute of Standards and Technology.

International Telecommunication Union. (2010). Measuring the information society 2010. *ITU*. Retrieved May 28, 2011, from http://www.itu.int/ITU-D/ict/publications/idi/2010/index.html

Kubasiak, R., Morrissey, S., & Varsalone, J. (2009). Forensic acquisition of an iPhone. *Macintosh OS X, iPod, and iPhone forensic analysis DVD toolkit* (pp. 357-390). Burlington, MA: Syngress.

Lessard, J., & Kessler, G. (2010, September). Android forensics: simplifying cell phone examination. *Small scale digital device forensics journal*. Retrieved June 2, 2011, from http://www.ssddfj.org/papers/SSDDFJ_V4_1_Lessard_Kessler.pdf

Lynch, J., & Ellickson, J. (2010, March 3). Obtaining and using evidence from social networking sites. Retrieved June 11, 2011, from www.eff.org/files/filenode/social_network/20100303__crim_socialnetworkin.pdf

Morrissey, S. (2010). *iOS forensic analysis for iPhone, iPad, and iPod touch* . New York: Apress.

References

New study shows 'intent' behind smart internet use. (2010). *PR Newswire*. Retrieved May 28, 2011, from http://www.prnewswire.com/news-releases/new-study-shows-intent-behind-smart-internet-use-84016487.html

NIST. (2010, October). Test results for smart device acquisition tool: Zdziarski's method. *iPhone Insecurity*. Retrieved June 2, 2011, from http://www.iphoneinsecurity.com/JZ_Method_Test_Results_jz_draft.pdf

Paula, A. (2009). Security aspects and future trends of social networks. *ICoFCS 2009*, (p. 12). Natal City, Brazil. Retrieved May 22, 2011, from http://www.icofcs.org/2009/ICoFCS2009-PP09.pdf

Punja, S., & Mislan, R. (2008). Smart device analysis. *Small scale digital device forensics*, *2*(1). Retrieved June 2, 2011, from http://www.ssddfj.org/papers/SSDDFJ_V2_1_Punja_Mislan.pdf

Saliba, J. (n.d.). Internet evidence finder v4. *JADsoftware Inc.*. Retrieved June 10, 2011, from http://www.jadsoftware.com/go/?page_id=141

Schroader, A., & Cohen, T. (2007). PDA, blackberry, and iPod forensic analysis. *Alternate data storage forensics* (pp. 120-124). Rockland, Mass.: Syngress.

Sofer, N. (n.d.). MyLastSearch v1.50. *NirSoft*. Retrieved June 10, 2011, from http://www.nirsoft.net/utils/my_last_search.html

The rise of social networking. (2010, August 24). *Information Policy*. Retrieved May 28, 2011, from http://www.i-policy.org/2010/08/the-rise-of-social-networking.html

Zdziarski Method FAQ. (2010, April 28). *iPhone insecurity*. Retrieved June 2, 2011, from http://www.iphoneinsecurity.com

Zellers, F. (2008). MySpace.com forensic artifacts keyword searches. *Inland Direct*. Retrieved June 10, 2011, from www.inlanddirect.com/CEIC-2008.pdf

Questions?
Thank You

baggili@gmail.com