



Forensic acquisition and analysis of palm webOS on mobile devices

Eoghan Casey*, Adrien Cheval, Jong Yeon Lee, David Oxley, Yong Jun Song

The Johns Hopkins University Information Security Institute, 216 Maryland Hall, Baltimore, MD 21218, USA

ARTICLE INFO

Article history:

Received 23 October 2010

Received in revised form

24 February 2011

Accepted 27 April 2011

Keywords:

Mobile device forensics

Palm forensics

webOS forensics

ABSTRACT

The emergence of webOS on Palm devices has created new challenges and opportunities for digital investigators. With the purchase of Palm by Hewlett Packard, there are plans to use webOS on an increasing number and variety of computer systems. These devices can store substantial amounts of information relevant to an investigation, including digital photographs, videos, call logs, SMS/MMS messages, e-mail, remnants of Web browsing and much more. Although some files can be obtained from such devices with relative ease, the majority of information of forensic interest is stored in databases on a system partition that many mobile forensic tools do not acquire. This paper provides a methodology for acquiring and examining forensic duplicates of user and system partitions from a device running webOS. The primary sources of digital evidence on these devices are covered with illustrative examples. In addition, the recovery of deleted items from various areas on webOS devices is discussed.

© 2011 Elsevier Ltd. All rights reserved.

1. Introduction

The newest operating system created by Palm, called webOS, presents challenges and opportunities for digital investigators. The operating system is Linux-based and uses Java, Ruby, and various Web technologies to provide functionality common to mobile devices. This system is currently included on the Palm Pre (Plus) and Pixi (Plus) devices. In addition to SMS/MMS and Instant Messaging, webOS can be used to access e-mail via POP3 and IMAP, Microsoft Exchange, and Web-based e-mail such as Yahoo! Mail, Gmail™, AOL, and Hotmail. In fact, certain applications on a Palm webOS device, such as the address book and calendar, are designed to automatically synchronize with online data sources. As such, these devices are tightly bound to cloud services and must be treated as networked devices.

With the purchase of Palm by Hewlett Packard in April 2010, the webOS platform will become more widely used

on mobile devices, tablet computers, and “web-aware” appliances.

The primary test device used for this work was webOS 1.4.1.1 on the Dual Band 3G CDMA “Palm Pre Plus” cell phone. This device did not have a SIM card or removable memory card. This device has built in GPS, supports Wi-Fi 802.11 b/g, and has a 3 mega pixel camera with multiple audio/video formats.

This paper begins with an overview of webOS internals, and covers various methods for acquiring data from Palm Pre (Plus) and Pixi (Plus) devices via a data cable. It is a generally accepted practice in mobile device forensics to interact with the device while acquiring data, but the goal is to make minimum changes necessary in order to acquire the most data possible. Within this context, the limitations and strengths of each acquisition method is discussed, providing illustrative examples using widely used forensic tools. The remainder of this paper covers the forensic examination of data on the system partition of webOS, including the recovery of deleted communications. A

* Corresponding author.

E-mail addresses: eoghan@jhu.edu (E. Casey), acheval1@jhu.edu (A. Cheval), jlee361@jhu.edu (J.Y. Lee), doxley4@jhu.edu (D. Oxley), ysong23AT@jhu.edu (Y.J. Song).

1742-2876/\$ – see front matter © 2011 Elsevier Ltd. All rights reserved.

doi:[10.1016/j.diin.2011.04.003](https://doi.org/10.1016/j.diin.2011.04.003)

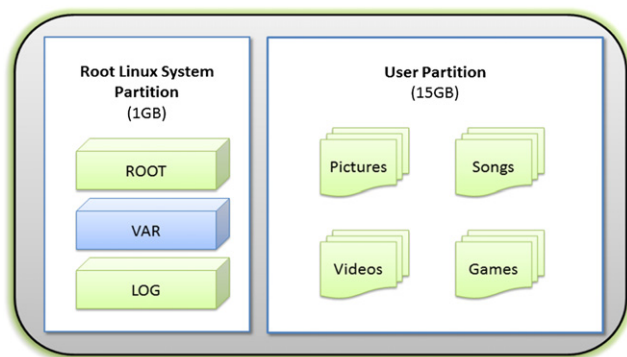


Fig. 1 – Two partitions on webOS devices.

detailed case example is provided to demonstrate the usefulness of these techniques in a real-world context.

2. webOS internals

A mobile device running webOS such as the Palm Pre Plus has a user partition and system partition as depicted in Fig. 1. The user partition generally contains multimedia and games, and is relatively simple in structure. The system partition is more complicated in structure and is protected from general user access. On this partition, there are databases that contain data relating to user activities on the mobile device,

including text messages, e-mail messages, and Web browsing activities.

Much of the useful information on the system partition is stored in SQLite databases. SQLite is a lightweight SQL database implementation that is becoming more widely used on other mobile devices platforms including Android and iPhone, as well as by applications such as Firefox and Skype. On webOS, these databases have a “.db3” file extension and can be analyzed using any SQLite viewer (examples in this paper use SQLiteSpy v1.8.12).

3. Acquisition

The user partition on a webOS device contains a FAT32 file system and is relatively easy to acquire using traditional file system forensic tools. The device simply needs to be connected to a forensic acquisition system via a USB write blocker, and it is mounted by the system as a USB drive. This partition can be examined using a file system forensic tool such as FTK as shown in Fig. 2.

The system partition on a webOS device contains a Linux (ext3) file system and is more difficult to access in order to acquire a forensic duplicate, and first requires the device to be put in developer mode. Putting a Palm device into developer or debug mode has no known side effects from a forensic standpoint and has become a common practice for acquiring forensic images of Palm devices.

The following steps were used to put the test device in developer mode:

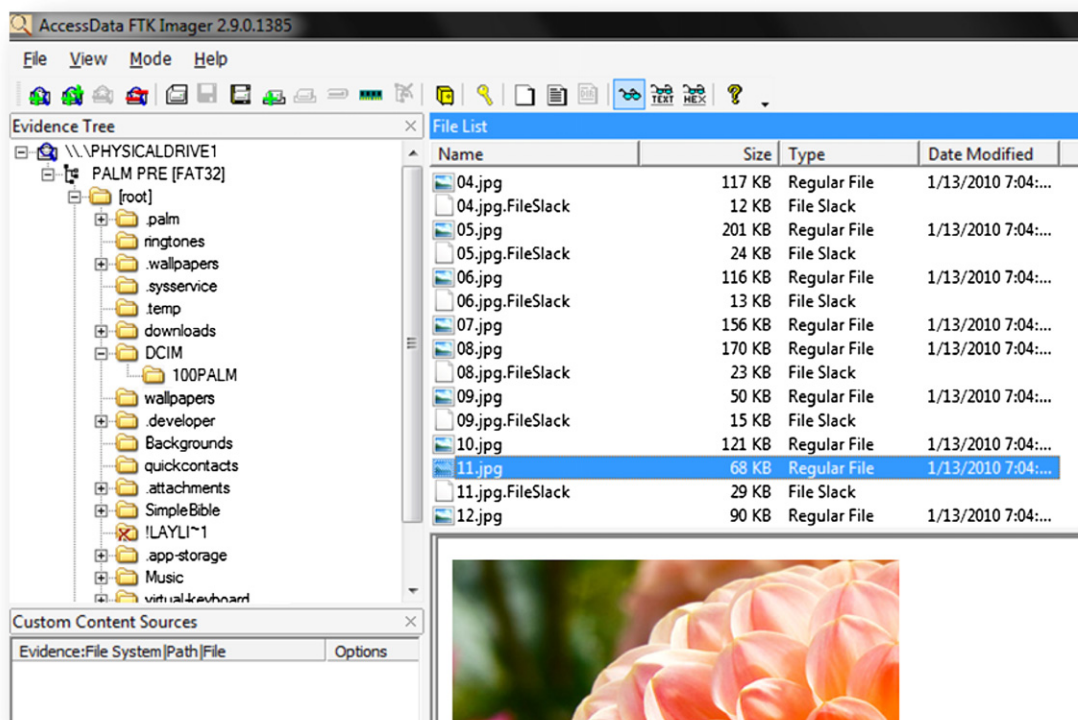


Fig. 2 – User Space Viewed with FTK Imager.

1. Slide open the device keyboard
2. Type-in “webos20090606” (without quotes)
3. Tap “Developer Mode Enabler”
4. Toggle “Developer Mode” to “On”
5. When prompted, allow the device to restart

There are other approaches to enabling developer mode on some webOS devices, such as typing “upupdownnlefttrightlefttrighbastart” in the Card view or Launch application. Once a device is in developer mode, data on the system partition can be accessed, even when the device that is secured using a user lock code.

In order to obtain a forensic duplicate of the system partition, one can use a Palm-supplied program called Novacom. Included as part of the Palm webOS SDK, Novacom communicates between the host OS and the underlying Linux operating system on the Palm mobile device. Novacom can be used to GET a file from the device and save it to the host OS, PUT a file from the host OS onto the device, or RUN a Linux command on the device locally with the command’s output returned to the host OS. One part of the Novacom package, novaterm, also allows one to get terminal access to the device. Both Novacom and novaterm can be used to retrieve a forensic duplicate of the three main components of the system partition:/(root),/var, and/log.

Once in developer mode, the most forensically-sound method of acquiring data from the system partition is the following:

1. Connect the phone with a computer through a USB cable.
2. Choose “Just Charge” on the phone.
3. Open a terminal in the computer.
4. Execute three commands.
 - a. novacom get file:///dev/mapper/store-log>log.dd
 - b. novacom get file:///dev/mapper/store-var>var.dd
 - c. novacom get file:///dev/mapper/store-root>root.dd

The above commands result in raw image files of the areas of the system partition that contain files and SQLite databases with user-related data such as text messages, call logs, calendar items and Web browsing artifacts. Using the Novacom GET function does not alter the contents of the partition being acquired. To confirm this, forensic analysts can verify that no files on the system were altered during the time the image was being acquired.

Alternative methods for getting these three images exist. However, they are less ideal than the previous method due to their propensity for making more changes to the device’s local file system, either by storing the forensic images on the User partition or by having acquisition commands logged by the underlying Linux operating system.

3.1. Alternative method 1: DD using novaterm to the user partition (ONLY after the user partition has already been imaged!)

1. (Steps 1–3 of the Preferred Method still apply)
2. Execute the command “novaterm”
3. In the resulting novaterm terminal, execute the following commands:

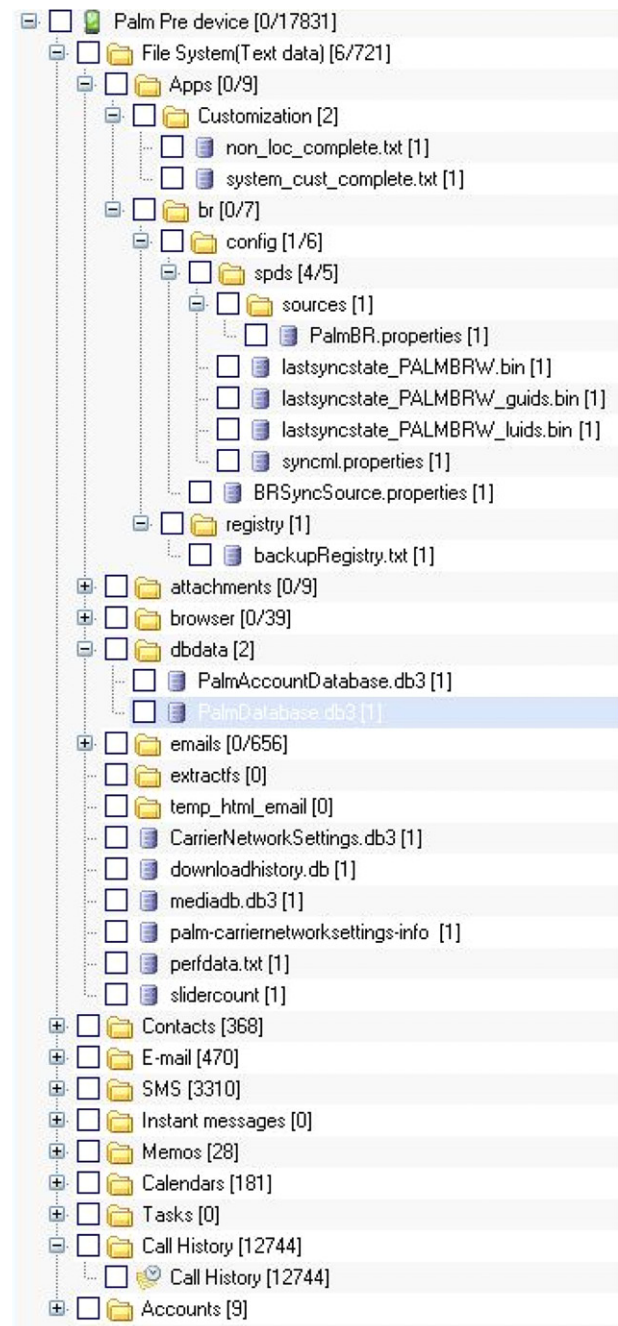


Fig. 3 – Data acquired from a Palm Pre device using Paraben.

- a. /bin/dd if=/dev/mapper/store-log of=/dev/mapper/store-media/log.dd
- b. /bin/dd if=/dev/mapper/store-var of=/dev/mapper/store-media/var.dd
- c. /bin/dd if=/dev/mapper/store-root of=/dev/mapper/store-media/root.dd

4. Disconnect the phone
5. Attach a USB write blocker to the USB connection
6. Reconnect it, and select “USB Mode”
7. Copy the files from the device to the host OS

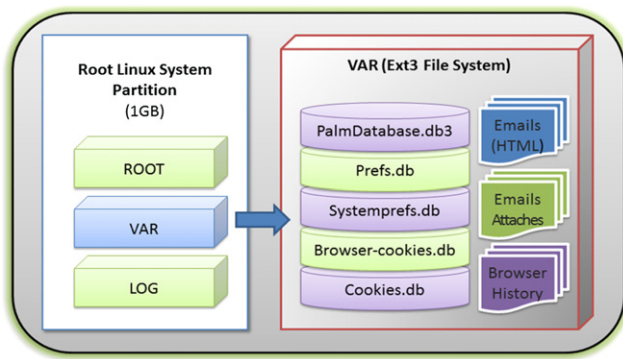


Fig. 4 – Files on the system partition.

3.2. Alternative method 2: DD using novacom to the host OS

1. With the “novacom run” command, we can execute dd or cat to store the raw images of the system partition into the computer.
2. (Steps 1–3 of the Preferred Method still apply)
3. Execute the following commands:
 - a. novacom run “file://bin/dd if=/dev/mapper/store-log”>log.dd
 - b. novacom run “file://bin/dd if=/dev/mapper/store-var”>var.dd
 - c. novacom run “file://bin/dd if=/dev/mapper/store-root”>root.dd
4. You now have three raw image files of the system partition.

In addition, Paraben’s Device Seizure tool can acquire data from the system partition on a webOS device that is in developer mode as shown in Fig. 3. In addition to extracting specific items such as SMS and call logs, Device Seizure acquires certain files from the system partition, including SQLite databases that may contain some of the additional information described in this paper. However, Device Seizure does not interpret the SQLite database format, making it necessary to export these files and perform a forensic examination using other tools as detailed in this

paper. Furthermore, Device Seizure does not acquire the full contents the system partition on a webOS device and, therefore, does not preserve deleted data in unallocated areas of the system partition. The acquisition method detailed above using Novacom acquires a forensic duplicate of the full system partition, including unallocated space.

4. Forensic examination of webOS

The system partition on webOS stores a number of files that contain data of potential forensic relevance, including text messages, e-mail and Web browsing history. The databases and files within/var that contain the majority of user-related data on the system partition are depicted in Fig. 4.

5. Overview of files and databases

A summary of files and databases on the system partition (all within/var/) are provided in Table 1.

Log files common on Linux systems can also be found on devices running webOS, and may provide useful information relating to the use of the device. For example, the wpa_supplicant.log file shows information about wireless access points that the device connected to, but no times are included.

The database of greatest forensic relevance is named PalmDatabase.db3 and is located at: /var/luna/data/dbdata/PalmDatabase.db3.

This database has more than 60 tables as shown in Fig. 5, including Accounts, Contacts, Calendar Events, Memos, Tasks, and SMS Messages.

Some of the most useful tables on a webOS within the system partition are summarized below with examples of their structure and the data they contain.

6. Online accounts

As shown in Fig. 6, the com_palm_accounts_Accounts table in PalmDatabase.db3 contains details about online user accounts, including the default Smart Folders and Palm

Table 1 – Files and databases of interest on webOS system partition.

Location (within/var/)	Description of contents
/luna/data/dbdata/PalmDatabase.db3	Main database containing details about user activities and device configuration
/preferences/com.palm.bluetooth/prefsDB.sl	The MAC address of the most recently paired device
/luna/data/emails/	HTML-formatted e-mails
/luna/data/attachments/	E-mail attachments
/luna/preferences/localtime	Time zone configured on the device
/luna/preferences/systemprefs.db	System preferences, including wallpaper/ringtone, time zone, language, search providers, etc.
/luna/files	Profile photos of contacts
/palm/data/browser-cookies.db	Browser cookies without date-time stamps
/palm/data/cookies.db	Cookies that are used by applications
/luna/data/dbdata/PalmDatabaseAccount.db	Links applications, including the browser, with the database files in which are stored their settings, histories, logs, etc.
/palm/file_usr.palm.applications.com.palm.app.browser_0/	Both the browser history (with date-time stamps) and the browser’s bookmarks

Name	Type	NN	PK	Default Value
Tables (68)				
+ _ChangeTracking				
+ _Class				
+ _ClassObject				
+ _ClassSequence				
+ _ClassTree				
+ _Master				
+ _Signature				
+ _SyncService				
+ _SyncServiceStatus				
+ com_palm_accounts_Account				
+ com_palm_accounts_Account_com_palm_accounts_AccountTypeService				
+ com_palm_accounts_Account_sync_delete				
+ com_palm_accounts_AccountType				
+ com_palm_accounts_AccountType_sync_delete				
+ com_palm_accounts_AccountTypeService				
+ com_palm_accounts_AccountTypeService_sync_delete				
+ com_palm_accounts_ActiveRecordFolder				
+ com_palm_accounts_ActiveRecordFolder_sync_delete				
+ com_palm_accounts_Credentials				
+ com_palm_accounts_Credentials_sync_delete				
+ com_palm_backup_data_BackupFileMetaDataDetails				
+ com_palm_backup_data_BackupSyncSourceSettings				
+ com_palm_backup_util_BackupConfig				
+ com_palm_calendar_CalendarPrefs				
+ com_palm_calendar_CalendarPrefs_sync_delete				
+ com_palm_luna_scheduler_Job				
+ com_palm_luna_scheduler_Job_sync_delete				
+ com_palm_mail_EmailAccountDefinition				
+ com_palm_mail_EmailAccountDefinition_sync_delete				
+ com_palm_mail_EmailHost				
+ com_palm_mail_EmailHost_sync_delete				
+ com_palm_mediaevents_service_MediaCarrierSettings				
+ com_palm_messaging_data_ChatThread				

Fig. 5 – Some of the 68 tables in PalmDatabase.db3.

com_palm_accounts_Account					
name	hiddenFromAccountsApp	accountDomain	isLoggedIn	username	authToken
Google	0	gmail	1	@_	GoogleLogin auth=...
	1	msgingAcct	0		
Google Talk	0	gmail	1	@_	
Palm Profile	1	local	0	JHU ISI	
Smart Folders	1	emailSmartFolders	0		
Gmail	0	gmail	1	@_	
Gmail	1	gmail	0	@_	

Fig. 6 – com_palm_accounts_Accounts Table.



login	password	accountDomain	uniqueLogin	appId
webosacf@gmail.com	qbXPjKSmQqR44yA=	local	webosacf@gmail.com*gmail*defaultAppId	defaultAppId
webosacf@gmail.com	qbXPjKSmQqR44yA=	gmail	webosacf@gmail.com*gmail*defaultAppId	defaultAppId

Fig. 7 – com_palm_accounts_Credentials Table.

Profile, and accounts created by the user of the mobile device, such as Gmail and Google Talk.

The com_palm_accounts_Credentials table contains the e-mail addresses and their corresponding hashed passwords created by the device user as shown in Fig. 7.

With proper authorization, the user accounts in this table can be used to obtain additional information from the service providers that run the servers for these accounts. For instance, the Gmail account referenced in the table shown in Fig. 7 may contain e-mail messages, documents, and other information that is not stored on the webOS device itself.

7. Text and multimedia messages

SMS and MMS messages are among the most commonly sought after evidence on mobile devices. In addition to retaining remnants of such messages, webOS devices may have a record of other forms of chat such as Google Talk. The com_palm_messaging_data_ChatThread table in PalmDatabase.db3 is shown in Fig. 8 with a summary of actual chat messages in the first column. This table also includes the first name, last name, chat address, phone number, and e-mail address of the recipient (sanitized in Fig. 8 to protect individual privacy). The dates in this table are stored in UNIX string format as can be seen in the “chatTimeS-tamp” field in Fig. 8.

Another table, named com_palm_messagingrouter_MessageFromTilBase, may contain information relating to SMS messages, including the message body, sender address, call back number and date-time stamp of the message.

Multimedia messages are more challenging to recover from webOS, partly because of their multiple components and partly because of the way they are handled by the operating system. The sender’s phone number for an MMS message is

stored in the chat address column of the com_palm_messaging_data_ChatThread table.

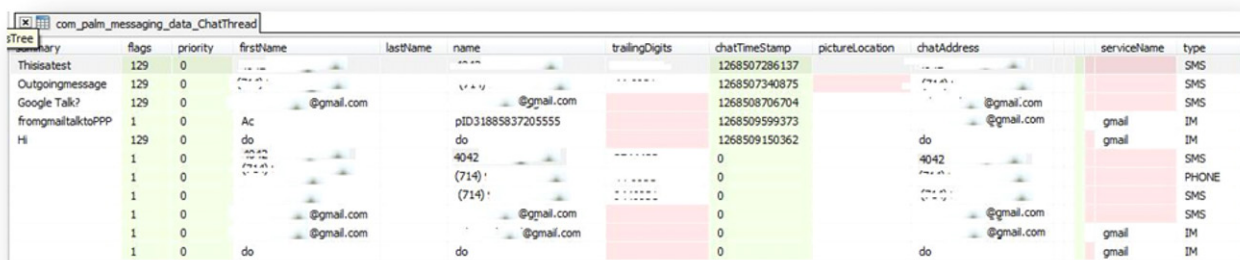
The text portion of an MMS is stored within the PalmDatabase.db3, in the partText field of the com_part_pim_Part table as shown in Fig. 9. After an MMS message is deleted, the text portion is no longer viewable using SQLite tools but the text remains in the database file until the space is reused. Therefore, the text portion of deleted MMS message may be recoverable by examining the PalmDatabase.db3 file using a hexadecimal viewer.

All attachments to MMS messages are stored on the User partition in subfolders under/media/internal/.attachments/mms/and the filename is the same as the original filename the multimedia attachment was assigned on the originating system. The specific directory for each MMS message is stored in the uniqueAttachmentFolderName column of the FolderEntry table in PalmDatabase.db3, and the full path for each attachment is stored in the URI column of the com_part_pim_Part table as shown in Fig. 9 above. Attachments to incoming MMS messages are accompanied by a Synchronized Multimedia Integration Language (SMIL) header file that is named based on the phone that sent the message.

8. Folder entry

The com_palm_pim_FolderEntry table contains information pertaining to Instant messages (IM), SMS and e-mails. The previewText field stores a certain amount of characters of the e-mail contents, and the Summary field in this table contains the e-mail subject. IM and SMS messages are stored in their entirety in the messageText field, as shown in Fig. 10.

Most of this information can be found in other tables, particularly ChatThread. FolderEntry is useful to an



flags	priority	firstName	lastName	name	trailingDigits	chatTimeStamp	pictureLocation	chatAddress	serviceName	type
129	0					1268507286137				SMS
129	0					1268507340875				SMS
129	0					1268508706704				SMS
1	0	Ac		pID31885837205555		1268509599373		@gmail.com	gmail	IM
129	0	do		do		1268509150362		@gmail.com	gmail	IM
1	0			4042		0		4042		SMS
1	0			(714)		0				PHONE
1	0			(714)		0				SMS
1	0	@gmail.com		@gmail.com		0		@gmail.com		SMS
1	0	@gmail.com		@gmail.com		0		@gmail.com	gmail	IM
1	0	do		do		0		do	gmail	IM

Fig. 8 – com_palm_messaging_data_ChatThread Table.

com_palm_pim_Part							
location	mimeType	displayName	size	uri	cont...	pa...	partText
AAAA	application/smil	AAAA	361	/media/internal/.attachments/mms/12874326670049855/AAAA	<AAA...	0	
1018101603.jpg	image/jpeg	1018101603.jpg	77991	/media/internal/.attachments/mms/12874326670049855/1018101603.jpg	<101...	1	
No Name951.txt	text/plain		36		<No ...	2	thisisaevidencephonefindtextmessages

Fig. 9 – MMS details in the com_part_pim_Part Table.

com_palm_pim_FolderEntry										
mmsResponseText	timeStamp	summary	messageText	flags	priority	displayName	firstName	lastName	remoteId	extraDetails
	1268507449037	Access Gmail on your mobile phone		5	0	Gmail Team				
	1268507449147	Import your contacts and old email		5	0	Gmail Team				
	1268507449342	Customize Gmail with colors and themes		5	0	Gmail Team				
	1268507807144	Incomingemail		5	0					
	1268507723458	Emailout		5	0					
	1268428146000		Test message	5	0					
	1268507289237		Thisisatest	133	0					
	1268507344120		Outgoingmessage	133	0					
	1268508710804		Google Talk?	133	0					
	1268509248580		YOYOYO	133	0					
	1268509599372		fromgmailtoPPP	5	0					
	1268509150362		Hi	4194437	0					

com_palm_pim_FolderEntry													
status	statusErrorcode	deviceTimeStamp	messageType	messageServiceName	callbackNumber	fromAddress	invitationGroupId	smsClass	smsType	smc	encoding	validity	isvoicemail
		1268507556033											
		1268507559144											
		1268507559339											
		1268508388140											
		1268509294455											
0	0	1268428160343	SMS					2	0			0	0
0	0	1268507286137	SMS					0	0			0	0
0	0	1268507340875	SMS					0	0			0	0
0	0	1268508706704	SMS					0	0			0	0
0	0	1268509248009	IM	gmail				0	0			0	0
0	0	1268509599373	IM	gmail				0	0			0	0
3	0	1268509150362	IM	gmail				0	0			0	0

Fig. 10 – com_palm_pim_FolderEntry Table.

investigator for several reasons. First and foremost, it is the only table that contains actual text from e-mail messages stored on the device, both the full subject and a preview of the message body text. In addition, it allows for verifying the contents of the other tables in regards to SMS and IM messaging.

9. Call logs

The com_palm_superlog_Superlog table contains data about calls (incoming, outgoing, missed) as well as telephone number and display name. All calls that were sent or received by device are stored in this table as shown in Fig. 11

This table provides digital investigators with a list of people with whom the device user may have communicated during the time of interest.

10. Contacts

Information about contacts on webOS is stored in several tables. The com_palm_pim_Contact and com_palm_pim_ContactPoint tables function as the primary address book, and

the com_palm_pim_Person table has much of the same information. Specifically, as shown in Fig. 12a, the com_palm_pim_Contact table stores the first name, middle name, last name, company name, job title, department name, and all other important information that can be stored in a contact field (e.g., picture, birthday, etc). For each entry in the contact database, the com_palm_pim_ContactPoint table shown in Fig. 12b contains details such as e-mail addresses and phone numbers.

Fig. 13 shows the com_palm_pim_Person table. The people listed in the contacts databases may be useful to digital investigators in establishing the identity of the owner of the device or relationships between people of interest.

Palm mobile devices running webOS sync data with online accounts. The com_palm_pimsync_data_SyncStatus table contains the e-mail account name created by the user as shown in Fig. 14.

11. Calendar events

The calendar on webOS is comprised of two tables: com_palm_pim_CalendarEvent and com_palm_CalendarEventAttendee. The com_palm_pim_CalendarEvent table stores the

com_palm_superlog_Superlog											
contactId	displayName	number	type	startTime	duration	pictureLoc	label	id	_class_id	_mod_num	_flags
-1	*22899	*22899	outgoing	12678083...	14488	no	-1	89060441849857	81	2208	
-1	*22899	*22899	outgoing	12678083...	11531	no	-1	89060441849858	81	2210	
-1	*22899	*22899	outgoing	12682534...	58650	no	-1	89060441849859	81	2712	
-1			incoming	12684281...	4608	no	-1	89060441849860	81	2935	
-1	VoiceMail		outgoing	12684316...	997		-1	89060441849861	81	3059	
-1			missed	12684425...	0	no	-1	89060441849862	81	3201	
-1			missed	12684426...	0	no	-1	89060441849863	81	3203	
-1	VoiceMail		outgoing	12684485...	49214		-1	89060441849864	81	3221	
-1			outgoing	12685071...	22519	no	-1	89060441849865	81	3345	
-1			outgoing	12685073...	4406	no	-1	89060441849866	81	3368	
31885837205557			outgoing	12685874...	5934		Mobile	89060441849867	81	8125	
31885837205552	#411	#411	outgoing	12686041...	5530	/var/jun...	Work	89060441849868	81	9333	

Fig. 11 – com_palm_superlog_Superlog Table showing all calls to and from the device.

a

com_palm_pim_Contact											
displayName	firstName	middleName	lastName	nickName	prefix	suffix	companyName	jobTitle	depthName	pictureLoc	
			VoiceMail							/var/juna/files/VOICEMAIL1268253403699.jpg	
			#BAL							/var/juna/files/BAL1268253403989.jpg	
			#MIN							/var/juna/files/MIN1268253405356.jpg	
			#PMT							/var/juna/files/PMT1268253405682.jpg	
			#DATA							/var/juna/files/DATA1268253405805.jpg	
			#411							/var/juna/files/4111268253405908.jpg	
			Verizon Wireless Accessories							/var/juna/files/VERIZONWIRELESSACCESSOR...	
			Technical Support							/var/juna/files/PALMTECHNICALSUPPORT126...	
Palm											
Ac											
Do											
Georgio			Armani				Armani	Designer			

b

com_palm_pim_ContactPoint											
gIMName	type	isVIPField	label	value	trailingDigits	serviceName	com_palm_pim_Contact_contactPts_id	id	_class_id	_mod_num	
IM	0	0		@gmail.com	@gmail.com	gmail	97856534872115	27487790694444	25	8137	
IM	0	0		@gmail.com	@gmail.com	gmail	97856534872116	27487790694445	25	3917	
IM	0	0		@gmail.com	@gmail.com	gmail	30786325577781	28587302322223	26	8133	
PHONE	0	1	#86	#86			29686813949995	86861418594341	79	2652	
PHONE	0	1	#225	#225			29686813949996	86861418594342	79	2660	
PHONE	0	1	#646	#646			29686813949997	86861418594343	79	2668	
PHONE	0	1	#768	#768			29686813949998	86861418594344	79	2676	
PHONE	0	1	#3282	#3282			29686813949999	86861418594345	79	2684	
PHONE	0	1	#411	#411			29686813950000	86861418594346	79	2692	
PHONE	0	1					29686813950001	86861418594347	79	2700	
PHONE	0	3					97856534872119	86861418594354	79	8087	
EMAIL	0	0		@gmail.com			30786325577781	98956046499886	90	3975	
EMAIL	0	0		@msn.com			97856534872119	98956046499891	90	8088	

com_palm_pim_ContactPoint											
displayName	isInvitationAddress	accountTag	contactServerID	availability	customMessage	activity	isIMAddress	imAddrHasMatchingIMName	type	isVIPField	
				4			0	0	IM	0	
				6			0	0	IM	0	
	0	defaultAppId*gmail*webosa...	0	4			1	1	IM	0	
									PHONE	0	
									PHONE	0	
									PHONE	0	
									PHONE	0	
									PHONE	0	
									PHONE	0	
									PHONE	0	
									PHONE	0	
									PHONE	0	
									EMAIL	0	
									EMAIL	0	

Fig. 12 – a): palm_pim_Contact Table. b): com_palm_pim_ContactPoint Table.

prefix	firstName	middleName	lastName	nickname	suffix	companyName	pictureLoc	pictureLocSquare	pictureLocBig	ringtoneLoc
			Voicemail				/var/juna/files/VOICEMAIL1268253403699.jpg	/var/juna/files/...	/var/juna/files/...	
			#BAL				/var/juna/files/BAL1268253403989.jpg	/var/juna/files/...	/var/juna/files/...	
			#MIN				/var/juna/files/MIN1268253405356.jpg	/var/juna/files/...	/var/juna/files/...	
			#PMT				/var/juna/files/PMT1268253405682.jpg	/var/juna/files/...	/var/juna/files/...	
			#DATA				/var/juna/files/DATA1268253405805.jpg	/var/juna/files/...	/var/juna/files/...	
			#411				/var/juna/files/4111268253405908.jpg	/var/juna/files/...	/var/juna/files/...	
			Verizon Wireless Accessories				/var/juna/files/VERIZONWIRELESSACCESSORIES...	/var/juna/files/...	/var/juna/files/...	
			Technical Support				/var/juna/files/PALMTECHNICALSUPPORT126825...	/var/juna/files/...	/var/juna/files/...	
Palm										
Ac										
Do										
Georgio			Armani			Armani				

Fig. 13 – com_palm_pim_Person Table.

domain	username	syncInProgress	taskId	isInitialSync	id	_class_id	_mod_num	_flags
gmail	webosacf@gmail.com	0	81363860455855	0	94557999988737	86	9331	

Fig. 14 – com_palm_pimsync_data_SyncStatus Table showing the online account(s) used to sync the device's data.

start and end date-time stamps, subject, location and time zone (e.g., America/New York) for each event. The com_palm_CalendarEventAttendee table stores the event organizer, names of attendees, associated e-mail address. Fig. 15 provides an example entry in the com_palm_pim_CalendarEvent table with date-time stamps stored in UNIX string format.

An entry in the calendar can be useful in a digital investigation to show that a meeting was scheduled to occur between individuals of interest, or that the victim or suspect planned specific activities around the time of the offense.

12. Memos and tasks

The com_palm_pim_Memo table contains memo title and text, along with created/modified date-time stamps as shown in Fig. 16.

timeZoneId	floating	startTimestamp	endTimestamp	originalTimestamp	allDay	rule	endValidity	com_palm_accounts_ActiveRecordFolder_id	subject	location	note
America/New_York	0	1268600400000	1268604000000	0	0		0	40681930227720	Neweventone	555 briardiff ct.	
America/New_York	0	1271174400000	1271178000000	0	0		0	40681930227720	Randomeventone		

Fig. 15 – com_palm_pim_CalendarEvent Table.

createdTimeStamp	modifiedTimeSt...	text	title	color	position	font	backupID	id	_class_id	_mod_num	_flags
0	0	Testmemo	Testmemo	green	m	16	1718864877926	10005558127...	91	4094	

Fig. 16 – com_palm_pim_Memo Table.

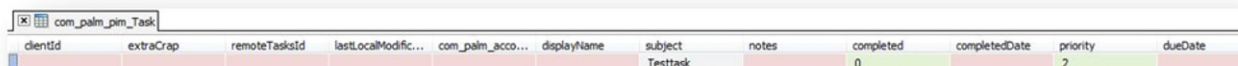
Information about Tasks are stored in two tables on webOS: com_palm_pim_Task and com_palm_pim_TaskList as shown in Fig. 17. The com_palm_pim_Task table contains the subject, notes, and completed date associated with a task. The com_palm_pim_TaskList table just contains the name of a task.

13. Instant message (IM) groups

The com_palm_messaging_data_IMGroup table stores instant message buddy groups as shown in Fig. 18.

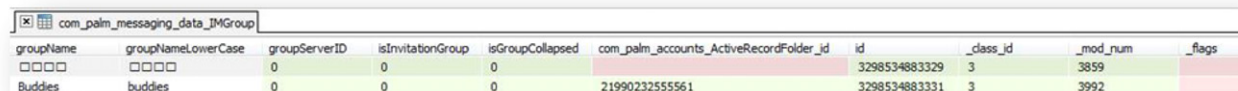
14. Web browsing

Accessing online resources leaves a variety of traces on webOS, including Web browsing history, bookmarks and cookies. The



clientId	extraCrap	remoteTaskId	lastLocalModif...	com_palm_acco...	displayName	subject	notes	completed	completedDate	priority	dueDate
						Testtask		0		2	

Fig. 17 – com_palm_pim_Task Table.



groupName	groupNameLowerCase	groupServerID	isInvitationGroup	isGroupCollapsed	com_palm_accounts_ActiveRecordFolder_id	id	_class_id	_mod_num	_flags
□□□□	□□□□	0	0	0		3298534883329	3	3859	
Buddies	buddies	0	0	0	21990232555561	3298534883331	3	3992	

Fig. 18 – com_palm_messaging_data_IMGroup Table.

most details about Web browsing the history are stored in `/var/palm/file_usr.palm.applications.com.palm.app.browser_0` as shown in Fig. 19.

Bookmarks are stored in the same database within the Bookmarks table. Cookies relating to Web browsing are stored in separate database files, named `Cookies.db` and `Browser_Cookies.db`, in the `/var/palm/data` directory.

15. E-mail messages and attachments

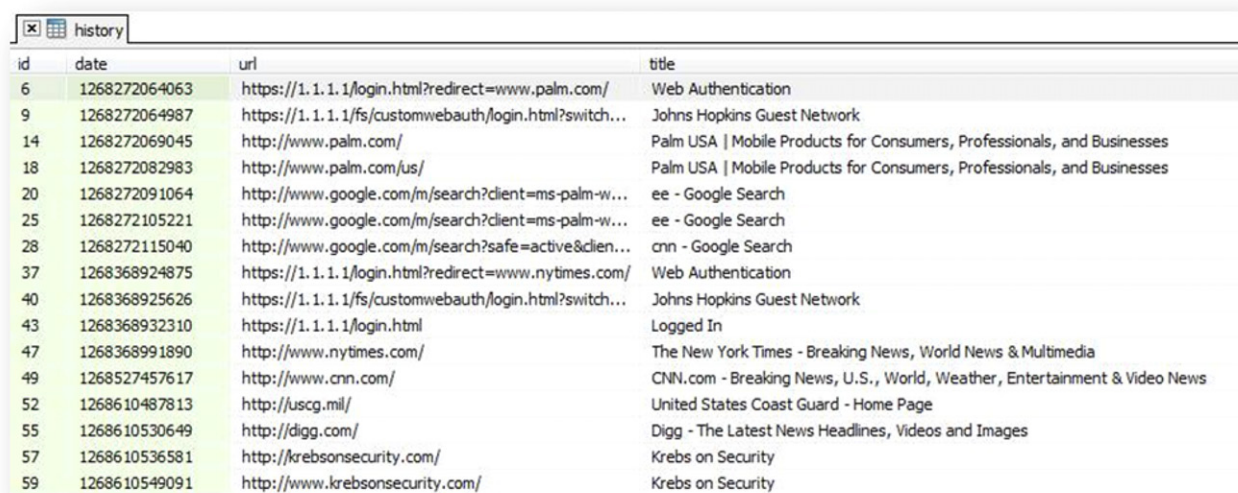
E-mails in HTML format and their attachments are stored outside of the PalmDatabase structure within the `/var/luna/data/emails/` and `/var/luna/data/attachments/directories/`, respectively. When a message is received, it is saved in HTML format regardless of whether it is opened. Attachments, however, are only saved when they are opened by the recipient. When an e-mail is deleted, evidence of it may remain:

- in the `/var/luna/data/emails/temp_html_e-mail` folder, which holds temporary copies of e-mails, even after deletion, for an undetermined period of time
- in the `PalmDatabase.db3` file, both within the database's tables for a short period (specifically within the `FolderEntry` table), and within the SQLite database structure even after the entries have been removed
- in recoverable space in the system partition

Attachment filenames may also be evident in the database file and the entire attachment may be recoverable from the file system as well.

16. Recovery of deleted data

Deleted data can be recovered from both the User and system partitions of a webOS device.



id	date	url	title
6	1268272064063	https://1.1.1.1/login.html?redirect=www.palm.com/	Web Authentication
9	1268272064987	https://1.1.1.1/fs/customwebauth/login.html?switch...	Johns Hopkins Guest Network
14	1268272069045	http://www.palm.com/	Palm USA Mobile Products for Consumers, Professionals, and Businesses
18	1268272082983	http://www.palm.com/us/	Palm USA Mobile Products for Consumers, Professionals, and Businesses
20	1268272091064	http://www.google.com/m/search?client=ms-palm-w...	ee - Google Search
25	1268272105221	http://www.google.com/m/search?client=ms-palm-w...	ee - Google Search
28	1268272115040	http://www.google.com/m/search?safe=active&clien...	cnn - Google Search
37	1268368924875	https://1.1.1.1/login.html?redirect=www.nytimes.com/	Web Authentication
40	1268368925626	https://1.1.1.1/fs/customwebauth/login.html?switch...	Johns Hopkins Guest Network
43	1268368932310	https://1.1.1.1/login.html	Logged In
47	1268368991890	http://www.nytimes.com/	The New York Times - Breaking News, World News & Multimedia
49	1268527457617	http://www.cnn.com/	CNN.com - Breaking News, U.S., World, Weather, Entertainment & Video News
52	1268610487813	http://uscg.mil/	United States Coast Guard - Home Page
55	1268610530649	http://digg.com/	Digg - The Latest News Headlines, Videos and Images
57	1268610536581	http://krebsonsecurity.com/	Krebs on Security
59	1268610549091	http://www.krebsonsecurity.com/	Krebs on Security

Fig. 19 – Web browsing history of the included browser.

Deleted files can be recovered from the FAT32 formatted User partition in much the same way as any piece of storage media. In one case, a Palm Pre was allegedly used to take illegal photographs. A digital investigator performed an on-scene manual examination of the device with the suspect's consent, but did not find the photographs. Digital investigators subsequently created a forensic duplicate of the User area on the device and used file system forensic tools to recover incriminating images and videos that had been deleted but were still intact in unallocated space. The file creation dates of the deleted files correlated with the EXIF data in the photographs, confirming that they were taken at the time of the offense.

Deleted records can be found within the SQLite database files on webOS devices. This is similar to the recovery of deleted items in Firefox databases [Murilo Tito, 2009](#). The reason this recovery is possible is that deleting a record removes the reference to it, but leaves the actual data.

In addition, deleted records may remain in unallocated space of the system partition and may be found by performing keyword searches of the forensic duplicate.

This retention of data on webOS devices allows for a wealth of deleted data for the digital investigators who knows how to attempt to recover them.

17. Conclusions

The emergence of webOS brings challenges and opportunities for digital investigators. Although some files can be

obtained from such devices with relative ease, the majority of information of forensic interest is stored in databases on a system partition that many mobile forensic tools do not acquire. Using the techniques and tools detailed in this paper, digital investigators can extract significant amounts of useful information from the system partition of webOS devices. This information includes call logs, SMS, e-mail communications, and remnants of Web browsing activities. In addition, by acquiring the system partition as described in this paper, it may be possible to recover deleted items.

Acknowledgements

Dr. Michael Lavine, Class Instructor, Advanced Computer Forensics, Johns Hopkins University Information Security Institute.

Steve Grimm and Andrew Hrenak, Regional Computer Crimes Education and Enforcement Group in St. Louis, MO.

Bryan Hoffman, former Systems Administrator, Johns Hopkins University Information Security Institute.

REFERENCE

Murilo Tito Pereira. Forensic analysis of the Firefox 3 Internet history and recovery of the deleted SQLite records. *Digital Investigation* 2009;5:93–103.