Blackberry Forensics

NIST Mobile Forensics Workshop June 2014

Shafik G. Punja
Cindy Murphy

TEELtechnologies

June-19-14

SPEAKER BACKGROUND

- **Shafik G. Punja**
  - Active duty LE, performing digital forensics since Nov 2003
  - Instructor for Teel Technologies US and Canada
  - Senior Technical Officer – QuByte Logic Ltd
  - Private sector work involves R n D partnerships with various LE colleagues, digital forensics training, data analytics and consulting services.
  - Shameless plug: Course developer and primary instructor for Advanced BlackBerry Forensics Class: http://www.teeltech.com/tt3/blackberry4.asp?cid=16
  - Contact: shafghp@gmail.com or qubytelogic@gmail.com

SPEAKER BACKGROUND

- **Cindy Murphy**
  - Detective, City of Madison, WI Police Department since 1985.
  - Involved in DFIR since 1999
  - MSc Forensic Computing and CyberCrime Investigation from Dublin in 2011
  - Part time DFIR Instructor at Madison College
  - Shameless plug: SANS 585 Advanced Smartphone Forensics Instructor
  - http://www.sans.org/event/for585-advanced-smartphone-mobile-device-forensics
  - Contact: CMurphy@cityofmadison.com

Coverage

- Locked BlackBerry’s: access options
- BES and BlackBerry
- Unlocked BlackBerry’s: Physical versus Logical
- Backup IPD, BBB v1, BBB v2 formats
- BlackBerry Messenger (BBM)
- BlackBerry Artifacts
- Malware/Spyware on BlackBerry devices
- BlackBerry 10

BlackBerry 7 (and lower)

- Developed by Research In Motion (now called BlackBerry) based out of Waterloo, ONT Canada.
- Device software design evolved from C++ to Java.
- Uses proprietary OS designed through JVM (Java Virtual Machine).
- The operating system is a collection of .cod files. You will not see a true file system in any analysis tool.
- Security of device rests with its relationship with the hardware.
- In Java based BB devices, BootROM is trust anchor.
- BlackBerry applications come packaged either as .COD files or JAD files which is associated to either OTW or OTA application installation.

Locked BlackBerry

- Option 1: If BES attached unlock via BES.

- Option 2:Attack info.mkf file on memory card if this is present.
  (**http://blog.crackpassword.com/2011/09/recovering-blackberry-device-passwords/**)

- Option 3: Chipoff (maybe JTAG which might work on older model devices).

Locked BlackBerry

- **Password is**
  - NOT stored on computer used by device owner for backup of
  - NOT present in the backup IPD file or any other version of the backup
- According to BlackBerry there is no backdoor into the device
- BlackBerry, may or may not help you in accessing the data on a locked BlackBerry device.

Locked BlackBerry

- Large Padlock lower right on handset screen = password locked
- Large Padlock lower right **AND** smaller padlock upper left = ***password locked and encrypted***
- Less secure passwords are rejected by the smartphone, such as those composed of identical characters, or characters that consist of natural sequences (i.e. 1234).
- If the device is locked **AND** you see the device prompting you to type the word “blackberry”, this means that half the password attempts have already been used.
- If a password is entered incorrectly ten consecutive times, this will automatically ***wipe*** all of the data on the BlackBerry.

Locked BlackBerry - BES

- BES (BlackBerry Enterprise Server): runs in server environment.
- A single BES can host as many as 500 BB devices.
- If a device is BES attached a password reset can be pushed from the BES Management Console.
- Password Reset does not affect the user data on the device.

Locked BlackBerry – BES 2

1. Open the BlackBerry Enterprise Server Management console.

2. Right-click the user account that requires a password change.

3. Click IT Admin > Set Password and Lock.

4. In the Set Handheld Password and Lock window, type the new password into the New Password and New Password Again fields.

5. Click OK.

Note: It takes approximately 30 minutes for the new IT Policy to be sent to the device.

6. When the device receives the IT Policy, the following message is displayed:

New IT Policy Changed Over The Air. Would you like to accept?

7. Click OK. The user can now use the new password on the device.

Source: http://www.blackberrycool.com/2005/10/23/changing-handheld-password-from-blackberry-enterprise-server/

TEELtechnologies

Locked BlackBerry – BES 2

- **You remembered to ask the friendly BES admin for the BES daily log files right?**

- BES stores daily logs in folders under default path **C:\Program Files\Research in Motion\BlackBerry Enterprise Server\Logs\** - grab them all and don't forget the email container which is stored separately.

- Depending upon BES version there may be over 15 or so different types of logs: SMS logs, PhoneCall logs, PINLog and BBM logs

- By default only PhoneCall logs are enabled on BES 5 and lower. In BES 10 and higher, it is believed that SMS, PhoneCall, PIN and BBM data is logged.

- SMS, PIN, PhoneCall and BBM are stored in CSV format contain both content and sender, receiver information

Locked BlackBerry – info.mkf file

- Non BES device, commonly referred to as BlackBerry Internet Service (BIS) device.

- If BlackBerry is locked AND if memory card is encrypted with either option 2: Security Password or option 3: Security Password and Device (default encryption is off)

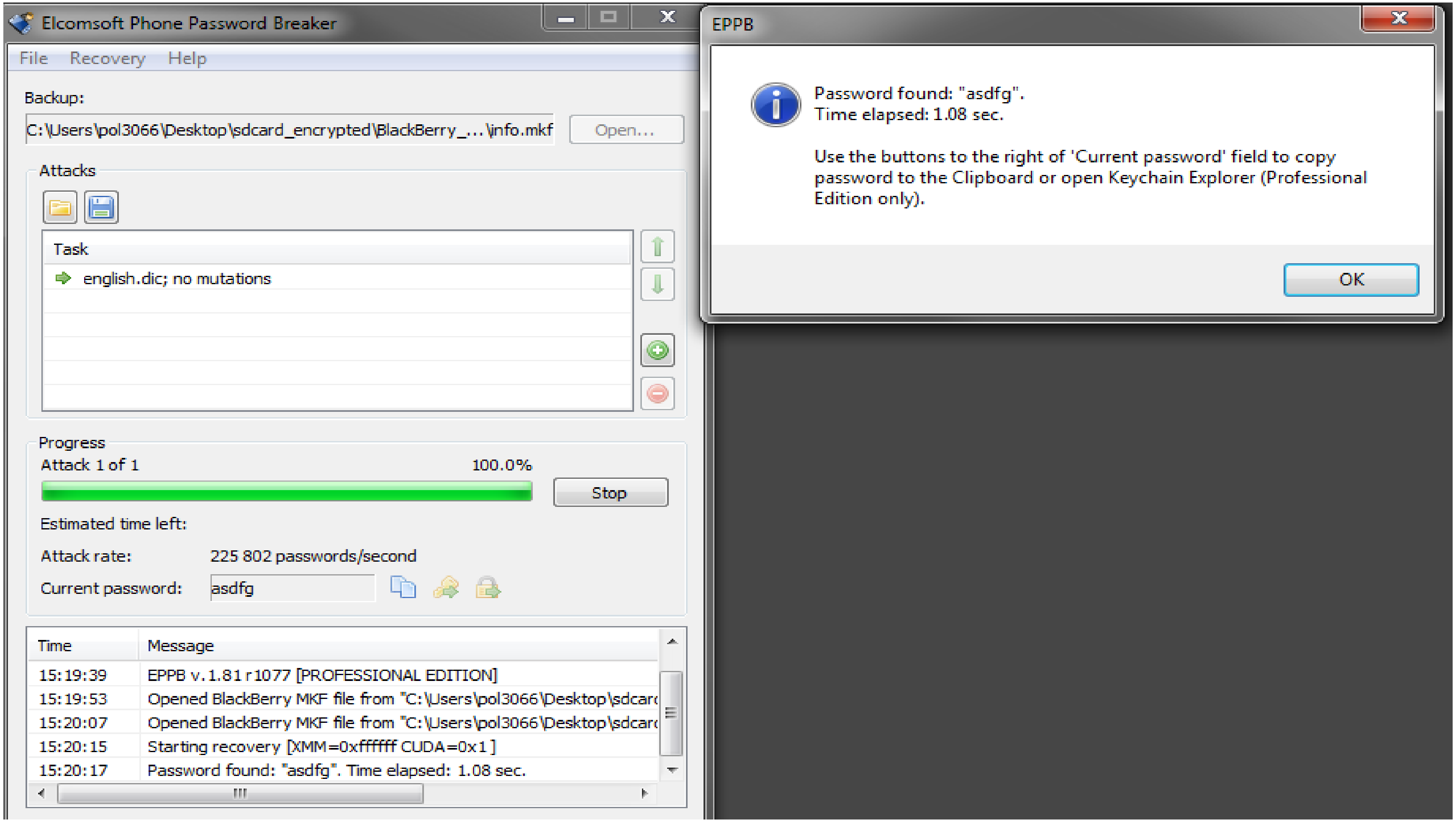
  - Then a hidden file info.mkf on the memory card at /BlackBerry/system/ will be found.

- EPPB attacks/exploits this file to obtain the password to the BlackBerry device

- **Source:* *http://blog.crackpassword.com/2011/09/recovering-blackberry-device-passwords/*

June-19-14

Locked BlackBerry – info.mkf file



Backup: C:\Users\pol3066\Desktop\sdcard_encrypted\BlackBerry_...\info.mkf

Attacks

Task
english.dic; no mutations

Progress

Attack 1 of 1 100.0%

Estimated time left:

Attack rate: 225 802 passwords/second

Current password: asdfg

```
Time      Message
15:19:39  EPPB v.1.81 r1077 [PROFESSIONAL EDITION]
15:19:53  Opened BlackBerry MKF file from "C:\Users\pol3066\Desktop\sdcar
15:20:07  Opened BlackBerry MKF file from "C:\Users\pol3066\Desktop\sdcar
15:20:15  Starting recovery [XMM=0xffffff CUDA=0x1]
15:20:17  Password found: "asdfg". Time elapsed: 1.08 sec.
```

Password found: "asdfg".
Time elapsed: 1.08 sec.

Use the buttons to the right of 'Current password' field to copy password to the Clipboard or open Keychain Explorer (Professional Edition only).

June-19-14

TEELtechnologies

Locked BlackBerry – info.mkf file

- When an upper case character is introduced, the english dictionary word list attack will always fail as it only examines lower case.

- So it might be worth while obtaining a keyword list from other related electronic exhibits which can be imported into EPPB or attempting a mutation attack.

Locked BlackBerry – Chipoff

- Option 1 and 2 are not available then only recourse is a chipoff.

- Consists of device disassembly, chip removal, chip cleaning, and chip reading with a chip programmer.

- This is destructive process to the device: you cannot power on the device to validate the parsing of the binary NAND/NOR dump.

Locked BlackBerry – Chipoff

- Best and currently the only tool that will decode a BlackBerry chipoff NAND dump obtained through a chip programmer is UFED Physical Analyzer (UFED PA)!

- If BlackBerry device is attached to a BES, and you don't have access to the BES, chip off is pointless as the data cannot be decrypted by any commercial tool at this time. Real world scenario: hostile BES, BlackBerry seized and is usually PGP encrypted then you are at a dead end, even with chipoff.

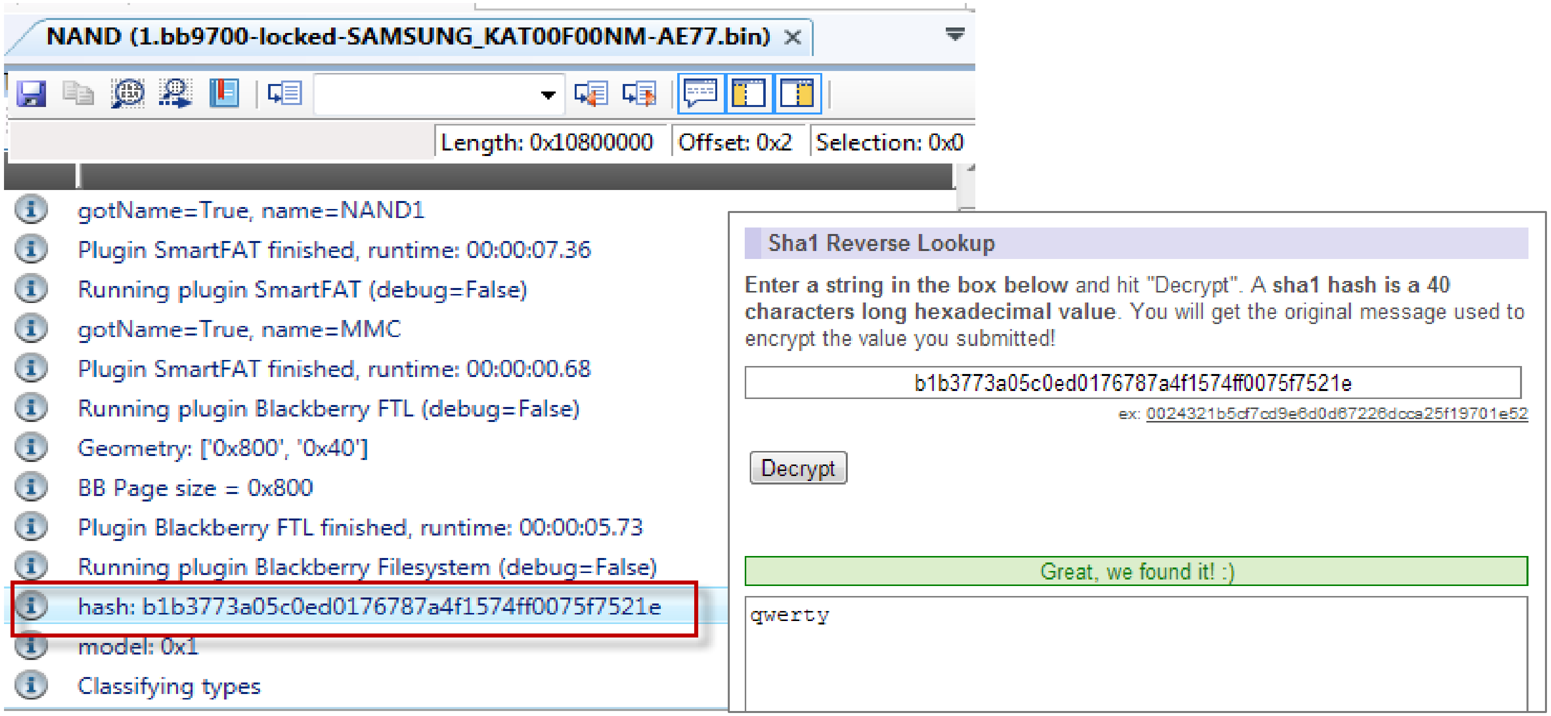
- Want to decode the device password from the chipoff NAND dump? Remember this password may also unlock other devices!

- Look at Trace Log and find SHA1 hash value; hash can be decrypted using these two links:

  http://www.stringfunction.com/sha1-decrypter.html
  http://www.md5decrypter.co.uk/sha1-decrypt.aspx

Locked BlackBerry – SHA1 Password

- The hash value is 40 characters in length, which is typically indicative of SHA1 value.



NAND (1.bb9700-locked-SAMSUNG_KAT00F00NM-AE77.bin)

Length: 0x10800000 | Offset: 0x2 | Selection: 0x0

```
gotName=True, name=NAND1
Plugin SmartFAT finished, runtime: 00:00:07.36
Running plugin SmartFAT (debug=False)
gotName=True, name=MMC
Plugin SmartFAT finished, runtime: 00:00:00.68
Running plugin Blackberry FTL (debug=False)
Geometry: ['0x800', '0x40']
BB Page size = 0x800
Plugin Blackberry FTL finished, runtime: 00:00:05.73
Running plugin Blackberry Filesystem (debug=False)
hash: b1b3773a05c0ed0176787a4f1574ff0075f7521e
model: 0x1
Classifying types
```

Sha1 Reverse Lookup

Enter a string in the box below and hit "Decrypt". A **sha1 hash is a 40 characters long hexadecimal value**. You will get the original message used to encrypt the value you submitted!

b1b3773a05c0ed0176787a4f1574ff0075f7521e

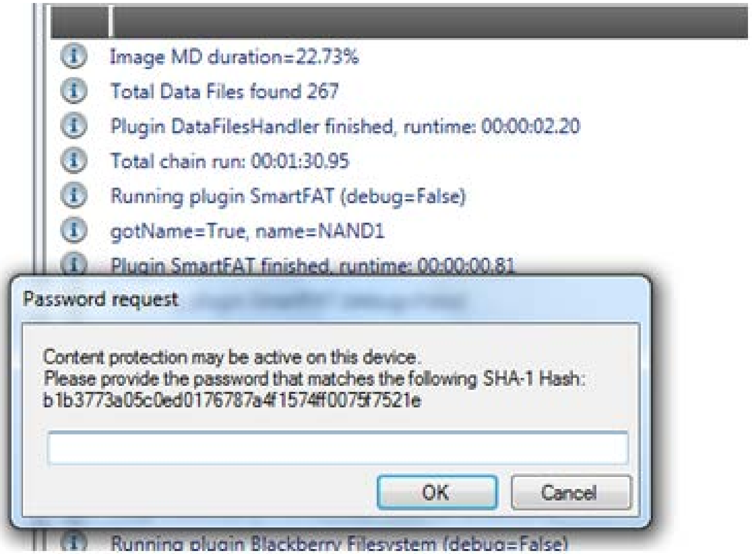
ex: 0024321b5cf7cd9e6d0d67226dcca25f19701e52

Great, we found it! :)

```
qwerty
```

Encrypted AND Locked BlackBerry

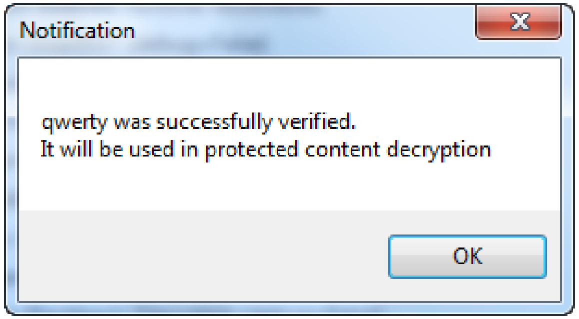
- This applies to **<u>non-BES devices</u>**, that just use the provided encryption (also called Content Protection options) for the device memory.
- Take the SHA1 value and decode the hash with links presented previously, enter the password into the field and UFED PA will decrypt the data.



```
Image MD duration=22.73%
Total Data Files found 267
Plugin DataFilesHandler finished, runtime: 00:00:02.20
Total chain run: 00:01:30.95
Running plugin SmartFAT (debug=False)
gotName=True, name=NAND1
Plugin SmartFAT finished, runtime: 00:00:00.81
Running plugin Blackberry Filesystem (debug=False)
```

Password request

Content protection may be active on this device.
Please provide the password that matches the following SHA-1 Hash:
b1b3773a05c0ed0176787a4f1574ff0075f7521e



Notification

qwerty was successfully verified.
It will be used in protected content decryption

Unlocked BlackBerry Devices - Physical

- Only tool that will obtain a physical read of the NAND over USB is UFED Classic or UFED Touch.

- This is done using a bootloader injection, into the RAM of the device.

- This is the only way to obtain deleted artifacts and non saved BBM chat.

- Resulting BIN file is opened in UFED PA for analysis.

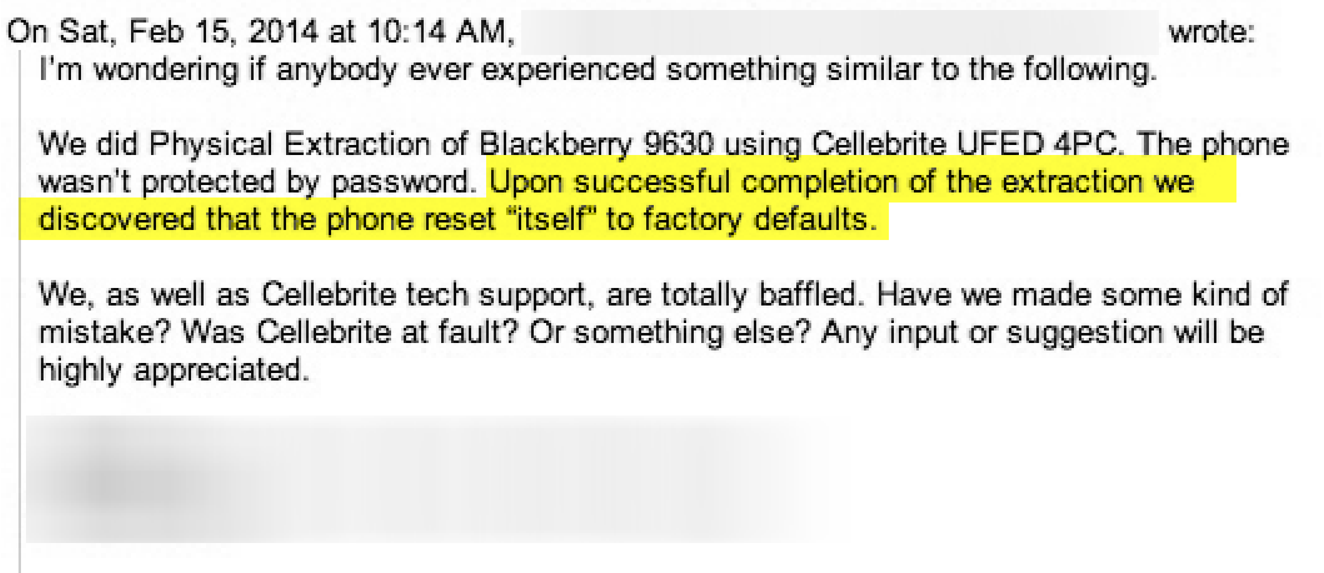
Unlocked BlackBerry Devices - Physical

- Process that I recommend typically is UFED physical extraction, followed by UFED file system (creation of IPD/backup) and UFED Logical parsed.

- Reason: to limit wear leveling functions on the NAND do physical first if UFED supports it then proceed to other extraction methods

Unlocked BlackBerry Devices – Physical – OOOPS!

BUT……This could happen to you if you go after the physical first and not logical:



On Sat, Feb 15, 2014 at 10:14 AM, [redacted] wrote:

> I'm wondering if anybody ever experienced something similar to the following.
>
> We did Physical Extraction of Blackberry 9630 using Cellebrite UFED 4PC. The phone wasn't protected by password. Upon successful completion of the extraction we discovered that the phone reset "itself" to factory defaults.
>
> We, as well as Cellebrite tech support, are totally baffled. Have we made some kind of mistake? Was Cellebrite at fault? Or something else? Any input or suggestion will be highly appreciated.
>
> [redacted]

So what happened to our unfortunate DFIR colleague?

Unlocked BlackBerry Devices – Physical – OOOPS!

Possible Scenarios:

1. The BlackBerry device must be turned and unlocked for the UFED boot loader injection process to occur.
   - Was it radio isolated, or did it briefly initiate a wireless connection?

2. If the device is attached to a BES, there is a BES IT policy that will initiate a device wipe if the BlackBerry device cannot receive an IT policy update or IT administration commands, after a specified period of time between 2 and 720 hours.
   - If the device is radio isolated then it cannot connect to the BES which could invoke the wipe IF this policy is enforced/enabled.

3. Could the bootloader injection have inadvertently triggered a device wipe?
   - In the non-volatile (NV) memory store the device sets the *Device Under Attack* flag. Once this bit is set, **nothing will clear this flag** except completion of the wipe.

Unlocked BlackBerry Devices – Physical – OOOPS!

What actually happened (cited from the listserve email):

- No “factory reset.” What happened, I would call it “wipeout”, and Cellebrite prefers calling it “cache memory reset”.

- Blackberry 9630, on Enterprise network, not used for more than half a year, and arrived in with the battery totally discharged.

- Connected to a charger, and as soon as it came to life, disabled Wireless and Bluetooth (both were seen as enabled first).

- Close to the end of the process Cellbrite displayed a message, something along the following lines “Cellebrite is completing the physical extraction by rebooting/resetting (?) the phone”.

Unlocked BlackBerry Devices – Physical – OOOPS!

What actually happened (cited from the listserve email):

- Post physical extraction: device checked, almost all the data was gone. Also, in the settings window “Connections” “Verizon Wireless” was replaced with “Mobile Network”.
- …good news is that all the data was collected by Cellebrite, before it was lost.
- Cellebrite’s explanation: Cellebrite installs a client on the phone for the extraction, and needs to remove it when the extraction is completed. On Blackberry 9.x and earlier versions the phone has to be rebooted and this is what triggers “cache memory reset” and loss of data.

Unlocked BlackBerry Devices - Logical

- For BlackBerry devices logical data extraction and parsing:
  - UFED Classic or Touch.
  - Oxygen Forensic Suite Analyst USB version.
  - XRY (Microsystemation)

- Don’t forget about using BlackBerry Desktop Software for Window or Mac in making a logical backup IPD file

Unlocked BlackBerry Devices – Other Tools

- **These tools connect to BlackBerry over USB and extract the logical data structure:**
  - EnCase 7
  - FTK MPE+
  - Secure View 3
  - Final Mobile (Final Data)
  - May be other tools, that are not listed here.

Unlocked BlackBerry Devices – Parsing Tools

- **These tools parse BlackBerry backup formats IPD and BBBv1:**
  - UFED PA
  - Oxygen Forensic Suite Analyst
  - XRY
  - FTK 3.x and higher with FTK MPE
  - Elcomsoft BlackBerry Explorer (EBBE)
  - EnCase 7
  - EnCase 6 – with script from Yogesh Khatri: www.swiftforensics.com
  - Secure View 3
  - Final Mobile (Final Data)
  - BlackBerry Backup Explorer (Reincubate) – this will do IPD, BBBv1 and BBBv2
  - phoneMiner
  - Rubus (CCL Forensics, this is FREE): this allows deconstruction of backup file into its raw structure; does not parse into clean reporting format
  - MagicBerry (FREE): does NOT support decoding of all database structures

BlackBerry Backup Formats

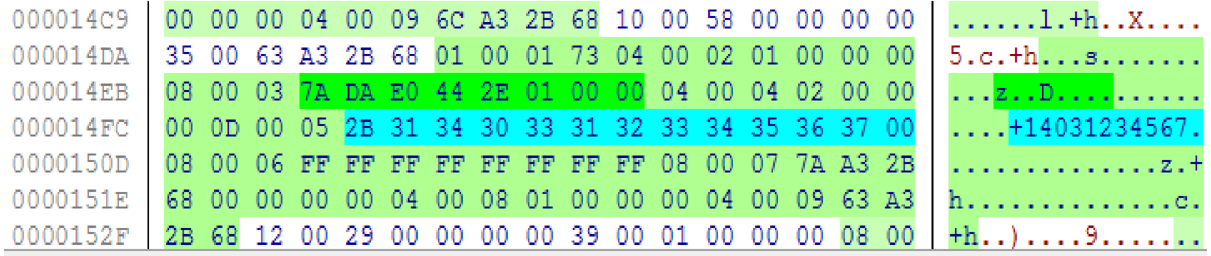
- IPD File(Inter@ctive Pager Backup): This is a collection of the data structures called databases all coagulated into one unique backup file.

- BBB File: v1 created by Mac version of BlackBerry Desktop Software, IPD file contained within .bbb file which has a PK header signature (zip file)

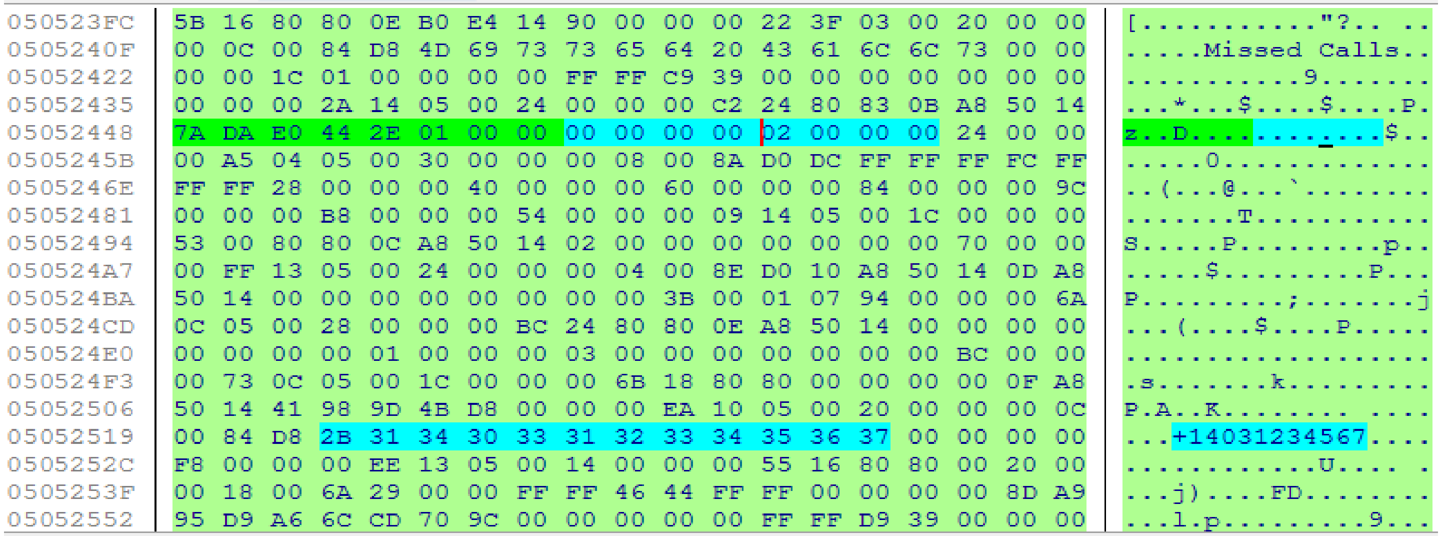
- BBB File: v2 created by Windows version of BlackBerry Desktop Software v7.1.x and higher; the backup is contained within the .bbb file but each data structure is stored as individual .DAT file

BlackBerry Backup Formats

- The IPD structure is not how the data exists on the BlackBerry device at a physical level: Logical versus physical of same record



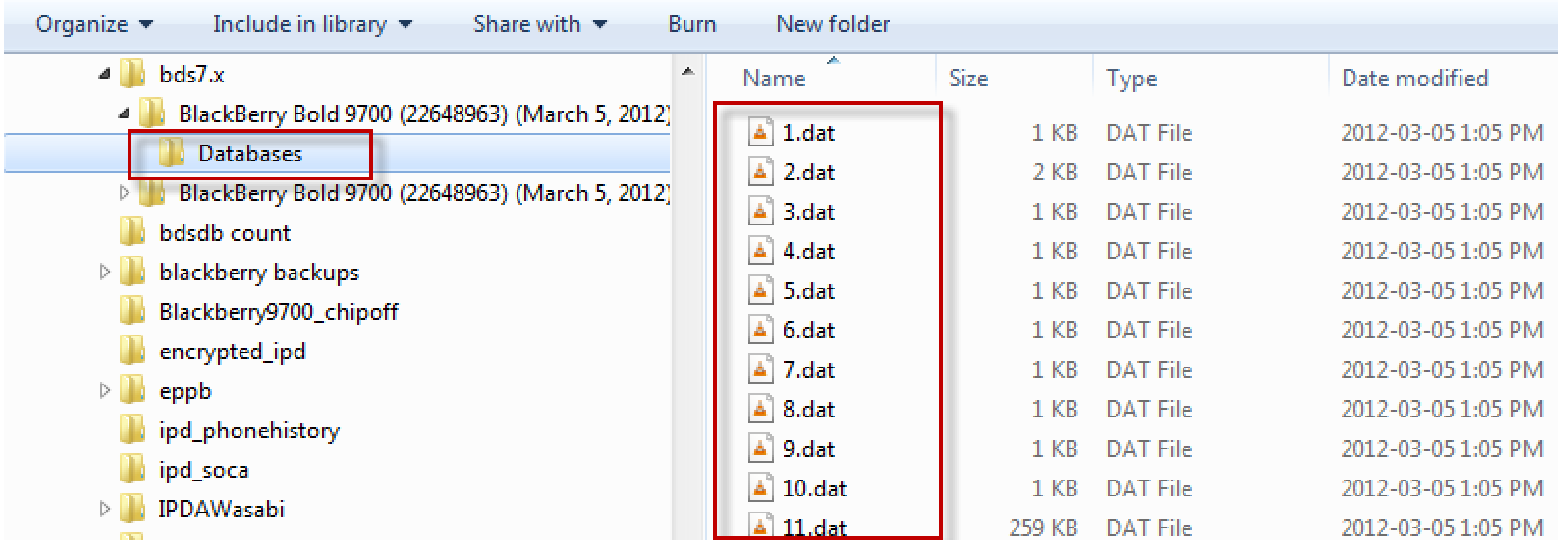
```
000014C9  00 00 00 04 00 09 6C A3 2B 68 10 00 58 00 00 00 00  ......l.+h..X....
000014DA  35 00 63 A3 2B 68 01 00 01 73 04 00 02 01 00 00 00  5.c.+h...s.......
000014EB  08 00 03 7A DA E0 44 2E 01 00 00 04 00 04 02 00 00  ...z..D..........
000014FC  00 0D 00 05 2B 31 34 30 33 31 32 33 34 35 36 37 00  ....+14031234567.
0000150D  08 00 06 FF FF FF FF FF FF FF FF 08 00 07 7A A3 2B  ..............z.+
0000151E  68 00 00 00 00 04 00 08 01 00 00 00 04 00 09 63 A3  h..............c.
0000152F  2B 68 12 00 29 00 00 00 00 39 00 01 00 00 00 08 00  +h..)....9.......
```



```
050523FC  5B 16 80 80 0E B0 E4 14 90 00 00 00 22 3F 03 00 20 00 00  [..........."?.. ..
0505240F  00 0C 00 84 D8 4D 69 73 73 65 64 20 43 61 6C 6C 73 00 00  .....Missed Calls..
05052422  00 00 1C 01 00 00 00 00 FF FF C9 39 00 00 00 00 00 00 00  ...........9.......
05052435  00 00 00 2A 14 05 00 24 00 00 00 C2 24 80 83 0B A8 50 14  ...*...$....$....P.
05052448  7A DA E0 44 2E 01 00 00 00 00 00 00 02 00 00 00 24 00 00  z..D............$..
0505245B  00 A5 04 05 00 30 00 00 00 08 00 8A D0 DC FF FF FF FC FF  .....0.............
0505246E  FF FF 28 00 00 00 40 00 00 00 60 00 00 00 84 00 00 00 9C  ..(...@...`........
05052481  00 00 00 B8 00 00 00 54 00 00 00 09 14 05 00 1C 00 00 00  .......T...........
05052494  53 00 80 80 0C A8 50 14 02 00 00 00 00 00 00 00 70 00 00  S.....P.........p..
050524A7  00 FF 13 05 00 24 00 00 00 04 00 8E D0 10 A8 50 14 0D A8  .....$.........P...
050524BA  50 14 00 00 00 00 00 00 00 00 3B 00 01 07 94 00 00 00 6A  P.........;.......j
050524CD  0C 05 00 28 00 00 00 BC 24 80 80 0E A8 50 14 00 00 00 00  ...(....$....P.....
050524E0  00 00 00 00 01 00 00 00 03 00 00 00 00 00 00 00 BC 00 00  ...................
050524F3  00 73 0C 05 00 1C 00 00 00 6B 18 80 80 00 00 00 00 0F A8  .s.......k.........
05052506  50 14 41 98 9D 4B D8 00 00 00 EA 10 05 00 20 00 00 00 0C  P.A..K........ ....
05052519  00 84 D8 2B 31 34 30 33 31 32 33 34 35 36 37 00 00 00 00  ...+14031234567....
0505252C  F8 00 00 00 EE 13 05 00 14 00 00 00 55 16 80 80 00 20 00  ............U.... .
0505253F  00 18 00 6A 29 00 00 FF FF 46 44 FF FF 00 00 00 00 8D A9  ...j)....FD........
05052552  95 D9 A6 6C CD 70 9C 00 00 00 00 00 FF FF D9 39 00 00 00  ...l.p.........9...
```

BlackBerry Backup Formats

- BBB v2 backup format



Name	Size	Type	Date modified
1.dat	1 KB	DAT File	2012-03-05 1:05 PM
2.dat	2 KB	DAT File	2012-03-05 1:05 PM
3.dat	1 KB	DAT File	2012-03-05 1:05 PM
4.dat	1 KB	DAT File	2012-03-05 1:05 PM
5.dat	1 KB	DAT File	2012-03-05 1:05 PM
6.dat	1 KB	DAT File	2012-03-05 1:05 PM
7.dat	1 KB	DAT File	2012-03-05 1:05 PM
8.dat	1 KB	DAT File	2012-03-05 1:05 PM
9.dat	1 KB	DAT File	2012-03-05 1:05 PM
10.dat	1 KB	DAT File	2012-03-05 1:05 PM
11.dat	259 KB	DAT File	2012-03-05 1:05 PM

- The number of DAT files present in the Databases folder should match the number of databases listed in the Manifest.xml; this file is found within the root of the BBB compressed archive.

TEELtechnologies

BlackBerry Date Formats

- 3 different date formats identified, and documented by Yogesh Khatri; http://www.swiftforensics.com/2012/03/blackberry-date-formats.htm

1. Phone Call Log, SMS, Phone History

- 8-byte length Java date value, which represents the timestamp in milliseconds, and is similar to Unix time values (which are 4 bytes).
- Also applies to BBM and PIN messages; dates in BE order (when data is viewed in BBM.db file or BBM Conversations file)
- The Win Hex/X-Ways Forensics Manual (1995-2006 Stefan Fleischmann), page 8, describes Java date as “a 64-bit integer value that specifies the number of milliseconds since January 1, 1970. Principally stored in big endian, which is the typical byte order in Java.”
- Unix timestamp (4 bytes, converted into their decimal equivalent) * 1000 = Java Date.
- Java Date/1000 = Unix Timestamp
- This is also referred to as the BlackBerry® Date

BlackBerry Date Formats

- 3 different date formats identified, and documented by Yogesh Khatri; http://www.swiftforensics.com/2012/03/blackberry-date-formats.htm

2. Calendar

- Calendar date values use number of minutes since 1 Jan 1900 0:0:0.
- Precision to only the number of minutes.
- Yogesh Khatri cites this formula to obtain the unix time value:
  - UnixTimestamp = (CalendarDate – 36816480) * 60

TEELtechnologies

BlackBerry Date Formats

- 3 different date formats identified, and documented by Yogesh Khatri; http://www.swiftforensics.com/2012/03/blackberry-date-formats.htm

3. Email

- Sent and Received dates are stored as a 2 byte date and 2 byte time value.

BlackBerry Endian Order

- There is no real clear direction from BlackBerry in any official technical specifications on how to read the byte order of the data and also whether the byte order is signed or unsigned.

- In the IPD structure both BE and LE ordering are used.

- The only fields that are identified by BlackBerry documentation, for the IPD/DAT file backup is the following as LE byte order:
  - record length
  - database version
  - database handle
  - record type

BlackBerry – BBM

- BlackBerry devices that cannot use BlackBerry Messenger 5.0 or higher = take pictures; there is no backup mechanism
- BBM Chat History: If save chat history option is enabled chat is saved in CSV format and stored in one of 2 locations: **memory card** or **content store data structure** on the device:
- Paths:
  - /store/home/im/BlackBerry Messenger/<pinnumber>
  - /SDCard/BlackBerry/im/BlackBerry Messenger/<pinnumber>
- These locations will store CSV, .CON and .BAK files; CON and BAK files is the device user's BBM contact list and the BAK is the backup of the contact (CON) file.

BlackBerry – BBM Chat CSV

- BBM Chat CSV File: Date/Time is 21 digit numeric value which, YYYYMMDD (first 8 digits reading from the left) followed by remainder 13 decimal values are actually the unix DATE AND TIME stamp numeric values in millisecond
- Example: 201001291264804385552
- Parsing CSV files: bbmessenger.py (Python 3 required) **https://sites.google.com/site/slosleuth/ (John Lehr)**
- Parsing CON/BAK files: ConParse (Java based) **https://github.com/sheran/bb-tools (Sheran Gunasekera)**

TEELtechnologies

BlackBerry – Artifacts BBM

- Using BBM 5.0 but no chat history save enabled;
- Must do a physical extraction with UFED Touch/Classic in order to obtain BBM chat data.
- Enabling the save chat history feature will not work on chat conversations currently on the device; only affects new chat from the date the option was enabled.

BlackBerry – BBM.db

- Found in BBM 6 and higher running BB OS 6.
- BBM database file: bbm.db.
- Proprietary database that contains BBM chat ***even if option of saving chat history was NOT enabled***.
- Also contains data similarly found in the CON and BAK files.

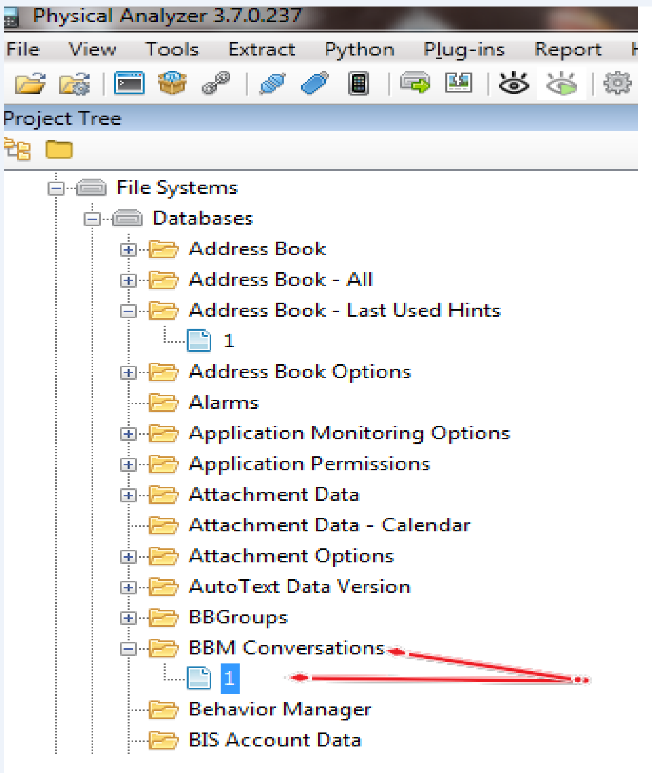
BlackBerry – BBM.db

- **A bbm.db file that is not encrypted can, generally, be divided into several areas:**
  - Device owner information
  - BBM contacts
  - Device owner time zone
  - BBM chat content

- Only one tool currently parses this right now – UFED PA; OFS may also do this, but not tested.
- bbm.db is only observed to retain chat based on BBM app or OS upgrade/downgrade; meaning that there may be chat present on device that is not stored in the bbm.db file.

BlackBerry – BBM Conversations

- This was discovered by a colleague on examination of a BlackBerry 9900 running OS 7.x.



June-19-14

BlackBerry – BBM Conversations

- This file appears not much different than BBM.db and follows similar structure (grouped by PINs/Chats etc.) like the bbm.db file.
- It has only been observed on devices running OS 7.x.
- It contains the BBM contacts, and chat history, believed to be saved regardless of whether BBM save chat history option is enabled.
- The BBM Conversations folder can be obtained with a logical file system extraction.
- Tools that do parse the BBM Conversations structure:
  - BlackBerry Backup Explorer (Reincubate)
- Tools that might or will likely parse the BBM Conversations structure:
  - UFED PA?
  - Oxygen Forensic Suite?
  - XRY?

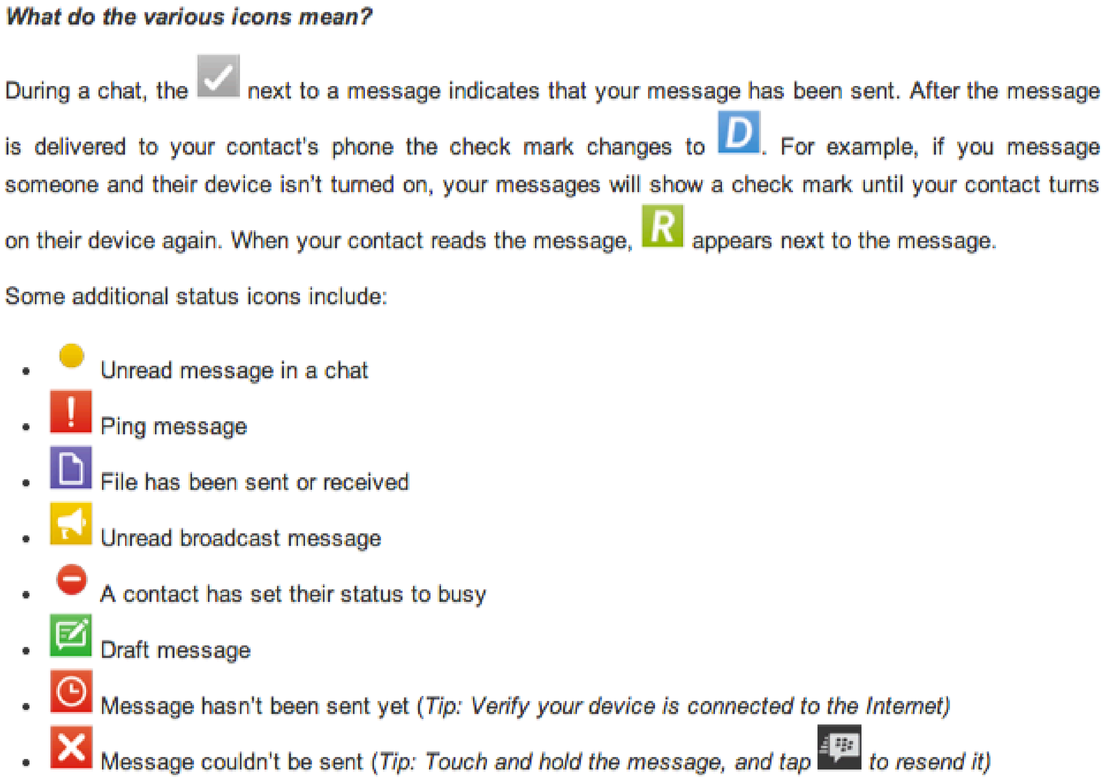
iOS and Android BBM

- BBM for iOS is only supported for iOS 6 and 7.
- BBM for Android is only supported for Android OS (AOS) 4.0 and later.
- A BlackBerry Messenger ID is required.
- The Android or iOS device will be assigned a unique PIN, 8 characters long, randomly generated.
- Observed by both Sheran Gunasekera (aka Gunny), and Jose Garcia, the iOS and Android BBM app uses SQLite database to store its data.
- BBM 10 for also offers voice and video, which connects over Wi-Fi.

iOS and Android BBM

Icons related to BBM 10 for Android, and iPhone cited from:

http://helpblog.blackberry.com/2013/10/getting-started-with-bbm-on-android-and-iphone/



What do the various icons mean?

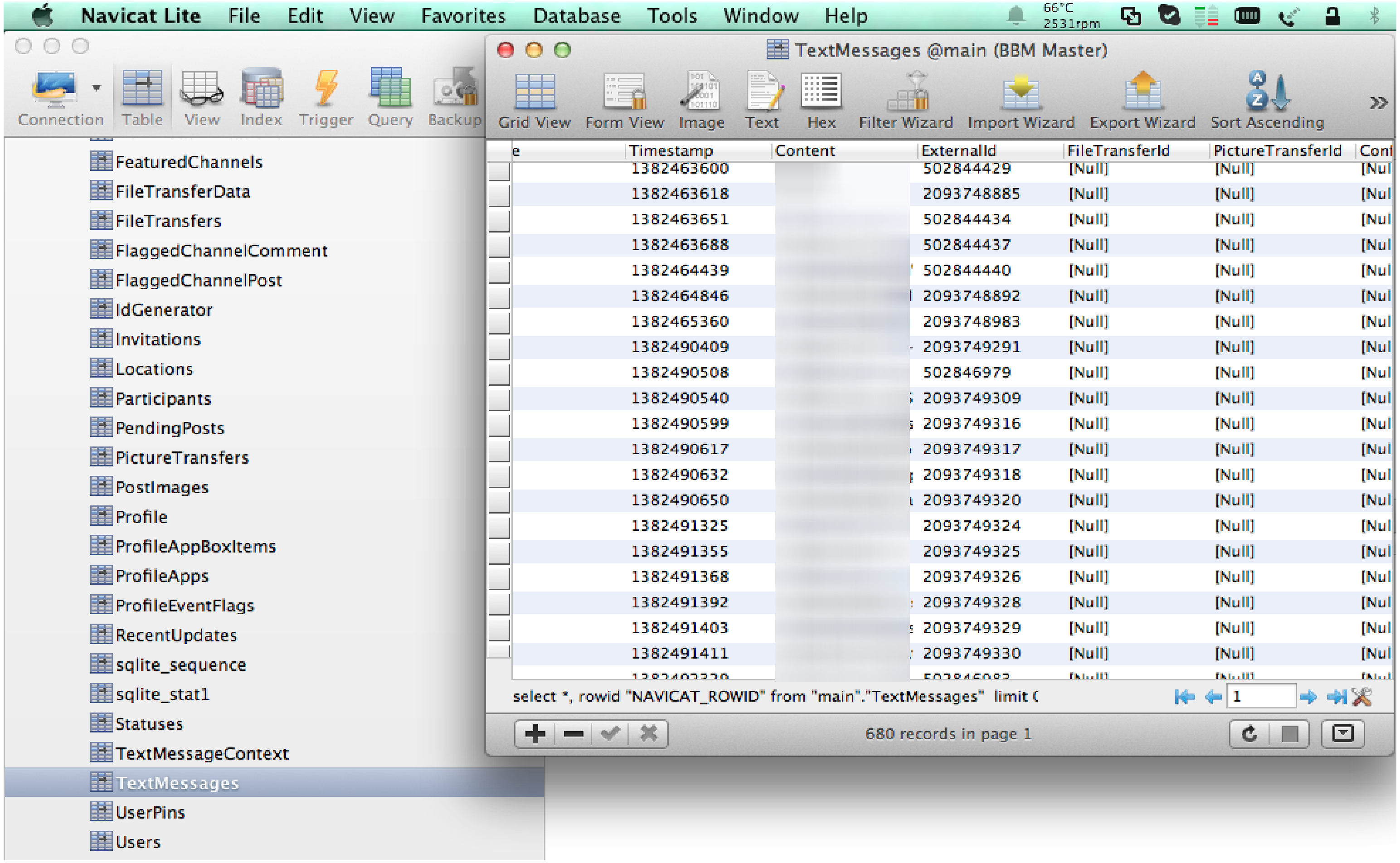
During a chat, the ✓ next to a message indicates that your message has been sent. After the message is delivered to your contact's phone the check mark changes to D. For example, if you message someone and their device isn't turned on, your messages will show a check mark until your contact turns on their device again. When your contact reads the message, R appears next to the message.

Some additional status icons include:

- ● Unread message in a chat
- ! Ping message
- 🗋 File has been sent or received
- 📢 Unread broadcast message
- ⛔ A contact has set their status to busy
- ✎ Draft message
- 🕒 Message hasn't been sent yet (*Tip: Verify your device is connected to the Internet*)
- ✕ Message couldn't be sent (*Tip: Touch and hold the message, and tap* 💬 *to resend it*)

TEELtechnologies

iOS and Android BBM



e	Timestamp	Content	ExternalId	FileTransferId	PictureTransferId	Cont
	1382463600	[redacted]	502844429	[Null]	[Null]	[Nul
	1382463618	[redacted]	2093748885	[Null]	[Null]	[Nul
	1382463651	[redacted]	502844434	[Null]	[Null]	[Nul
	1382463688	[redacted]	502844437	[Null]	[Null]	[Nul
	1382464439	[redacted]	502844440	[Null]	[Null]	[Nul
	1382464846	[redacted]	2093748892	[Null]	[Null]	[Nul
	1382465360	[redacted]	2093748983	[Null]	[Null]	[Nul
	1382490409	[redacted]	2093749291	[Null]	[Null]	[Nul
	1382490508	[redacted]	502846979	[Null]	[Null]	[Nul
	1382490540	[redacted]	2093749309	[Null]	[Null]	[Nul
	1382490599	[redacted]	2093749316	[Null]	[Null]	[Nul
	1382490617	[redacted]	2093749317	[Null]	[Null]	[Nul
	1382490632	[redacted]	2093749318	[Null]	[Null]	[Nul
	1382490650	[redacted]	2093749320	[Null]	[Null]	[Nul
	1382491325	[redacted]	2093749324	[Null]	[Null]	[Nul
	1382491355	[redacted]	2093749325	[Null]	[Null]	[Nul
	1382491368	[redacted]	2093749326	[Null]	[Null]	[Nul
	1382491392	[redacted]	2093749328	[Null]	[Null]	[Nul
	1382491403	[redacted]	2093749329	[Null]	[Null]	[Nul
	1382491411	[redacted]	2093749330	[Null]	[Null]	[Nul

```
select *, rowid "NAVICAT_ROWID" from "main"."TextMessages"  limit (
```

680 records in page 1

June-19-14

TEELtechnologies

BlackBerry – Artifacts BBThumbs.dat

- **BBThumbs.dat:** Thumbnail cache of pictures currently or previously stored on the BlackBerry device or its associated memory card; typically observed in OS 5.x and older (pre OS 6.x)
- Magic String/File Header: /x24/x05/x20/x03/
- Paths:
  - SDCard/BlackBerry/foldername/BBThumbs.dat
  - store/home/user/foldername/BBThumbs.dat
- The "foldername" referred to in the path can be videos, pictures, voicenotes, and likely also audiobooks, documents, music, podcasts and ringtones.
- Records the file names of all files stored within that specific directory even if that file has been deleted.
- BBThumbs.dat file related to the pictures directory only stores pictures (PNG, JPG, GIF) inside it; for video BBThumbs.dat only filename is present, no image.

BlackBerry – Artifacts BBThumbs.dat

Parsing BBThumbs.dat

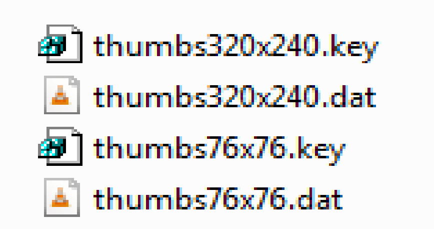
1. bbt.py (Python 2): https://github.com/sheran/bb-tools (Sheran Gunasekera) can be used to parse the key/dat pair files and the older BBThumbs.dat files.

- bbt.py will extract all the records in the BBThumbs.dat file.
- If the record is a picture, then it extracts the thumbnail that is stored inside the BBThumbs.dat file and saves it.
- Script output will show the filename, time stamp local to the device time and the SHA1 hash value for the record.
- If the record inside BBThumbs.dat is not a picture file, then bbt.py will extract the metadata from the file. In this case the BBThumbs.dat file is from another folder such as video or voicenotes. The SHA1 will be for this record.

BlackBerry – Artifacts key/dat

thumbsXXxXX.key/thumbsXXxXX.dat:

- Instead of BBThumbs.dat, for OS 6.x, the files come in .key and .dat pairs named by the image size of the pictures that it is cataloguing – ONLY FOR PICTURES



thumbs320x240.key
thumbs320x240.dat
thumbs76x76.key
thumbs76x76.dat

- Paths:
  - SDCard/BlackBerry/system/media/thumbsXXxXX.dat
  - store/appdata/rim/media/thumbsXXxXX.dat

BlackBerry – Artifacts key/dat

- thumbsXXxXX.key/thumbsXXxXX.dat:
  - It is believed based on examination of multimedia content that the dat/key files only store metadata related to images and picture images present on the BlackBerry® device.
  - The KEY file is like an index table that contains byte values that provide indication of where the records exist with the DAT file:
  - The record in the DAT file contains images and other meta-data.

TEELtechnologies

BlackBerry – Artifacts key/dat Parsing

- Parsing thumbsXXxXX.key/thumbsXXxXX.dat:

- **1. bbt.py** (Python 2): https://github.com/sheran/bb-tools (Sheran Gunasekera) can be used to parse the key/dat pair files and the older BBThumbs.dat files.

- **2. bbt.exe** (Windows executable): Based on Sheran Gunasekera’s work, Detective John Thompson (Special Investigations Section - Technical Services Unit, Lakeland Police Department) wrote a Windows based command line EXE that will work very similar to bbt.py.

BlackBerry – Artifacts key/dat Parsing

-Parsing thumbsXXxXX.key/thumbsXXxXX.dat:

- **3. BBThumbs EnScript**: For those that use EnCase 6.x, a fellow colleague and very good friend, Special Constable Jeremy Dupuis (Ontario Provincial Police) has developed an EnScript that will run against thumbsXX and thumbsXX files with a DAT extension. Using the script: Blue checkmark one to multiple thumbs??x??.dat files and run script.

- **4. Commerical Tools:** UFED PA, Oxygen Forensic Suite Analyst, Final Mobile etc – don't forget to check these tools, as they do handle either the BBThumbs.dat variant and/or the KEY/DAT files.

BlackBerry – Artifacts art.dat files

- *xxxx*art.dat files (OS 6.x and higher):

  - Other multi-media content such as video, podcasts, music are stored in files that end with DAT;

  - the file name is typically *xxxx*art.dat where xxxx represents the name of the type of multimedia content that it is referencing.

  - The xxxxxart.dat files are SQLite format 3 database files

BlackBerry – Artifacts Voicenotes

- Voicenotes metadata strangely is still stored in the BBThumbs.dat format.

- Parsing videoart.dat files (OS 6.x and higher):
  - **bbvideo.py:** we can parse the videoart.dat file and extract the BLOB data in from the SQLite database file.
  - http://linuxsleuthing.blogspot.com (John Lehr)

BlackBerry – Artifacts EXIF Pictures and Movies

- **Exif Data:**
  - To understand how EXIF data is stored within multimedia content, refer to the JEITA CP-3451 Exchangeable image file format for digital still cameras: Exif Version 2.2.
  - pictures: can contain geotag data along with traditional date/time values, and make/model values.

TEELtechnologies

BlackBerry – Artifacts EXIF Pictures and Movies

- Exif Data:
  - movies: no geo tagging or make/model embedded within movie files; usual time stamps values for media creation and embedded within the video file; and also the encoder value called “rimm” will be observed.
  - voicenotes: none observed.
- **BEST Exif Analysis Tool of Choice: ExifTool by Phil Harvey, does a great job!!!**

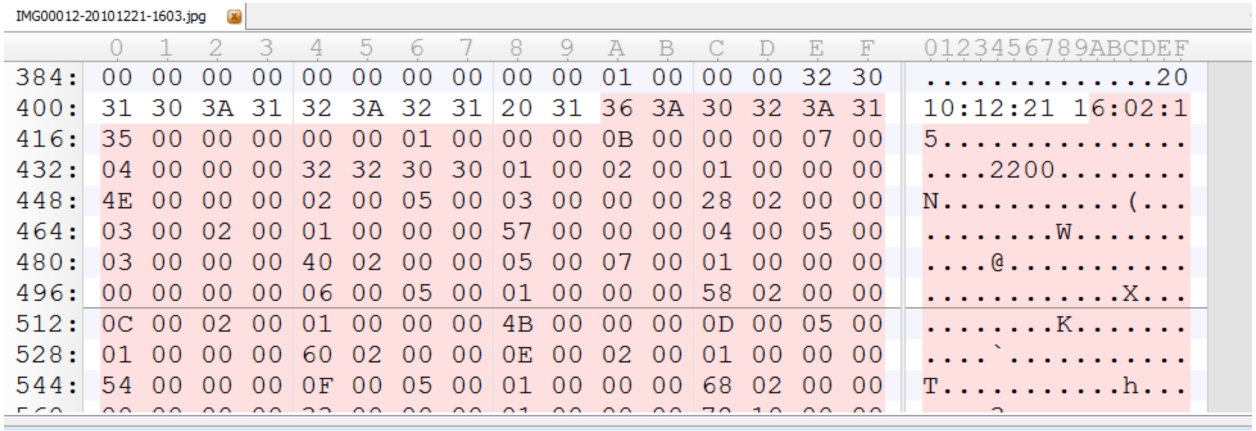
EXIF Geo Data

- For Geo Data to be written to a device created picture/image the following conditions must be present:
  - Device GPS Services must be enabled.

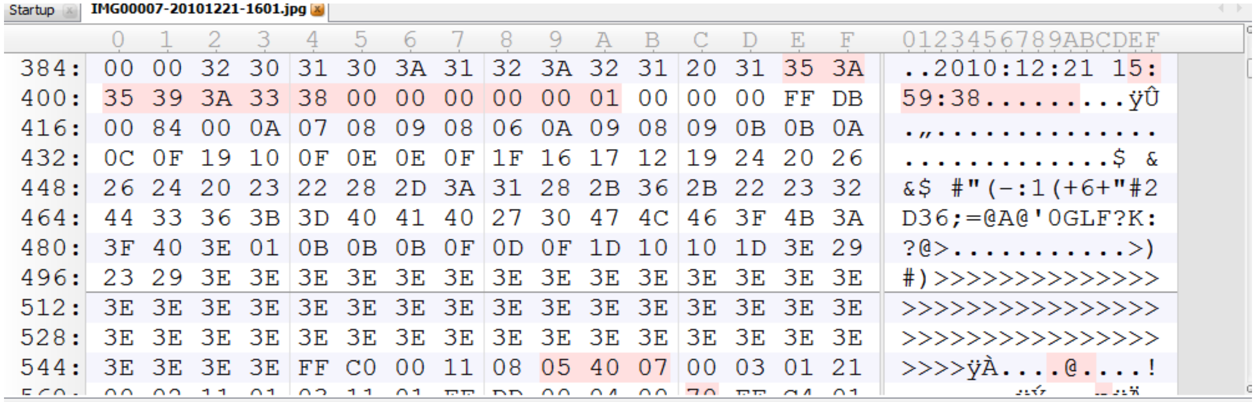
    AND
  - The Camera GPS function must be enabled, by default it is disabled.

    AND
  - Device must be capable of receiving GPS data.

EXIF Geo Data: Which Picture/Image Contains Geo Data?



```
IMG00012-20101221-1603.jpg
      0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
384: 00 00 00 00 00 00 00 00 00 00 01 00 00 00 32 30   ..............20
400: 31 30 3A 31 32 3A 32 31 20 31 36 3A 30 32 3A 31   10:12:21 16:02:1
416: 35 00 00 00 00 00 01 00 00 00 0B 00 00 00 07 00   5...............
432: 04 00 00 00 32 32 30 30 01 00 02 00 01 00 00 00   ....2200........
448: 4E 00 00 00 02 00 05 00 03 00 00 00 28 02 00 00   N...........(...
464: 03 00 02 00 01 00 00 00 57 00 00 00 04 00 05 00   ........W.......
480: 03 00 00 00 40 02 00 00 05 00 07 00 01 00 00 00   ....@...........
496: 00 00 00 00 06 00 05 00 01 00 00 00 58 02 00 00   ............X...
512: 0C 00 02 00 01 00 00 00 4B 00 00 00 0D 00 05 00   ........K.......
528: 01 00 00 00 60 02 00 00 0E 00 02 00 01 00 00 00   ....`...........
544: 54 00 00 00 0F 00 05 00 01 00 00 00 68 02 00 00   T...........h...
```



```
Startup   IMG00007-20101221-1601.jpg
      0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
384: 00 00 32 30 31 30 3A 31 32 3A 32 31 20 31 35 3A   ..2010:12:21 15:
400: 35 39 3A 33 38 00 00 00 00 00 01 00 00 00 FF DB   59:38.........ÿÛ
416: 00 84 00 0A 07 08 09 08 06 0A 09 08 09 0B 0B 0A   .„..............
432: 0C 0F 19 10 0F 0E 0E 0F 1F 16 17 12 19 24 20 26   .............$ &
448: 26 24 20 23 22 28 2D 3A 31 28 2B 36 2B 22 23 32   &$ #"(-:1(+6+"#2
464: 44 33 36 3B 3D 40 41 40 27 30 47 4C 46 3F 4B 3A   D36;=@A@'0GLF?K:
480: 3F 40 3E 01 0B 0B 0B 0F 0D 0F 1D 10 10 1D 3E 29   ?@>...........>)
496: 23 29 3E 3E 3E 3E 3E 3E 3E 3E 3E 3E 3E 3E 3E 3E   #)>>>>>>>>>>>>>>
512: 3E 3E 3E 3E 3E 3E 3E 3E 3E 3E 3E 3E 3E 3E 3E 3E   >>>>>>>>>>>>>>>>
528: 3E 3E 3E 3E 3E 3E 3E 3E 3E 3E 3E 3E 3E 3E 3E 3E   >>>>>>>>>>>>>>>>
544: 3E 3E 3E 3E FF C0 00 11 08 05 40 07 00 03 01 21   >>>>ÿÀ.....@....!
```

EXIF DATA INCORRECT TIMESTAMPS IN BLACKBERRY DEVICES

One critical observation made by a fellow research colleague, Sam Brothers, Department of Homeland Security about EXIF values regarding BlackBerry® devices:

"Wrong EXIF data gets written for the 1st picture every time the phone goes to sleep or the screensaver goes on! So, EXIF in a BB cannot be relied upon. This has been validated on (2) devices thus far."

It is unknown if the behavior described by Sam Brothers is consistent for every BlackBerry® device, across every OS iteration.

But this has been observed on BlackBerry OS 4, 5, 6 and 7 devices.

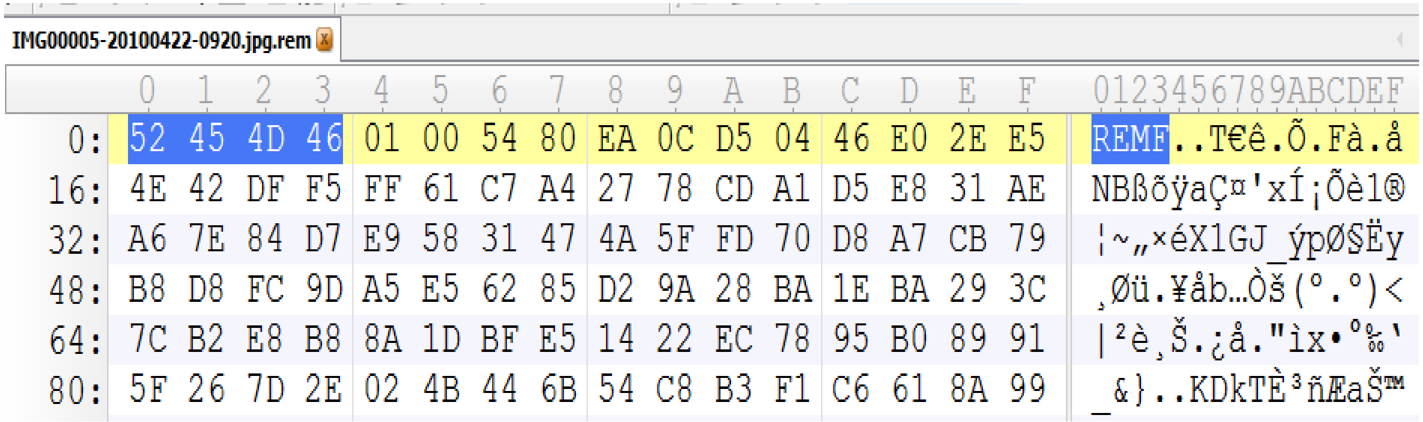
Blog Post where Steve Zenone also observes the same behavior:
http://blog.zenone.org/2009/01/forensics-blackberry-curve-8310-and.html

BlackBerry – Artifacts REMF

- REMF observed in file header? (Depending on your perspective REMF could also mean Rear Echelon..ahemmm…….well…I am sure you get the rest!).
- The .rem extension denotes an encrypted file, which can only be decrypted by the device that encrypted the files.
- Another method is to use the latest version of UFED PA, or Elcomsoft Phone Password Breaker and see if the .rem files can be decrypted.
- The metadata files (like .dat, .key or BBThumb.dat) do not appear to be affected by the encryption despite having a .rem at the end of these files.

BlackBerry – Artifacts REMF

- Looking at the file header of a rem encrypted JPG image we can see the header in ASCII is "REMF", or 52 45 4D 46h.



IMG00005-20100422-0920.jpg.rem

```
     0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
 0: 52 45 4D 46 01 00 54 80 EA 0C D5 04 46 E0 2E E5   REMF..T€ê.Õ.Fà.å
16: 4E 42 DF F5 FF 61 C7 A4 27 78 CD A1 D5 E8 31 AE   NBßõÿaÇ¤'xÍ¡Õè1®
32: A6 7E 84 D7 E9 58 31 47 4A 5F FD 70 D8 A7 CB 79   ¦~„×éX1GJ_ýpØ§Ëy
48: B8 D8 FC 9D A5 E5 62 85 D2 9A 28 BA 1E BA 29 3C   ¸Øü.¥åb…Òš(º.º)<
64: 7C B2 E8 B8 8A 1D BF E5 14 22 EC 78 95 B0 89 91   |²è¸Š.¿å."ìx•°‰'
80: 5F 26 7D 2E 02 4B 44 6B 54 C8 B3 F1 C6 61 8A 99   _&}..KDkTÈ³ñÆaŠ™
```

BlackBerry – Artifacts Event Logs

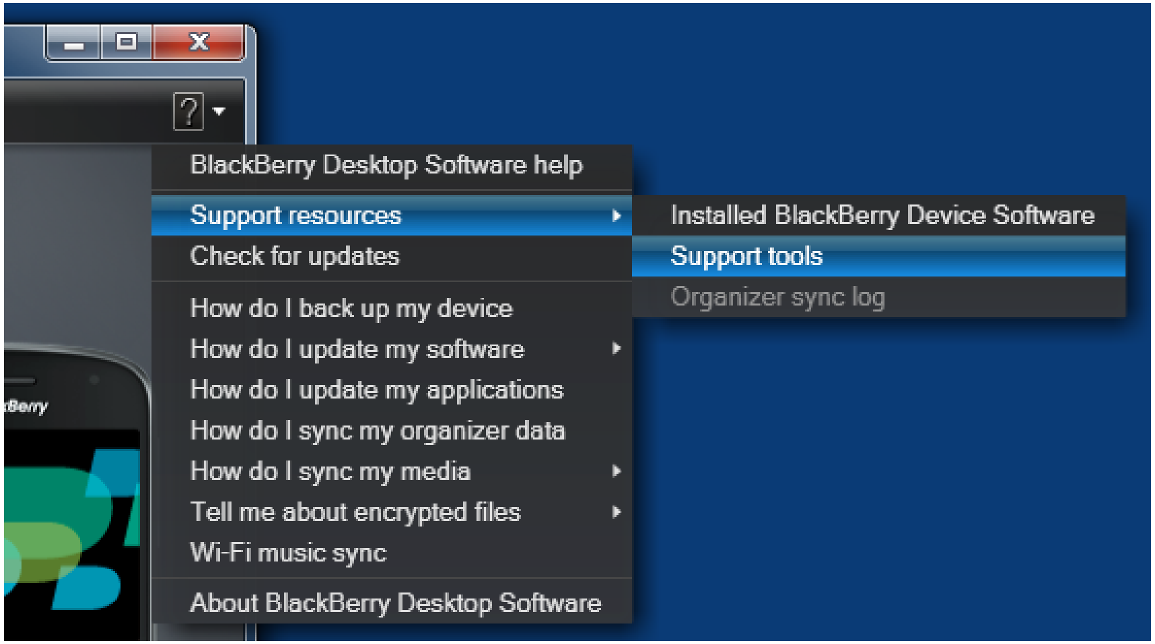
- Event Logs: Similar to Windows Event Logs, the BlackBerry® handheld device keeps event logs where applications and the BlackBerry® operating system can log information such as recently run events and system processes.
- To view the event log, press ALT and press key sequence LGLG from the main (home) screen, which should work on all BB devices with a QWERTY keyboard.

BlackBerry – Artifacts Event Logs

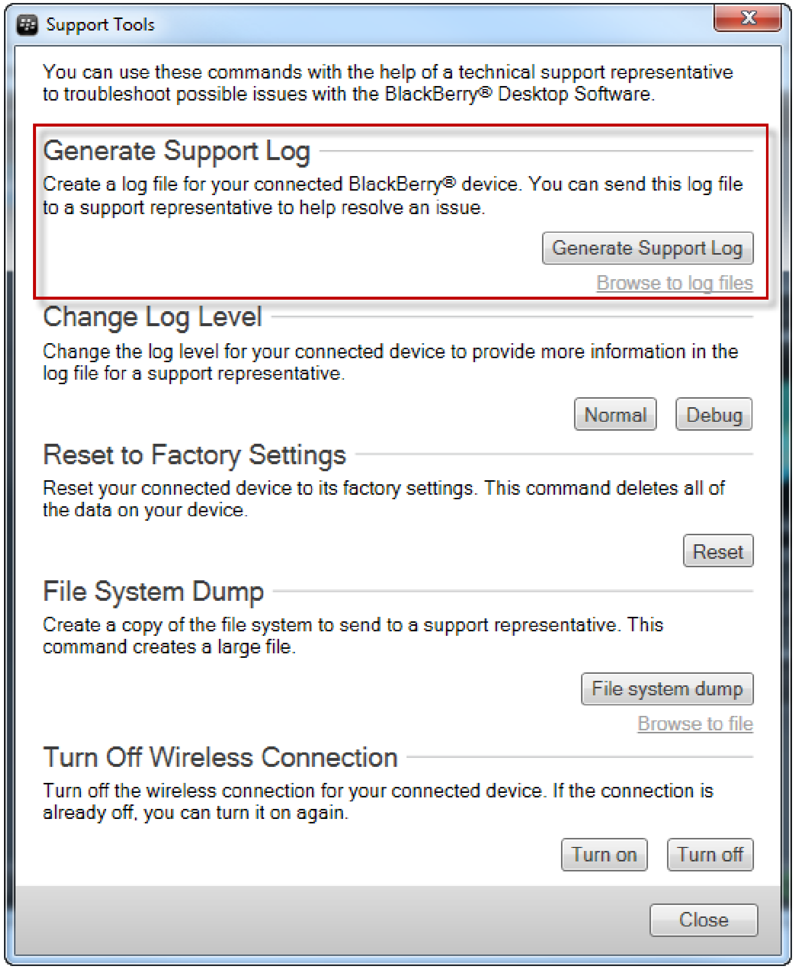
- Event Logs:
  - The main purpose of these logs is to assist developers with debugging applications or services on the BlackBerry® handheld device.
  - However, unintentionally, the Event Logs may also serve as a potential source of previously untapped digital evidence.
  - There has been no official documentation released by BlackBerry® that the author can find, regarding how to interpret or read the event log data.
  - This data is volatile in that logs can roll over within 24-48 hours depending upon device usage and maximum log size limit.

BlackBerry – Artifacts Event Logs

- Easiest way to get the event logs from a device is using BlackBerry Desktop Software: Then access Support tools from: **Help (?) -> Support Resources -> Support Tools -> Generate Support Log**


BlackBerry Desktop Software help
Support resources
Check for updates
How do I back up my device
How do I update my software
How do I update my applications
How do I sync my organizer data
How do I sync my media
Tell me about encrypted files
Wi-Fi music sync
About BlackBerry Desktop Software
Installed BlackBerry Device Software
Support tools
Organizer sync log

BlackBerry – Artifacts Event Logs



You can use these commands with the help of a technical support representative to troubleshoot possible issues with the BlackBerry® Desktop Software.

Generate Support Log

Create a log file for your connected BlackBerry® device. You can send this log file to a support representative to help resolve an issue.

Change Log Level

Change the log level for your connected device to provide more information in the log file for a support representative.

Reset to Factory Settings

Reset your connected device to its factory settings. This command deletes all of the data on your device.

File System Dump

Create a copy of the file system to send to a support representative. This command creates a large file.

Turn Off Wireless Connection

Turn off the wireless connection for your connected device. If the connection is already off, you can turn it on again.

June-19-14

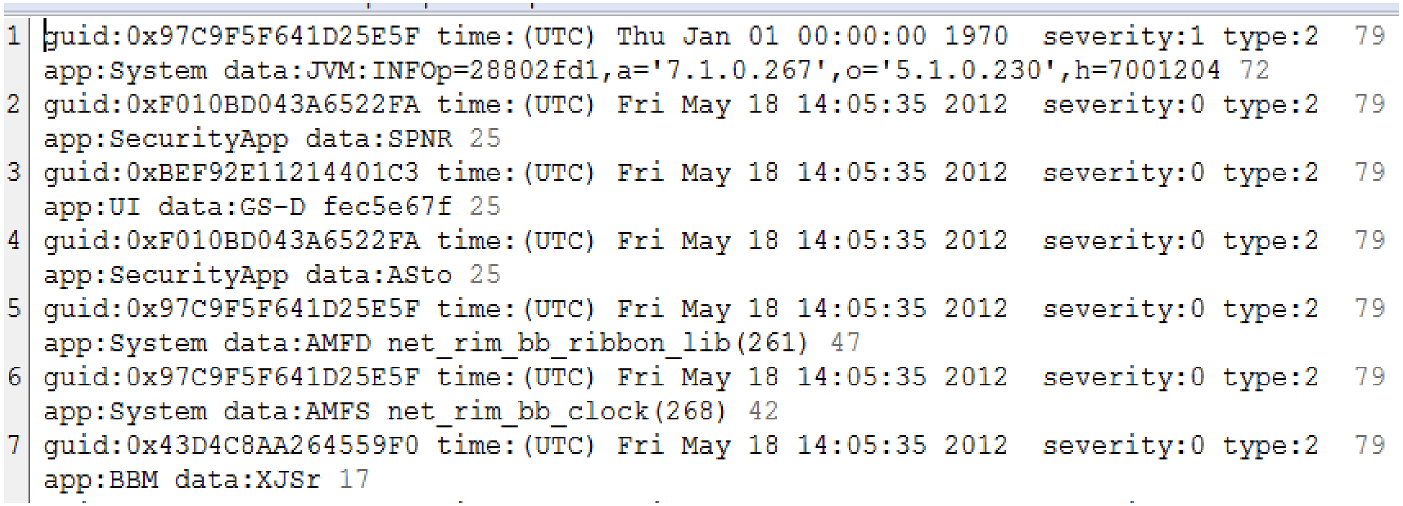
TEELtechnologies

BlackBerry – Artifacts Event Logs

- In doing research with fellow colleague, Sheran Gunasekera, we discovered that event logs retained call history data even after user deleted it from their device Phone Call app.
- http://chirashi.zenconsult.net/you-want-the-blackberry-event-log-beg-damnit/
- Only forensic tool that allows event log extraction during its logical stage is Oxygen Forensic Suite
- UFED will obtain this only through a physical dump, which is later parsed by UFED PA; the BlackBerry Event Log plugin must be run in order to review this data.

BlackBerry – Artifacts Event Logs

- The date/time values are local to the device user's time zone, in this case, Mountain Time (-7) GMT
- The application that generated the event log will be preceded by the value "app:", followed by the name of the application.
- GUID: 16 alphanumeric characters associated to an event or occurrence.



```
guid:0x97C9F5F641D25E5F time:(UTC) Thu Jan 01 00:00:00 1970  severity:1 type:2  79
app:System data:JVM:INFOp=28802fd1,a='7.1.0.267',o='5.1.0.230',h=7001204 72
guid:0xF010BD043A6522FA time:(UTC) Fri May 18 14:05:35 2012  severity:0 type:2  79
app:SecurityApp data:SPNR 25
guid:0xBEF92E11214401C3 time:(UTC) Fri May 18 14:05:35 2012  severity:0 type:2  79
app:UI data:GS-D fec5e67f 25
guid:0xF010BD043A6522FA time:(UTC) Fri May 18 14:05:35 2012  severity:0 type:2  79
app:SecurityApp data:ASto 25
guid:0x97C9F5F641D25E5F time:(UTC) Fri May 18 14:05:35 2012  severity:0 type:2  79
app:System data:AMFD net_rim_bb_ribbon_lib(261) 47
guid:0x97C9F5F641D25E5F time:(UTC) Fri May 18 14:05:35 2012  severity:0 type:2  79
app:System data:AMFS net_rim_bb_clock(268) 42
guid:0x43D4C8AA264559F0 time:(UTC) Fri May 18 14:05:35 2012  severity:0 type:2  79
app:BBM data:XJSr 17
```

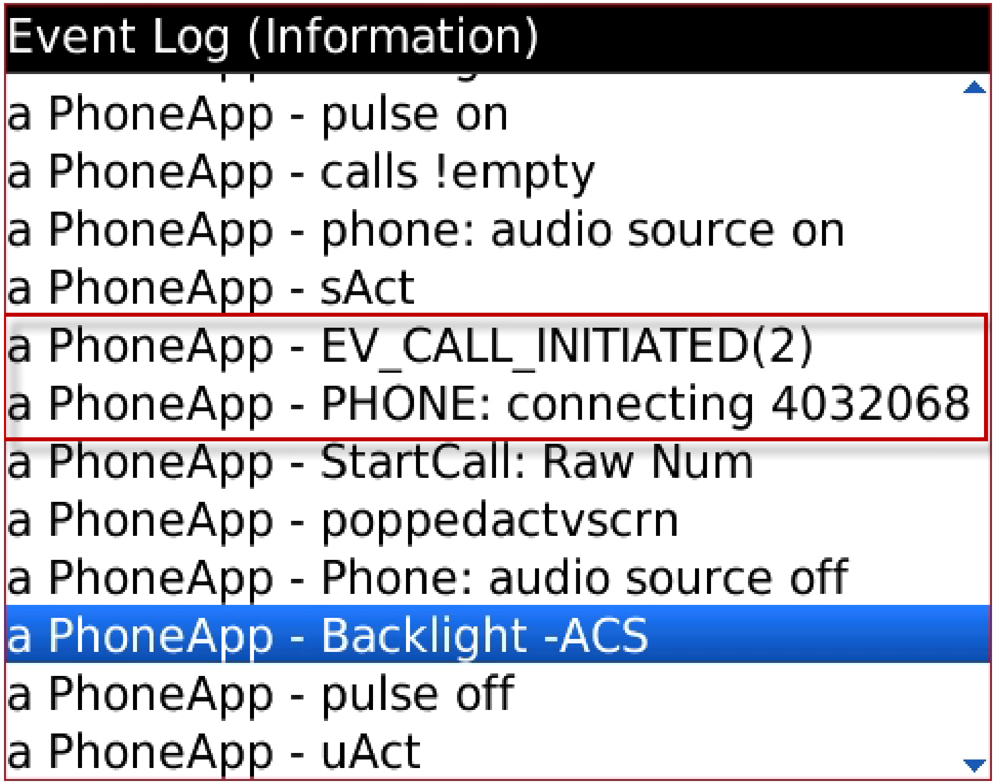
BlackBerry – Artifacts Event Logs

- The first two lines have consistently been observed by the author in all event log extractions on a BlackBerry® Bold 9700 (OS 5.0.0.862, Bundle 1446, Platform 5.1.0.175).
  - guid:0x97C9F5F641D25E5F time: Wed Dec 31 17:00:00 1969 severity:0 type:2 app:System
  - data:JVM:INFOp=33759974,a='5.0.0.862',o='5.1.0.175', h=4001507
    - The PIN # of device in hexadecimal is identified as p=33759974
    - OS version: a='5.0.0.862'
    - Platform: o='5.1.0.175'
    - Hardware ID: h=4001507

TEELtechnologies

BlackBerry – Artifacts Event Logs

- Evidence of call history in BlackBerry 9700 device event log



```
Event Log (Information)
a PhoneApp - pulse on
a PhoneApp - calls !empty
a PhoneApp - phone: audio source on
a PhoneApp - sAct
a PhoneApp - EV_CALL_INITIATED(2)
a PhoneApp - PHONE: connecting 4032068
a PhoneApp - StartCall: Raw Num
a PhoneApp - poppedactvscrn
a PhoneApp - Phone: audio source off
a PhoneApp - Backlight -ACS
a PhoneApp - pulse off
a PhoneApp - uAct
```

TEELtechnologies

BlackBerry – Artifacts Event Logs

```
guid:0xDDA0BC913B6AAEEC time: Thu Dec 02 20:53:56 2010  severity:0
type:2 app:PhoneApp data:StartCall: Raw Num

guid:0xDDA0BC913B6AAEEC time: Thu Dec 02 20:53:56 2010  severity:0
type:2 app:PhoneApp data:PHONE: connecting 4032068645

guid:0xE68C69BA0F2EBC4D time: Thu Dec 02 20:53:56 2010  severity:0 type:2
app:CC data:StartCall,"4032068645",0

guid:0xE68C69BA0F2EBC4D time: Thu Dec 02 20:53:56 2010  severity:0 type:2
app:CC data:Conf t+1

guid:0xE68C69BA0F2EBC4D time: Thu Dec 02 20:53:56 2010  severity:0 type:2
app:CC data:Ret,1

guid:0xDDA0BC913B6AAEEC time: Thu Dec 02 20:53:56 2010  severity:0
type:2 app:PhoneApp data:EV_CALL_INITIATED(1)

guid:0xE68C69BA0F2EBC4D time: Thu Dec 02 20:53:56 2010  severity:0 type:2
app:CC data:CallName,1,"false",""

guid:0xDDA0BC913B6AAEEC time: Thu Dec 02 20:53:56 2010  severity:0
type:2 app:PhoneApp data:sAct

guid:0xDDA0BC913B6AAEEC time: Thu Dec 02 20:53:56 2010  severity:0
type:2 app:PhoneApp data:phone: audio source on
```

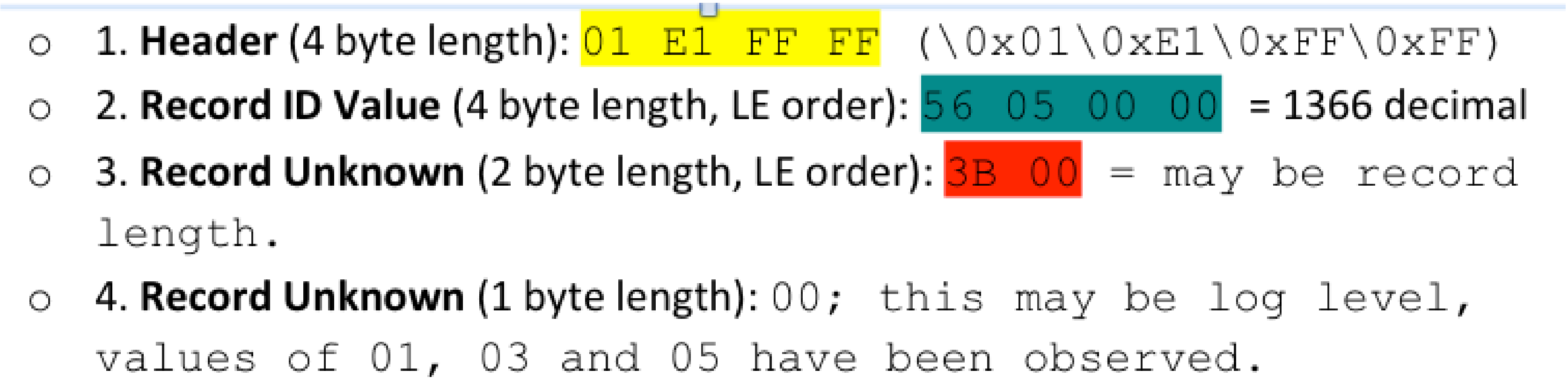
BlackBerry – Artifacts Event Logs

```
guid:0xE68C69BA0F2EBC4D time: Thu Dec 02 20:54:00 2010  severity:0 type:2 app:CC
data:CallName,1,"false",""

guid:0xE68C69BA0F2EBC4D time: Thu Dec 02 20:54:00 2010  severity:0 type:2 app:CC
data:CallName,1,"false",""

guid:0xE68C69BA0F2EBC4D time: Thu Dec 02 20:54:02 2010  severity:0 type:2 app:CC
data:Delivered,1

guid:0xDDA0BC913B6AAEEC time: Thu Dec 02 20:54:03 2010  severity:0 type:2
app:PhoneApp data:endcallbyuser 1

guid:0xE68C69BA0F2EBC4D time: Thu Dec 02 20:54:03 2010  severity:0 type:2 app:CC
data:StopCall,1

guid:0xDDA0BC913B6AAEEC time: Thu Dec 02 20:54:03 2010  severity:0 type:2
app:PhoneApp data:dAct

guid:0xDDA0BC913B6AAEEC time: Thu Dec 02 20:54:03 2010  severity:0 type:2
app:PhoneApp data:callsmpt; switchbg=false

guid:0xDDA0BC913B6AAEEC time: Thu Dec 02 20:54:03 2010  severity:0 type:2
app:PhoneApp data:PHONE: callId 1 stops listening.

guid:0xDDA0BC913B6AAEEC time: Thu Dec 02 20:54:03 2010  severity:0 type:2
app:PhoneApp data:uAct

guid:0xDDA0BC913B6AAEEC time: Thu Dec 02 20:54:03 2010  severity:0 type:2
app:PhoneApp data:EV_CALL_DISCONNECTED(1)
```

BlackBerry – Artifacts Event Logs

- BlackBerry Event log timestamps from a physical memory acquisition are stored as 4 byte length (32 bytes total), LE order

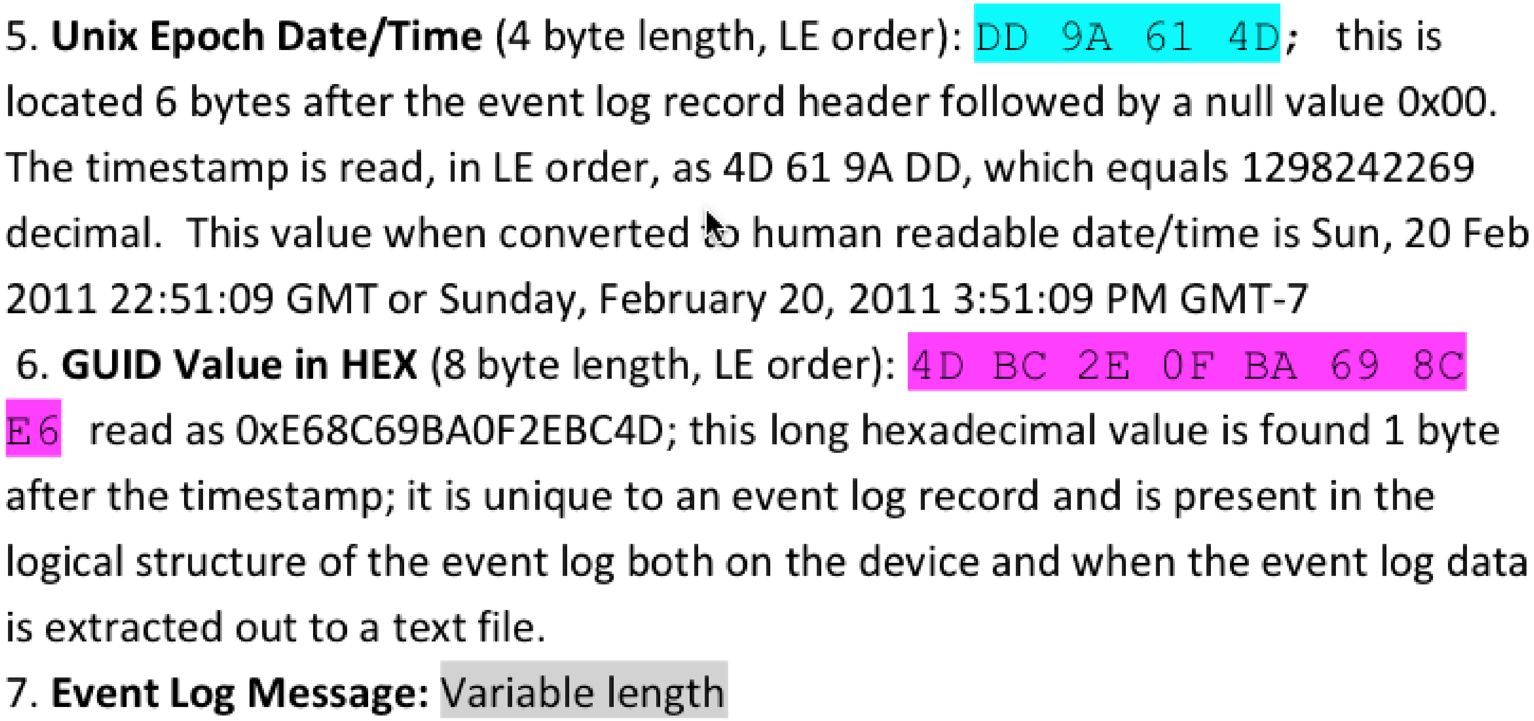
```
01 E1 FF FF 56 05 00 00 3B 00 DD 9A 61 4D 00 4D BC 2E
0F BA 69 8C E6 47 65 74 43 61 6C 6C 4E 75 6D 62 65 72
2C 38 2C 22 66 61 6C 73 65 22 2C 22 34 30 33 38 37 35
36 37 36 36 22 FF 2C 00 00 00 00 00 FF FF
```



- ○ 1. **Header** (4 byte length): `01 E1 FF FF (\0x01\0xE1\0xFF\0xFF)`
- ○ 2. **Record ID Value** (4 byte length, LE order): `56 05 00 00` = 1366 decimal
- ○ 3. **Record Unknown** (2 byte length, LE order): `3B 00 = may be record length.`
- ○ 4. **Record Unknown** (1 byte length): `00; this may be log level, values of 01, 03 and 05 have been observed.`

BlackBerry – Artifacts Event Logs

```
01 E1 FF FF 56 05 00 00 3B 00 DD 9A 61 4D 00 4D BC 2E
0F BA 69 8C E6 47 65 74 43 61 6C 6C 4E 75 6D 62 65 72
2C 38 2C 22 66 61 6C 73 65 22 2C 22 34 30 33 38 37 35
36 37 36 36 22 FF 2C 00 00 00 00 00 FF FF
```



5. **Unix Epoch Date/Time** (4 byte length, LE order): DD 9A 61 4D; this is located 6 bytes after the event log record header followed by a null value 0x00. The timestamp is read, in LE order, as 4D 61 9A DD, which equals 1298242269 decimal. This value when converted to human readable date/time is Sun, 20 Feb 2011 22:51:09 GMT or Sunday, February 20, 2011 3:51:09 PM GMT-7

6. **GUID Value in HEX** (8 byte length, LE order): 4D BC 2E 0F BA 69 8C E6 read as 0xE68C69BA0F2EBC4D; this long hexadecimal value is found 1 byte after the timestamp; it is unique to an event log record and is present in the logical structure of the event log both on the device and when the event log data is extracted out to a text file.

7. **Event Log Message:** Variable length

BlackBerry – Artifacts Event Logs

- **Real world example:**
  - A Bluetooth (BT) device has been paired with BlackBerry device. Question – 'Are you aware of any timestamp information related to the TIME the device was in use recorded on a BB?'
  - Answer: Check the event log – but I don't know what event log strings identify BT activity, as I have not had an opportunity to test this. Run the UFED PA plugin for BlackBerry event log.

BlackBerry – Artifacts Event Logs

- **Real world example:**
  - Results: LE entity had a UFED Physical memory acquisition of BlackBerry device and they found……
    - Bluetooth pairing is always logged! And in this case, the BT pairing was not observed, hence BT was not used during vehicular operation
    - Device in hand of driver while two calls were being manually placed 17 minutes before the 911 call.
    - Event log recorded the device has been manually slid open by the user (only certain types of BlackBerry 7 devices came in a slider form factor).

BlackBerry Malware

2006:

- First known BlackBerry® malware (August 2006), developed by security researcher, Jesse D'Aguanno, called BBProxy, which exploits the link of a BES connected device via its email server.

- A BES connected BlackBerry® has a constant connection to its corporate Local Area Network (LAN) which was used in this exploit, also making it difficult to detect the compromise into the corporate network as the data traffic is going through RIM’s encrypted tunnel between the BlackBerry® and its BES network.

2009: “spyware” that was pushed to Etisalat users as update, in the UAE by its telecommunications provider.

2010: Zeus: malware Trojan targeting the BlackBerry® and Symbian series 60 devices designed to capture banking credential login data.

BlackBerry Malware

Infection Vectors (IV):

- Can be grouped into two overall categories:

1. Wired: Memory Card, Synchronization between computer/laptop and device.

2. Wireless: BT, IR, SMS, MMS, IM, Email, PIN to PIN.

BlackBerry Malware

Commercial Spy Ware:

- There are numerous commercial spy ware programs that promote themselves as monitoring software (parental control, employee monitoring, GPS tracking):
  - MobiStealth
  - FlexiSpy
  - Mobile-Spy
  - eBlaster Mobile
  - Spy Bubble
  - Neo-Call
  - eStealth
  - Spyera

BlackBerry Malware: Installation/Infection Requirements

- As tested by the author on a BES and non BES device using eBlaster Mobile.
  - BES connected BlackBerry installation was unsuccessful, due to the BES and device policies in effect = VERY SECURE!
  - Need to have physical control of device.
  - If device is password protected, need to know the password.
  - BlackBerry OS 5, 6, 7 , there is a setting for having the device prompt the device user on application install; default is No.
  - Installation of spyware is either OTA or OTW.
  - The spyware will likely use a keystroke combination to invoke the application settings and configuration.

BlackBerry Malware: Detection Measures/Steps

Start simple and work your way through the continuum:

1. Device battery draining quicker than usual which cannot be attributed to battery or device malfunction. Device overheating may also be another symptom that presents along with battery exhaustion. This was experienced by Etilsalat compromised devices.

2. Review of device owner’s carrier billing records indicates a sudden data spike in data usage that is outside of the normal data usage over a given time period.

3. Does review of data traffic logs from carrier point to specific external IP address, email address or phone number?

4. Receipt of unusual emails from unknown recipients or presence of SMS and PIN messages not identifiable by the device owner; this data may represent control channel messages, which are control commands sent to the malware application.

BlackBerry Malware: Detection Measures/Steps

Data Analytics:

1. BlackBerry Event Log: may or may not present signs that device is infected. Applications are not required to write to the device event log.

2. Device running, dormant and hidden processes: May need to place device into EScreen or Engineering Screen mode in order to obtain this information.

3. Extraction and Review of System COD Modules and Files: A malware application can cause itself to be hidden from view. The FLAG_HIDDEN bit must be set to false in order for an application to hide itself from view in the applications list.

BlackBerry Malware: Detection Measures/Steps

Data Analytics:

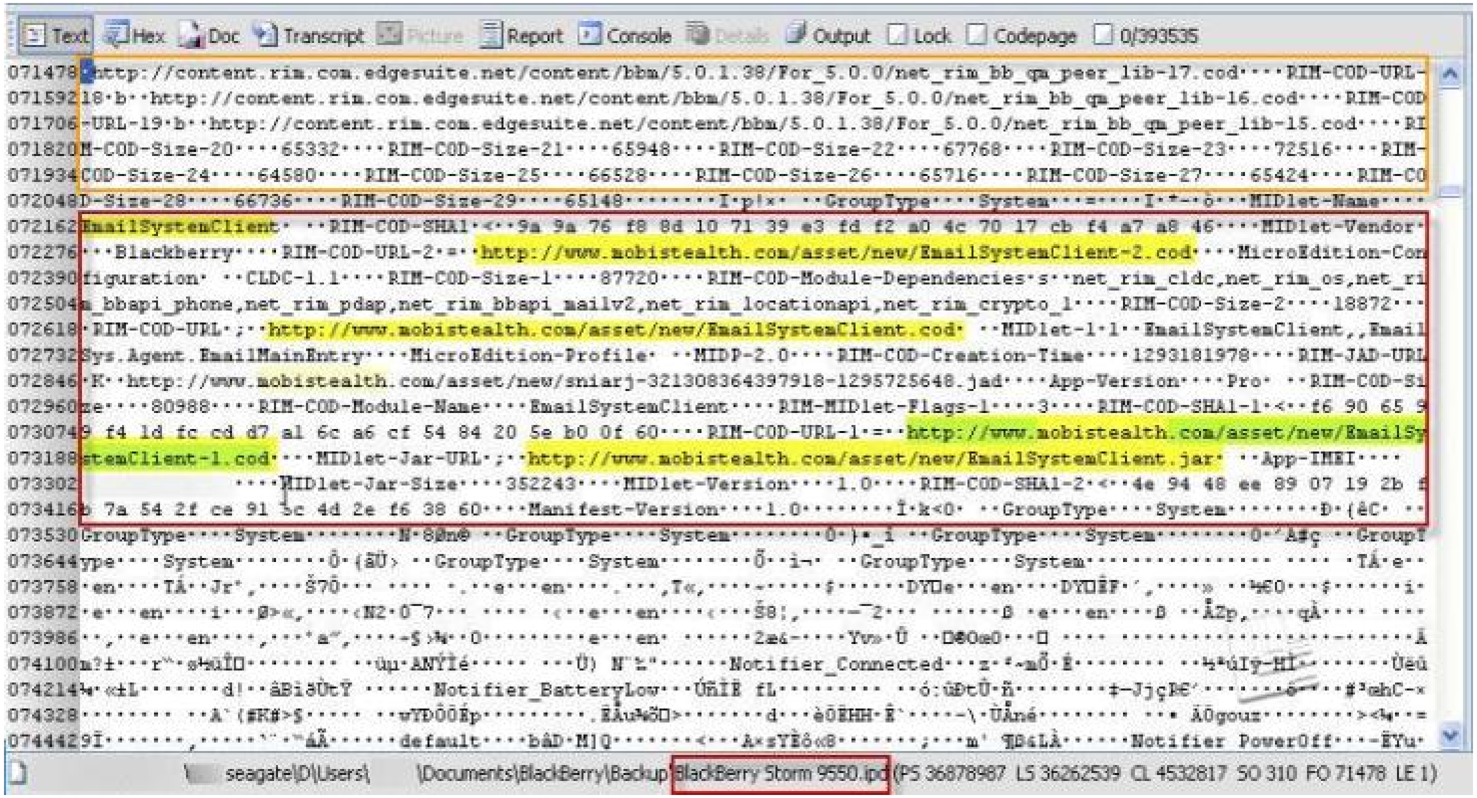
4. Extraction and analysis of device physical memory (if possible), IPD (backup file), as well as any associated memory and/or SIM card.

5. Review of each applications permission categories.

6. Device Malware Scan: may or may not be successful. Either through on device installation of a scanner or scan of acquired data.

BlackBerry Malware Case Study: MobiStealth Infection

- MobiStealth infected device: Screenshot of data resident from an Blackberry 9550 IPD file:



```
071478·http://content.rim.com.edgesuite.net/content/bbm/5.0.1.38/For_5.0.0/net_rim_bb_qm_peer_lib-17.cod····RIM-COD-URL-
07159218·b··http://content.rim.com.edgesuite.net/content/bbm/5.0.1.38/For_5.0.0/net_rim_bb_qm_peer_lib-16.cod····RIM-COD
071706-URL-19·b··http://content.rim.com.edgesuite.net/content/bbm/5.0.1.38/For_5.0.0/net_rim_bb_qm_peer_lib-15.cod····RI
071820M-COD-Size-20····65332····RIM-COD-Size-21····65948····RIM-COD-Size-22····67768····RIM-COD-Size-23····72516····RIM-
071934COD-Size-24····64580····RIM-COD-Size-25····66528····RIM-COD-Size-26····65716····RIM-COD-Size-27····65424····RIM-CO
072048D-Size-28····66736····RIM-COD-Size-29····65148········I·p!×· ··GroupType····System···=····I·*-·ò···MIDlet-Name····
072162EmailSystemClient· ··RIM-COD-SHA1·<··9a 9a 76 f8 8d 10 71 39 e3 fd f2 a0 4c 70 17 cb f4 a7 a8 46····MIDlet-Vendor·
072276···Blackberry····RIM-COD-URL-2·=··http://www.mobistealth.com/asset/new/EmailSystemClient-2.cod····MicroEdition-Con
072390figuration· ··CLDC-1.1····RIM-COD-Size-1····87720····RIM-COD-Module-Dependencies·s··net_rim_cldc,net_rim_os,net_ri
072504m_bbapi_phone,net_rim_pdap,net_rim_bbapi_mailv2,net_rim_locationapi,net_rim_crypto_1····RIM-COD-Size-2····18872···
072618·RIM-COD-URL·;··http://www.mobistealth.com/asset/new/EmailSystemClient.cod· ··MIDlet-1·1··EmailSystemClient,,Email
072732Sys.Agent.EmailMainEntry····MicroEdition-Profile· ··MIDP-2.0····RIM-COD-Creation-Time····1293181978····RIM-JAD-URL
072846·K··http://www.mobistealth.com/asset/new/sniarj-321308364397918-1295725648.jad····App-Version····Pro· ··RIM-COD-Si
072960ze····80988····RIM-COD-Module-Name····EmailSystemClient····RIM-MIDlet-Flags-1····3····RIM-COD-SHA1-1·<··f6 90 65 9
0730749 f4 1d fc cd d7 a1 6c a6 cf 54 84 20 5e b0 0f 60····RIM-COD-URL-1·=··http://www.mobistealth.com/asset/new/EmailSy
073188stemClient-1.cod····MIDlet-Jar-URL·;··http://www.mobistealth.com/asset/new/EmailSystemClient.jar· ··App-IMEI····
073302                ····MIDlet-Jar-Size····352243····MIDlet-Version····1.0····RIM-COD-SHA1-2·<··4e 94 48 ee 89 07 19 2b f
073416b 7a 54 2f ce 91 3c 4d 2e f6 38 60····Manifest-Version····1.0········Î·k<0· ··GroupType····System········Ð·(êC· ··
073530GroupType····System········N·8ØnΘ ··GroupType····System········Ô·)•_i ··GroupType····System········Ö·´A#ç ··GroupT
073644ype····System········Ô·(ãÜ› ··GroupType····System········Õ··ì¬· ··GroupType····System················ ···· ·TÁ·e··
073758·en····TÁ··Jr",····Š7Ö··· ···· ·.··e···en···.···,T«,···-····$······DYÐe···en····DYÐÊF·´,····» ··¼€0···$······i·
073872·e···en····i···Ø>«,····‹N2·Ö¯7··· ···· ·‹··e···en···‹···Š8¦,····—¯2··· ······ß ·e···en····ß ··ÅZp,····qÀ··· ····
073986··,··e···en····,···ª"',····-$›¼··0·········e···en· ······2æ¿-····Yv»·Û ··Ð®0æ0···□ ···· ··················-······Ã
074100m?±···r˜·ø½ùÎ□········ ··ùµ·ANŸÌé····· ···Ü) N¨±"······Notifier_Connected···z·f¬mÕ·Ë········ ··½ªúIÿ-HI·······Ùëû
074214¼·«±L·······d!··âBiðÙtŸ ······Notifier_BatteryLow···ÚñÌË fL·········· ··ó:ûÐtÛ·ñ·········‡-JjçÞ€´·········ó····#³æhC-×
074328········ ··A`(#K#>$····· ··wŸÐÔÖÉp·········.ËÅu¼ö□>········d···èÖËHH·Ê`····-\·ÙÅné········ ···• ÃÖgouz········><¼··=
0744429Ï·······,·····`¨·¯áÃ······default····bâD·M]Q········<···A×sYÈô«8·······;···m' ¶Ð¿LÀ······Notifier PowerOff···-ËYu·
```

[redacted] seagate\D\Users\ [redacted] \Documents\BlackBerry\Backup\BlackBerry Storm 9550.ipd (PS 36878987 LS 36262539 CL 4532817 SO 310 FO 71478 LE 1)

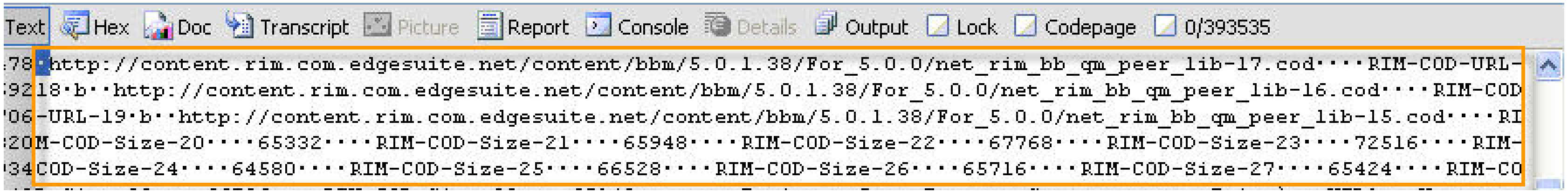
June-19-14

TEELtechnologies

BlackBerry Malware Case Study: MobiStealth Infection

Observation 1:

- What we are observing within the orange rectangle is device downloads from the internet for BlackBerry® Messenger (BBM).



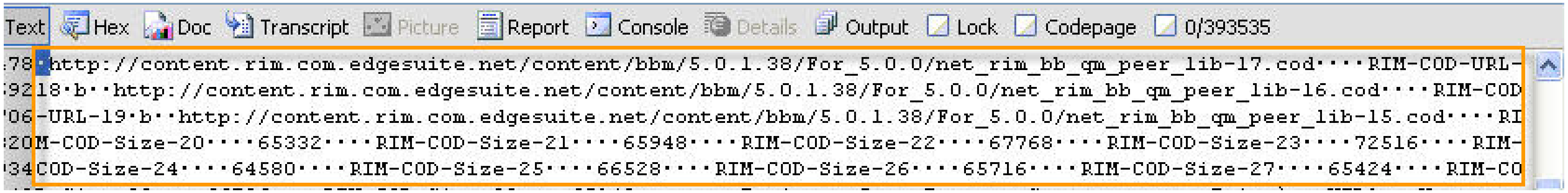
```
:78·http://content.rim.com.edgesuite.net/content/bbm/5.0.1.38/For_5.0.0/net_rim_bb_qm_peer_lib-17.cod····RIM-COD-URL-
;9218·b··http://content.rim.com.edgesuite.net/content/bbm/5.0.1.38/For_5.0.0/net_rim_bb_qm_peer_lib-16.cod····RIM-COD
'06-URL-19·b··http://content.rim.com.edgesuite.net/content/bbm/5.0.1.38/For_5.0.0/net_rim_bb_qm_peer_lib-15.cod····RI
:20M-COD-Size-20····65332····RIM-COD-Size-21····65948····RIM-COD-Size-22····67768····RIM-COD-Size-23····72516····RIM-
'34COD-Size-24····64580····RIM-COD-Size-25····66528····RIM-COD-Size-26····65716····RIM-COD-Size-27····65424····RIM-CO
```

June-19-14

BlackBerry Malware Case Study: MobiStealth Infection

Observation 2:

- What we are observing within the orange rectangle is device downloads from the internet for BlackBerry® Messenger (BBM).



```
:78·http://content.rim.com.edgesuite.net/content/bbm/5.0.1.38/For_5.0.0/net_rim_bb_qm_peer_lib-17.cod····RIM-COD-URL-
:9218·b··http://content.rim.com.edgesuite.net/content/bbm/5.0.1.38/For_5.0.0/net_rim_bb_qm_peer_lib-16.cod····RIM-COD
'06-URL-19·b··http://content.rim.com.edgesuite.net/content/bbm/5.0.1.38/For_5.0.0/net_rim_bb_qm_peer_lib-15.cod····RI
:20M-COD-Size-20····65332····RIM-COD-Size-21····65948····RIM-COD-Size-22····67768····RIM-COD-Size-23····72516····RIM-
'34COD-Size-24····64580····RIM-COD-Size-25····66528····RIM-COD-Size-26····65716····RIM-COD-Size-27····65424····RIM-CO
```

- Due to the large size of the file (and restrictions upon maximum file size for COD files) we see at least 27 COD files, based on RIM-COD-Size-27, related to BBM that vary in size from 65 KB to 72 KB.

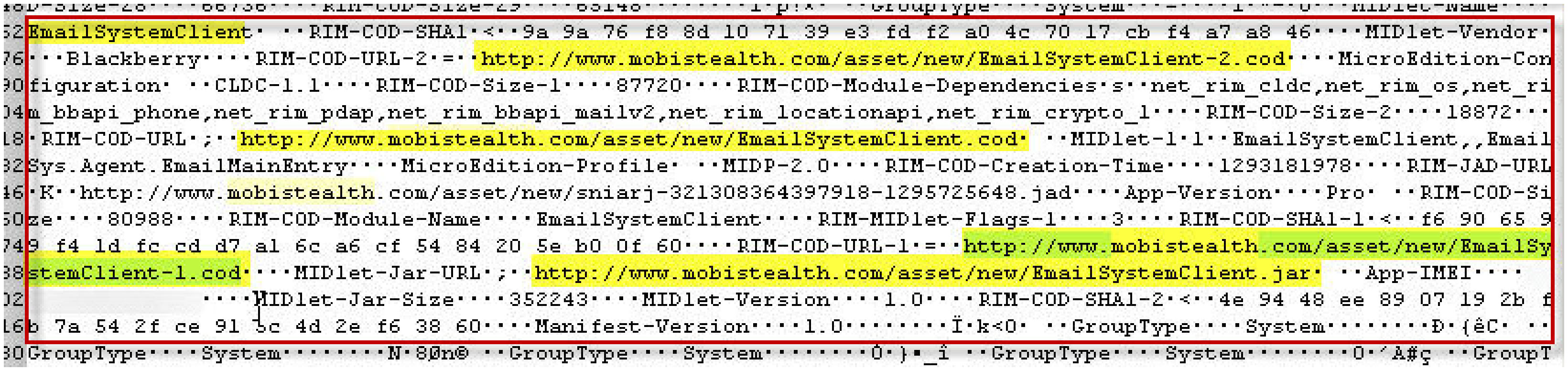
TEELtechnologies

BlackBerry Malware Case Study: MobiStealth Infection

Observation 3:

We see access from the device to a number of resources from URL link:

http://mobistealth.com/asset/new/



```
COD-Size-28····66736····RIM-COD-Size-29····63148·········1·p!^· ··GroupType····System····-·····1·"-·0···MIDlet-Name····
52 EmailSystemClient· ··RIM-COD-SHA1·<··9a 9a 76 f8 8d 10 71 39 e3 fd f2 a0 4c 70 17 cb f4 a7 a8 46····MIDlet-Vendor·
76 ···Blackberry····RIM-COD-URL-2·=··http://www.mobistealth.com/asset/new/EmailSystemClient-2.cod···MicroEdition-Con
90 figuration· ··CLDC-1.1····RIM-COD-Size-1····87720····RIM-COD-Module-Dependencies·s··net_rim_cldc,net_rim_os,net_ri
04 m_bbapi_phone,net_rim_pdap,net_rim_bbapi_mailv2,net_rim_locationapi,net_rim_crypto_1····RIM-COD-Size-2····18872···
18 ·RIM-COD-URL·;··http://www.mobistealth.com/asset/new/EmailSystemClient.cod· ··MIDlet-1·1··EmailSystemClient,,Email
32 Sys.Agent.EmailMainEntry····MicroEdition-Profile· ··MIDP-2.0····RIM-COD-Creation-Time····1293181978····RIM-JAD-URL
46 ·K··http://www.mobistealth.com/asset/new/sniarj-321308364397918-1295725648.jad····App-Version····Pro· ··RIM-COD-Si
50 ze····80988····RIM-COD-Module-Name····EmailSystemClient····RIM-MIDlet-Flags-1····3····RIM-COD-SHA1-1·<··f6 90 65 9
74 9 f4 1d fc cd d7 a1 6c a6 cf 54 84 20 5e b0 0f 60····RIM-COD-URL-1·=··http://www.mobistealth.com/asset/new/EmailSy
38 stemClient-1.cod····MIDlet-Jar-URL·;··http://www.mobistealth.com/asset/new/EmailSystemClient.jar· ··App-IMEI····
02                 ····MIDlet-Jar-Size····352243····MIDlet-Version····1.0····RIM-COD-SHA1-2·<··4e 94 48 ee 89 07 19 2b f
16 b 7a 54 2f ce 91 5c 4d 2e f6 38 60····Manifest-Version····1.0·········Ï·k<0· ··GroupType····System········Ð·{êC· ··
30 GroupType····System········N·8Øn® ··GroupType····System········Ö·}▪_î ··GroupType····System········0·´A#ç ··GroupT
```

June-19-14

BlackBerry Malware Case Study: MobiStealth Infection

Observation 4:

To verify if the resources still reside at the specific URL’s visit http://mobistealth.com/asset/new/EmailSystemClient.cod;

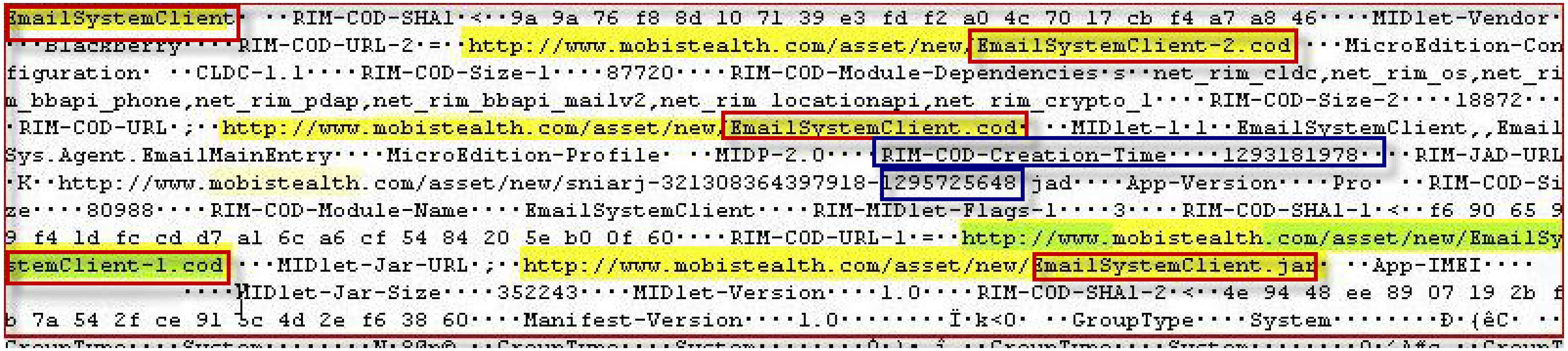
Result: total of three COD files that make up the entire MobiStealth application for this specific device:

- EmailSystemClient.cod
- EmailSystemClient-1.cod
- EmailSystemClient-2.cod

BlackBerry Malware Case Study: MobiStealth Infection

Observation 5: Artifact Identification:

- Multiple COD filenames that identify the actual name of the rogue software that should also be observed on the infected host.
- Creation Times in Unix epoch time format
- SHA1 hash values of COD files
- IMEI value of host device (sanitized in the screenshot)

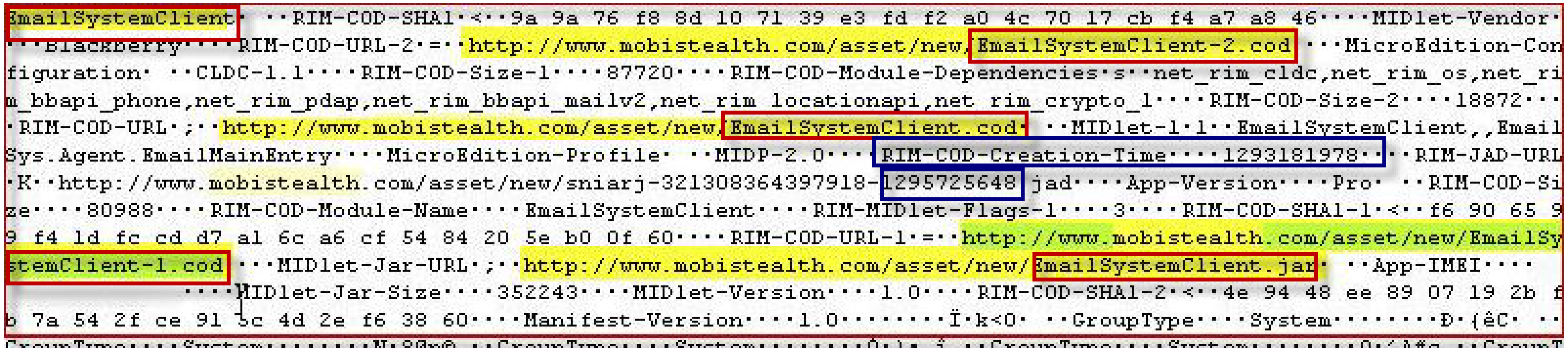


```
EmailSystemClient· ··RIM-COD-SHA1·<··9a 9a 76 f8 8d 10 71 39 e3 fd f2 a0 4c 70 17 cb f4 a7 a8 46····MIDlet-Vendor·
···BlackBerry····RIM-COD-URL-2·=··http://www.mobistealth.com/asset/new/EmailSystemClient-2.cod ···MicroEdition-Con
figuration· ··CLDC-1.1····RIM-COD-Size-1····87720····RIM-COD-Module-Dependencies·s··net_rim_cldc,net_rim_os,net_ri
m_bbapi_phone,net_rim_pdap,net_rim_bbapi_mailv2,net_rim locationapi,net rim_crypto_1····RIM-COD-Size-2····18872···
·RIM-COD-URL·;··http://www.mobistealth.com/asset/new/EmailSystemClient.cod· ··MIDlet-1·1··EmailSystemClient,,Email
Sys.Agent.EmailMainEntry····MicroEdition-Profile· ··MIDP-2.0····RIM-COD-Creation-Time····1293181978····RIM-JAD-URL
·K··http://www.mobistealth.com/asset/new/sniarj-321308364397918-1295725648 jad····App-Version····Pro· ··RIM-COD-Si
ze····80988····RIM-COD-Module-Name····EmailSystemClient····RIM-MIDlet-Flags-1····3····RIM-COD-SHA1-1·<··f6 90 65 9
9 f4 1d fc cd d7 a1 6c a6 cf 54 84 20 5e b0 0f 60····RIM-COD-URL-1·=··http://www.mobistealth.com/asset/new/EmailSy
stemClient-1.cod ···MIDlet-Jar-URL·;··http://www.mobistealth.com/asset/new/EmailSystemClient.jar· ··App-IMEI····
            ····MIDlet-Jar-Size····352243····MIDlet-Version····1.0····RIM-COD-SHA1-2·<··4e 94 48 ee 89 07 19 2b f
b 7a 54 2f ce 91 5c 4d 2e f6 38 60····Manifest-Version····1.0········Ï·k<0· ··GroupType····System········Đ·{êC· ··
```

BlackBerry Malware Case Study: MobiStealth Infection

Observation 5: Artifact Identification:

- Multiple COD filenames that identify the actual name of the rogue software that should also be observed on the infected host.
- Creation Times in Unix epoch time format
- SHA1 hash values of COD files
- IMEI value of host device (sanitized in the screenshot)



```
EmailSystemClient· ··RIM-COD-SHA1·<··9a 9a 76 f8 8d 10 71 39 e3 fd f2 a0 4c 70 17 cb f4 a7 a8 46····MIDlet-Vendor·
···BlackBerry····RIM-COD-URL-2·=··http://www.mobistealth.com/asset/new/EmailSystemClient-2.cod ···MicroEdition-Con
figuration· ··CLDC-1.1····RIM-COD-Size-1····87720····RIM-COD-Module-Dependencies·s··net_rim_cldc,net_rim_os,net_ri
m_bbapi_phone,net_rim_pdap,net_rim_bbapi_mailv2,net_rim locationapi,net rim_crypto_1····RIM-COD-Size-2····18872···
·RIM-COD-URL·;··http://www.mobistealth.com/asset/new/EmailSystemClient.cod· ··MIDlet-1·1··EmailSystemClient,,Email
Sys.Agent.EmailMainEntry····MicroEdition-Profile· ··MIDP-2.0····RIM-COD-Creation-Time····1293181978····RIM-JAD-URL
·K··http://www.mobistealth.com/asset/new/sniarj-321308364397918-1295725648 jad····App-Version····Pro· ··RIM-COD-Si
ze····80988····RIM-COD-Module-Name····EmailSystemClient····RIM-MIDlet-Flags-1····3····RIM-COD-SHA1-1·<··f6 90 65 9
9 f4 1d fc cd d7 a1 6c a6 cf 54 84 20 5e b0 0f 60····RIM-COD-URL-1·=··http://www.mobistealth.com/asset/new/EmailSy
stemClient-1.cod ···MIDlet-Jar-URL·;··http://www.mobistealth.com/asset/new/EmailSystemClient.jar· ··App-IMEI····
                ····MIDlet-Jar-Size····352243····MIDlet-Version····1.0····RIM-COD-SHA1-2·<··4e 94 48 ee 89 07 19 2b f
b 7a 54 2f ce 91 5c 4d 2e f6 38 60····Manifest-Version····1.0········Ï·k<0· ··GroupType····System········Ð·{êC· ··
```

June-19-14

BlackBerry Malware Case Study: MobiStealth Infection

Investigator also provided this snippet to me:

- Keyword search in EnCase 6.x of hard drive image for “mobistealth” shows hits in unallocated space (of the suspect hard drive) that appear like the following:

```
··GET /bbchat_history.php?cmd=search
    HTTP/1.1  Host:www.mobistealth.com  User-Agent: Mozilla/5.0
    (Windows ; U; Windows NT 6.1; en-US; rv:1.9.2.13)
    Gecko/20101203 Firefox/3.6.13  Accept:
    text/html,application/xhtml+
    xml,application/xml;q=0.9,*/*;q=0.8  Accept-Language: en-
    us,en;q=0.5  Accept-Encoding: gzip,deflate  Accept- Charset:
    ISO-8859-1,utf-8;q=0.7,*;q=0.7  Keep-Alive: 115  Connection:
    keep-
    alive  Referer: http://www.mobistealth.com/sms_history.php?cmd=
    search  Cookie: PHPSESSID=1c1aq7t5pu8l9c450ta9duh4i6;
    MobistealthVisitor=32c06 ffa5972c8cc8e00b0b86a1257cc;
    SERVERID=web2;
    __utma=192346166.1897014666.1297088891.1297088891.1297088891.1;
      __utmb=192346166.4.10.1297088891; __utmc=192346166;
    __utmz=192346166.1297088891.1.1.utmcsr=(direct)|utmccn=(
    direct)|utmcmd=(none)                    ö£n;an·€··hn»t·ì·f–ØŠ¸õ˜
    ›óçKÉ:Î·ý|·,é>9·¹DœXð|Q_‘×·œ5¶%•¼û9?·P·ð¾ ñ)·Sm ƒðÕZ3¸æã‡ÈÂè·ù
    >·zHÂéš¡¹‡”æÊ L =ÎÃPÝz!›rÓo1ª·™´·4 Ö? qÆÝ·· Ë
```

June-19-14

BlackBerry Malware Case Study: MobiStealth Infection

- GET request using likely a Mozilla type browser; user has logged into mobistealth user account and is accessing sms history and bbm chat.

```
··GET /bbchat_history.php?cmd=search
  HTTP/1.1  Host:www.mobistealth.com  User-
  Agent: Mozilla/5.0 (Windows ; U; Windows NT
  6.1; en-US; rv:1.9.2.13) Gecko/20101203
  Firefox/3.6.13  Accept:

 Referer: http://www.mobistealth.com/sms_his
  tory.php?cmd=search  Cookie:
  PHPSESSID=1c1aq7t5pu8l9c450ta9duh4i6;
  MobistealthVisitor=32c06
  ffa5972c8cc8e00b0b86a1257cc; SERVERID=web2;
```

BlackBerry Malware Case Study: MobiStealth Infection

- UTM = Urchin Tracking Module

- Google Cookie Data:
  - various types of utm values: utm[a|b|c|z]

- Anatomy of _umta:
  - __utma=<domain hash>.<unique visitor id>.<timstamp of first visit>.<timestamp of previous (most recent) visit>.<timestamp of current visit>.<visit count>

BlackBerry Malware Case Study: MobiStealth Infection

- __utma=<**domain hash**>.<**unique visitor id**>.<**timstamp of first visit**>.<**timestamp of previous (most recent) visit>.<timestamp of current visit**>.**<visit count>**

- __utma=**192346166**.**1897014666**.**1297088891**.**1297088891.1297088891**.**1**; __utmb=192346166.4.10.1297088891; __utmc=192346166; __utmz=192346166.1297088891.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)

<domain hash>.192346166

<unique visitor id>.1897014666

<timstamp of first visit>.1297088891 = Mon, 07 February 2011 14:28:11. UTC = date of visit to Mobistealth

<timestamp of previous (most recent) visit>.1297088891

<timestamp of current visit>. 1297088891

<visit count> 1

BlackBerry Malware Case Study: MobiStealth Infection

Summary

1. Suspect’s computer hard drive contains a BlackBerry backup IPD file of the victim’s BlackBerry device, which shows her device accessing and downloading (OTA install) the mobistealth software as segmented files.

2.Suspect’s computer hard drive shows, that computer was used to login to a mobistealth user account where the BBM chat and SMS history web pages were accessed.

3. If the ‘infected’ device has been analyzed, it should show the presence of the EmailSystemClient.cod file.

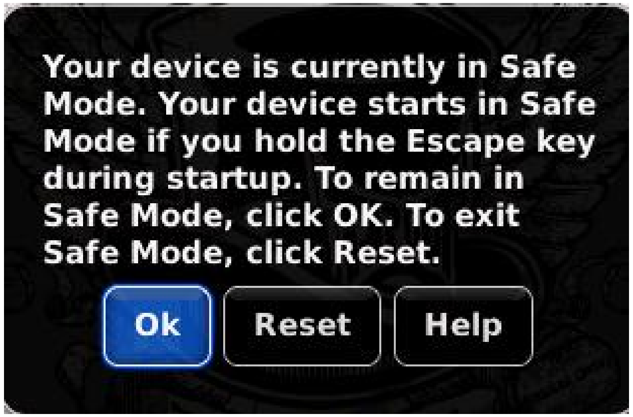
BlackBerry Safe Mode/JVM Error Codes

Safe mode:

- **can be used to prevent third-party applications from running automatically.**
- **Safe mode is designed to allow troubleshooting or remove any unwanted applications.**
- **only works on OS 4.6 and higher.**

Steps to enabling safe mode:

- **Remove and reinsert the BlackBerry® smartphone battery.**
- **When the red light-emitting diode (LED) light goes out, press and hold the Escape key as the BlackBerry® smartphone is loading. See KB05470 for the location of the Escape key.**
- **When the dialog box appears, click OK.**



Your device is currently in Safe Mode. Your device starts in Safe Mode if you hold the Escape key during startup. To remain in Safe Mode, click OK. To exit Safe Mode, click Reset.

BlackBerry Safe Mode/JVM Error Codes

JVM Error Codes

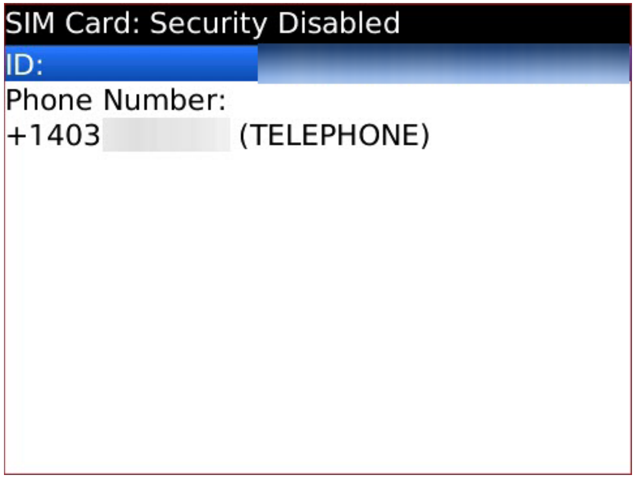
- It is possible for JVM Errors to occur when interacting with the underlying BlackBerry® smartphone hardware that is no longer operating as expected.
- An example of such a failure would be the corruption of the physical flash memory.
- JVM errors may also occur as a result of software related issues.
- Reloading BlackBerry® Device Software is not option for a device that is considered to have evidence on it.
- Safe Mode may help you resolve Java Errors
- If Safe Mode does not work, then your only recourse is a chip off solution (no guarantee of success).

BlackBerry: SIM Number Spoofing

Could one edit the phone number assigned to the SIM and spoof's one number to appear as something different through the Edit Phone Number feature?

The author did perform some limited testing on a BlackBerry Bold 9700; OS 6.0.0.448; Platform 6.6.0.124 in May 2012.

- In OS 6 this is found under: Options -> Device -> Advanced System Settings -> SIM Card.
- Shows SIM ICCID and Phone Number assigned to SIM.



SIM Card: Security Disabled

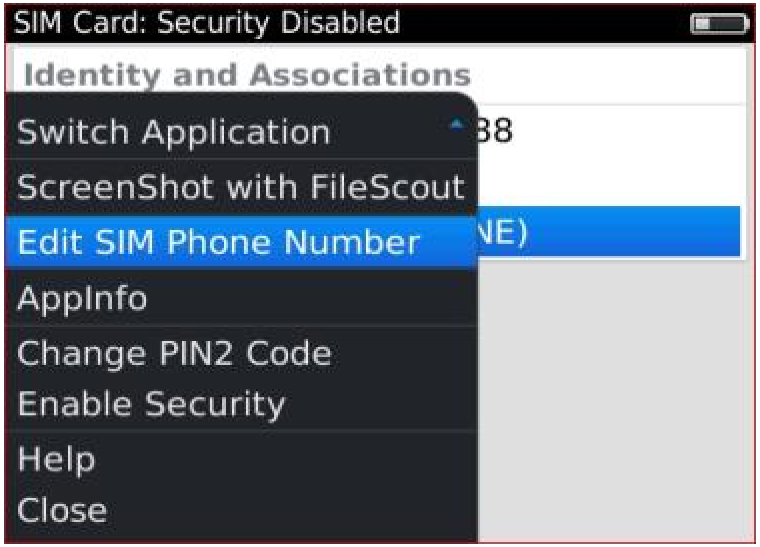
ID: [redacted]

Phone Number:
+1403 [redacted] (TELEPHONE)

June-19-14

BlackBerry: SIM Number Spoofing

Press Menu key to invoke the context options window: Access the Edit SIM Phone Number function: Options -> Device -> Advanced System Settings -> SIM Card -> Menu Key -> Edit SIM Phone Number


SIM Card: Security Disabled

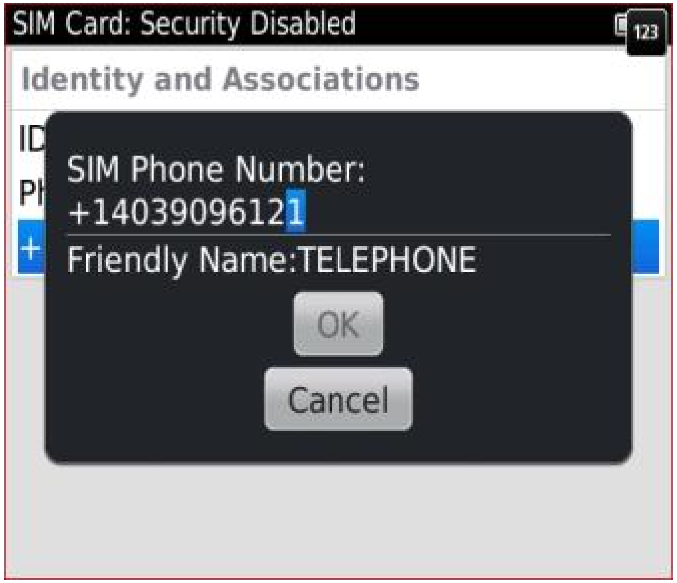
Identity and Associations

June-19-14

TEELtechnologies

BlackBerry: SIM Number Spoofing

Phone number is changed by 1 digit: from +14039096120 to +14039096121

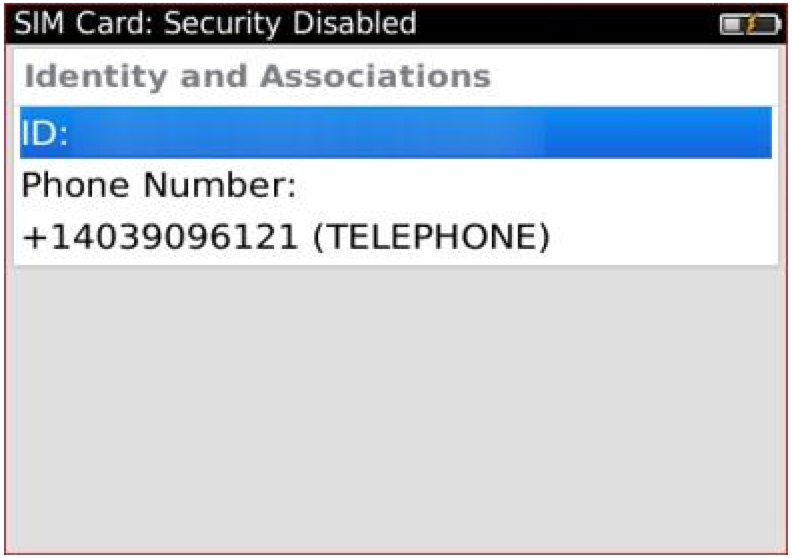


SIM Card: Security Disabled

Identity and Associations

SIM Phone Number: +14039096121

Friendly Name:TELEPHONE



SIM Card: Security Disabled

Identity and Associations

ID:

Phone Number:

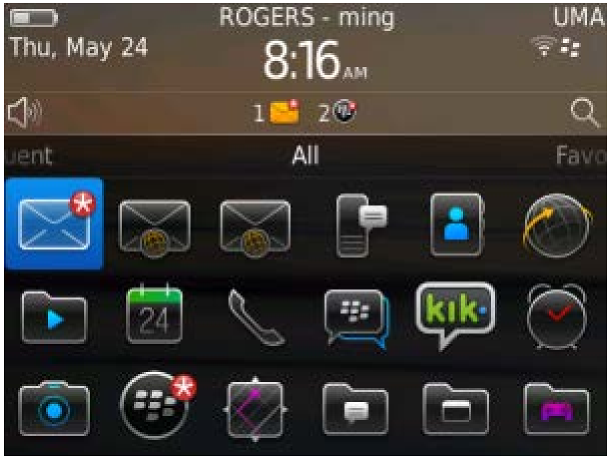
+14039096121 (TELEPHONE)

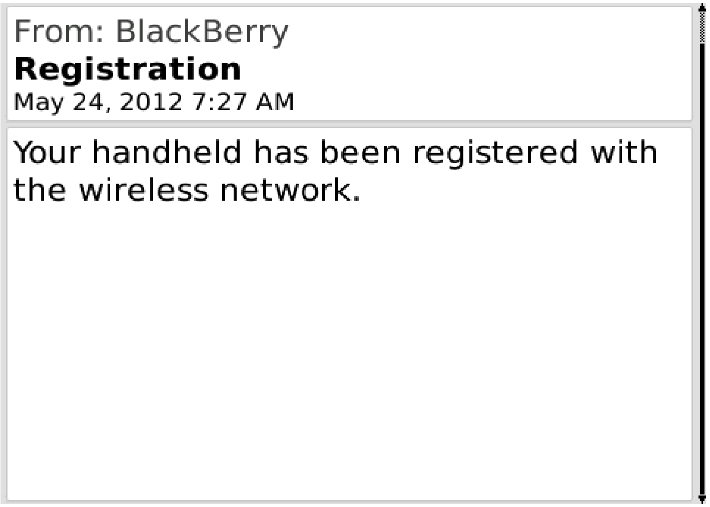
June-19-14

TEELtechnologies

BlackBerry: SIM Number Spoofing

New message indicator also appears after edit of SIM phone number.





From: BlackBerry

Registration

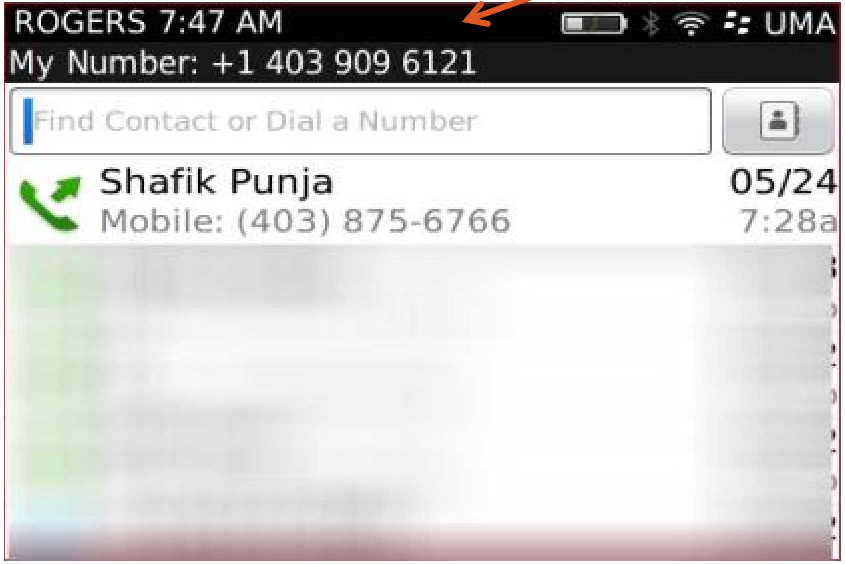
May 24, 2012 7:27 AM

Your handheld has been registered with the wireless network.

June-19-14

BlackBerry: SIM Number Spoofing

In the call history screen what appears on the author's private BlackBerry® device as My Number is: +1 403 909 6121 and not the carrier assigned number of +1 403 909 6120.



ROGERS 7:47 AM UMA

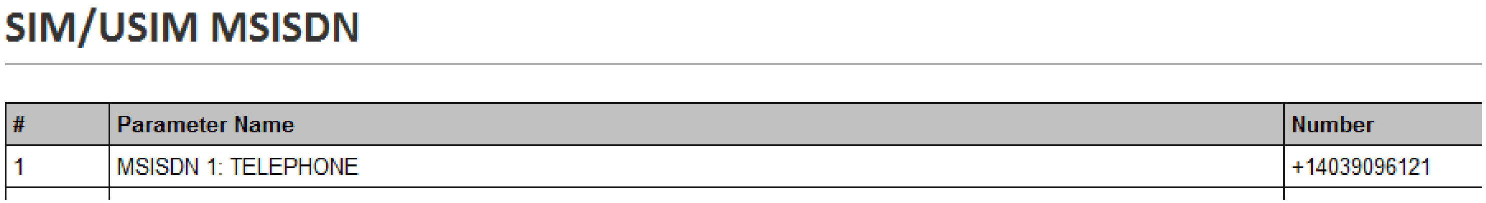
My Number: +1 403 909 6121

Shafik Punja 05/24
Mobile: (403) 875-6766 7:28a

June-19-14

BlackBerry: SIM Number Spoofing

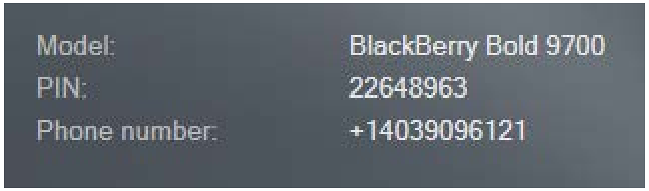
A screenshot from a SIM extraction performed only with Cellebrite UFED shows the MISDN value as +1 403 909 6121. This shows that the Edit SIM Phone Number function, through the device, will cause a write to occur to the SIM.



SIM/USIM MSISDN

#	Parameter Name	Number
1	MSISDN 1: TELEPHONE	+14039096121

Connecting the device (with SIM in the device) to BlackBerry Desktop Software, it shows the edited phone number of +1 403 909 6121.



Model:	BlackBerry Bold 9700
PIN:	22648963
Phone number:	+14039096121

BlackBerry: SIM Number Spoofing

- Calls from this number spoofed device, show up as the original number!
- The device event log was extracted, and shows that a phone number change did take place.

BlackBerry 10

- First released in January 2013 as a Z10; this was followed by Q10 (keyboard) and then Z30.
- The BB 10 device essentially comes with 16GB internal flash memory, 2GB RAM and accepts up to a 32GB memory card and contains the same basic hardware infrastructure commonly observed in smartphones.

BlackBerry 10 - Hardware

- The Z10 model is touch screen, and comes in several sub-variants for its baseband configurations.
- STL100-[1-4]
  - The STL100-1, which is non-LTE, uses the ST-Ericsson Thor chipset with TI OMAP; this uses a PowerVR SGX 544 GPU.
  - The STL100-[2-4] variants, which are all LTE, use the Qualcomm MSM8960 (Qualcomm Snapdragon S4 Plus) chipset which are dual core 1.5GHz and contain an Adreno 225 GPU.

Source: Ralf-Philipp Weinmann., BlackBerry 10 OS from a security perspective, University of Luxembourg, black hat USA 2013 Presentation.

BlackBerry 10 - OS

- Runs the QNX (Unix) based operating system and is considered a micro kernel architecture for embedded systems in comparison to the Monolithic Android Kernel.
- The function of the micro kernel
  - handle execution of processes passed to it by the process manager;
  - it does not deal with the file system
  - and does not contain device drivers.

BlackBerry 10 - OS

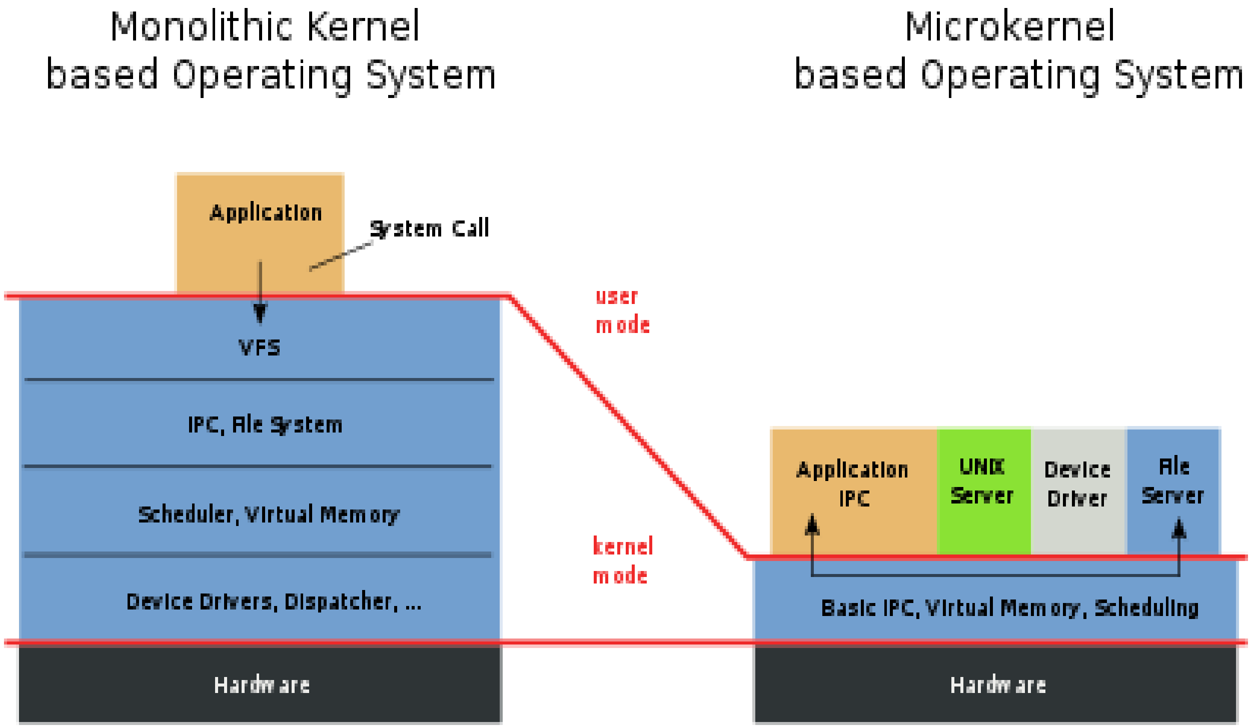


**Image Source:* http://upload.wikimedia.org/wikipedia/commons/thumb/6/67/OS-structure.svg/450px-OS-structure.svg.png from http://en.wikipedia.org/wiki/Microkernel

BlackBerry 10 - OS

- Within the logical file system, QNX is mounted at /pps.
- A number of different functions are running on top of kernel and user land [4]:
  - PIM (Personal Information Manager) certain parts of the PIM are written in Python.
  - Adobe Air and QT are used in some of the apps like Weather app.
  - Android 2.3 Java runtime is present: but you need to convert APK files into BAR files in order to run Android app in BB OS 10.

Sources:

1. Antukh, A., BlackBerry Z10 Research Primer: Dissecting BlackBerry 10 – An initial analysis, SEC Consult Vulnerability Lab, Vienna, 05/2013, V 1.0 Whitepaper

2. Plasket, A., Is BlackBerry Dead? An Introduction to Blackberry 10 Security (BB10 - QNX), MWR InfoSecurity, PowerPoint Presentation

3. Lanier, Z., & Nell, B., Voight-Kampff'ing The BlackBerry PlayBook, Intrepidus Group Mobile Security, PowerPoint Presentation

Blog: http://blog.n0where.org/2012/04/voight-kampff-blackberry-playbook.html

4. Ralf-Philipp Weinmann., BlackBerry 10 OS from a security perspective, University of Luxembourg, black hat USA 2013 Presentation.

BlackBerry 10 - OS

QNX firmware contains the following unique artifacts from analysis perspective [1,2]:

- ***File header: mfcq* (ASCII), 6d 66 63 71h**
- ***Partition header: qcfp* (ASCII), 71 63 66 70h**
  - There are a number of partitions that follow the follow the file header; in the BlackBerry Playbook for example, 5 QCFP partitions are observed in the firmware.

Sources:

1. Antukh, A., BlackBerry Z10 Research Primer: Dissecting BlackBerry 10 – An initial analysis, SEC Consult Vulnerability Lab, Vienna, 05/2013, V 1.0 Whitepaper

2. Lanier, Z., & Nell, B., Voight-Kampff'ing The BlackBerry PlayBook, Intrepidus Group Mobile Security, PowerPoint Presentation

Blog: http://blog.n0where.org/2012/04/voight-kampff-blackberry-playbook.html

BlackBerry 10 – OS Permissions

- Permissions in QNX in BB OS 10 are handled by 'authman' which is located at /etc/authman/sys.acl [2,3,4].
- Applications are installed to /apps and they cannot read another application's code or data; this is controlled by 'authman' [2].
- Application permissions are handled by authman: permission categories allow, prompt and deny [2,3].
  - Allow: identified apps can use the permission assigned to them.
  - Prompt: the app must prompt the user first.
  - Deny: the app cannot use a capability.

Sources:
2. Plasket, A., Is BlackBerry Dead? An Introduction to Blackberry 10 Security (BB10 - QNX), MWR InfoSecurity, PowerPoint Presentation
3. Lanier, Z., & Nell, B., Voight-Kampff'ing The BlackBerry PlayBook, Intrepidus Group Mobile Security, PowerPoint Presentation
Blog: http://blog.n0where.org/2012/04/voight-kampff-blackberry-playbook.html
4. Ralf-Philipp Weinmann., BlackBerry 10 OS from a security perspective, University of Luxembourg, black hat USA 2013 Presentation.

BlackBerry 10 – Security

1. The BlackBerry device contains the same foundation of security feature as observed in BB OS 7:

- Password Protection
- Encryption for device and/or memory card
- Device wipe for device and/or memory card

2. BlackBerry ID: The device user is asked to create or sign in with their BlackBerry ID before they can go any further into the device on first setup.

3. BlackBerry Protect: This comes installed as part of the operating system and a BlackBerry ID is required for this feature to work. This allows device geo location, device wiping, and device backup/restore.

BlackBerry 10 – Security

4. Application Permissions: This lets the user control what an application can access. Permissions settings for applications are located in: **Settings -> Security and Privacy -> Application Permissions**.

5. If the device is attached to a BES 10, the BlackBerry Balance feature can be applied to the BlackBerry 10 device allowing separation of work and personal areas. This separation allows the BES administrator to easily remove the data from the workspace without affecting the personal space.

BlackBerry 10 – Security

6. From an operating system security perspective the BlackBerry 10 has the following exploit mitigation measures [4]:

- DEP/XN (Data Execution Prevention)
- ASRL (Address Space Randomization Layout),
- PIE (Position Independent Execution),
- full RELRO (RELocation Read Only): see this link for an explanation about RELRO http://tk-blog.blogspot.ca/2009/02/relro-not-so-well-known-memory.html
- But no heap hardening.

Source: 4. Ralf-Philipp Weinmann., BlackBerry 10 OS from a security perspective, University of Luxembourg, black hat USA 2013 Presentation.

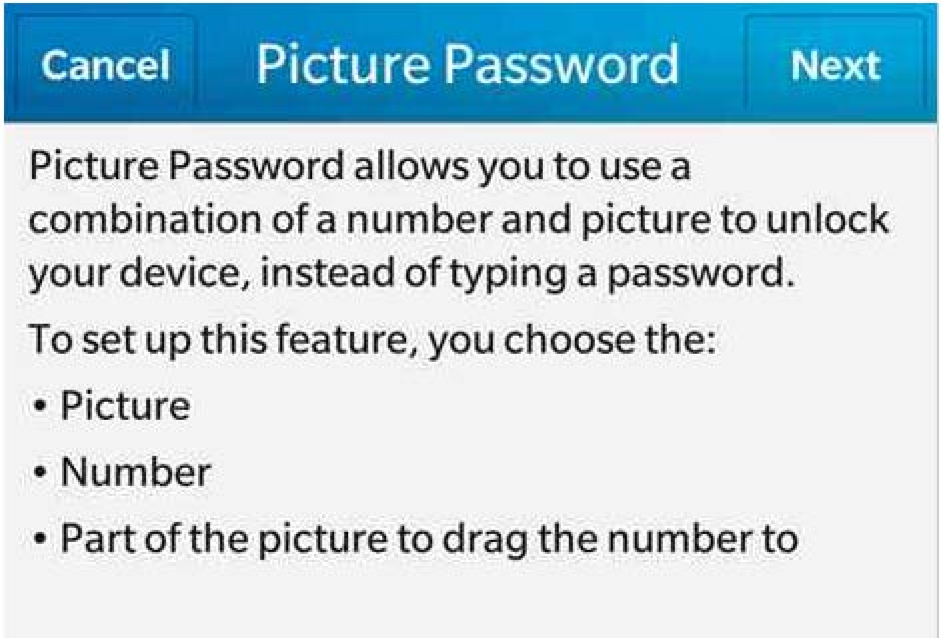
BlackBerry 10: Picture Password

Picture Password:

- Introduced in in OS 10.2.1.
- Uses a number combination of 0-9 and a picture to lock and unlock the device.
- Requires a device password to be set in case you forget your Picture Password or if you need to access your device from a computer using BlackBerry Link.
- After five failed attempts to unlock your device using Picture Password you'll be prompted for your device password instead.

TEELtechnologies

BlackBerry 10: Picture Password



Picture Password allows you to use a combination of a number and picture to unlock your device, instead of typing a password.

To set up this feature, you choose the:

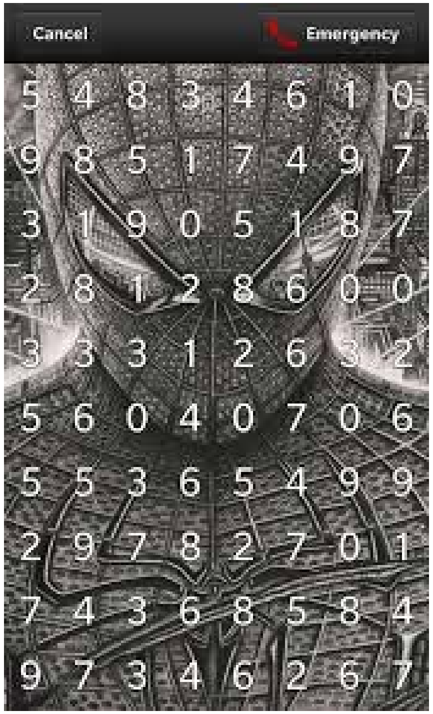
- Picture
- Number
- Part of the picture to drag the number to

Source: http://n4bb.com/wp-content/uploads/2013/11/Picture-Password.jpg

June-19-14

BlackBerry 10: Picture Password

- To unlock the device you drag the number you have chosen, to the specific point on the picture you have chosen.
- You do not need to tap the number. The number is moved by sliding the number grid so the number you have chosen is in the correct place on the picture.
- Difficult to ascertain what your password is as the numbers and size of the grid varies each time.

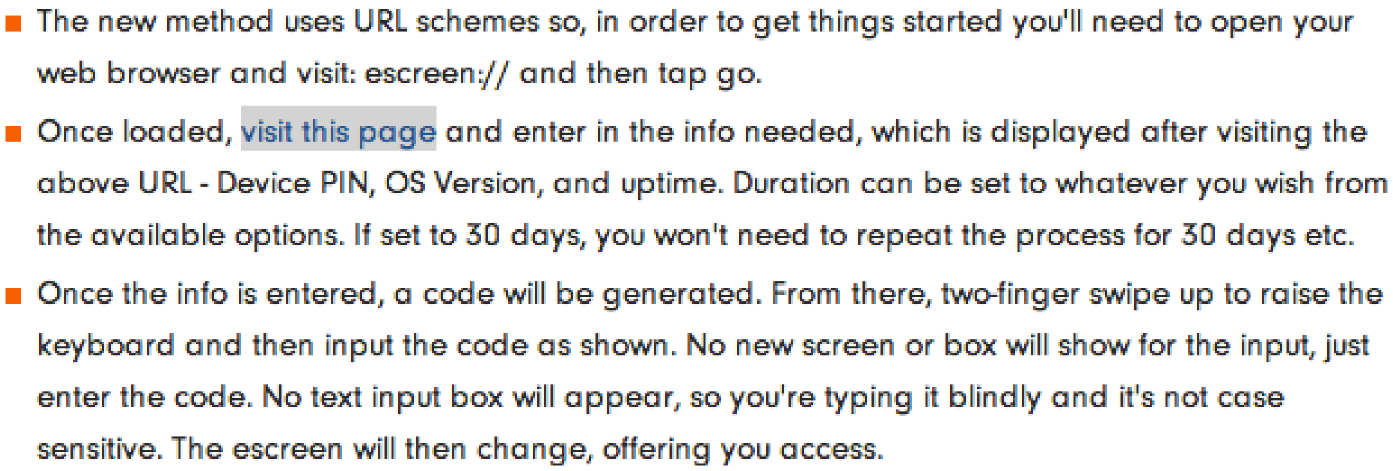


5	4	8	3	4	6	1	0
9	8	5	1	7	4	9	7
3	1	9	0	5	1	8	7
2	8	1	2	8	6	0	0
3	3	3	1	2	6	3	2
5	6	0	4	0	7	0	6
5	5	3	6	5	4	9	9
2	9	7	8	2	7	0	1
7	4	3	6	8	5	8	4
9	7	3	4	6	2	6	7

Image Source: https://encrypted-tbn3.gstatic.com/images?q=tbn:ANd9GcTDqcTcNqszN1lNzOEt4k3DiQ8SOd9winkCQfeDPHASWEZ4hSNe

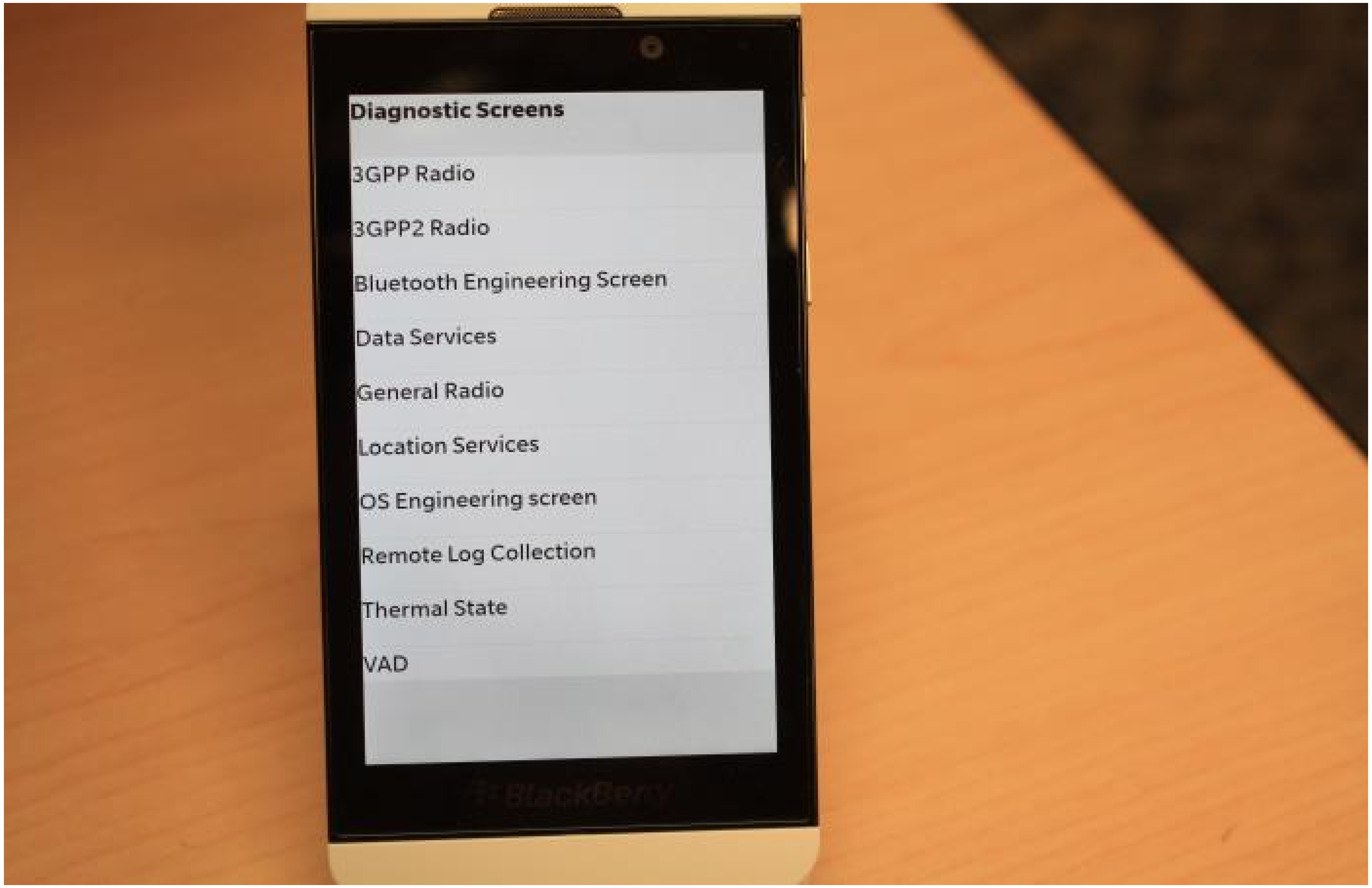
BlackBerry 10 – EScreen

- BlackBerry 10 also has an engineering screen, or EScreen which is invoked in a very similar manner to its predecessors.
- Several websites that show how to do this: one is **http://crackberry.com/how-access-engineering-screen-blackberry-10**



- The new method uses URL schemes so, in order to get things started you'll need to open your web browser and visit: escreen:// and then tap go.
- Once loaded, visit this page and enter in the info needed, which is displayed after visiting the above URL - Device PIN, OS Version, and uptime. Duration can be set to whatever you wish from the available options. If set to 30 days, you won't need to repeat the process for 30 days etc.
- Once the info is entered, a code will be generated. From there, two-finger swipe up to raise the keyboard and then input the code as shown. No new screen or box will show for the input, just enter the code. No text input box will appear, so you're typing it blindly and it's not case sensitive. The escreen will then change, offering you access.

BlackBerry 10 – EScreen



Diagnostic Screens

3GPP Radio

3GPP2 Radio

Bluetooth Engineering Screen

Data Services

General Radio

Location Services

OS Engineering screen

Remote Log Collection

Thermal State

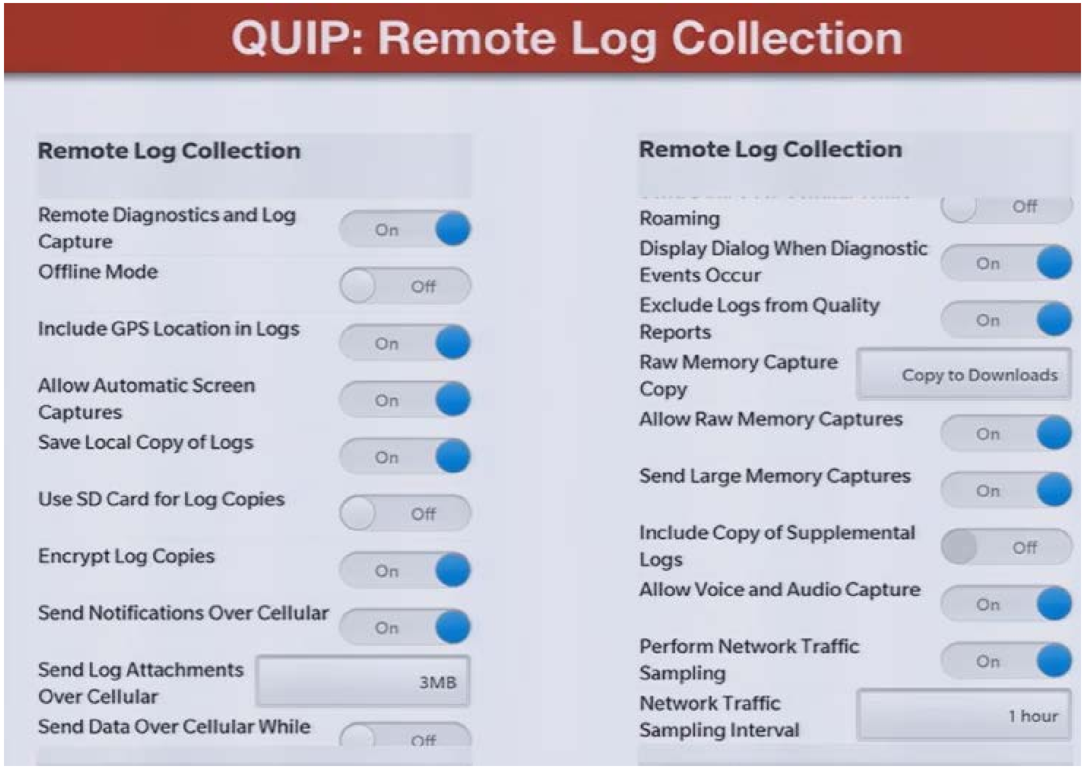
VAD

BlackBerry 10 – EScreen

- One interesting aspect of the engineering screen is Remote Log Collection.
- On the device user first has to manually enable diagnostic and usage data collection under **Settings->Privacy & Security -> Diagnostics**.
- The feature ‘Send diagnostics and usage data’ is set to ‘Off’ by default. The data collected by this function is tied to the settings that are enabled in the QUIP Remote Log Collection.

BlackBerry 10 – EScreen

- A screenshot shows the QUIP Remote Collection features. By default this is not enabled and what you are seeing are not default settings.



QUIP: Remote Log Collection

Remote Log Collection

Remote Diagnostics and Log Capture	On
Offline Mode	Off
Include GPS Location in Logs	On
Allow Automatic Screen Captures	On
Save Local Copy of Logs	On
Use SD Card for Log Copies	Off
Encrypt Log Copies	On
Send Notifications Over Cellular	On
Send Log Attachments Over Cellular	3MB
Send Data Over Cellular While	Off

Remote Log Collection

Roaming	Off
Display Dialog When Diagnostic Events Occur	On
Exclude Logs from Quality Reports	On
Raw Memory Capture Copy	Copy to Downloads
Allow Raw Memory Captures	On
Send Large Memory Captures	On
Include Copy of Supplemental Logs	Off
Allow Voice and Audio Capture	On
Perform Network Traffic Sampling	On
Network Traffic Sampling Interval	1 hour

**Image Source:* Ralf-Philipp Weinmann., BlackBerry 10 OS from a security perspective, University of Luxembourg, black hat USA 2013 Presentation.

BlackBerry 10 – EScreen

- With Diagnostics enabled in the Settings->Privacy & Security -> Diagnostics **AND**

- Remote Diagnostics and Log Capture turned on, different types of data can be collected which includes: **screen captures, raw memory dumps, audio, video, and GPS location**.

**Image Source:* Ralf-Philipp Weinmann., BlackBerry 10 OS from a security perspective, University of Luxembourg, black hat USA 2013 Presentation.

BlackBerry 10 Connected to Windows 7 or Mac OS X

- When a password protected BlackBerry 10 device connects to the computer, regardless of operating system, the user will be prompted to enter the password in BlackBerry Link.

- The total number of password attempts is 5. In contrast BB OS 7 and lower devices with BlackBerry Desktop Software are allowed 10 attempts.

BlackBerry 10 Connected to Windows 7 or Mac OS X

- BlackBerry 10 devices can be accessed over Wi-Fi using BlackBerry Link software on Windows or Mac; this allows the ability to sync multi-media content, and documents between the device and computer over Wi-Fi instead of USB.

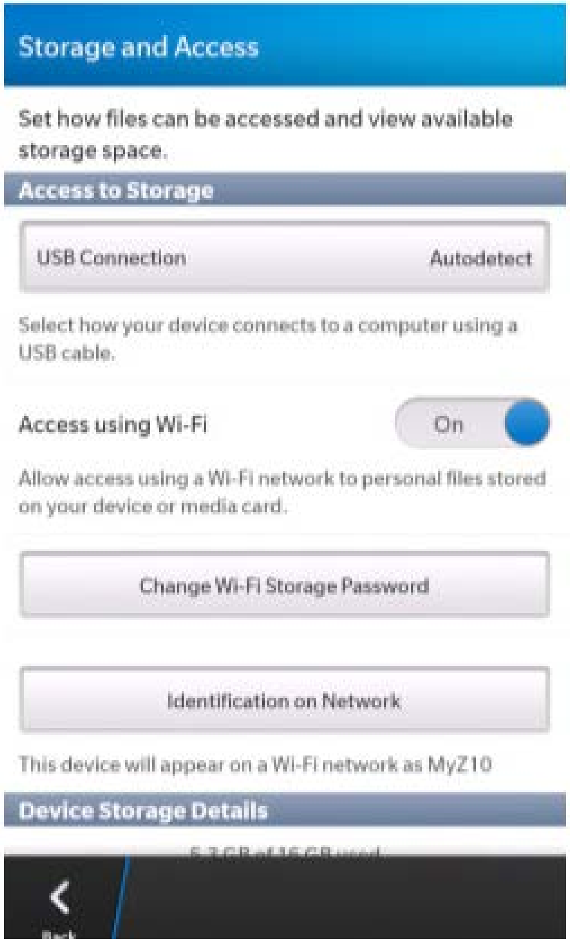
- **By default the option to connect the BlackBerry device to BlackBerry Link over Wi-Fi is enabled**. Disabling this feature within BlackBerry Link does not affect the Wi-Fi settings on the device.

BlackBerry 10 Connected to Windows 7 or Mac OS X

- Within the BlackBerry Z10 device specifically under **‘Storage and Access’** the device can be accessed using Wi-Fi through either a Windows or Mac OS X computer.

- This is disabled by default on the device and is different than the Wi-Fi access via BlackBerry Link. If this is enabled on the device, the user will be prompted to create a Password Wi-Fi Storage Access.

BlackBerry 10 Connected to Windows 7 or Mac OS X



Storage and Access

Set how files can be accessed and view available storage space.

Access to Storage

USB Connection — Autodetect

Select how your device connects to a computer using a USB cable.

Access using Wi-Fi — On

Allow access using a Wi-Fi network to personal files stored on your device or media card.

Change Wi-Fi Storage Password

Identification on Network

This device will appear on a Wi-Fi network as MyZ10

Device Storage Details

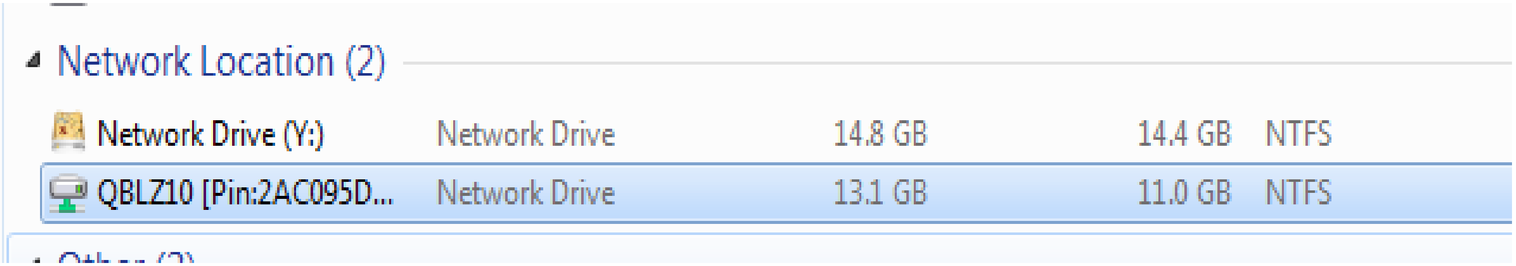
6.3 GB of 16 GB used

Image Source: http://helpblog.blackberry.com/2013/03/copy-z10-files-wifi/

June-19-14

BlackBerry 10 Connected to Windows 7 or Mac OS X

- When a BlackBerry Z10 device connects to a Windows machine, two network drive locations were mounted on the author's machine; they are recognized as NTFS file systems by Windows 7.



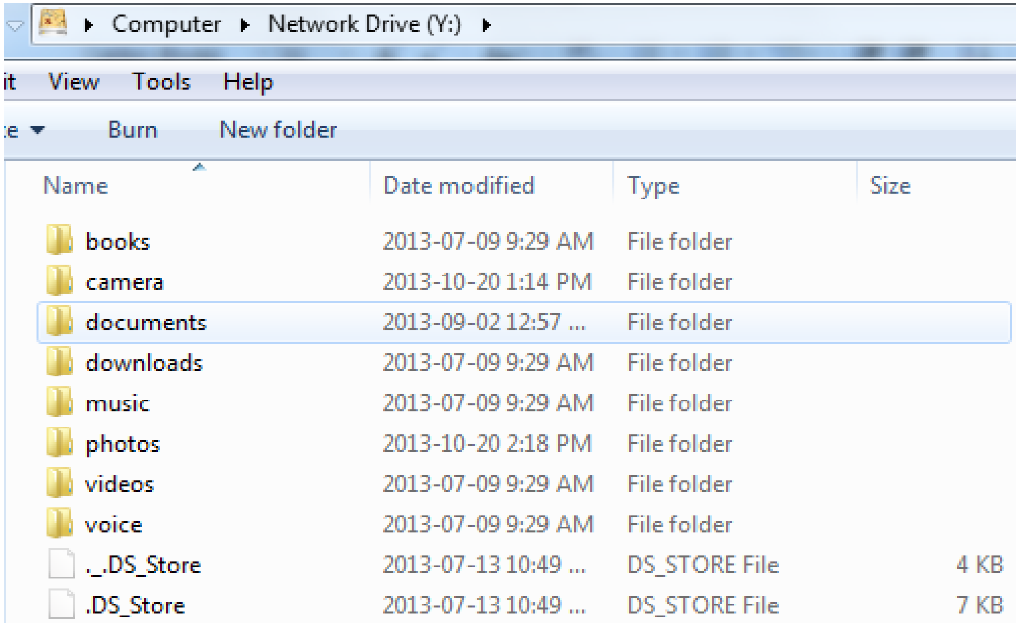
Network Location (2)

Network Drive (Y:)	Network Drive	14.8 GB	14.4 GB	NTFS
QBLZ10 [Pin:2AC095D...	Network Drive	13.1 GB	11.0 GB	NTFS

Other (2)

BlackBerry 10 Connected to Windows 7 or Mac OS X

- If the device is password protected, the password must be entered on the first instance of connecting, within BlackBerry Link, before the volumes will be mounted.

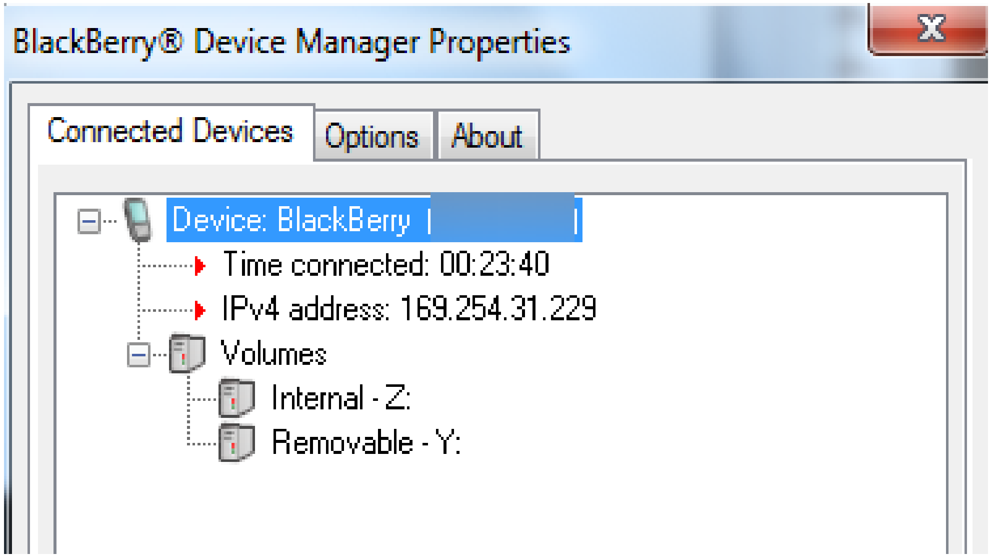


Name	Date modified	Type	Size
books	2013-07-09 9:29 AM	File folder	
camera	2013-10-20 1:14 PM	File folder	
documents	2013-09-02 12:57 ...	File folder	
downloads	2013-07-09 9:29 AM	File folder	
music	2013-07-09 9:29 AM	File folder	
photos	2013-10-20 2:18 PM	File folder	
videos	2013-07-09 9:29 AM	File folder	
voice	2013-07-09 9:29 AM	File folder	
._.DS_Store	2013-07-13 10:49 ...	DS_STORE File	4 KB
.DS_Store	2013-07-13 10:49 ...	DS_STORE File	7 KB

June-19-14

BlackBerry 10 Connected to Windows 7 or Mac OS X

- Using the BlackBerry Device Manager Properties, Connected Devices tab, we can see that Volume Z is internal memory and Volume Y is the Removable SD card.

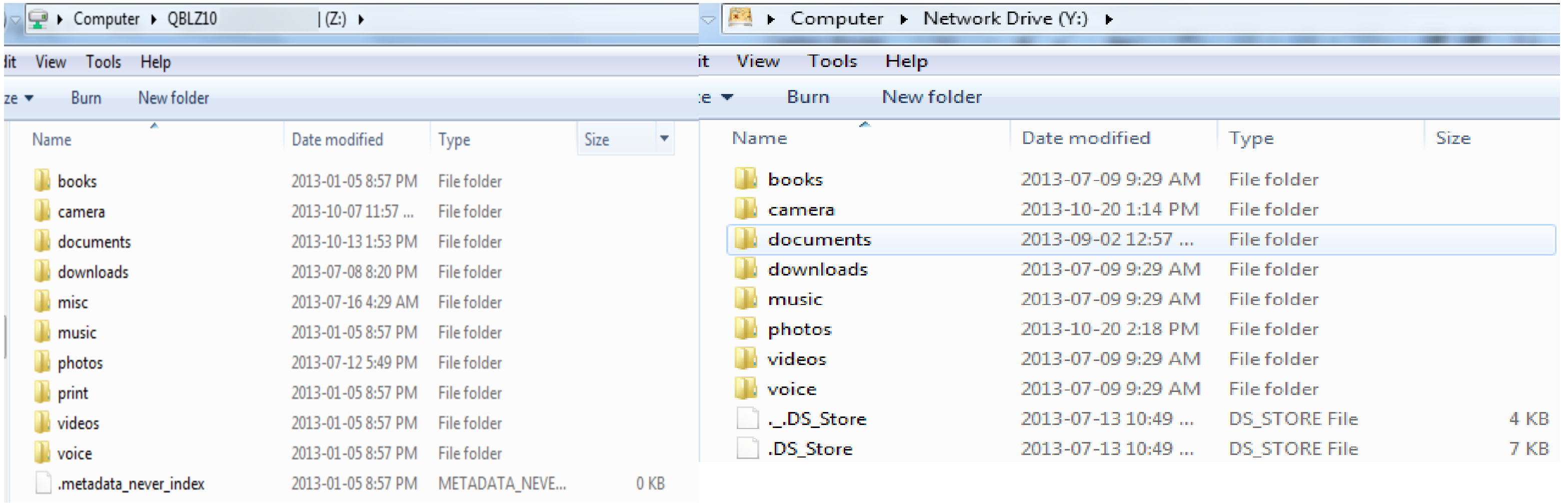


Device: BlackBerry |[redacted]|
Time connected: 00:23:40
IPv4 address: 169.254.31.229
Volumes
Internal - Z:
Removable - Y:

June-19-14

BlackBerry 10 Connected to Windows 7 or Mac OS X

- The internal volume (Z:) contains two more folders: misc and print.



Name	Date modified	Type	Size
books	2013-01-05 8:57 PM	File folder	
camera	2013-10-07 11:57 ...	File folder	
documents	2013-10-13 1:53 PM	File folder	
downloads	2013-07-08 8:20 PM	File folder	
misc	2013-07-16 4:29 AM	File folder	
music	2013-01-05 8:57 PM	File folder	
photos	2013-07-12 5:49 PM	File folder	
print	2013-01-05 8:57 PM	File folder	
videos	2013-01-05 8:57 PM	File folder	
voice	2013-01-05 8:57 PM	File folder	
.metadata_never_index	2013-01-05 8:57 PM	METADATA_NEVE...	0 KB

Name	Date modified	Type	Size
books	2013-07-09 9:29 AM	File folder	
camera	2013-10-20 1:14 PM	File folder	
documents	2013-09-02 12:57 ...	File folder	
downloads	2013-07-09 9:29 AM	File folder	
music	2013-07-09 9:29 AM	File folder	
photos	2013-10-20 2:18 PM	File folder	
videos	2013-07-09 9:29 AM	File folder	
voice	2013-07-09 9:29 AM	File folder	
._.DS_Store	2013-07-13 10:49 ...	DS_STORE File	4 KB
.DS_Store	2013-07-13 10:49 ...	DS_STORE File	7 KB

BlackBerry 10 Connected to Windows 7 or Mac OS X

- When a BB 10 device connects to this Mac OS X the following volumes are mounted:
  - media, dtm and if the device contains a removable SD card this too will be mounted.

- In terminal the 'mount' command was run which identifies the mounted volumes, which shows 3 volumes mounted in Mac OS X.

```
//dtm@169.254.249.49/removable_SDCARD on
/Volumes/removable_SDCARD (smbfs, nodev, nosuid, mounted
by qubyte)

//dtm@169.254.249.49/media on /Volumes/media (smbfs,
nodev, nosuid, mounted by qubyte)

//dtm@169.254.249.49/dtm on /Volumes/dtm (smbfs, nodev,
nosuid, mounted by qubyte)
```

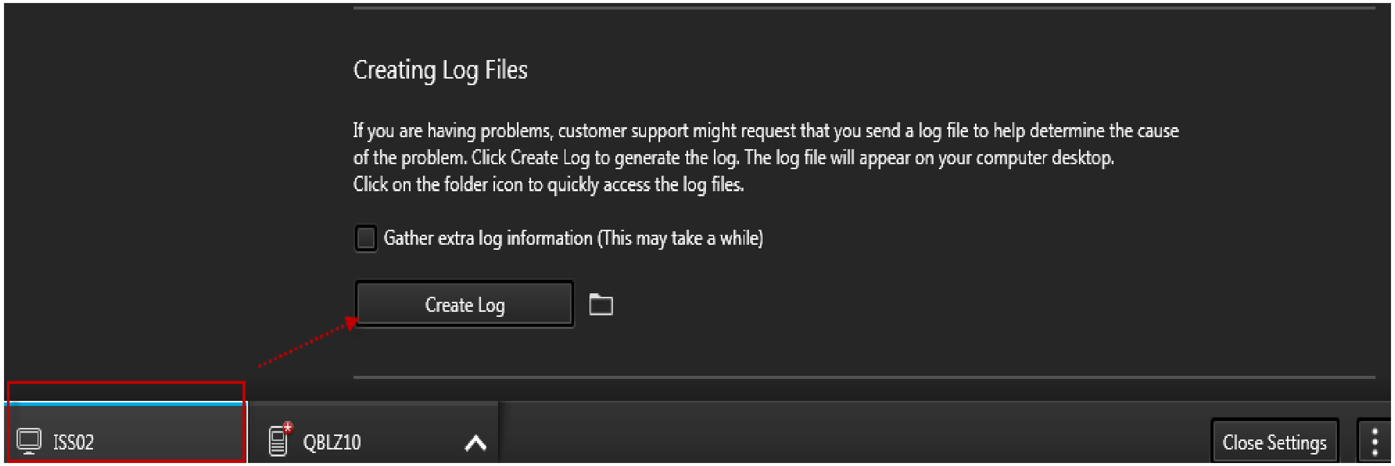
BlackBerry 10 Connected to Windows 7 or Mac OS X

- The 'smbfs' indicates Samba file system which is accessed over a network path a smb://169.254.251.197/volumename.
- Because it recognized as a network share, even though it contains an NTFS file system, the Mac OS X system can also write to it. If this were mounted as block device, the user would not be able to write to either drive natively because contains an NTFS file system.
- Backup files on a Mac OS X are stored to the following location:
  - /volumename/Users/username/Documents/BlackBerry Backups
  - A synchronization folder for multimedia content will also be created usually in the same path location:

    /volumename/Users/username/Documents.

BlackBerry 10: Log Files

- BlackBerry 10 log files can be collected using the BlackBerry Link Software:



Creating Log Files

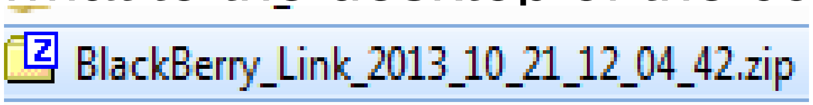
If you are having problems, customer support might request that you send a log file to help determine the cause of the problem. Click Create Log to generate the log. The log file will appear on your computer desktop. Click on the folder icon to quickly access the log files.

□ Gather extra log information (This may take a while)

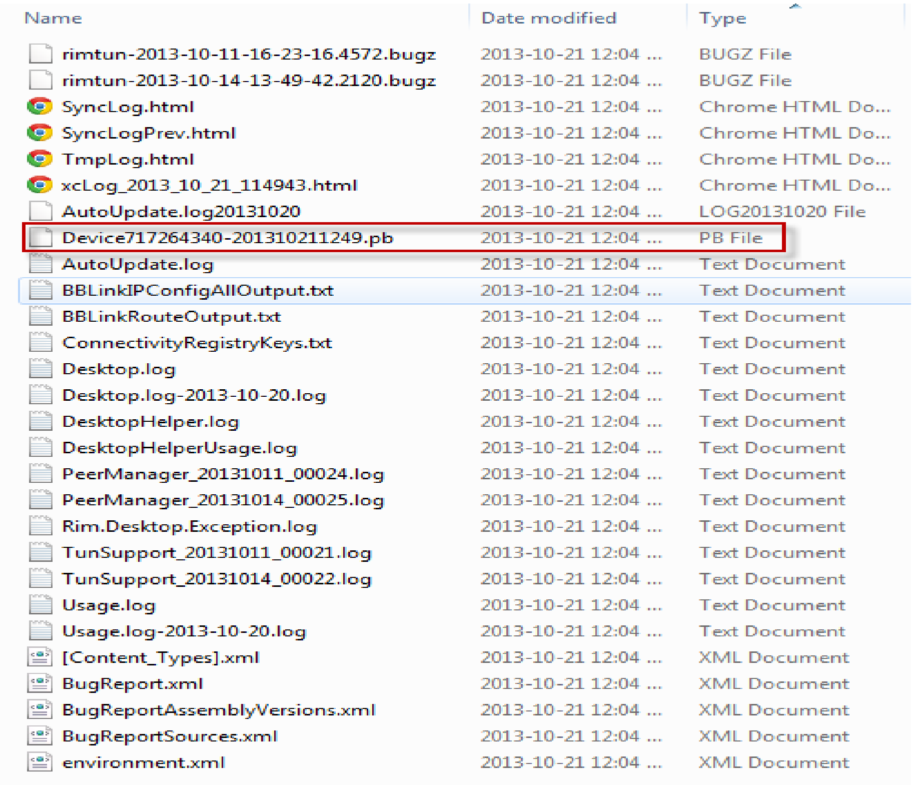
- Checking the ‘Gather extra log information’ requires the BlackBerry 10 or Blackberry Playbook to be connected to BlackBerry Link. This is how event logs are obtained from these devices.

BlackBerry 10: Log Files

- The log file (from a BlackBerry Playbook) is stored in a ZIP archive format to the desktop of the computer in this case.



BlackBerry_Link_2013_10_21_12_04_42.zip



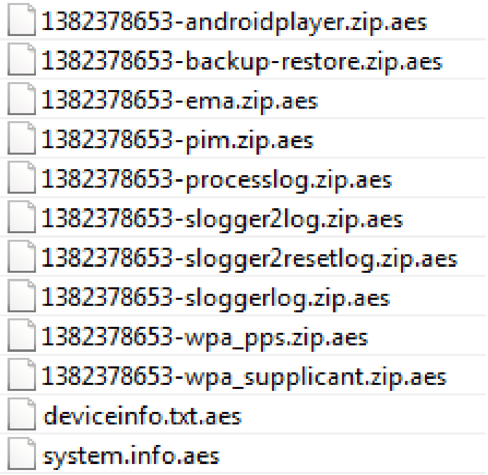
Name	Date modified	Type
rimtun-2013-10-11-16-23-16.4572.bugz	2013-10-21 12:04 ...	BUGZ File
rimtun-2013-10-14-13-49-42.2120.bugz	2013-10-21 12:04 ...	BUGZ File
SyncLog.html	2013-10-21 12:04 ...	Chrome HTML Do...
SyncLogPrev.html	2013-10-21 12:04 ...	Chrome HTML Do...
TmpLog.html	2013-10-21 12:04 ...	Chrome HTML Do...
xcLog_2013_10_21_114943.html	2013-10-21 12:04 ...	Chrome HTML Do...
AutoUpdate.log20131020	2013-10-21 12:04 ...	LOG20131020 File
Device717264340-201310211249.pb	2013-10-21 12:04 ...	PB File
AutoUpdate.log	2013-10-21 12:04 ...	Text Document
BBLinkIPConfigAllOutput.txt	2013-10-21 12:04 ...	Text Document
BBLinkRouteOutput.txt	2013-10-21 12:04 ...	Text Document
ConnectivityRegistryKeys.txt	2013-10-21 12:04 ...	Text Document
Desktop.log	2013-10-21 12:04 ...	Text Document
Desktop.log-2013-10-20.log	2013-10-21 12:04 ...	Text Document
DesktopHelper.log	2013-10-21 12:04 ...	Text Document
DesktopHelperUsage.log	2013-10-21 12:04 ...	Text Document
PeerManager_20131011_00024.log	2013-10-21 12:04 ...	Text Document
PeerManager_20131014_00025.log	2013-10-21 12:04 ...	Text Document
Rim.Desktop.Exception.log	2013-10-21 12:04 ...	Text Document
TunSupport_20131011_00021.log	2013-10-21 12:04 ...	Text Document
TunSupport_20131014_00022.log	2013-10-21 12:04 ...	Text Document
Usage.log	2013-10-21 12:04 ...	Text Document
Usage.log-2013-10-20.log	2013-10-21 12:04 ...	Text Document
[Content_Types].xml	2013-10-21 12:04 ...	XML Document
BugReport.xml	2013-10-21 12:04 ...	XML Document
BugReportAssemblyVersions.xml	2013-10-21 12:04 ...	XML Document
BugReportSources.xml	2013-10-21 12:04 ...	XML Document
environment.xml	2013-10-21 12:04 ...	XML Document

TEELtechnologies

June-19-14

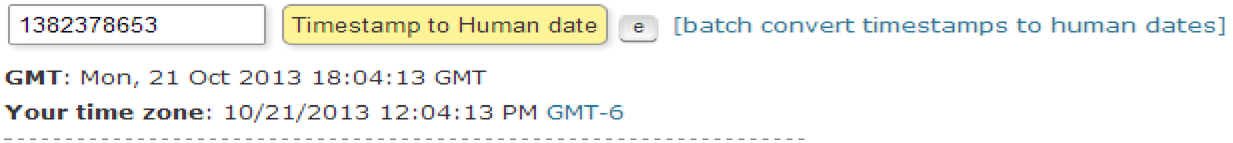
BlackBerry 10: Log Files

- Device717264340-201310211249.pb archive contents.



```
1382378653-androidplayer.zip.aes
1382378653-backup-restore.zip.aes
1382378653-ema.zip.aes
1382378653-pim.zip.aes
1382378653-processlog.zip.aes
1382378653-slogger2log.zip.aes
1382378653-slogger2resetlog.zip.aes
1382378653-sloggerlog.zip.aes
1382378653-wpa_pps.zip.aes
1382378653-wpa_supplicant.zip.aes
deviceinfo.txt.aes
system.info.aes
```

- The filenames are prefixed with a UNIX epoch time value in decimal and contain an 'aes' extension, which is likely indicative of AES encryption.



1382378653

GMT: Mon, 21 Oct 2013 18:04:13 GMT
Your time zone: 10/21/2013 12:04:13 PM GMT-6

BlackBerry 10 – Backups

- BlackBerry 10 device backups can be created ONLY using BlackBerry Link for Windows and Mac (this does not include any third party tools capable of creating backups).
- For the BlackBerry Playbook, both BlackBerry Desktop Software and BlackBerry Link for Windows and Mac can be used.
- The resultant files are identified with a ‘.bbb’ extension.

BlackBerry 10 – BBB Files

- The BBB files are ZIP archives that contain two child files and one child folder called ‘Archive’.
- Two files: these two files do not get encrypted during the backup process, at the present time.
  - PkgInfo: Contents of this file can also be viewed in a text or notepad type editor as shown below.

```
BlackBerryBackupFormatV2.0.0
Research In Motion
http://www.blackberry.com/
http://www.rim.com
1726dfe6f5336a9f1a3da1ceb11ecb69
```

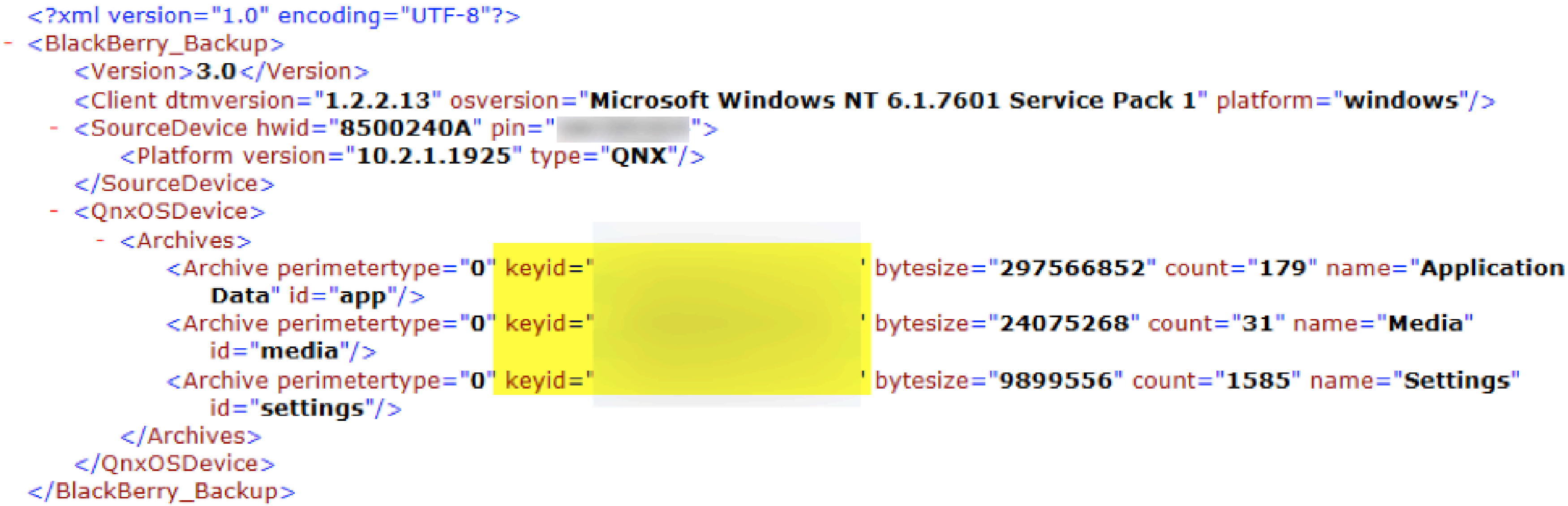
BlackBerry 10 – BBB Files

- Manifest.xml for a BlackBerry Playbook:

  -
    ```
    <?xml version="1.0" encoding="UTF-8"?>
    <BlackBerry_Backup>
      <Client platform="windows" osversion="Microsoft Windows NT 6.0.6002 Service Pack 2"
    dtmversion="6.1.0.35" />
      <Version>2.0</Version>
      <Encryption type="RIM_AES_CBC" version="1.0" Salt="" />
      <SourceDevice pin="500F54B8" hwid="6001A06">
        <Platform type="QNX" version="1.0.7.2670" />
      </SourceDevice>
      <QnxOSDevice>
        <Archives>
          <Archive id="app" name="Application Data" count="51" bytesize="541257216" />
          <Archive id="media" name="Media" count="11" bytesize="1728000" />
          <Archive id="settings" name="Settings" count="994" bytesize="1368064" />
        </Archives>
      </QnxOSDevice>
    </BlackBerry_Backup>
    ```

BlackBerry 10 – BBB Files

- Manifest.xml for a BlackBerry 10:
  - Note the ‘keyid=‘ value, which is the BlackBerry 10 user’s BlackBerry ID value as an email address



```
  <?xml version="1.0" encoding="UTF-8"?>
- <BlackBerry_Backup>
    <Version>3.0</Version>
    <Client dtmversion="1.2.2.13" osversion="Microsoft Windows NT 6.1.7601 Service Pack 1" platform="windows"/>
  - <SourceDevice hwid="8500240A" pin="[redacted]">
      <Platform version="10.2.1.1925" type="QNX"/>
    </SourceDevice>
  - <QnxOSDevice>
    - <Archives>
        <Archive perimetertype="0" keyid="[redacted]' bytesize="297566852" count="179" name="Application
          Data" id="app"/>
        <Archive perimetertype="0" keyid="[redacted]' bytesize="24075268" count="31" name="Media"
          id="media"/>
        <Archive perimetertype="0" keyid="[redacted]' bytesize="9899556" count="1585" name="Settings"
          id="settings"/>
      </Archives>
    </QnxOSDevice>
  </BlackBerry_Backup>
```

BlackBerry 10 – BBB Files

- Within the ‘Archive’ folder three TAR files are present: apps.tar, media.tar and settings.tar.
- The contents of these files are encrypted regardless of which BlackBerry backup software was used and regardless of the device being password protected or not.
- The decryption of the BBB cannot be disabled from within the software or the device.
- The TAR files headers differ between the Playbook and BlackBerry Z10.

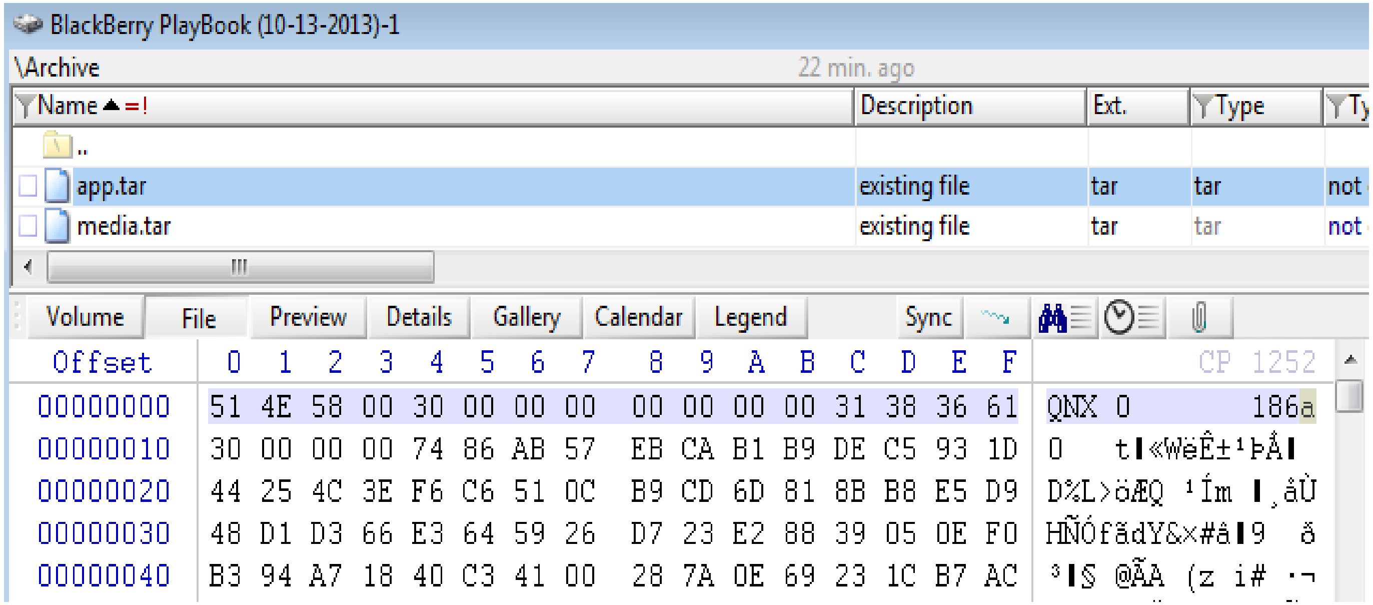
BlackBerry 10 – Playbook TAR Header

- File Header: This consistently appears in all three TAR files regardless of software used or the OS platform the BBB is generated on.

  - 51 4E 58 00 30 00 00 00 00 00 00 00 31 38 36 61 h

  - 'QNX 0   186a' in ASCII; the gap between the '0' and the start of '186' is separated by 7 null values or 0x00.

BlackBerry 10 – Playbook TAR Header



Name ▲=!	Description	Ext.	Type	Ty
..				
□ app.tar	existing file	tar	tar	not
□ media.tar	existing file	tar	tar	not

```
 Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F          CP 1252
00000000  51 4E 58 00 30 00 00 00  00 00 00 00 31 38 36 61  QNX 0       186a
00000010  30 00 00 00 74 86 AB 57  EB CA B1 B9 DE C5 93 1D  0   t▌«WëÊ±¹ÞÅ▌
00000020  44 25 4C 3E F6 C6 51 0C  B9 CD 6D 81 8B B8 E5 D9  D%L>öÆQ ¹Ím ▌¸åÙ
00000030  48 D1 D3 66 E3 64 59 26  D7 23 E2 88 39 05 0E F0  HÑÓfãdY&×#â▌9  ð
00000040  B3 94 A7 18 40 C3 41 00  28 7A 0E 69 23 1C B7 AC  ³▌§ @ÃA (z i# ·¬
```

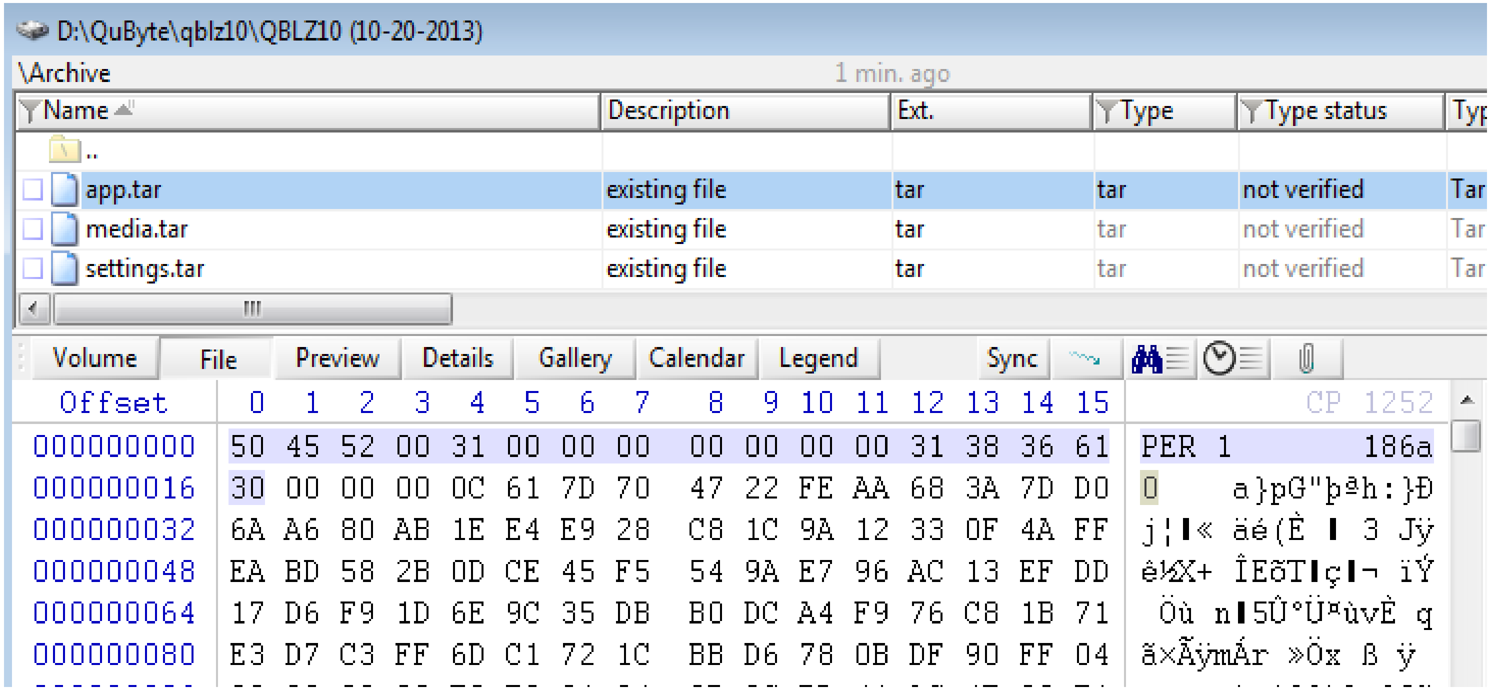
June-19-14

TEELtechnologies

BlackBerry 10 – Z10 TAR Header

- File Header: This consistently appears in all three TAR files regardless of software used or the OS platform the BBB is generated on.
  - 50 45 52 00 31 00 00 00 00 00 00 00 31 38 36 61 30h
  - 'PER 1   186a0' in ASCII; the gap between the '0' and the start of '186' is separated by 7 null values or 0x00.

BlackBerry 10 – Z10 TAR Header



D:\QuByte\qblz10\QBLZ10 (10-20-2013)

\Archive 1 min. ago

Name	Description	Ext.	Type	Type status	Typ
..					
□ app.tar	existing file	tar	tar	not verified	Tar
□ media.tar	existing file	tar	tar	not verified	Tar
□ settings.tar	existing file	tar	tar	not verified	Tar

```
   Offset    0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15          CP 1252
000000000   50 45 52 00 31 00 00 00  00 00 00 00 31 38 36 61   PER 1       186a
000000016   30 00 00 00 0C 61 7D 70  47 22 FE AA 68 3A 7D D0   0     a}pG"þªh:}Ð
000000032   6A A6 80 AB 1E E4 E9 28  C8 1C 9A 12 33 0F 4A FF   j¦▮« äé(È ▮ 3 Jÿ
000000048   EA BD 58 2B 0D CE 45 F5  54 9A E7 96 AC 13 EF DD   ê½X+ ÎEõT▮ç▮¬ ïÝ
000000064   17 D6 F9 1D 6E 9C 35 DB  B0 DC A4 F9 76 C8 1B 71    Öù n▮5Û°Ü¤ùvÈ q
000000080   E3 D7 C3 FF 6D C1 72 1C  BB D6 78 0B DF 90 FF 04   ã×ÃÿmÁr »Öx ß ÿ
```

BlackBerry 10: Data Extraction/Analysis

- Oxygen Forensics has a solution in place for the BlackBerry 10 backups.

- UFED can acquire limited amount of data at this time. This may improve in future versions.

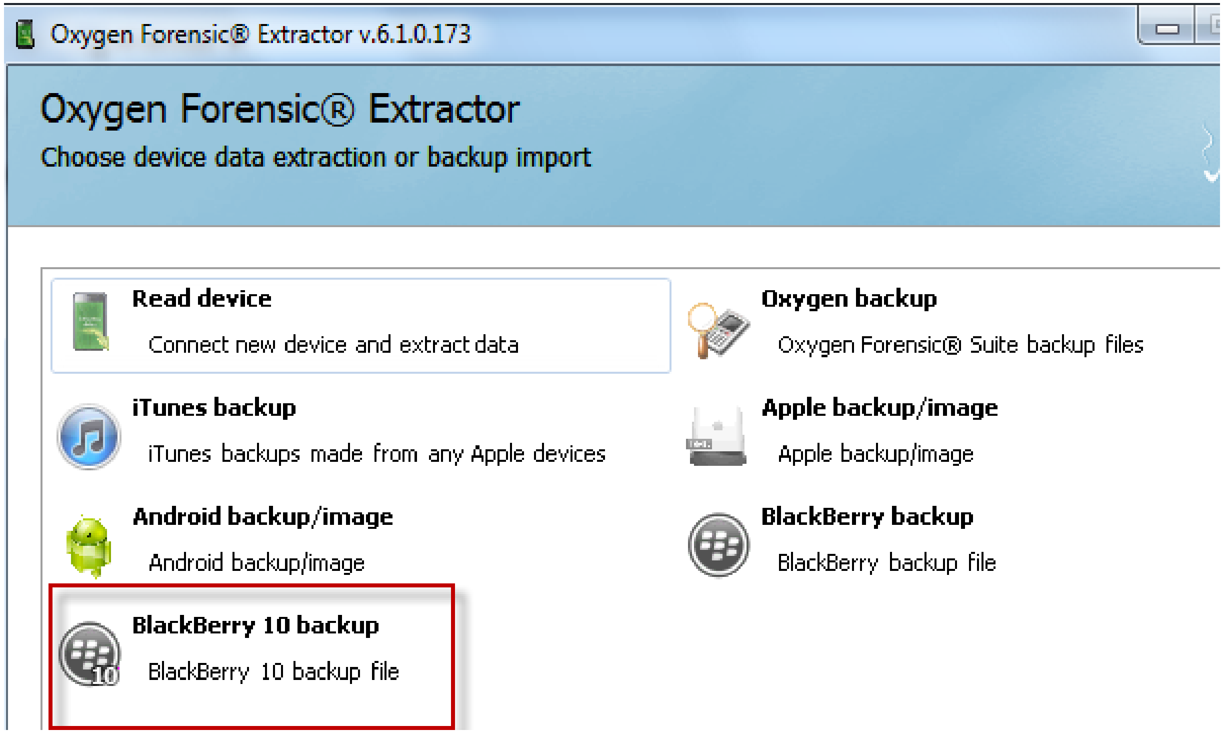
- A chip off dump of the BB 10 device is encrypted at the chip level, as discovered by Bob Elder.

BlackBerry 10: BBB Backup File

- Oxygen Forensic Suite (OFS) Analyst 6.1.x and higher can parse a BlackBerry 10 backup file:
    - **provided you know the password to the device owner's BlackBerry ID account** (which may or may not be the same as the device password).

BlackBerry 10 Backup Files with OFS

- Import the BBB file using either File -> Import or the Oxygen Forensic Extractor.



Oxygen Forensic® Extractor v.6.1.0.173

Oxygen Forensic® Extractor

Choose device data extraction or backup import

Read device
Connect new device and extract data

Oxygen backup
Oxygen Forensic® Suite backup files

iTunes backup
iTunes backups made from any Apple devices

Apple backup/image
Apple backup/image

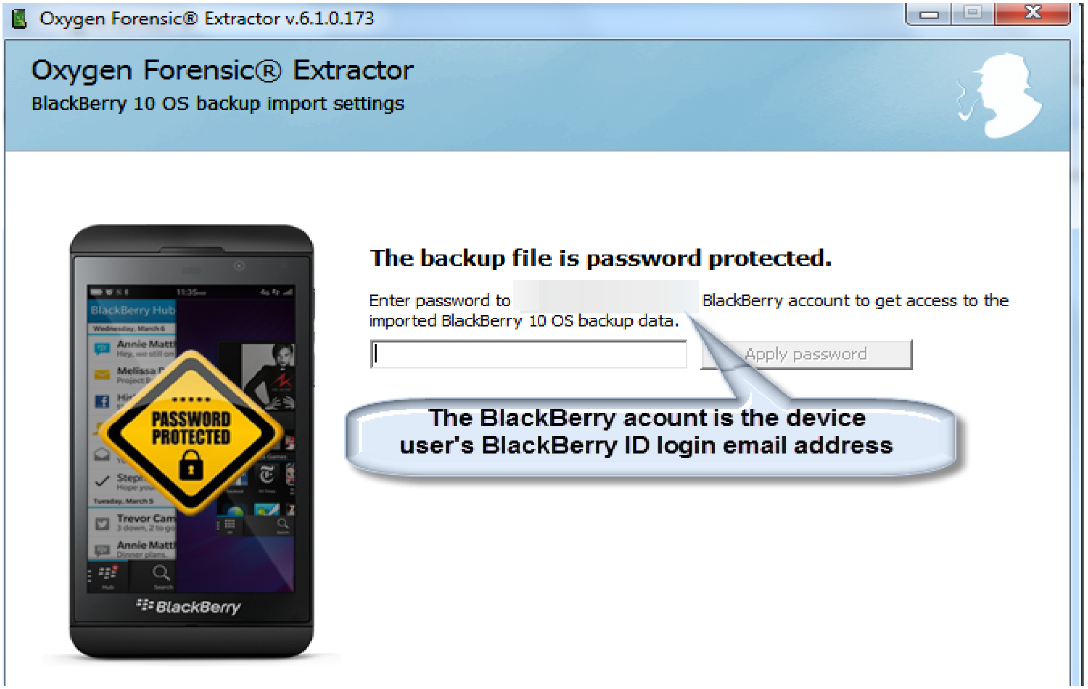
Android backup/image
Android backup/image

BlackBerry backup
BlackBerry backup file

BlackBerry 10 backup
BlackBerry 10 backup file

BlackBerry 10 Backup Files with OFS

Once you have selected the backup file, OFS will identify the email account used by the device owner to access his/her BlackBerry ID account. The password to the BlackBerry ID account will be required in order for OFS to decrypt the backup and subsequently parse the data.



Oxygen Forensic® Extractor v.6.1.0.173

Oxygen Forensic® Extractor

BlackBerry 10 OS backup import settings

The backup file is password protected.

Enter password to [redacted] BlackBerry account to get access to the imported BlackBerry 10 OS backup data.

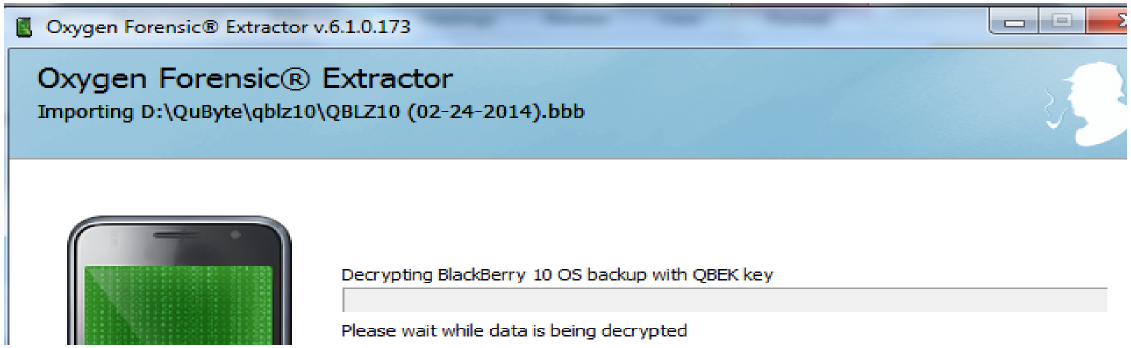
The BlackBerry acount is the device user's BlackBerry ID login email address

June-19-14

TEELtechnologies

BlackBerry 10 Backup Files with OFS

- OFS decrypting BBB TAR files with QBEK Key.



Oxygen Forensic® Extractor v.6.1.0.173

Oxygen Forensic® Extractor

Importing D:\QuByte\qblz10\QBLZ10 (02-24-2014).bbb

Decrypting BlackBerry 10 OS backup with QBEK key

Please wait while data is being decrypted

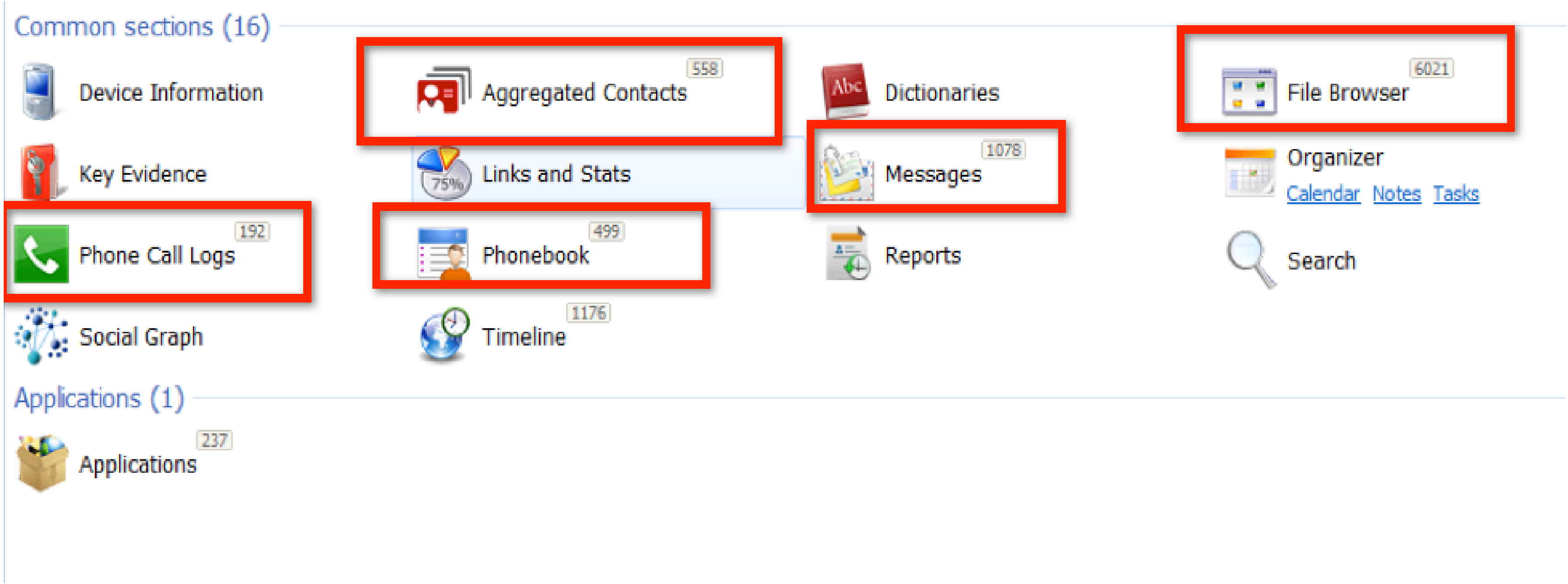
- **The QBEK Key is associated to the urn:bbid:backupandrestore key [7,8]:**
  - urn = uniform resource name
  - The remainder of URN syntax consists of the namespace-identifier (NID), separated by a colon, and then the namespace-specific string (NSS).

- The BlackBerry ID is associated to the encryption of the BlackBerry 10 backup.

TEELtechnologies

BlackBerry 10 Backup Files with OFS

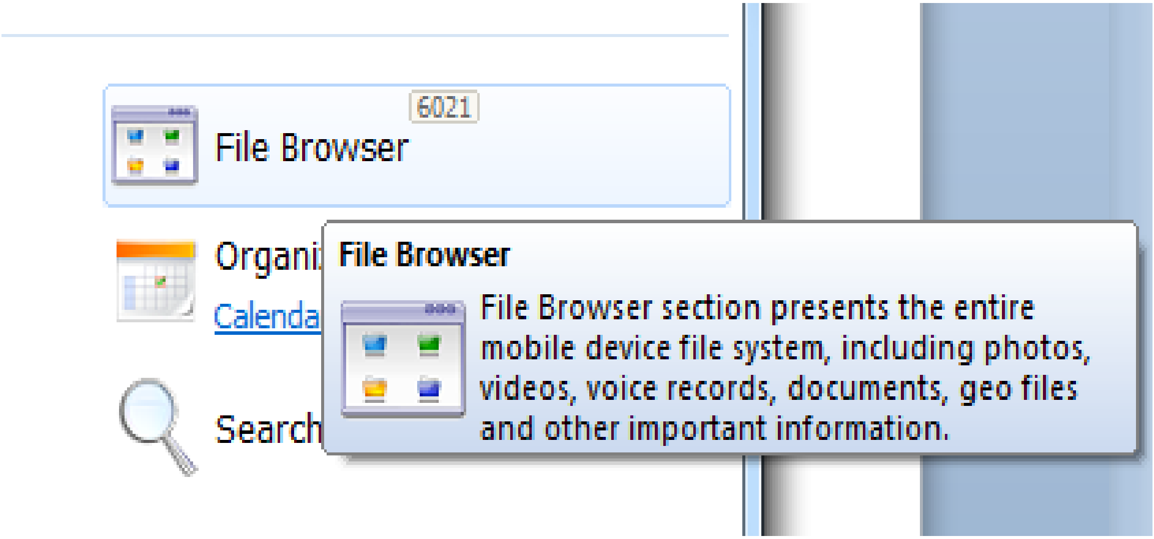
- End result of decryption and parsing



June-19-14

BlackBerry 10 Backup Files with OFS

- The File Browser feature allows you to export the folders/files out of OFS for use in other forensic tools like UFED PA or XWF.



File Browser

File Browser section presents the entire mobile device file system, including photos, videos, voice records, documents, geo files and other important information.

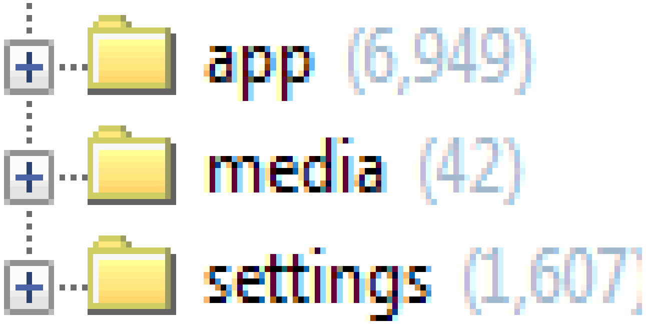
BlackBerry 10 Backup Structure

The BlackBerry logical file system data consists of the following types:

- SQLite databases in .db and .dat format
- XML files
- INI files
- BIN files
- And various other types of files whose contents are in plain text such as .conf files.

BlackBerry 10 Backup Structure

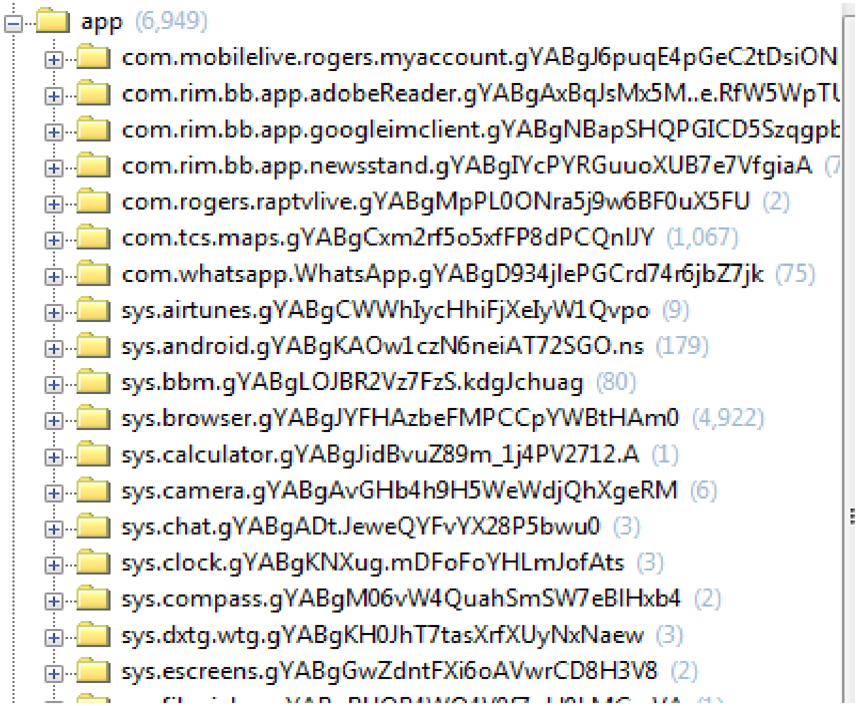
The three TAR files when decrypted consist of three folders: app, media and settings:



BlackBerry 10 Backup Structure

app Folder

This folder contains the applications that are on the device, containing folders with long names.



```
app (6,949)
  com.mobilelive.rogers.myaccount.gYABgJ6puqE4pGeC2tDsiON
  com.rim.bb.app.adobeReader.gYABgAxBqJsMx5M..e.RfW5WpTL
  com.rim.bb.app.googleimclient.gYABgNBapSHQPGICD5Szqgpb
  com.rim.bb.app.newsstand.gYABgIYcPYRGuuoXUB7e7VfgiaA (7
  com.rogers.raptvlive.gYABgMpPL0ONra5j9w6BF0uX5FU (2)
  com.tcs.maps.gYABgCxm2rf5o5xfFP8dPCQnIJY (1,067)
  com.whatsapp.WhatsApp.gYABgD934jlePGCrd74r6jbZ7jk (75)
  sys.airtunes.gYABgCWWhIycHhiFjXeIyW1Qvpo (9)
  sys.android.gYABgKAOw1czN6neiAT72SGO.ns (179)
  sys.bbm.gYABgLOJBR2Vz7FzS.kdgJchuag (80)
  sys.browser.gYABgJYFHAzbeFMPCCpYWBtHAm0 (4,922)
  sys.calculator.gYABgJidBvuZ89m_1j4PV2712.A (1)
  sys.camera.gYABgAvGHb4h9H5WeWdjQhXgeRM (6)
  sys.chat.gYABgADt.JeweQYFvYX28P5bwu0 (3)
  sys.clock.gYABgKNXug.mDFoFoYHLmJofAts (3)
  sys.compass.gYABgM06vW4QuahSmSW7eBIHxb4 (2)
  sys.dxtg.wtg.gYABgKH0JhT7tasXrfXUyNxNaew (3)
  sys.escreens.gYABgGwZdntFXi6oAVwrCD8H3V8 (2)
```

June-19-14

BlackBerry 10 Backup Structure

app Folder

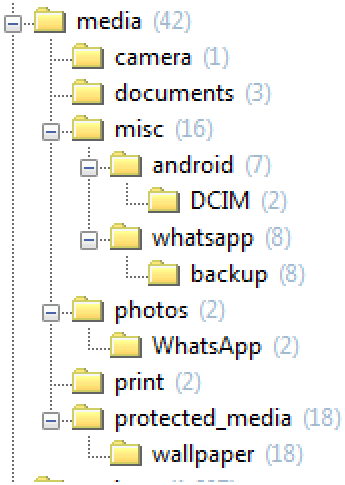
- Naming convention follows as:
  - com.XXXX.gYABG string
  - sys.XXXX.gYABG string

- The XXXX = resource or application name then followed by a gYABg, which appears to an obfuscated string of alphanumeric characters.
- Expanding the folder structure shows that in almost all, if not all, folder sub paths, there is an folder structure as:
  - /com.resrouce.gYABg string/appdata/data

BlackBerry 10 Backup Structure

media Folder

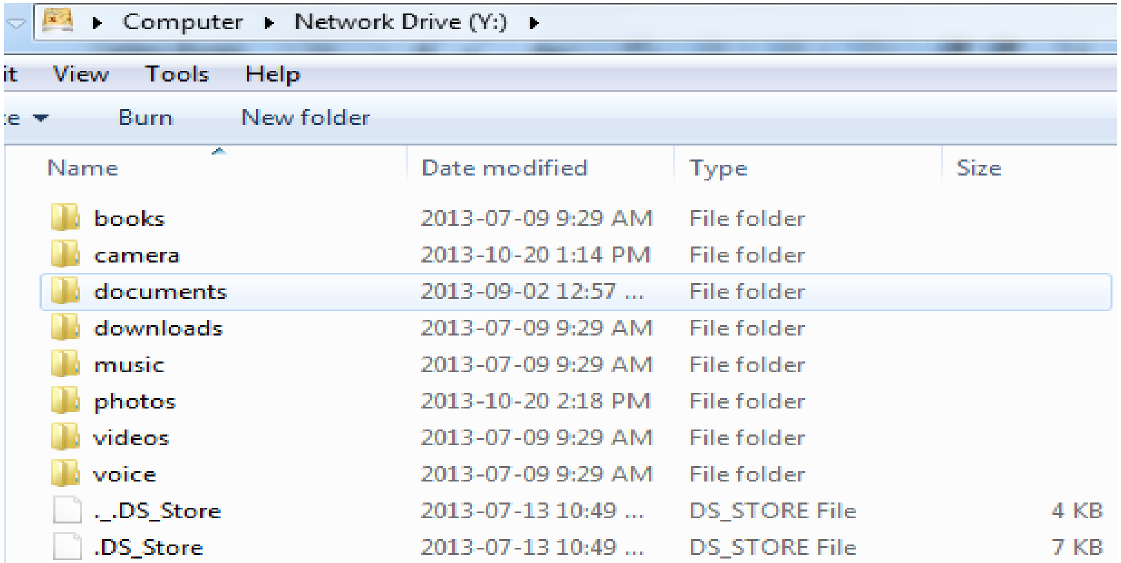
This folder contains the storage areas for user created content, and downloaded content as shown below.



```
media (42)
    camera (1)
    documents (3)
    misc (16)
        android (7)
            DCIM (2)
        whatsapp (8)
            backup (8)
    photos (2)
        WhatsApp (2)
    print (2)
    protected_media (18)
        wallpaper (18)
```

BlackBerry 10 Backup Structure

- Be cognizant that all BlackBerry 10 smart phone devices come with an microSD memory card, which will contain a similar directory structures as shown below.

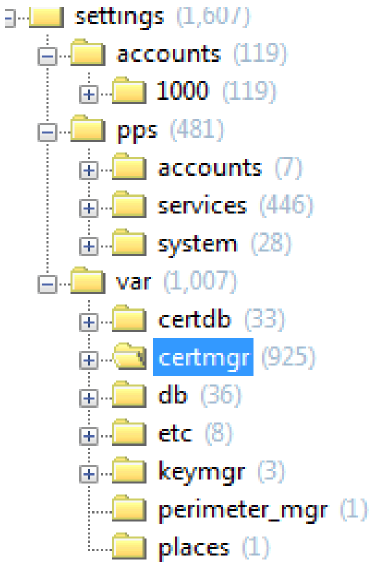


Name	Date modified	Type	Size
books	2013-07-09 9:29 AM	File folder	
camera	2013-10-20 1:14 PM	File folder	
documents	2013-09-02 12:57 ...	File folder	
downloads	2013-07-09 9:29 AM	File folder	
music	2013-07-09 9:29 AM	File folder	
photos	2013-10-20 2:18 PM	File folder	
videos	2013-07-09 9:29 AM	File folder	
voice	2013-07-09 9:29 AM	File folder	
._.DS_Store	2013-07-13 10:49 ...	DS_STORE File	4 KB
.DS_Store	2013-07-13 10:49 ...	DS_STORE File	7 KB

BlackBerry 10 Backup Structure

settings Folder

This folder contains the storage areas for the user account, system/device settings and var (variable data) folders with subfolders.



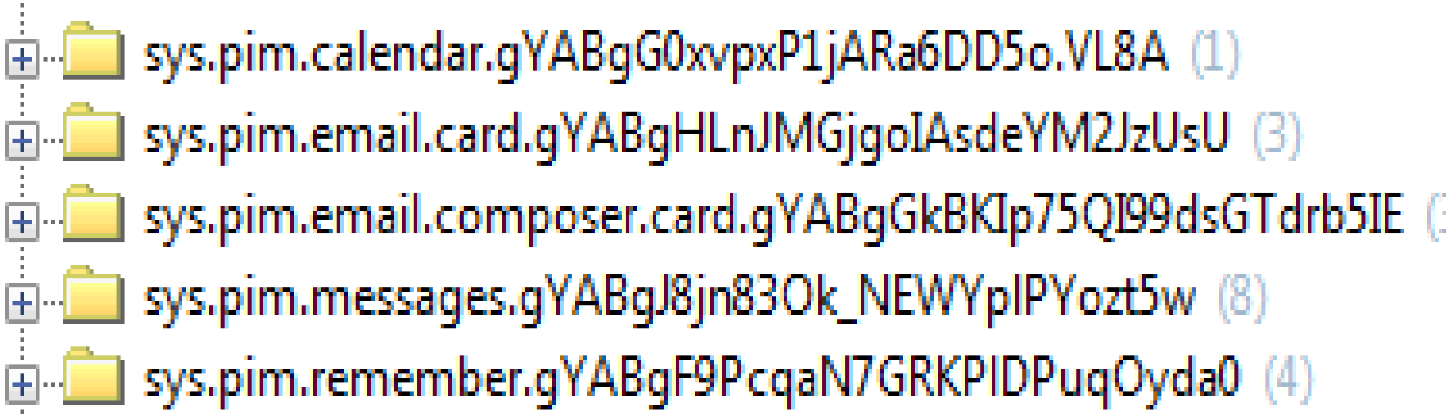
```
settings (1,607)
  accounts (119)
    1000 (119)
  pps (481)
    accounts (7)
    services (446)
    system (28)
  var (1,007)
    certdb (33)
    certmgr (925)
    db (36)
    etc (8)
    keymgr (3)
    perimeter_mgr (1)
    places (1)
```

June-19-14

TEELtechnologies

BlackBerry 10 PIM Data

- Refers to personal information organized in a range of different application functions such as calendar, emails, address/contact book, tasks, and reminders.
- **/app: subfolders contained in various sub-folders, is found under the following sys.pim folders.**



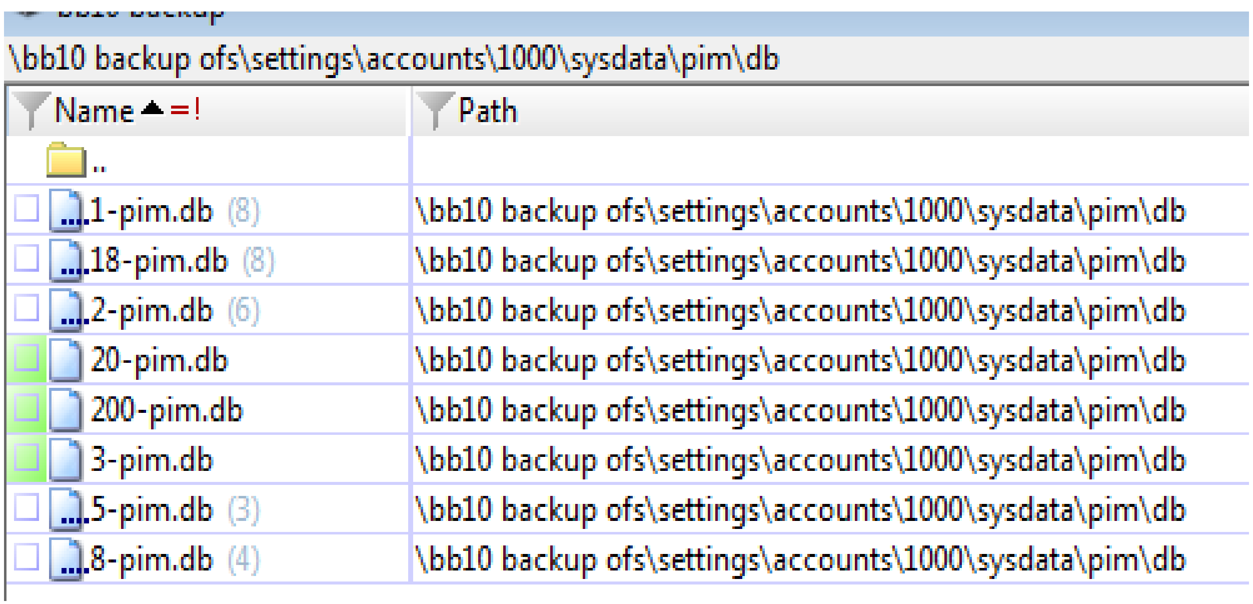
```
sys.pim.calendar.gYABgG0xvpxP1jARa6DD5o.VL8A (1)
sys.pim.email.card.gYABgHLnJMGjgoIAsdeYM2JzUsU (3)
sys.pim.email.composer.card.gYABgGkBKIp75QI99dsGTdrb5IE (
sys.pim.messages.gYABgJ8jn83Ok_NEWYpIPYozt5w (8)
sys.pim.remember.gYABgF9PcqaN7GRKPIDPuqOyda0 (4)
```

June-19-14

TEELtechnologies

BlackBerry 10 PIM Data

- **/settings/accounts/1000/sysdata/pim**



bb10 backup

\bb10 backup ofs\settings\accounts\1000\sysdata\pim\db

Name =!	Path
..	
□ 1-pim.db (8)	\bb10 backup ofs\settings\accounts\1000\sysdata\pim\db
□ 18-pim.db (8)	\bb10 backup ofs\settings\accounts\1000\sysdata\pim\db
□ 2-pim.db (6)	\bb10 backup ofs\settings\accounts\1000\sysdata\pim\db
□ 20-pim.db	\bb10 backup ofs\settings\accounts\1000\sysdata\pim\db
□ 200-pim.db	\bb10 backup ofs\settings\accounts\1000\sysdata\pim\db
□ 3-pim.db	\bb10 backup ofs\settings\accounts\1000\sysdata\pim\db
□ 5-pim.db (3)	\bb10 backup ofs\settings\accounts\1000\sysdata\pim\db
□ 8-pim.db (4)	\bb10 backup ofs\settings\accounts\1000\sysdata\pim\db

BlackBerry 10 PIM Data - Calendar

- 1-pim.db located at:
  - \settings\accounts\1000\sysdata\pim\db.

- CalendarEvent table

- Time values: two time stamp columns in human readable time, stored relative to UTC/GMT.

BlackBerry 10 PIM Data - Contacts

- 2-pim.db located at
  - \settings\accounts\1000\sysdata\pim\db.

- The information related to a contact is spread across these various tables.

BlackBerry 10 PIM Data - Call History/Call Log

- 8-pim.db located at
  - \settings\accounts\1000\sysdata\pim\db.
- Two tables, 'Call' and 'CallDetail' contain similar records; both tables should be analyzed and cross-referenced to detect differences in the data contained therein.
- Time values stored in human readable time, stored relative to UTC/GMT.

BlackBerry 10 PIM Data – Tasks/Reminders

- 18-pim.db located at
  - \settings\accounts\1000\sysdata\pim\db.

- On the BlackBerry device this data is classified under the 'Remember' application.

- Time values stored in human readable time, are presumed to be stored relative to UTC/GMT.

BlackBerry 10 - SMS/MMS

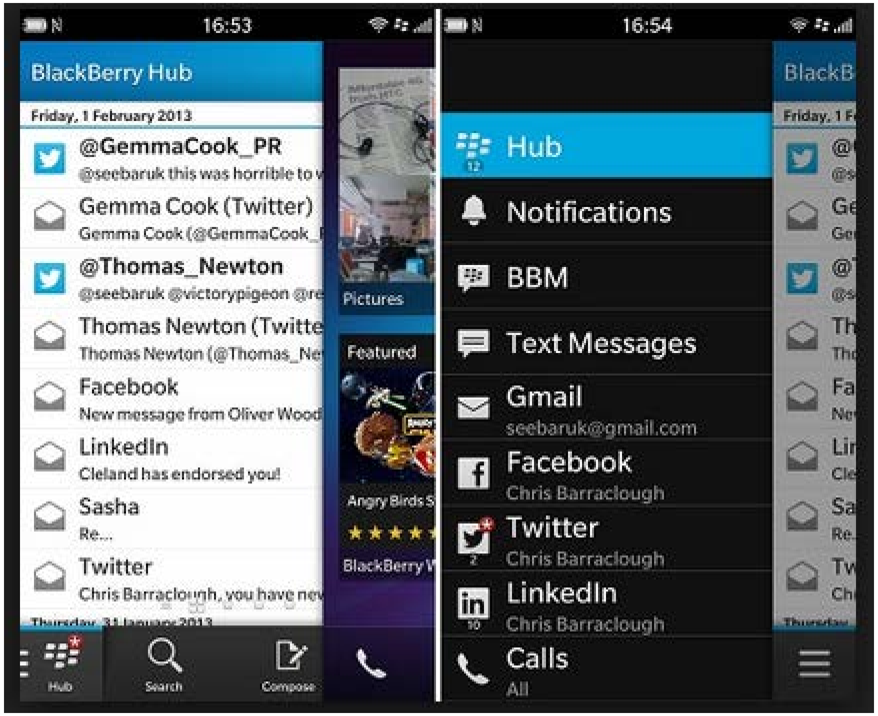
- messages.db located at
  - \settings\var\db\text_messagingsettings\.
- Message content in the Attachments table.
- Timestamp values in Messages table under timeStamp and creationDate columns are stored as 13 character decimal value, which is a Unix epoch time stamp.
  - the inbound fields in the Messages table:0 = sent message, and 1 = received message.
  - the senders name address for sent messages are empty, and the sendersid value is negative integer, -1.

BlackBerry 10 – BBM

- the master.db located at
  - \sys.bbm.gYABgLOJBR2Vz7FzS.kdgJchuag\appdata\data.
- BBM avatar picture resides the in the photos subdirectory, and is named using the BlackBerry PIN value of the device.
- Timestamp field is a 10 character decimal value (compared to the 13 digits for text messages), which is Unix epoch time.
- Because BBM allows voice and video chat, these events are also stored in the messages.db; the CallEventId field assigns an incremental decimal value for the start and end of each voice or video chat.
- IsInbound value: 0 = sent message, and 1 = received message

BlackBerry 10 – BlackBerry Hub (BBH)

- The BlackBerry Hub includes: call log, voicemail notification, email, sms, mms, social networking notifications, BBM, instant messaging, BBM calendar events, and notifications.



BlackBerry Hub

Friday, 1 February 2013

@GemmaCook_PR
@seebaruk this was horrible to w

Gemma Cook (Twitter)
Gemma Cook (@GemmaCook_

@Thomas_Newton
@seebaruk @victorypigeon @re

Thomas Newton (Twitte
Thomas Newton (@Thomas_Ne

Facebook
New message from Oliver Wood

LinkedIn
Cleland has endorsed you!

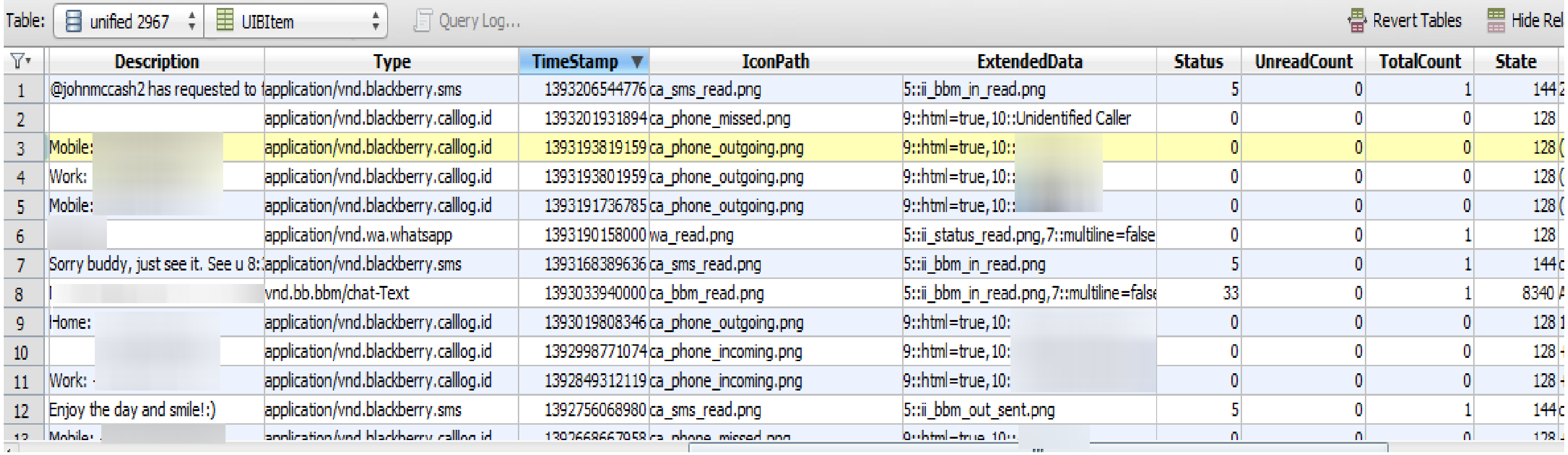
Sasha
Re...

Twitter
Chris Barraclough, you have nev

Thursday, 31 January 2013

BlackBerry 10 – BlackBerry Hub (BBH)

- BBH unintentionally acts as timeline of activity of the BlackBerry 10 device, as it includes data from a number of application areas.
- Path: \sys.pim.messages.gYABgJ8jn83Ok_NEWYplPYozt5w\appdata\data\unfied.db



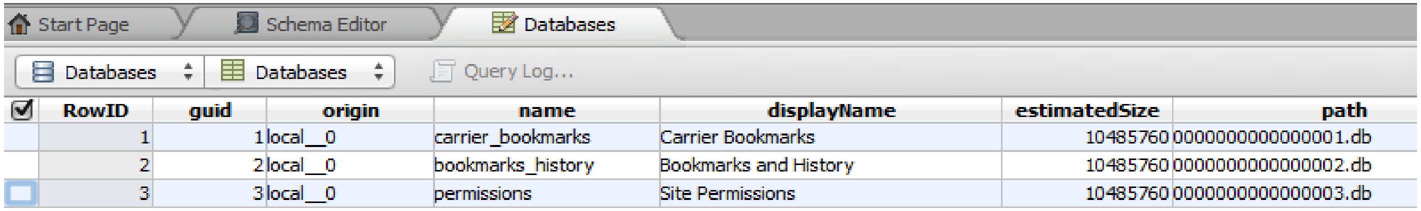
	Description	Type	TimeStamp	IconPath	ExtendedData	Status	UnreadCount	TotalCount	State
1	@johnmccash2 has requested to f	application/vnd.blackberry.sms	1393206544776	ca_sms_read.png	5::ii_bbm_in_read.png	5	0	1	144
2		application/vnd.blackberry.callog.id	1393201931894	ca_phone_missed.png	9::html=true,10::Unidentified Caller	0	0	0	128
3	Mobile: [redacted]	application/vnd.blackberry.callog.id	1393193819159	ca_phone_outgoing.png	9::html=true,10:: [redacted]	0	0	0	128
4	Work: [redacted]	application/vnd.blackberry.callog.id	1393193801959	ca_phone_outgoing.png	9::html=true,10:: [redacted]	0	0	0	128
5	Mobile: [redacted]	application/vnd.blackberry.callog.id	1393191736785	ca_phone_outgoing.png	9::html=true,10:: [redacted]	0	0	0	128
6	[redacted]	application/vnd.wa.whatsapp	1393190158000	wa_read.png	5::ii_status_read.png,7::multiline=false	0	0	1	128
7	Sorry buddy, just see it. See u 8::	application/vnd.blackberry.sms	1393168389636	ca_sms_read.png	5::ii_bbm_in_read.png	5	0	1	144
8	I [redacted]	vnd.bb.bbm/chat-Text	1393033940000	ca_bbm_read.png	5::ii_bbm_in_read.png,7::multiline=false	33	0	1	8340
9	Home: [redacted]	application/vnd.blackberry.callog.id	1393019808346	ca_phone_outgoing.png	9::html=true,10: [redacted]	0	0	0	128
10	[redacted]	application/vnd.blackberry.callog.id	1392998771074	ca_phone_incoming.png	9::html=true,10: [redacted]	0	0	0	128
11	Work: - [redacted]	application/vnd.blackberry.callog.id	1392849312119	ca_phone_incoming.png	9::html=true,10: [redacted]	0	0	0	128
12	Enjoy the day and smile!:)	application/vnd.blackberry.sms	1392756068980	ca_sms_read.png	5::ii_bbm_out_sent.png	5	0	1	144
13	Mobile: [redacted]	application/vnd.blackberry.callog.id	1392668667958	ca_phone_missed.png	9::html=true,10:: [redacted]	0	0	0	128

BlackBerry 10 – BlackBerry Hub (BBH)

- The unified.db database holds some excellent artifacts such as:
  - Type: identifies the application such as callog, whatsapp, sms, notification, bbm.
  - TimeStamp: 13 character decimal value, Unix epoch time.
  - IconPath: indicates the status of the data such as
    - sms_read
    - phone_missed
    - phone_outgoing
    - phone_incoming
    - bbm_read
    - notification_read

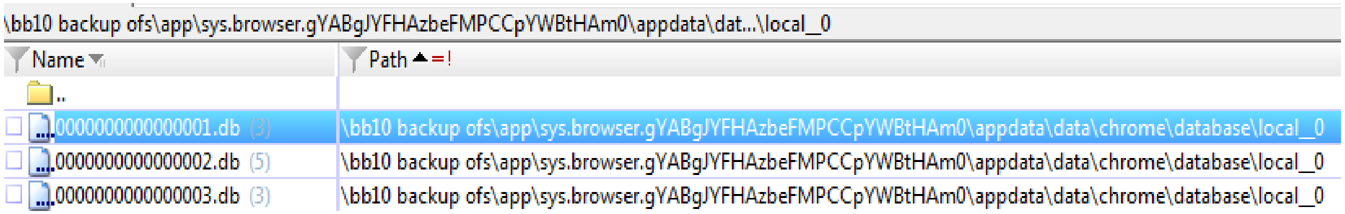
BlackBerry 10 – Internet

- The Internet history artifacts are stored in several areas within the backup structure.
- **Internet Artifacts Location 1:** \app\sys.browser.gYABgJYFHAzbeFMPCCpYWBtHAm0\appdata\data\chrome\database\Databases.db



☑	RowID	guid	origin	name	displayName	estimatedSize	path
	1	1	local__0	carrier_bookmarks	Carrier Bookmarks	10485760	0000000000000001.db
	2	2	local__0	bookmarks_history	Bookmarks and History	10485760	0000000000000002.db
	3	3	local__0	permissions	Site Permissions	10485760	0000000000000003.db

- This file identifies the name of three databases, so next we examine the database files listed in the path field, which are all stored in the same sub directory structure.

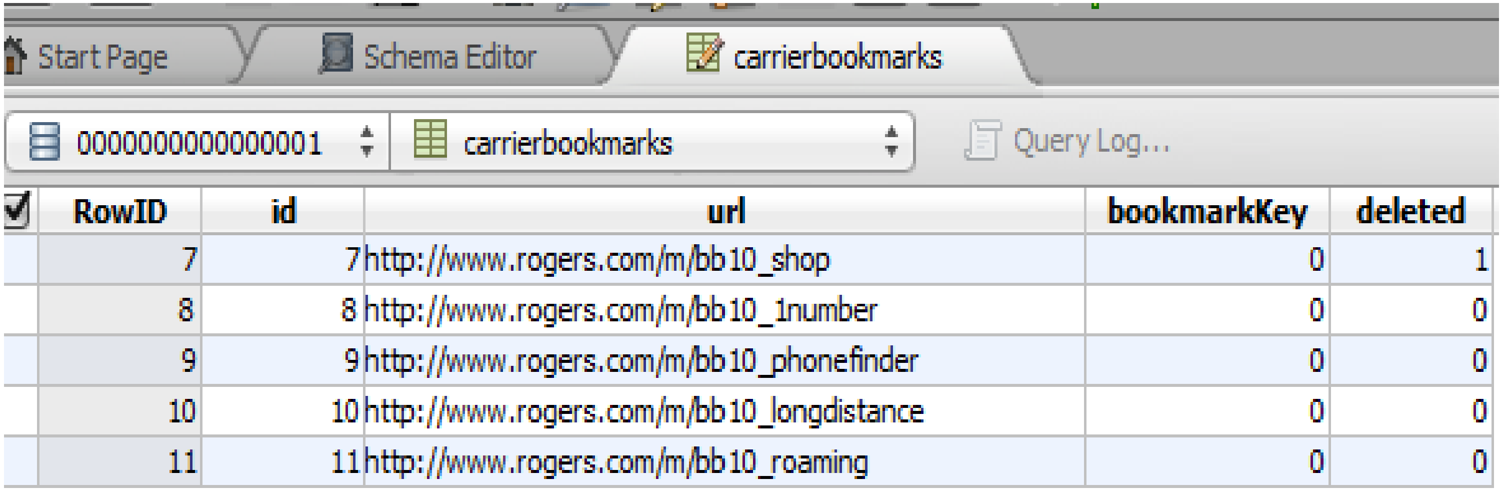


\bb10 backup ofs\app\sys.browser.gYABgJYFHAzbeFMPCCpYWBtHAm0\appdata\dat...\local_0

Name	Path
..	
□ 0000000000000001.db (3)	\bb10 backup ofs\app\sys.browser.gYABgJYFHAzbeFMPCCpYWBtHAm0\appdata\data\chrome\database\local_0
□ 0000000000000002.db (5)	\bb10 backup ofs\app\sys.browser.gYABgJYFHAzbeFMPCCpYWBtHAm0\appdata\data\chrome\database\local_0
□ 0000000000000003.db (3)	\bb10 backup ofs\app\sys.browser.gYABgJYFHAzbeFMPCCpYWBtHAm0\appdata\data\chrome\database\local_0

BlackBerry 10 – Internet

- Carrier bookmarks = 0000000000000001.db: this contains the carrier provided website bookmarks.



☑	RowID	id	url	bookmarkKey	deleted
	7	7	http://www.rogers.com/m/bb10_shop	0	1
	8	8	http://www.rogers.com/m/bb10_1number	0	0
	9	9	http://www.rogers.com/m/bb10_phonefinder	0	0
	10	10	http://www.rogers.com/m/bb10_longdistance	0	0
	11	11	http://www.rogers.com/m/bb10_roaming	0	0

June-19-14

BlackBerry 10 – Internet

- Bookmarks and History = 0000000000000002.db: this contains the device user's Internet history and user bookmarks:
  - The history table, urlKey field, is related to the urls table id field

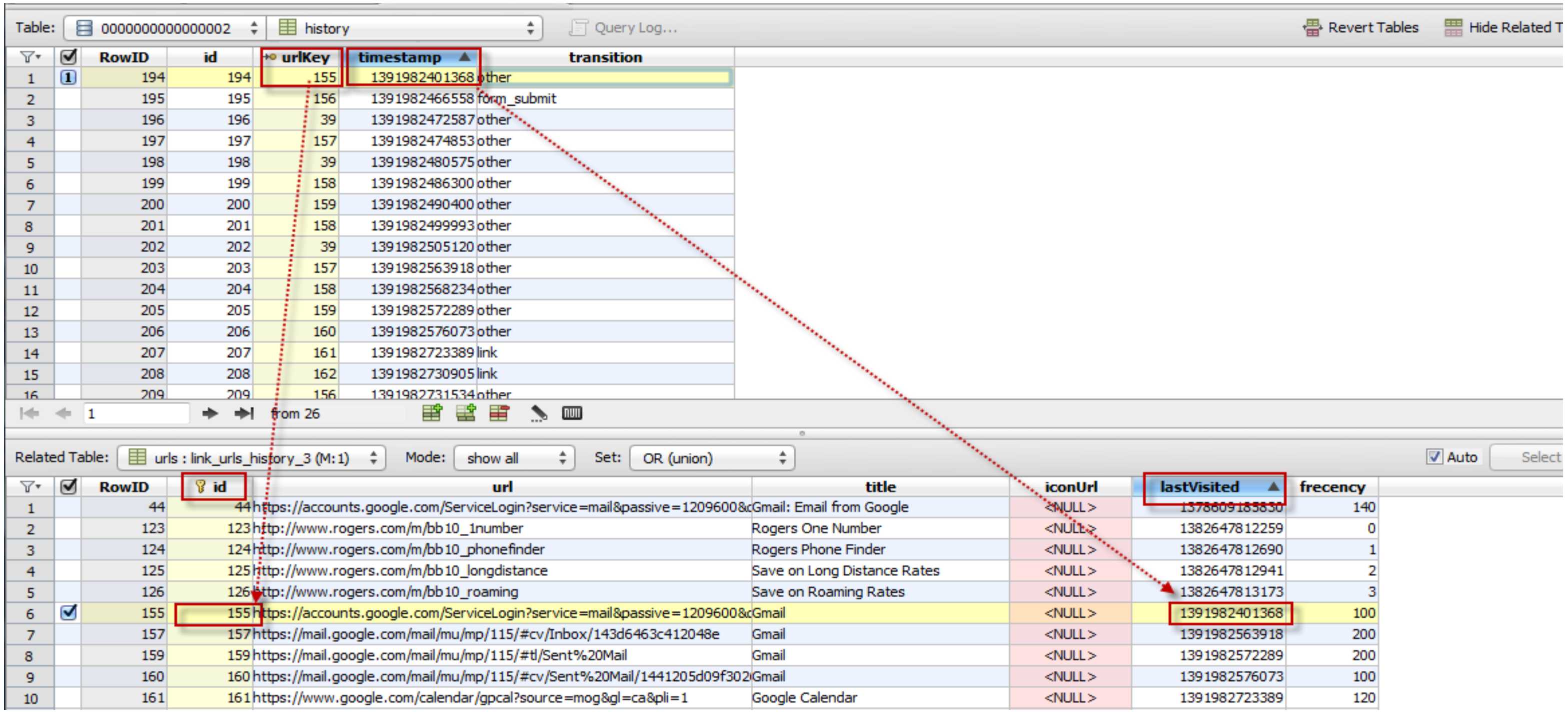


Table: 0000000000000002 history

	☑	RowID	id	urlKey	timestamp ▲	transition
1	1	194	194	155	1391982401368	other
2		195	195	156	1391982466558	form_submit
3		196	196	39	1391982472587	other
4		197	197	157	1391982474853	other
5		198	198	39	1391982480575	other
6		199	199	158	1391982486300	other
7		200	200	159	1391982490400	other
8		201	201	158	1391982499993	other
9		202	202	39	1391982505120	other
10		203	203	157	1391982563918	other
11		204	204	158	1391982568234	other
12		205	205	159	1391982572289	other
13		206	206	160	1391982576073	other
14		207	207	161	1391982723389	link
15		208	208	162	1391982730905	link
16		209	209	156	1391982731534	other

1 from 26

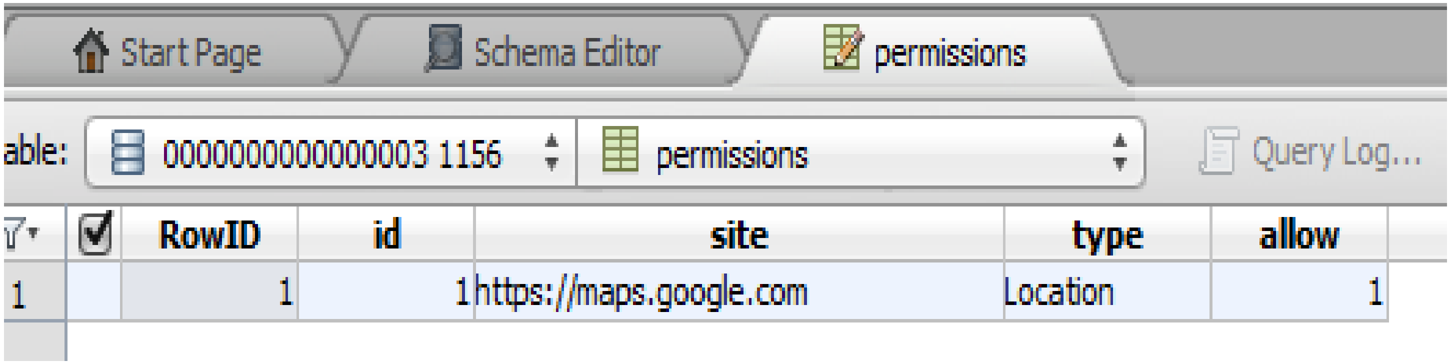
Related Table: urls : link_urls_history_3 (M:1) Mode: show all Set: OR (union) ☑ Auto

	☑	RowID	id	url	title	iconUrl	lastVisited ▲	frecency
1		44	44	https://accounts.google.com/ServiceLogin?service=mail&passive=1209600&c	Gmail: Email from Google	<NULL>	1378609185830	140
2		123	123	http://www.rogers.com/m/bb10_1number	Rogers One Number	<NULL>	1382647812259	0
3		124	124	http://www.rogers.com/m/bb10_phonefinder	Rogers Phone Finder	<NULL>	1382647812690	1
4		125	125	http://www.rogers.com/m/bb10_longdistance	Save on Long Distance Rates	<NULL>	1382647812941	2
5		126	126	http://www.rogers.com/m/bb10_roaming	Save on Roaming Rates	<NULL>	1382647813173	3
6	☑	155	155	https://accounts.google.com/ServiceLogin?service=mail&passive=1209600&c	Gmail	<NULL>	1391982401368	100
7		157	157	https://mail.google.com/mail/mu/mp/115/#cv/Inbox/143d6463c412048e	Gmail	<NULL>	1391982563918	200
8		159	159	https://mail.google.com/mail/mu/mp/115/#tl/Sent%20Mail	Gmail	<NULL>	1391982572289	200
9		160	160	https://mail.google.com/mail/mu/mp/115/#cv/Sent%20Mail/1441205d09f302	Gmail	<NULL>	1391982576073	100
10		161	161	https://www.google.com/calendar/gpcal?source=mog&gl=ca&pli=1	Google Calendar	<NULL>	1391982723389	120

TEELtechnologies

BlackBerry 10 – Internet

- Permissions = 0000000000000003.db: this database contains permissions that are assigned to it by the device user.
  - In this case, it appears as though the Google Maps URL has been given permission to access the device, based on the allow value of 1. The value of 0 = not allowed.



able: 0000000000000003 1156 | permissions

	☑	RowID	id	site	type	allow
1		1	1	https://maps.google.com	Location	1

BlackBerry 10 – Internet

- **Internet Artifacts Location 2:**
- The next file of interest is the local__0.localstorage SQLite file located at:

\app\sys.browser.gYABgJYFHAzbeFMPCCpYWBtHAm0\appdata\data\chrome

- This contain the browser settings in the local__0.localstorage SQLite file.

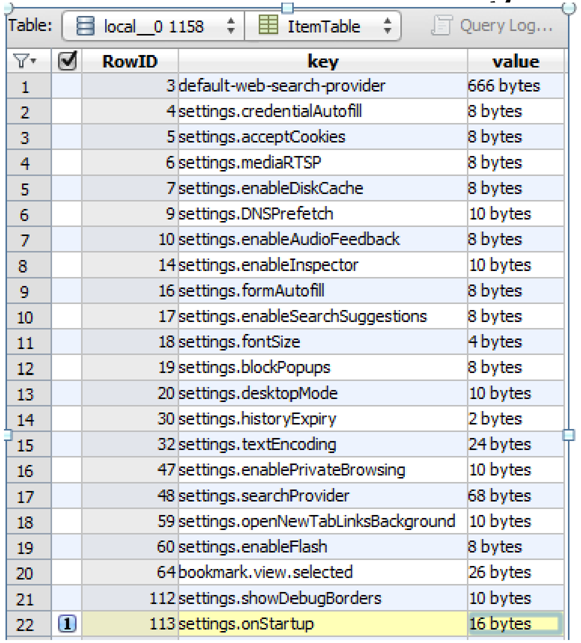


Table: local__0 1158 ItemTable Query Log...

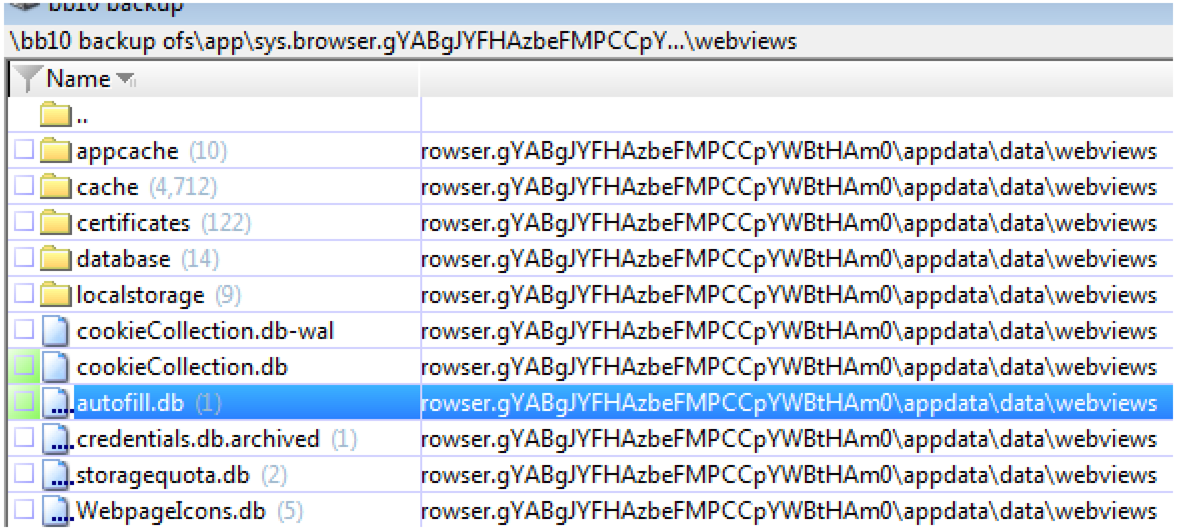
	☑	RowID	key	value
1		3	default-web-search-provider	666 bytes
2		4	settings.credentialAutofill	8 bytes
3		5	settings.acceptCookies	8 bytes
4		6	settings.mediaRTSP	8 bytes
5		7	settings.enableDiskCache	8 bytes
6		9	settings.DNSPrefetch	10 bytes
7		10	settings.enableAudioFeedback	8 bytes
8		14	settings.enableInspector	10 bytes
9		16	settings.formAutofill	8 bytes
10		17	settings.enableSearchSuggestions	8 bytes
11		18	settings.fontSize	4 bytes
12		19	settings.blockPopups	8 bytes
13		20	settings.desktopMode	10 bytes
14		30	settings.historyExpiry	2 bytes
15		32	settings.textEncoding	24 bytes
16		47	settings.enablePrivateBrowsing	10 bytes
17		48	settings.searchProvider	68 bytes
18		59	settings.openNewTabLinksBackground	10 bytes
19		60	settings.enableFlash	8 bytes
20		64	bookmark.view.selected	26 bytes
21		112	settings.showDebugBorders	10 bytes
22	1	113	settings.onStartup	16 bytes

June-19-14

BlackBerry 10 – Internet

- **Internet Artifacts Location 3:**
- The areas of interest are the files and folders stored in the path at:

\app\sys.browser.gYABgJYFHAzbeFMPCCpYWBtHAm0\appdata\data\webviews



bb10 backup

\bb10 backup ofs\app\sys.browser.gYABgJYFHAzbeFMPCCpY...\webviews

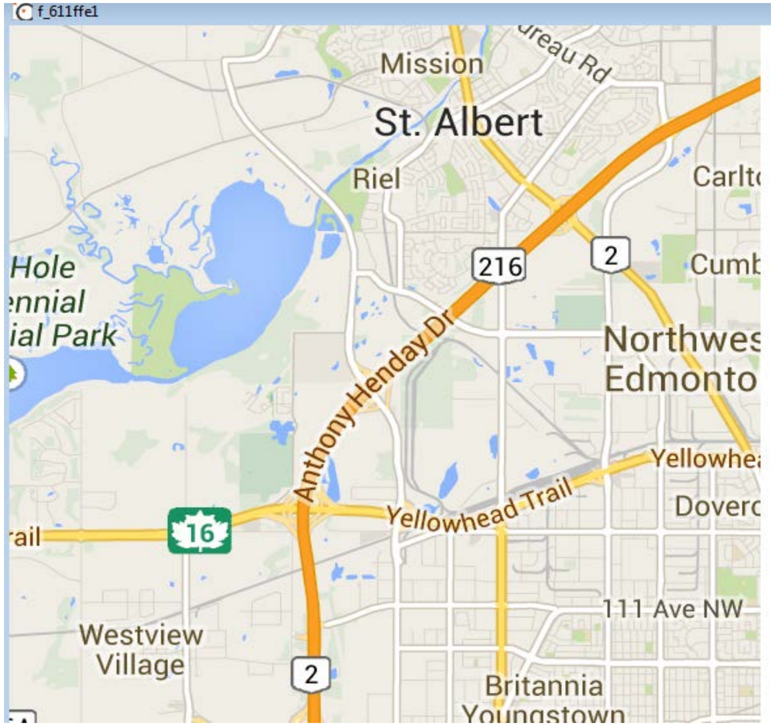
	Name	
	..	
□	appcache (10)	rowser.gYABgJYFHAzbeFMPCCpYWBtHAm0\appdata\data\webviews
□	cache (4,712)	rowser.gYABgJYFHAzbeFMPCCpYWBtHAm0\appdata\data\webviews
□	certificates (122)	rowser.gYABgJYFHAzbeFMPCCpYWBtHAm0\appdata\data\webviews
□	database (14)	rowser.gYABgJYFHAzbeFMPCCpYWBtHAm0\appdata\data\webviews
□	localstorage (9)	rowser.gYABgJYFHAzbeFMPCCpYWBtHAm0\appdata\data\webviews
□	cookieCollection.db-wal	rowser.gYABgJYFHAzbeFMPCCpYWBtHAm0\appdata\data\webviews
☑	cookieCollection.db	rowser.gYABgJYFHAzbeFMPCCpYWBtHAm0\appdata\data\webviews
☑	autofill.db (1)	rowser.gYABgJYFHAzbeFMPCCpYWBtHAm0\appdata\data\webviews
□	credentials.db.archived (1)	rowser.gYABgJYFHAzbeFMPCCpYWBtHAm0\appdata\data\webviews
□	storagequota.db (2)	rowser.gYABgJYFHAzbeFMPCCpYWBtHAm0\appdata\data\webviews
□	WebpageIcons.db (5)	rowser.gYABgJYFHAzbeFMPCCpYWBtHAm0\appdata\data\webviews

BlackBerry 10 – Internet

- **Internet Artifacts Location 4:**
- Browser cache files are stored at the path:
  - \app\sys.browser.gYABgJYFHAzbeFMPCCpYWBtHAm0\appdata\data\webviews\cache
  - \app\sys.browser.gYABgJYFHAzbeFMPCCpYWBtHAm0\appdata\data\webviews\cache\[data_1|data_2|data_3]
- The cache can also include Google Map tiles that are cached when accessing Google Maps for location and map information from the device.

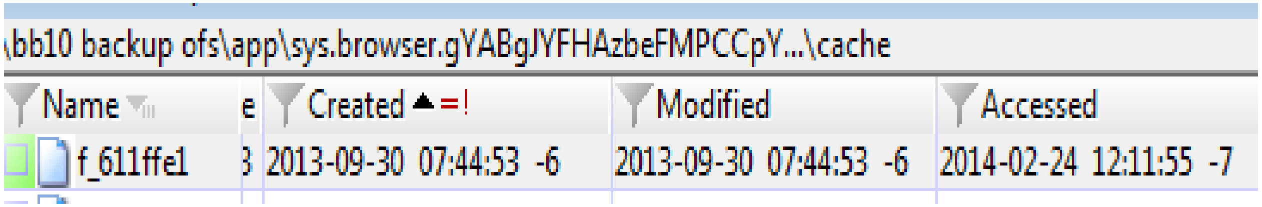
BlackBerry 10 – Internet

Cache Example: this google map tile shows an area of northwest Edmonton AB along the ring road, Anthony Henday Dr.



BlackBerry 10 – Internet

- The file system time stamps from XWF 17.5 SR6 show that the file was created on 2013-09-30 07:44:53 -6. During that week the author (along with another colleague) was in Edmonton, attending an X-Ways Forensics Class!



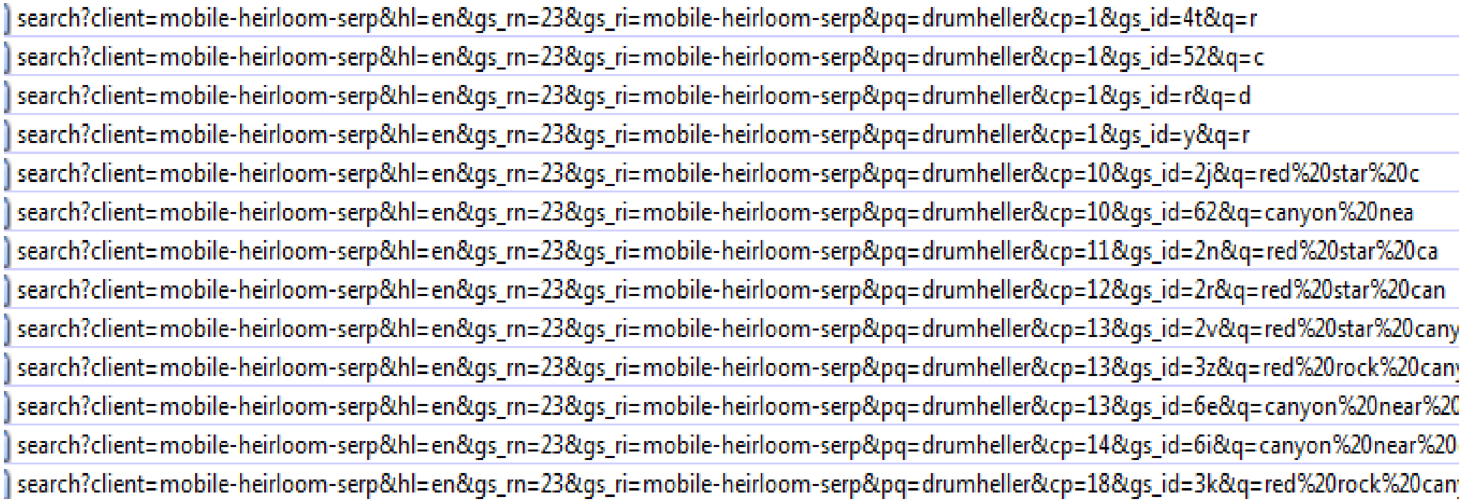
\bb10 backup ofs\app\sys.browser.gYABgJYFHAzbeFMPCCpY...\cache

Name	e	Created ▲=!	Modified	Accessed
f_611ffe1	3	2013-09-30 07:44:53 -6	2013-09-30 07:44:53 -6	2014-02-24 12:11:55 -7

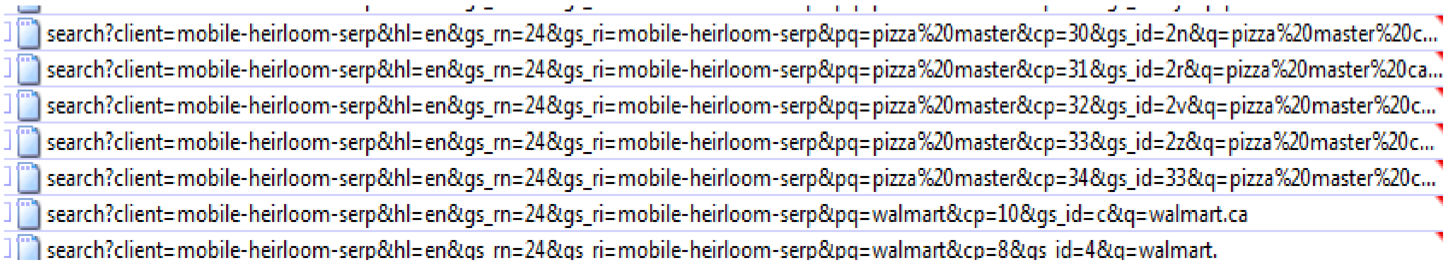
- By looking at the remainder of the google map tile files, and the proximity of the time stamps for the surrounding google map tiles, an inference can be drawn as to where the device (and possibly the device owner/user) was.

BlackBerry 10 – Internet

- Examining the subfolder below the cache, which is the data_1 (and the remaining ‘data_X’ folders, we can see that it contains search query strings.



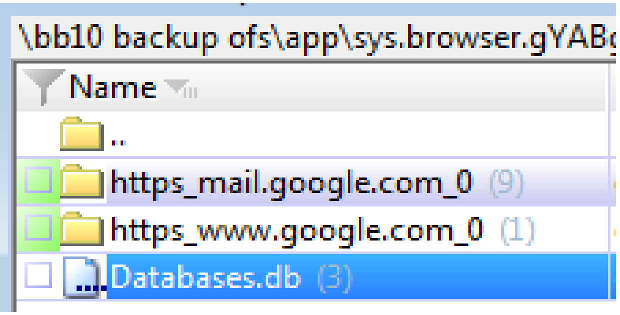
```
search?client=mobile-heirloom-serp&hl=en&gs_rn=23&gs_ri=mobile-heirloom-serp&pq=drumheller&cp=1&gs_id=4t&q=r
search?client=mobile-heirloom-serp&hl=en&gs_rn=23&gs_ri=mobile-heirloom-serp&pq=drumheller&cp=1&gs_id=52&q=c
search?client=mobile-heirloom-serp&hl=en&gs_rn=23&gs_ri=mobile-heirloom-serp&pq=drumheller&cp=1&gs_id=r&q=d
search?client=mobile-heirloom-serp&hl=en&gs_rn=23&gs_ri=mobile-heirloom-serp&pq=drumheller&cp=1&gs_id=y&q=r
search?client=mobile-heirloom-serp&hl=en&gs_rn=23&gs_ri=mobile-heirloom-serp&pq=drumheller&cp=10&gs_id=2j&q=red%20star%20c
search?client=mobile-heirloom-serp&hl=en&gs_rn=23&gs_ri=mobile-heirloom-serp&pq=drumheller&cp=10&gs_id=62&q=canyon%20nea
search?client=mobile-heirloom-serp&hl=en&gs_rn=23&gs_ri=mobile-heirloom-serp&pq=drumheller&cp=11&gs_id=2n&q=red%20star%20ca
search?client=mobile-heirloom-serp&hl=en&gs_rn=23&gs_ri=mobile-heirloom-serp&pq=drumheller&cp=12&gs_id=2r&q=red%20star%20can
search?client=mobile-heirloom-serp&hl=en&gs_rn=23&gs_ri=mobile-heirloom-serp&pq=drumheller&cp=13&gs_id=2v&q=red%20star%20cany
search?client=mobile-heirloom-serp&hl=en&gs_rn=23&gs_ri=mobile-heirloom-serp&pq=drumheller&cp=13&gs_id=3z&q=red%20rock%20can
search?client=mobile-heirloom-serp&hl=en&gs_rn=23&gs_ri=mobile-heirloom-serp&pq=drumheller&cp=13&gs_id=6e&q=canyon%20near%20
search?client=mobile-heirloom-serp&hl=en&gs_rn=23&gs_ri=mobile-heirloom-serp&pq=drumheller&cp=14&gs_id=6i&q=canyon%20near%20
search?client=mobile-heirloom-serp&hl=en&gs_rn=23&gs_ri=mobile-heirloom-serp&pq=drumheller&cp=18&gs_id=3k&q=red%20rock%20can
```



```
search?client=mobile-heirloom-serp&hl=en&gs_rn=24&gs_ri=mobile-heirloom-serp&pq=pizza%20master&cp=30&gs_id=2n&q=pizza%20master%20c...
search?client=mobile-heirloom-serp&hl=en&gs_rn=24&gs_ri=mobile-heirloom-serp&pq=pizza%20master&cp=31&gs_id=2r&q=pizza%20master%20ca...
search?client=mobile-heirloom-serp&hl=en&gs_rn=24&gs_ri=mobile-heirloom-serp&pq=pizza%20master&cp=32&gs_id=2v&q=pizza%20master%20c...
search?client=mobile-heirloom-serp&hl=en&gs_rn=24&gs_ri=mobile-heirloom-serp&pq=pizza%20master&cp=33&gs_id=2z&q=pizza%20master%20c...
search?client=mobile-heirloom-serp&hl=en&gs_rn=24&gs_ri=mobile-heirloom-serp&pq=pizza%20master&cp=34&gs_id=33&q=pizza%20master%20c...
search?client=mobile-heirloom-serp&hl=en&gs_rn=24&gs_ri=mobile-heirloom-serp&pq=walmart&cp=10&gs_id=c&q=walmart.ca
search?client=mobile-heirloom-serp&hl=en&gs_rn=24&gs_ri=mobile-heirloom-serp&pq=walmart&cp=8&gs_id=4&q=walmart.
```

BlackBerry 10 – Internet

- **Internet Artifacts Location 5:**
- This location path contains cached web based email content, stored in SQLite databases.
- Path: \app\sys.browser.gYABgJYFHAzbeFMPCCpYWBtHAm0\appdata\data\webviews\database



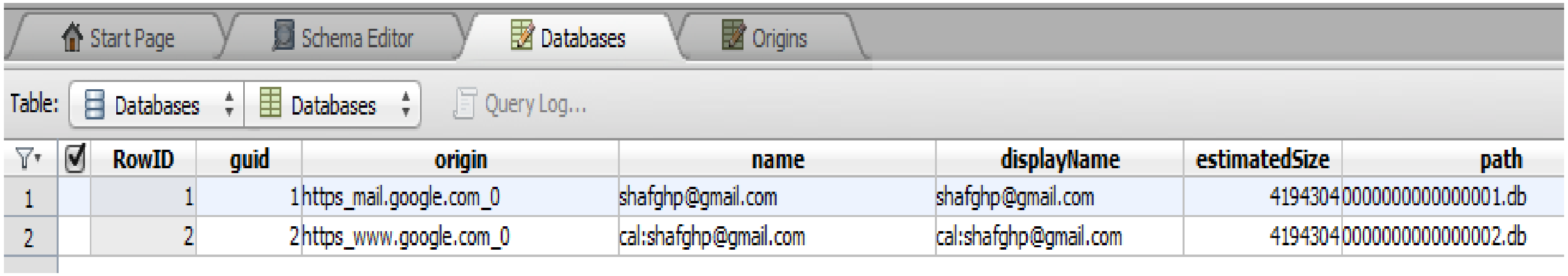
\bb10 backup ofs\app\sys.browser.gYABg

Name
..
https_mail.google.com_0 (9)
https_www.google.com_0 (1)
Databases.db (3)

June-19-14

BlackBerry 10 – Internet

- In the root of the database folder there is a Databases.db which identifies the email account relative to its corresponding database file.

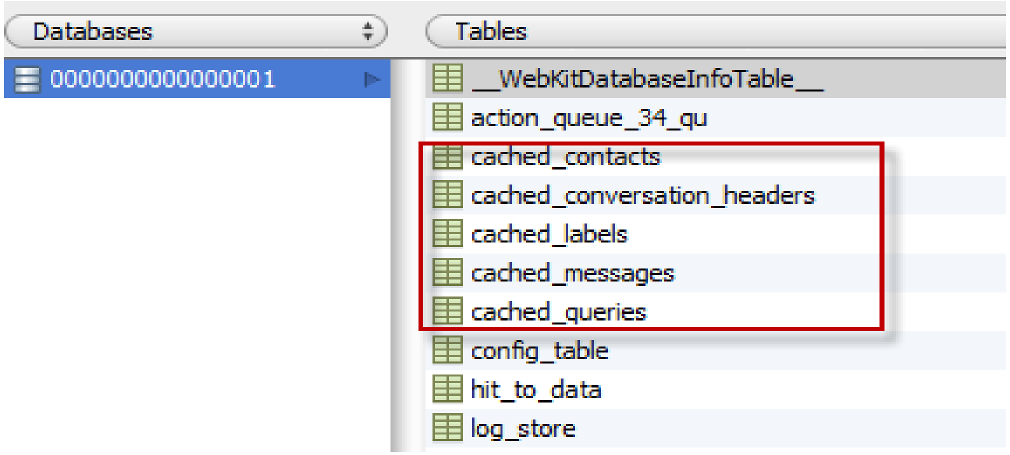


	☑	RowID	guid	origin	name	displayName	estimatedSize	path
1		1	1	https_mail.google.com_0	shafghp@gmail.com	shafghp@gmail.com	4194304	0000000000000001.db
2		2	2	https_www.google.com_0	cal:shafghp@gmail.com	cal:shafghp@gmail.com	4194304	0000000000000002.db

June-19-14

BlackBerry 10 – Internet

- **0000000000000001.db:**
  - The tables contain time values as Unix epoch time, from 13 – 16 decimal characters in length.

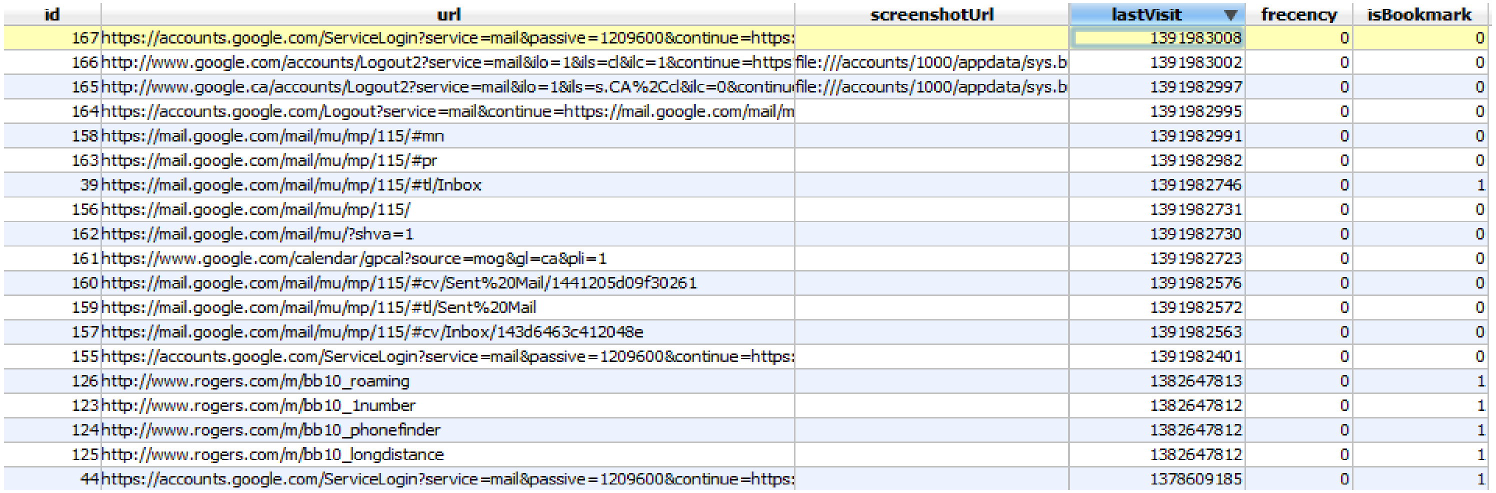


0000000000000001

__WebKitDatabaseInfoTable__
action_queue_34_qu
cached_contacts
cached_conversation_headers
cached_labels
cached_messages
cached_queries
config_table
hit_to_data
log_store

BlackBerry 10 – Internet

- **Internet Artifacts Location 6:**
- This path location contains the visited URL's accessed by the device.
- Path \app\sys.browser.gYABgJYFHAzbeFMPCCpYWBtHAm0 \sharewith\search



id	url	screenshotUrl	lastVisit	frecency	isBookmark
167	https://accounts.google.com/ServiceLogin?service=mail&passive=1209600&continue=https:		1391983008	0	0
166	http://www.google.com/accounts/Logout2?service=mail&ilo=1&ils=cl&ilc=1&continue=https	file:///accounts/1000/appdata/sys.b	1391983002	0	0
165	http://www.google.ca/accounts/Logout2?service=mail&ilo=1&ils=s.CA%2Ccl&ilc=0&continu	file:///accounts/1000/appdata/sys.b	1391982997	0	0
164	https://accounts.google.com/Logout?service=mail&continue=https://mail.google.com/mail/m		1391982995	0	0
158	https://mail.google.com/mail/mu/mp/115/#mn		1391982991	0	0
163	https://mail.google.com/mail/mu/mp/115/#pr		1391982982	0	0
39	https://mail.google.com/mail/mu/mp/115/#tl/Inbox		1391982746	0	1
156	https://mail.google.com/mail/mu/mp/115/		1391982731	0	0
162	https://mail.google.com/mail/mu/?shva=1		1391982730	0	0
161	https://www.google.com/calendar/gpcal?source=mog&gl=ca&pli=1		1391982723	0	0
160	https://mail.google.com/mail/mu/mp/115/#cv/Sent%20Mail/1441205d09f30261		1391982576	0	0
159	https://mail.google.com/mail/mu/mp/115/#tl/Sent%20Mail		1391982572	0	0
157	https://mail.google.com/mail/mu/mp/115/#cv/Inbox/143d6463c412048e		1391982563	0	0
155	https://accounts.google.com/ServiceLogin?service=mail&passive=1209600&continue=https:		1391982401	0	0
126	http://www.rogers.com/m/bb10_roaming		1382647813	0	1
123	http://www.rogers.com/m/bb10_1number		1382647812	0	1
124	http://www.rogers.com/m/bb10_phonefinder		1382647812	0	1
125	http://www.rogers.com/m/bb10_longdistance		1382647812	0	1
44	https://accounts.google.com/ServiceLogin?service=mail&passive=1209600&continue=https:		1378609185	0	1

BlackBerry 10 – Pictures

- Several categories of pictures that can be found on the Blackberry 10 device.

1. First category is user created pictures taken with the BlackBerry 10 device:

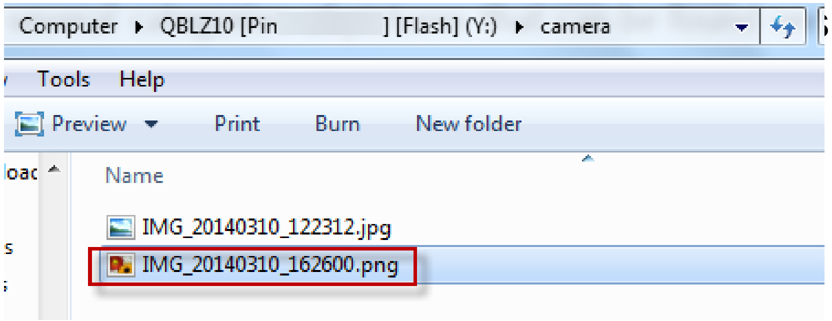
- Under 'Camera Settings' if the 'Save on Media Card is 'On' then device created pictures are saved to the memory card under the path /sdcard/camera.

- If the 'Save on Media Card' is set to 'Off' then the device created pictures are saved to the device memory at /media/camera.

- Under 'Camera Settings' if the 'Geotag Pictures' is 'On' this will add the device's GPS location to the pictures, provided that it can receive the GPS signal.

BlackBerry 10 – Pictures

2. Second category is device created screenshots.

- This refers to the device user taking a screenshot of the contents being displayed on the BlackBerry 10 device by pressing the Volume Up AND Volume Down buttons. **There is no EXIF data present in a BlackBerry 10 PNG screenshot picture.**
- The image is saved as a PNG file in the \media\camera, NOT the memory card regardless of the 'Camera Settings' -> 'Save on Media Card is 'On' feature.
  - The PNG file name will be IMG_YYYYMMDD_XXXXX.PNG and contains the date and time the PNG file was created.
    - YYYYMMDD = 4 decimal values to represent year, 2 decimal values to represent, 2 decimal values to represent day.
    - 

Computer ▸ QBLZ10 [Pin] [Flash] (Y:) ▸ camera

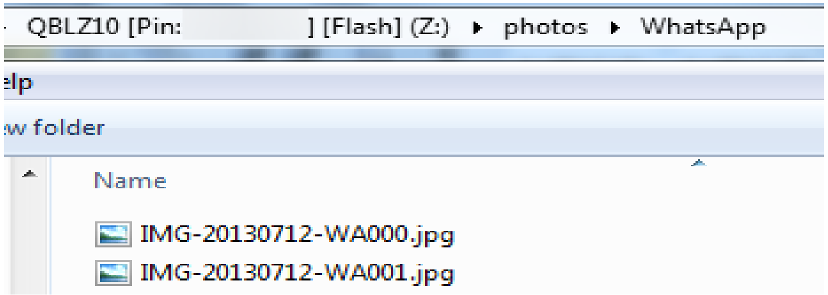
IMG_20140310_122312.jpg
IMG_20140310_162600.png

s.

BlackBerry 10 – Pictures

3. Third category is pictures stored in /sdcard/photos or /media/photos.

- The author has observed the /media/photos folder location will store pictures transferred, during an upgrade from an older BlackBerry device that contains pictures, to a BlackBerry 10 device.



QBLZ10 [Pin: [redacted]] [Flash] (Z:) ▸ photos ▸ WhatsApp

elp

w folder

Name

IMG-20130712-WA000.jpg

IMG-20130712-WA001.jpg

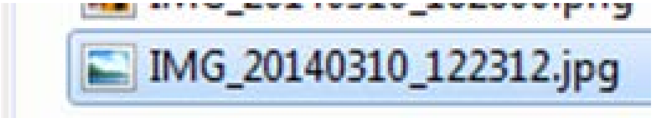
- The file name convention of a WA image contains a date value as YYYMMDD followed by WAXXX, where the XXX is a 3 digit numeric sequence.
- The date value will match the date the picture is received by the device.
- **The images are stripped of any of the usual EXIF data.**

BlackBerry 10 – EXIF Pictures

EXIF Summary

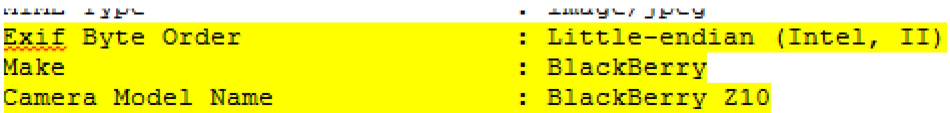
1. BlackBerry 10 software 10.2.1.2141:

- Embeds the date and time value, local to device time, within the file name of the picture created using the Camera application of the device.



IMG_20140310_122312.jpg

- Now adds the Model value of BlackBerry Z10 within the EXIF, which was not done prior to 10.2.1.2141.



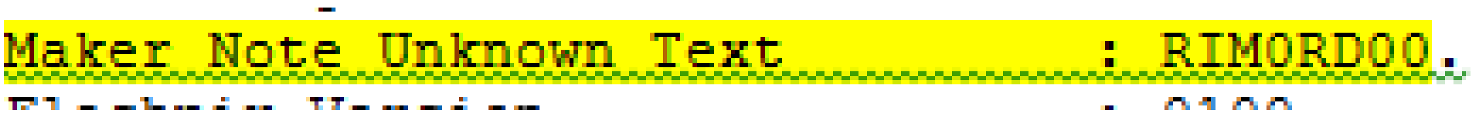
```
MIME Type                               : image/jpeg
Exif Byte Order                         : Little-endian (Intel, II)
Make                                    : BlackBerry
Camera Model Name                       : BlackBerry Z10
```

- If the BlackBerry 10 device OS was **less than** 10.2.1.214, the file name convention DOES NOT contain date or time value. It is formatted as IMG_ XXXXXXXX.JPG, where XXXXXXXX equals an 8 character, sequential numeric value.

BlackBerry 10 – EXIF Pictures

EXIF Summary

2. Regardless of the BlackBerry 10 OS version, within the EXIF, there is a unique string value, 'RIM0RD00' in pictures created with the camera application. I refer to this as the ‘**MNUT Value**’.



```
Maker Note Unknown Text                    : RIM0RD00.
Flashpix Version                           : 0100
```

BlackBerry 10 – EXIF Pictures

EXIF Summary

3. Pictures, taken with a BlackBerry Z10, viewed on the memory card, through the device, under the camera folder, appear to show a Modified Date value with wrong offset calculation being applied.

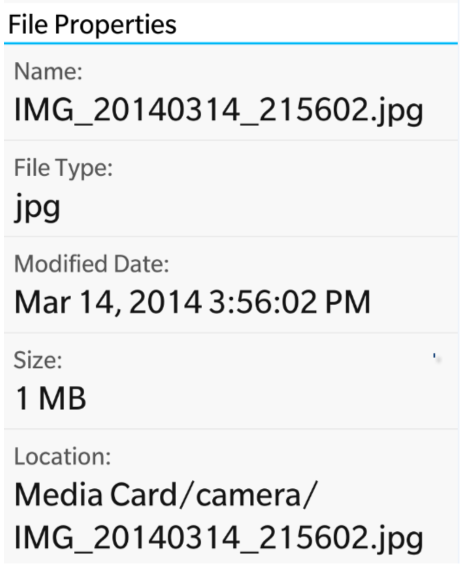
As an example we are going to look at file properties of the following files as displayed by the BlackBerry Z10:

- IMG_20140314_215602.jpg: As the filename indicates, the picture was taken with a BlackBerry Z10 on 2013-03-14, 21:56:02, local device time.

BlackBerry 10 – EXIF Pictures

EXIF Summary

3. The 'Modified Date' value is shown with a ***minus 6 hour difference*** in time relative to the filename time value.



File Properties

Name:
IMG_20140314_215602.jpg

File Type:
jpg

Modified Date:
Mar 14, 2014 3:56:02 PM

Size:
1 MB

Location:
Media Card/camera/
IMG_20140314_215602.jpg

- offset should be 6 hours (plus 6 hours) ahead of the filename time value, so the Modified Date value should show as Mar 15, 2014 at 3:56:02 AM.

- offset is being calculated in the wrong direction, if the intent is to show the Modified Date value in UTC.

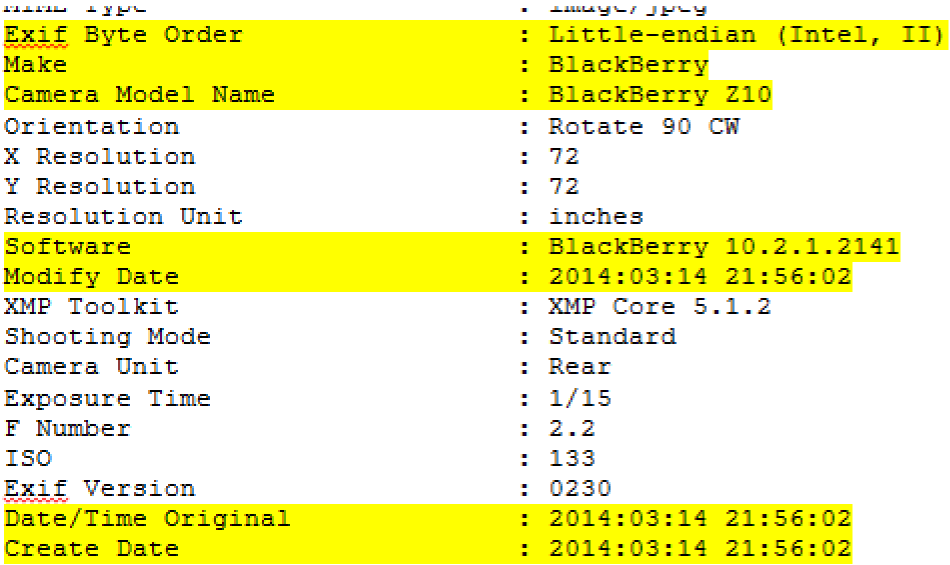
June-19-14

TEELtechnologies

BlackBerry 10 – EXIF Pictures

EXIF Summary

3. ExifTool 9.56 output of IMG_20140314_215602.jpg.



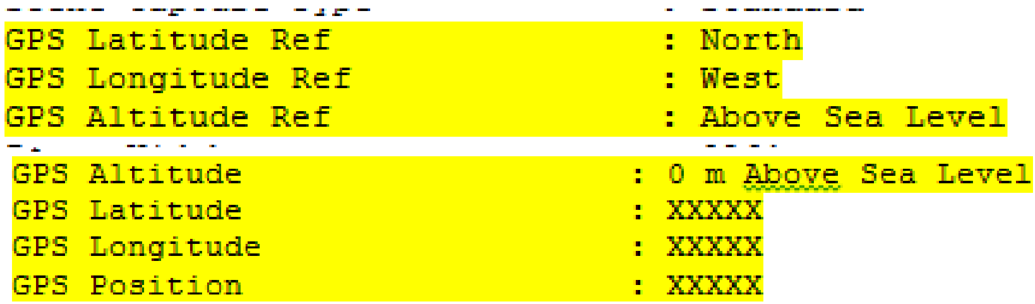
```
MIME Type                       : image/jpeg
Exif Byte Order                 : Little-endian (Intel, II)
Make                            : BlackBerry
Camera Model Name               : BlackBerry Z10
Orientation                     : Rotate 90 CW
X Resolution                    : 72
Y Resolution                    : 72
Resolution Unit                 : inches
Software                        : BlackBerry 10.2.1.2141
Modify Date                     : 2014:03:14 21:56:02
XMP Toolkit                     : XMP Core 5.1.2
Shooting Mode                   : Standard
Camera Unit                     : Rear
Exposure Time                   : 1/15
F Number                        : 2.2
ISO                             : 133
Exif Version                    : 0230
Date/Time Original              : 2014:03:14 21:56:02
Create Date                     : 2014:03:14 21:56:02
```

BlackBerry 10 – EXIF Pictures

EXIF Summary

4. The time values that are within the EXIF data of pictures created with BlackBerry Z10 device contain the time values of picture creation relative to the device's local time.

5. GPS data is present in EXIF so long as that option is enabled in the Camera settings and the device can receive the GPS signal. In the screens shots below the GPS Lat and Long values have been sanitized.



```
GPS Latitude Ref                      : North
GPS Longitude Ref                     : West
GPS Altitude Ref                      : Above Sea Level

GPS Altitude                        : 0 m Above Sea Level
GPS Latitude                        : XXXXX
GPS Longitude                       : XXXXX
GPS Position                        : XXXXX
```

June-19-14

BlackBerry 10 – Movies

There are several categories of movies that can be found on the Blackberry 10 device.

1. First category is user created movies taken with the BlackBerry 10 device:

- Under 'Camera Settings' if the 'Save on Media Card is 'On' then device created movies are saved to the memory card under the path /sdcard/camera.

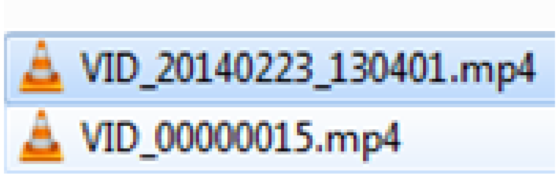
- If the 'Save on Media Card' is set to 'Off' then the device created pictures are saved the device memory at /media/camera.

BlackBerry 10 – Movies

2. Second category is movies stored in /sdcard/videos or /media/videos.

- These locations are believed to contain content downloaded by the device or sent by messaging to the device.

- Note the file naming convention difference between first and second file indicates the MP4 files were created with two different BlackBerry 10 operating system versions. This follows the same pattern as was noted with the pictures.

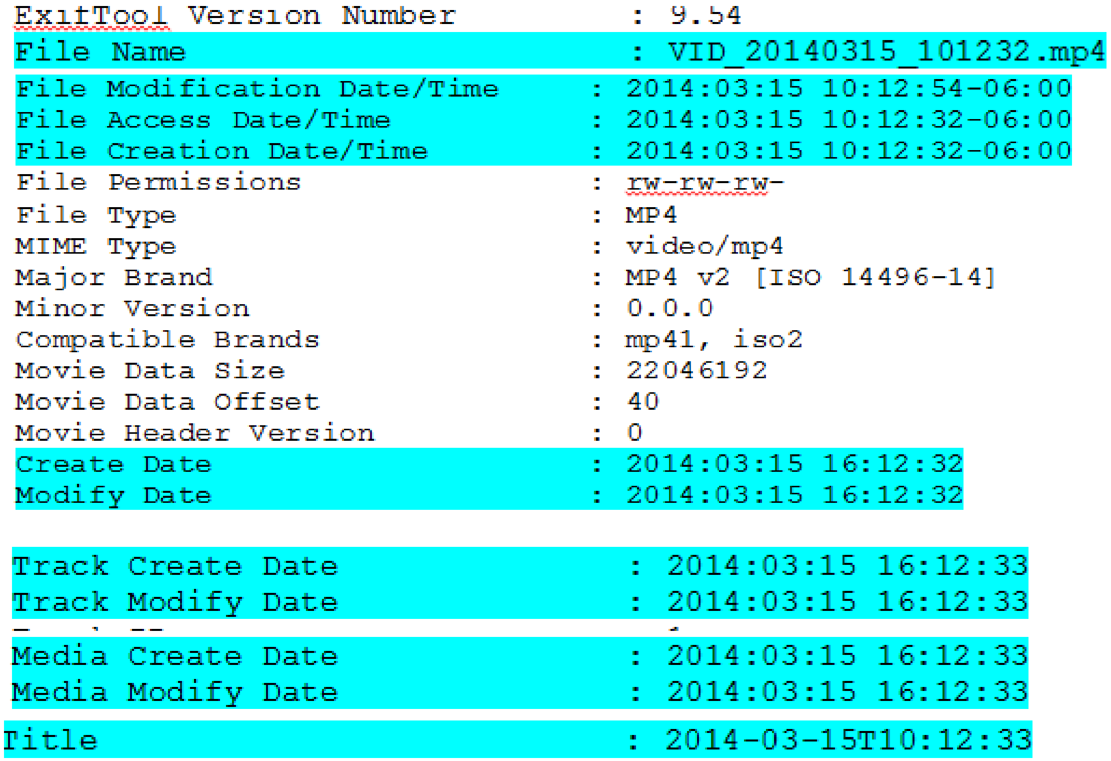


VID_20140223_130401.mp4
VID_00000015.mp4

BlackBerry 10 – Movies

VID_20140315_101232.mp4

- **This movie file was created on 2014:03:15 10:12:54 -06:00.**



```
ExifTool Version Number         : 9.54
File Name                       : VID_20140315_101232.mp4
File Modification Date/Time   : 2014:03:15 10:12:54-06:00
File Access Date/Time         : 2014:03:15 10:12:32-06:00
File Creation Date/Time       : 2014:03:15 10:12:32-06:00
File Permissions              : rw-rw-rw-
File Type                     : MP4
MIME Type                     : video/mp4
Major Brand                   : MP4 v2 [ISO 14496-14]
Minor Version                 : 0.0.0
Compatible Brands             : mp41, iso2
Movie Data Size               : 22046192
Movie Data Offset             : 40
Movie Header Version          : 0
Create Date                   : 2014:03:15 16:12:32
Modify Date                   : 2014:03:15 16:12:32

Track Create Date               : 2014:03:15 16:12:33
Track Modify Date               : 2014:03:15 16:12:33
Media Create Date               : 2014:03:15 16:12:33
Media Modify Date               : 2014:03:15 16:12:33
Title                           : 2014-03-15T10:12:33
```

June-19-14

BlackBerry 10 – EXIF Movies

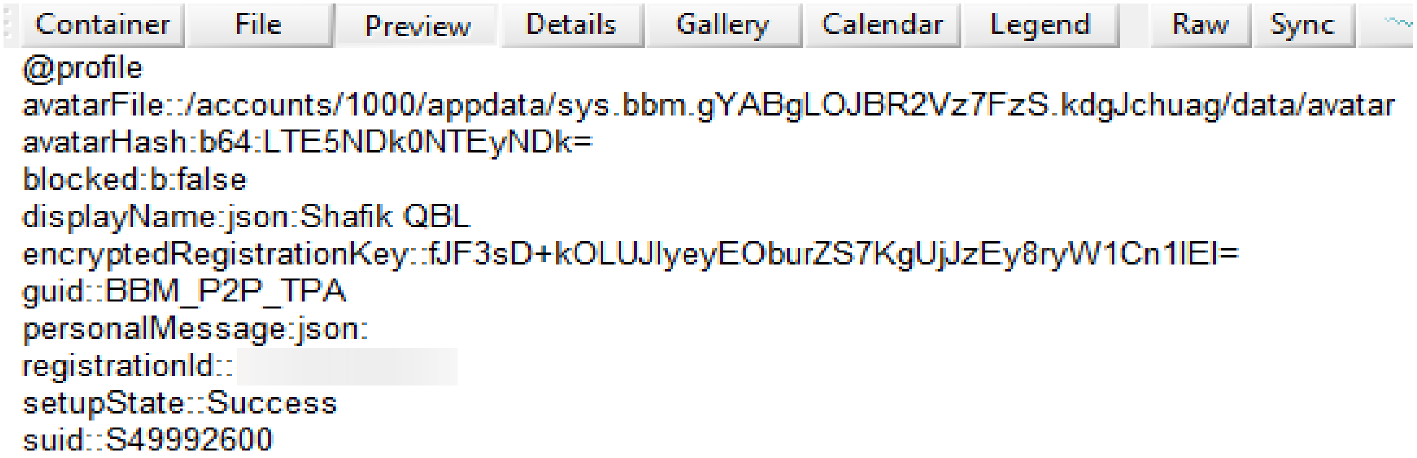
EXIF Movie Summary

- File format or file type is mp4.
- The EXIF time values are stored in UTC relative to the local device time zone offset.
- There is no indication the movie files are created with a BlackBerry device compared to BlackBerry 7 and lower where movie files had a string value in the EXIF called 'rimm'.
- Naming convention, in BlackBerry 10 device lower than 10.2.1.214, will not include the date and time local to the device in the file name.
- No geo-data is present in a movie file created with the BlackBerry 10.

BlackBerry 10 – Settings: BBM PROFILE CORE

The profile file stores the device user's BBM profile information.

- Artifact Path: \settings\pps\services\bbmcore\profile



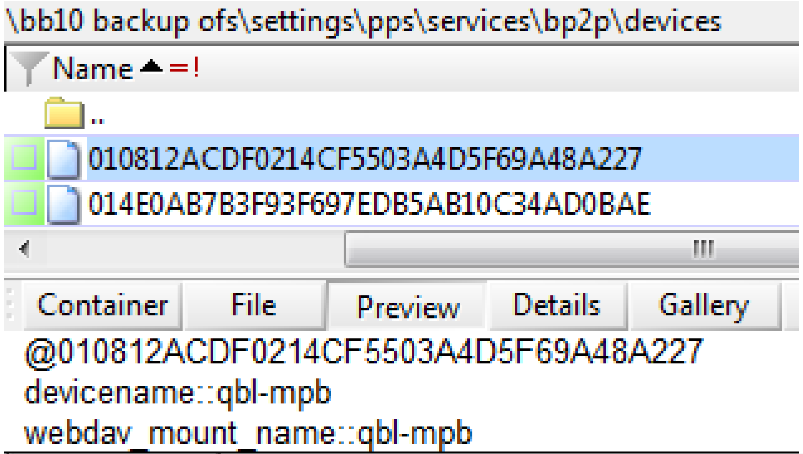
```
@profile
avatarFile::/accounts/1000/appdata/sys.bbm.gYABgLOJBR2Vz7FzS.kdgJchuag/data/avatar
avatarHash:b64:LTE5NDk0NTEyNDk=
blocked:b:false
displayName:json:Shafik QBL
encryptedRegistrationKey::fJF3sD+kOLUJlyeyEOburZS7KgUjJzEy8ryW1Cn1IEI=
guid::BBM_P2P_TPA
personalMessage:json:
registrationId::[redacted]
setupState::Success
suid::S49992600
```

- The 'registrationId' value is 12 decimal characters in length.

BlackBerry 10 – Settings: BP2P DEVICES

This stores the devices the BlackBerry 10 has connected with.

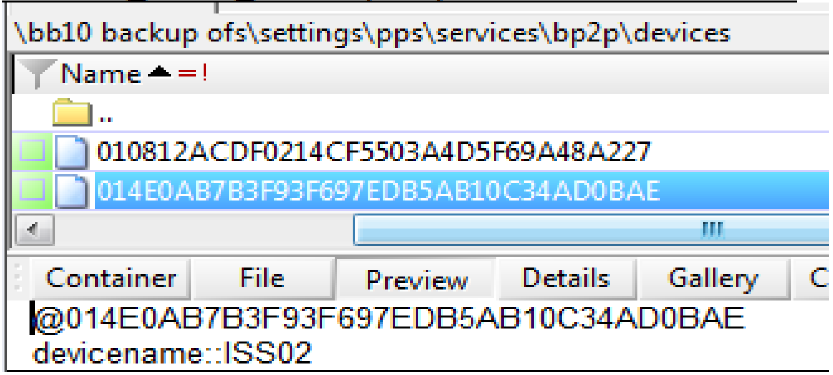
- Artifact Path: \settings\pps\services\bp2p\devices



\bb10 backup ofs\settings\pps\services\bp2p\devices

010812ACDF0214CF5503A4D5F69A48A227
014E0AB7B3F93F697EDB5AB10C34AD0BAE

```
@010812ACDF0214CF5503A4D5F69A48A227
devicename::qbl-mpb
webdav_mount_name::qbl-mpb
```



\bb10 backup ofs\settings\pps\services\bp2p\devices

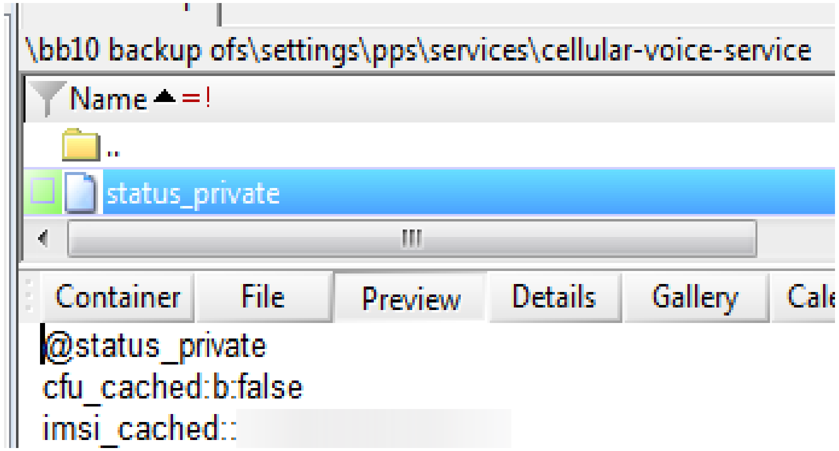
010812ACDF0214CF5503A4D5F69A48A227
014E0AB7B3F93F697EDB5AB10C34AD0BAE

```
@014E0AB7B3F93F697EDB5AB10C34AD0BAE
devicename::ISS02
```

BlackBerry 10 – Settings: IMSI VALUE

IMSI value is found in the status_private file:

- Artifact Path: \settings\pps\services\cellular-voice service\status_private



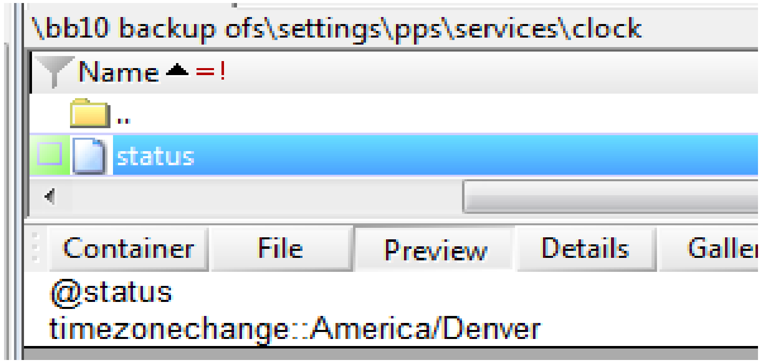
\bb10 backup ofs\settings\pps\services\cellular-voice-service

```
@status_private
cfu_cached:b:false
imsi_cached::
```

BlackBerry 10 – Settings: TIMEZONE

Time Zone Artifact 1:

Artifact Path: \settings\pps\services\clock\status

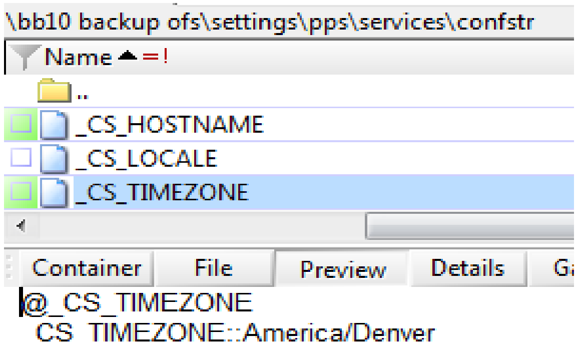


\bb10 backup ofs\settings\pps\services\clock

@status
timezonechange::America/Denver

Time Zone Artifact 2:

Artifact Path: \settings\pps\services\confstr\ _CS_TIMEZONE



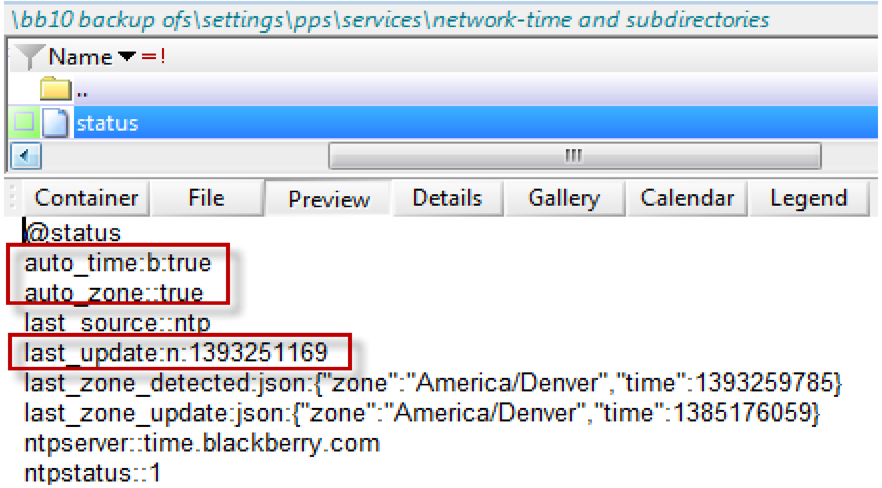
\bb10 backup ofs\settings\pps\services\confstr

@_CS_TIMEZONE
CS TIMEZONE::America/Denver

BlackBerry 10 – Settings: DATE & TIME

Stores the device date & time settings.

- Artifact Path: \settings\pps\services\network-time



\bb10 backup ofs\settings\pps\services\network-time and subdirectories
Name
..
status
Container
File
Preview
Details
Gallery
Calendar
Legend

```
@status
auto_time:b:true
auto_zone::true
last_source::ntp
last_update:n:1393251169
last_zone_detected:json:{"zone":"America/Denver","time":1393259785}
last_zone_update:json:{"zone":"America/Denver","time":1385176059}
ntpserver::time.blackberry.com
ntpstatus::1
```

The status file, shown in the above screenshots contains the settings for:

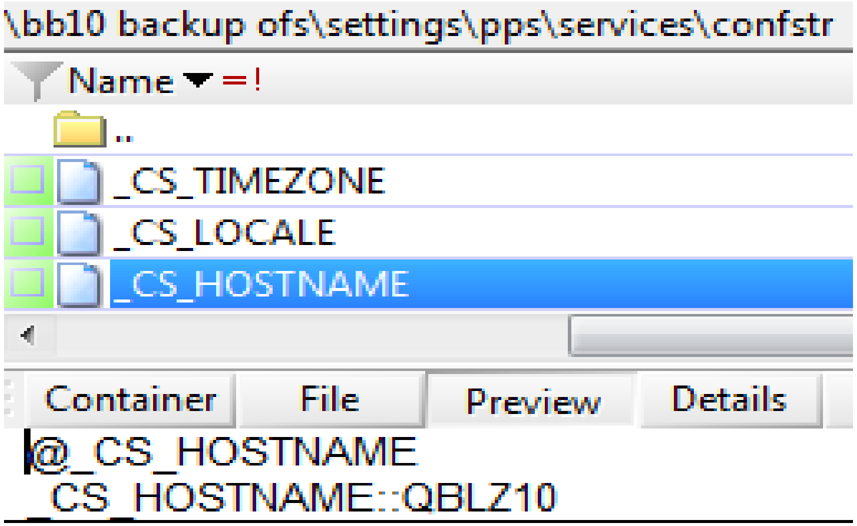
- auto_time value = Set Date and Time Automatically is set to 'On' in Date and Time settings on the device.
- auto_zone value = Auto Update Time Zone is set to 'On' in Date and Time settings on the device.
- The last_update value is a 10 character decimal value, Unix epoch time.

June-19-14

BlackBerry 10 – Settings: HOSTNAME

Contains the device name.

- Artifact Path: \settings\pps\services\confstr\ _CS_HOSTNAME



\bb10 backup ofs\settings\pps\services\confstr

```
@_CS_HOSTNAME
_CS_HOSTNAME::QBLZ10
```

June-19-14

TEELtechnologies

BlackBerry 10 – Settings: PHONE NUMBER

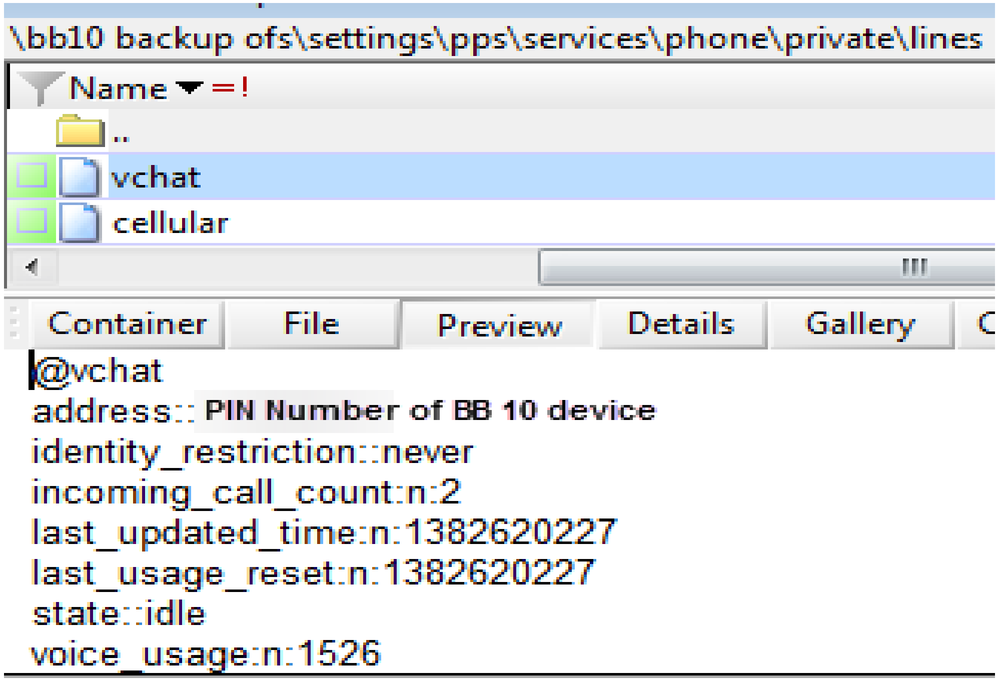
Phone number used by BlackBerry 10 through its SIM.

- Artifact Path: \settings\pps\services\phone\
- This folder path contains 3 sub folders each contain files with names ‘vchat’ and ‘cellular’.
- The path shown below contains vchat and cellular files.

\settings\pps\services\phone\private\lines

BlackBerry 10 – Settings: PHONE NUMBER

- vchat file contains the PIN number.

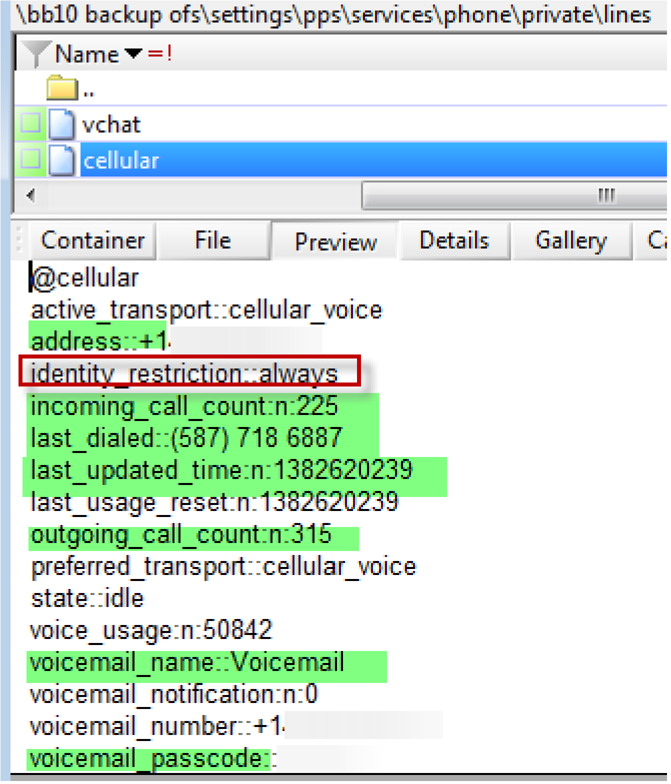


```
@vchat
address:: PIN Number of BB 10 device
identity_restriction::never
incoming_call_count:n:2
last_updated_time:n:1382620227
last_usage_reset:n:1382620227
state::idle
voice_usage:n:1526
```

June-19-14

BlackBerry 10 – Settings: PHONE NUMBER

- cellular file contains a number of interesting artifacts, which includes the phone number, voicemail passcode, and the value that caller identify is restricted.



\bb10 backup ofs\settings\pps\services\phone\private\lines

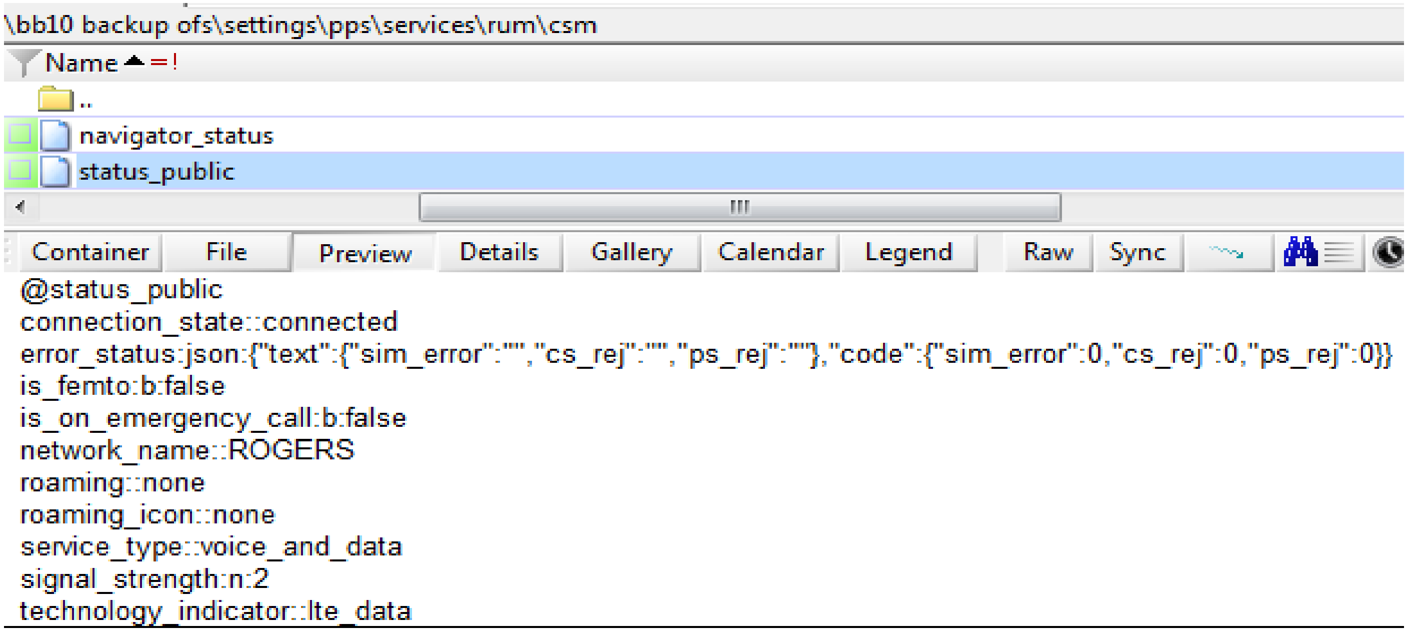
```
@cellular
active_transport::cellular_voice
address::+1
identity_restriction::always
incoming_call_count:n:225
last_dialed::(587) 718 6887
last_updated_time:n:1382620239
last_usage_reset:n:1382620239
outgoing_call_count:n:315
preferred_transport::cellular_voice
state::idle
voice_usage:n:50842
voicemail_name::Voicemail
voicemail_notification:n:0
voicemail_number::+1
voicemail_passcode::
```

June-19-14

BlackBerry 10 – Settings: NETWORK NAME

There are two files that contain the network operator name: navigator_status and status_public.

- Artifact Path: \settings\pps\services\rum\csm

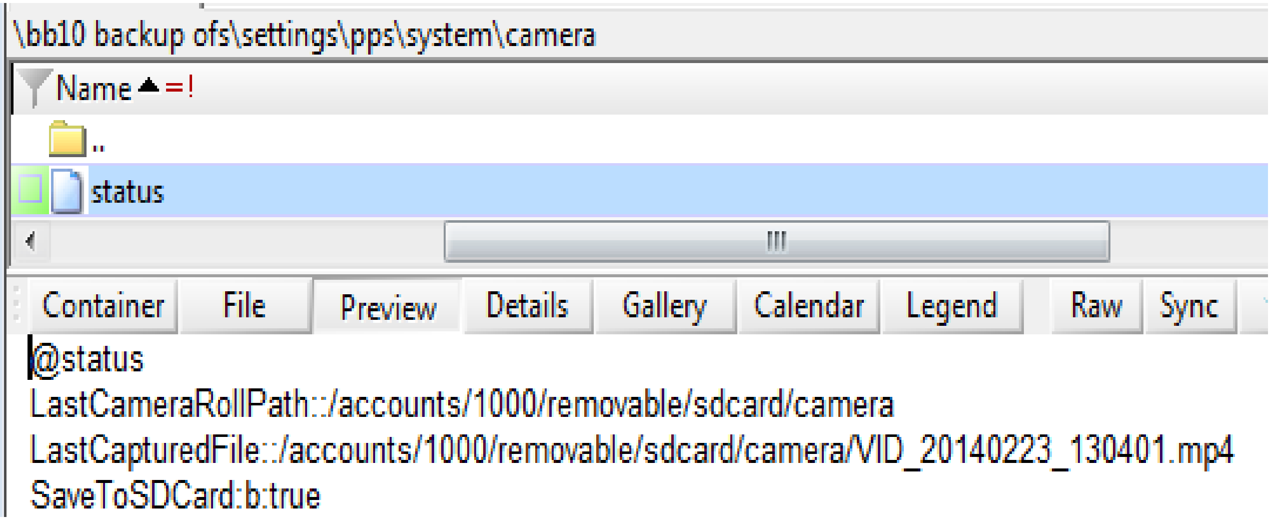


```
@status_public
connection_state::connected
error_status:json:{"text":{"sim_error":"","cs_rej":"","ps_rej":""},"code":{"sim_error":0,"cs_rej":0,"ps_rej":0}}
is_femto:b:false
is_on_emergency_call:b:false
network_name::ROGERS
roaming::none
roaming_icon::none
service_type::voice_and_data
signal_strength:n:2
technology_indicator::lte_data
```

BlackBerry 10 – Settings: CAMERA

The status file stores save location of the data created using the Camera application, and also records the filename of the last captured file.

- Artifact Path: \settings\pps\system\camera

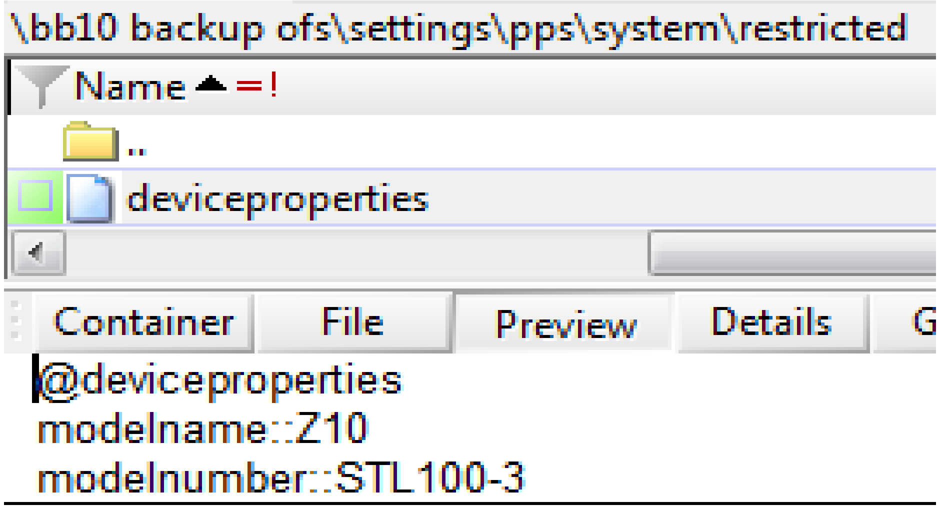


```
@status
LastCameraRollPath::/accounts/1000/removable/sdcard/camera
LastCapturedFile::/accounts/1000/removable/sdcard/camera/VID_20140223_130401.mp4
SaveToSDCard:b:true
```

BlackBerry 10 – Settings: DEVICE MODEL NAME AND MODEL NUMBER

The device properties file stores the device model name and model number information.

- Artifact Path: \settings\pps\system\restricted



```
@deviceproperties
modelname::Z10
modelnumber::STL100-3
```

June-19-14

TEELtechnologies

BlackBerry Forensics - CONCLUSION

- **BlackBerry 7 and lower versus BlackBerry 10/BlackBerry Playbook: Two different schisms.**
- **BB7 (proprietary JVM) has no real file system from a physical level perspective compared to its BB10 (QNX) successor.**
- **BB 10 backup files are encrypted by default using BlackBerry Link.**
- **Remember to validate what you have observed in this presentation, as there is no official support from BlackBerry on the interpretation of any BB7 or BB10 artifacts.**
- **And finally – thanks for your patience and looking through all the slides! ☺**

TEELtechnologies