Attachment A to Letter from Virgin Mobile USA to the Copyright Office dated August 28, 2009: Response to EFF DCMA Submission

Handset Engineering Mobile Devices

Summary

DCMA Response

- VMU's Handset Engineering team was able to reproduce on VMU's Oystr handset the test procedure that EFF reports it employed and is described on pages 4-6 of EFF's July 13, 2009 DCMA submission. The team used the same tool, BitPim. To compare the functionality, the team also used Qualcomm QPST tool to access the same set of files.
  - Note that BitPim is a universal PST tool that provides unauthorized access to phone systems without SPC security code. The tool only works for certain devices.
- The team was able to copy the two sound files with the BitPim and QPST tools from an Oystr device to a PC successfully, demonstrating that the test results reported on page 6 of EFF DCMA submission are not accurate. VMU's test procedure is described in detail, with screen shots, below, pages 3-12.
- Oystr is a fairly old handset by industry standards, developed 3 or 4 years ago, and is no longer manufactured. In fact, the Oystr handset is not representative of security measures used on VMU's current handsets. Moreover, the Qualcomm MSM-6050 chipset is no longer supported by the manufacturer and cannot be further developed and customized to support DRM for commercial purposes, a key point EFF failed to acknowledge.

Summary (continued)

DRM

- The VMU handsets do not have any DRM implementation.
- The Open Mobile Alliance ("OMA") is the leading industry forum for developing market driven, interoperable mobile service enablers. It develops and releases open specifications for the mobile market. Among those it has released are specifications for DRM. OMA has two major release of DRM specifications: OMA v1.0 & 2.0 (http://www.openmobilealliance.org/).
- VMU does not provide DRM capability on its low-end handsets based on OMA's DRM specifications: the handsets do not comply with OMA requirements for any of the three recognized types of DRM for mobile devices, as described below, pages 13-15.
- Specifically, VMU's handsets only provide partial implementation of Forward Lock (as described below) by limiting sharing/forwarding capability in specific folder.
- As a side note, DRM capability should NOT be evaluated from PST access as this is not a primary use case. DRM is implemented to control digital contents. Almost all carriers protect their devices from PST access with SPC lock code. They don't expect a user to use a PST tool to extract the content. DRM is developed to be enforced at a device software level, for example, SMS/MMS, Mobile Browser, Java Apps, etc. If you think of the device as a house, PST access from a PC is like going through the backdoor.

Test Setup

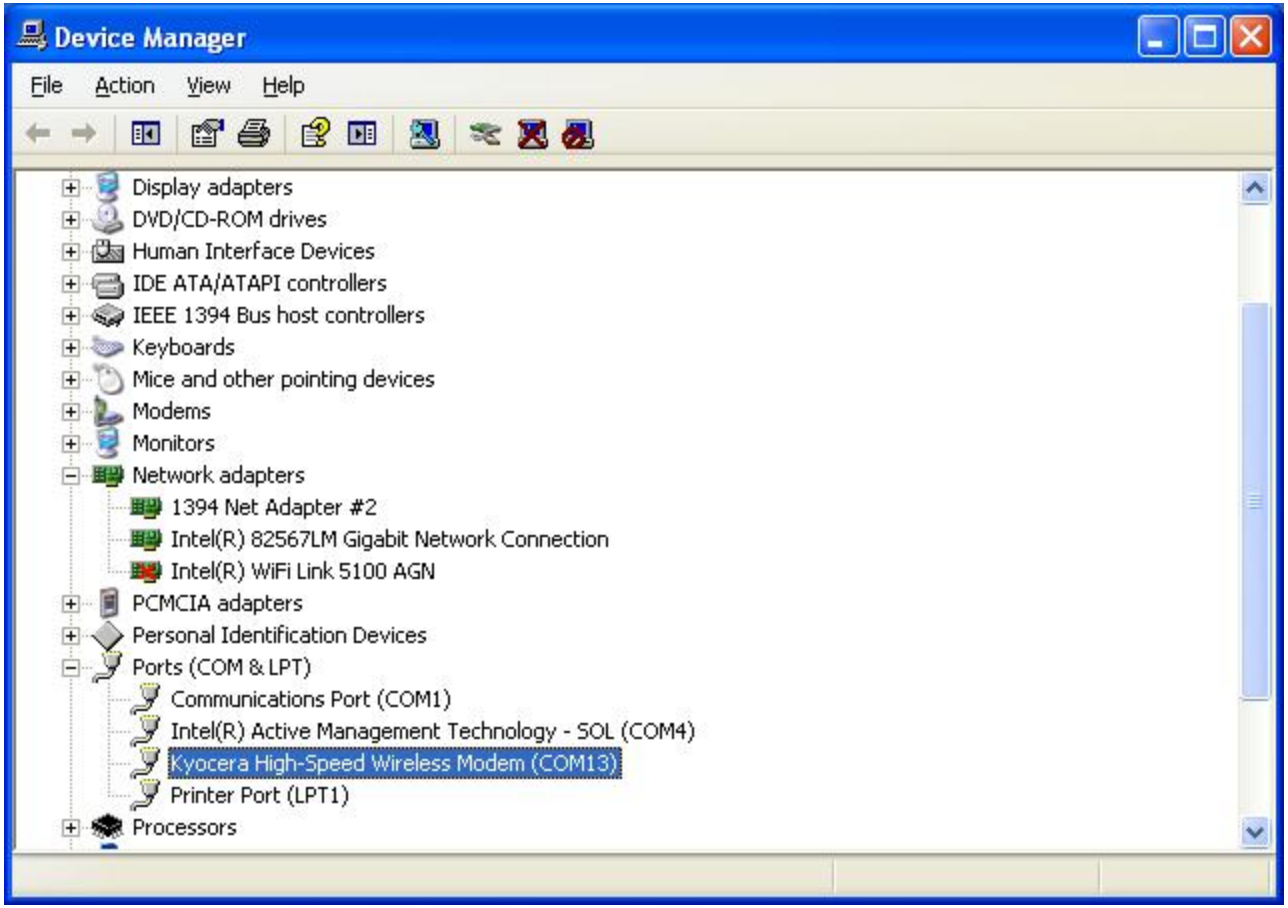
- **Device Info**
  - Device: **Kyocera Oystr**
  - Software Version: 1.0.00 (VB1000)
  - Hardware Version: 67-N780F-01
  - PRI Version: KX9D_VMU_VB1000_P01
  - PRL Version: 10029

- **Data cable**
  - TXDTA 10146

- **USB driver**
  - Download and install the corresponding driver in PC from the URL below
  - http://www.kyocera-wireless.com/support/drivers.htm

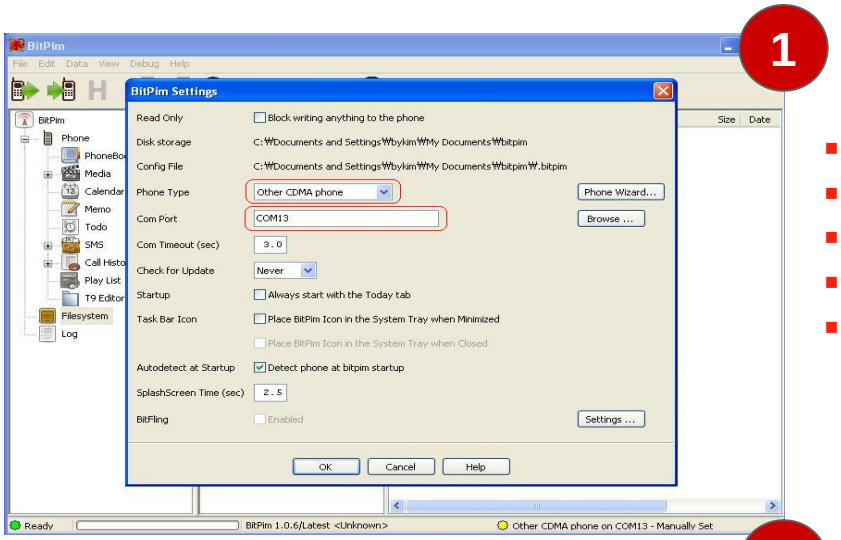
- **MSL/SPC**
  - SPC code is available to unlock the phone to access file system (required for QPST tool access but not for BitPim)

Checking the USB port status



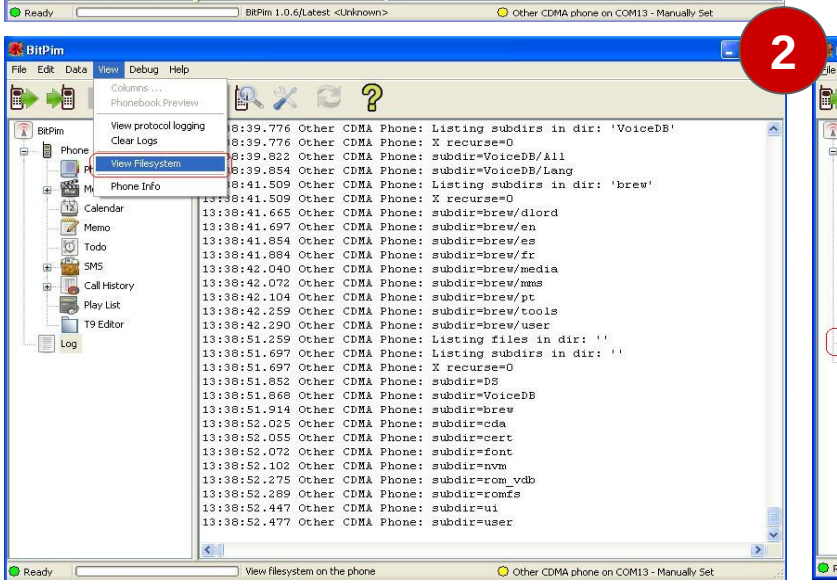
- Connect Oystr device via TXDTA 10146 data cable to PC after finishing installing the corresponding USB driver
- Verify that Device Manager of PC recognizes the Kyo's device as shown in the above image

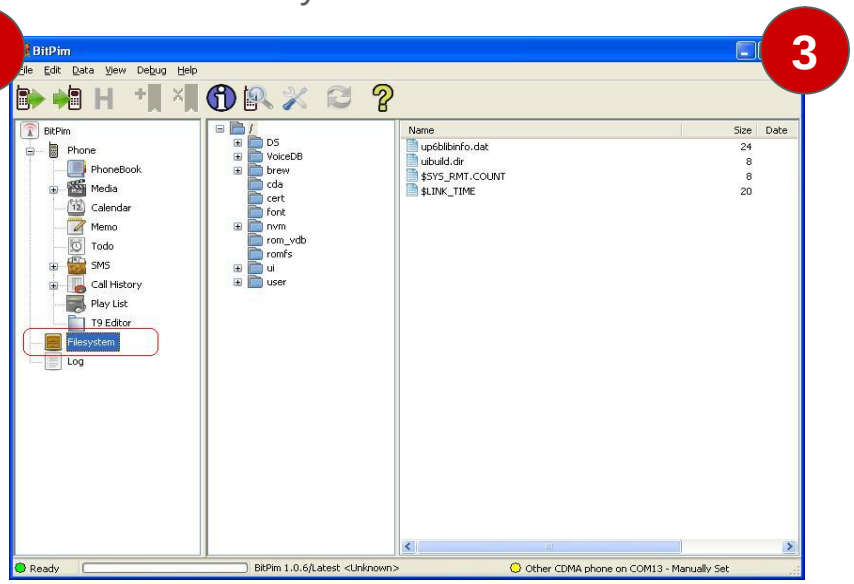
Contents copy via BitPim



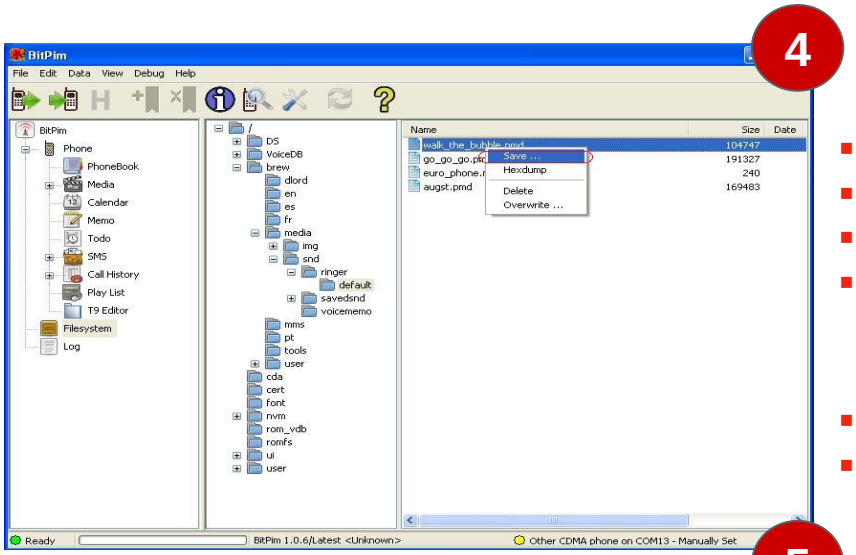
- Run the BitPim application
- Select “Edit → Setting” menu
- Select “Other CDMA Phone” in Phone Type field
- Choose the corresponding Com port in Com Port field
- Press “OK” button

- Check up the “View Filesystem” menu
- Choose “FileSystem” in leftmost menu



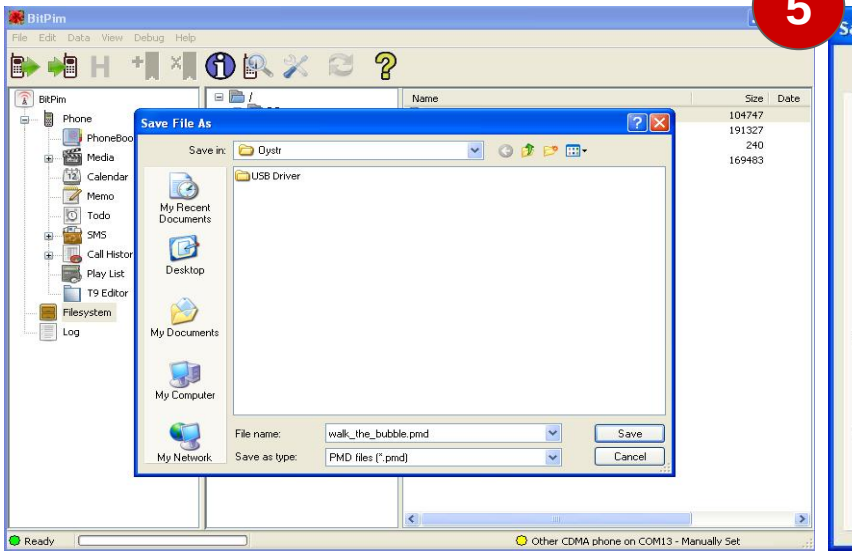


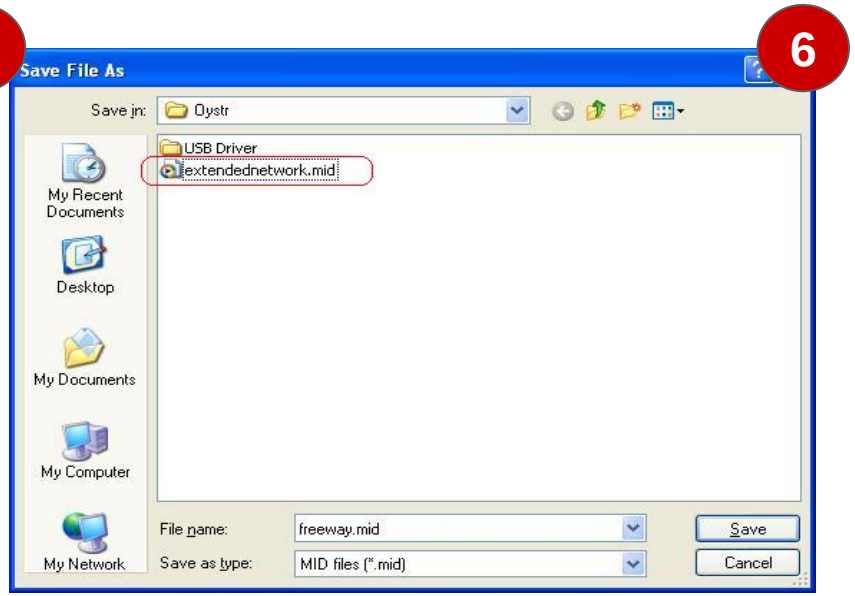
Contents copy via BitPim



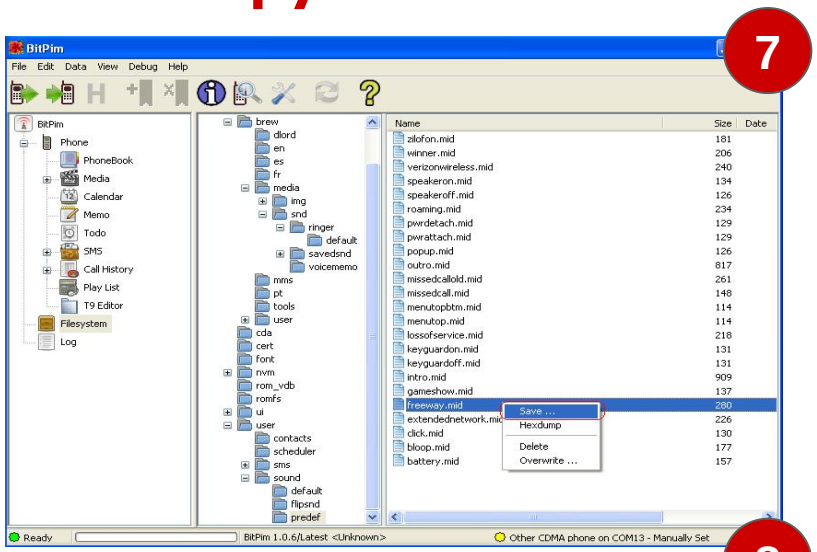
- Go to “/brew/media/snd/ringer/default” folder
- Hightlight “walk_the bubble.pmd”
- Press right button of Mouse
- Select “Save…” menu

- Choose the Path you want to copy to
- Press “Save” button

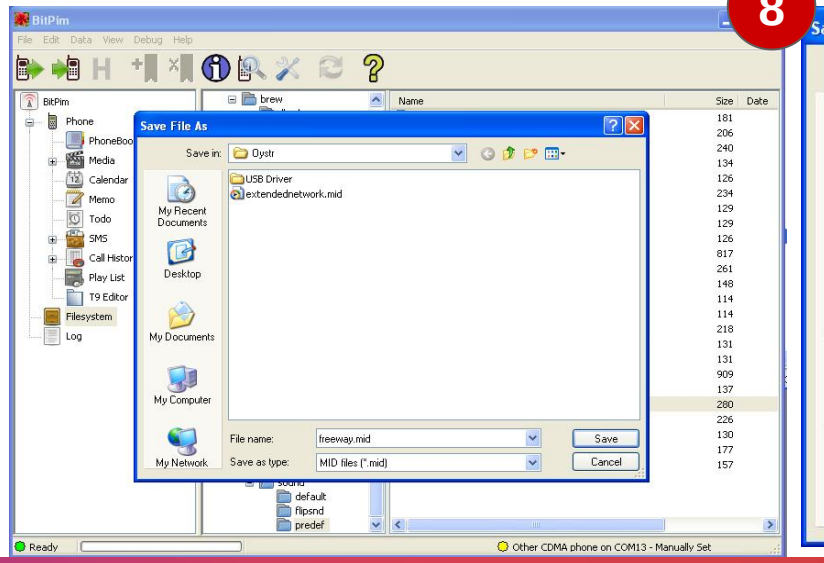




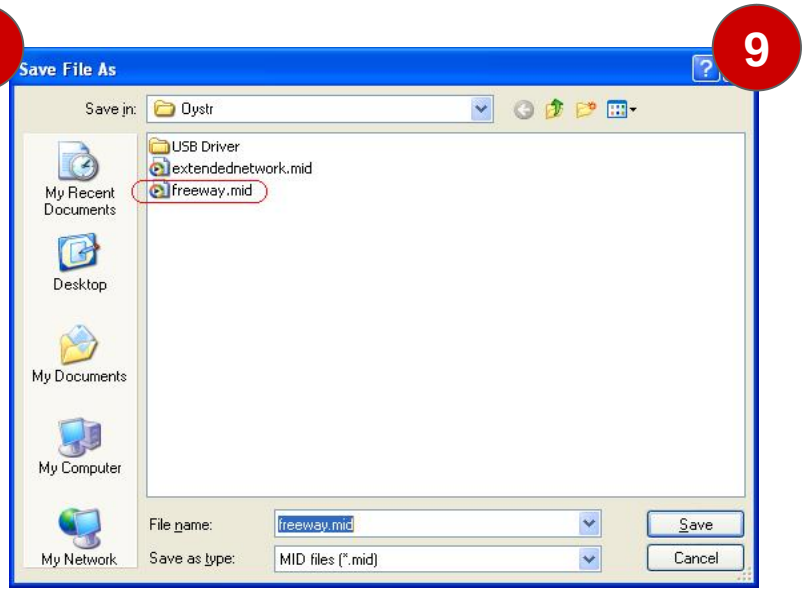
Contents copy via BitPim



- Go to “/user/sound/predef” folder
- Hightlight “freeway.mid” file
- Press right button of Mouse
- Select “Save…” menu



- Choose the Path you want to copy to
- Press “Save” button



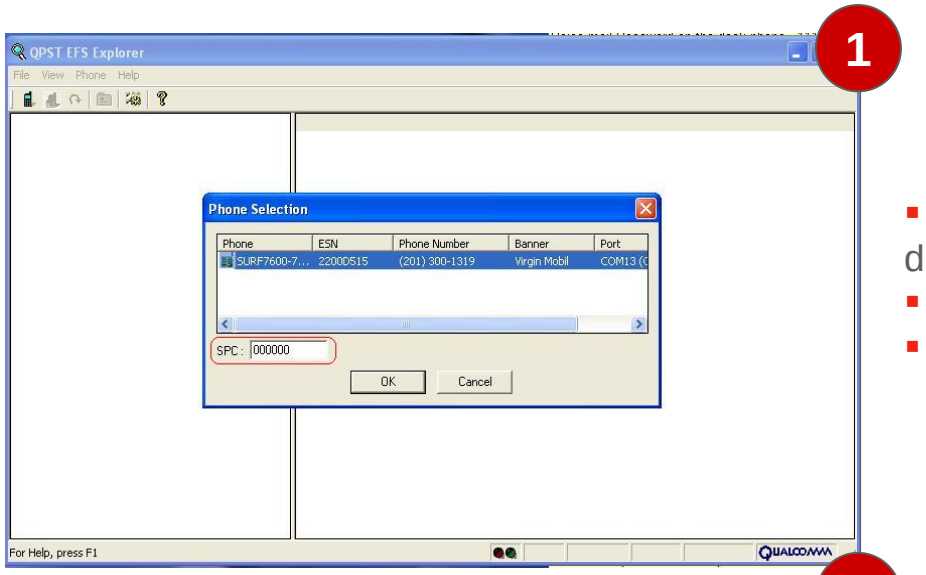
Results

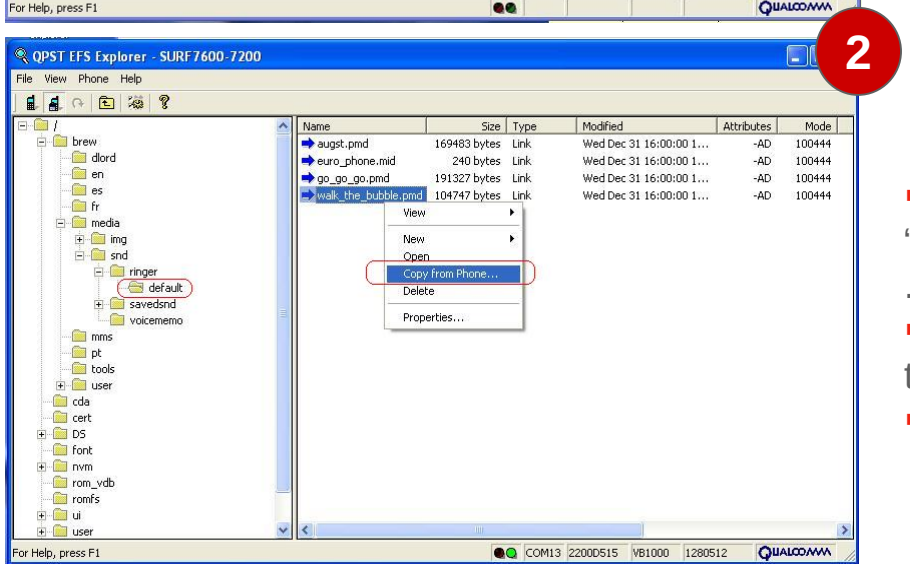
- **With BitPim tool**
  - Didn’t require MSL code to access EFS explorer
  - There was no problem with copying the following two sound files
    - /brew/media/snd/ringer/default/walk_the_bubble.pmd
    - /user/sound/predef/freeway.mid

- **Sample file extracted from Oystr:**

freeway.mid

Contents copy via Qualcomm QPST EFS explorer

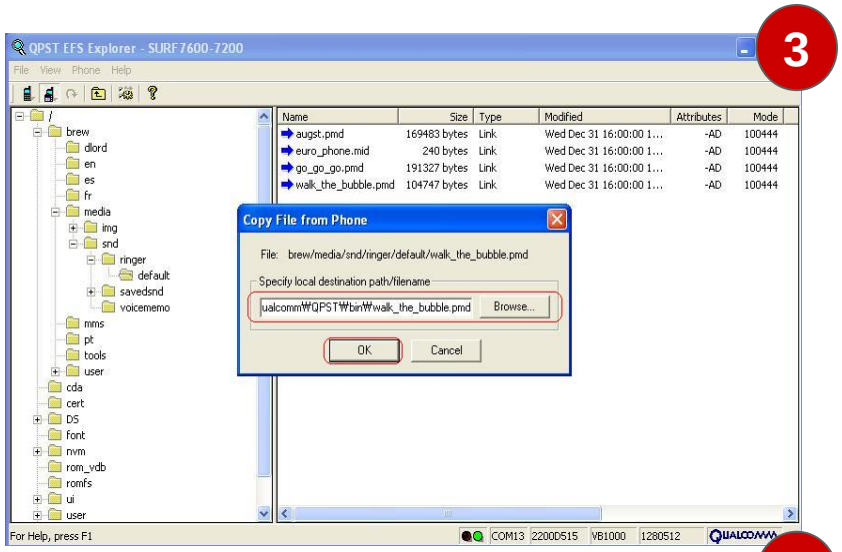


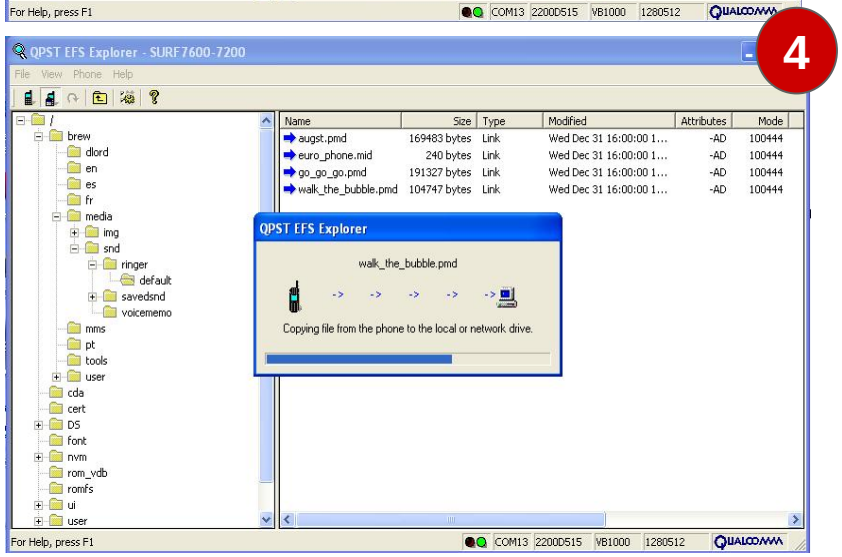


- Verify that EFS explorer recognizes the Oystr device
- Verify that “000000” is shown in SPC area
- Press OK button

- Go to “/brew/media/snd/ringer/default/walk_the_bubble.pmd”
- Press right button of Mouse to copy the content to PC
- Select “Copy from Phone…” menu

Contents copy via Qualcomm QPST EFS explorer





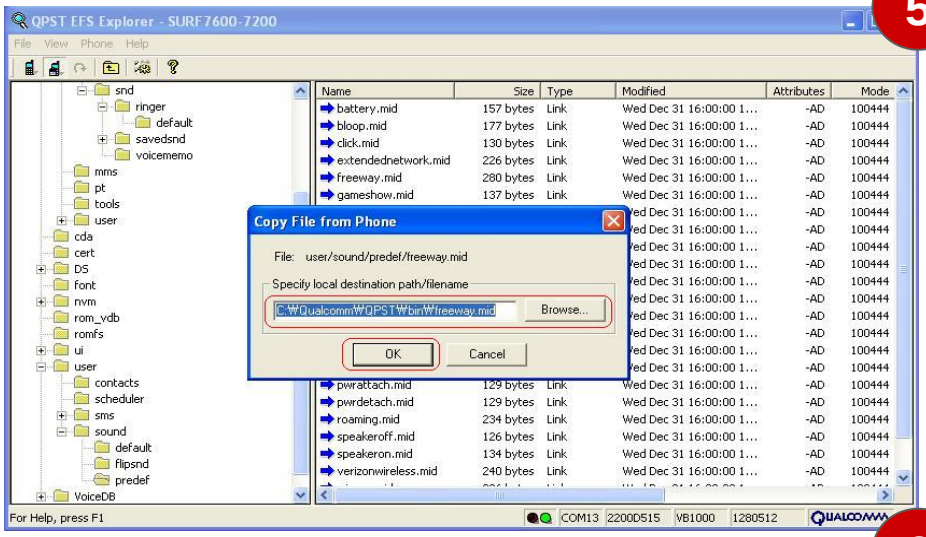
- Fill out the Path you want to copy to
- Press “OK” button

- Verify that the content was copied in the path you filled out

walk_the_bubble.pmd

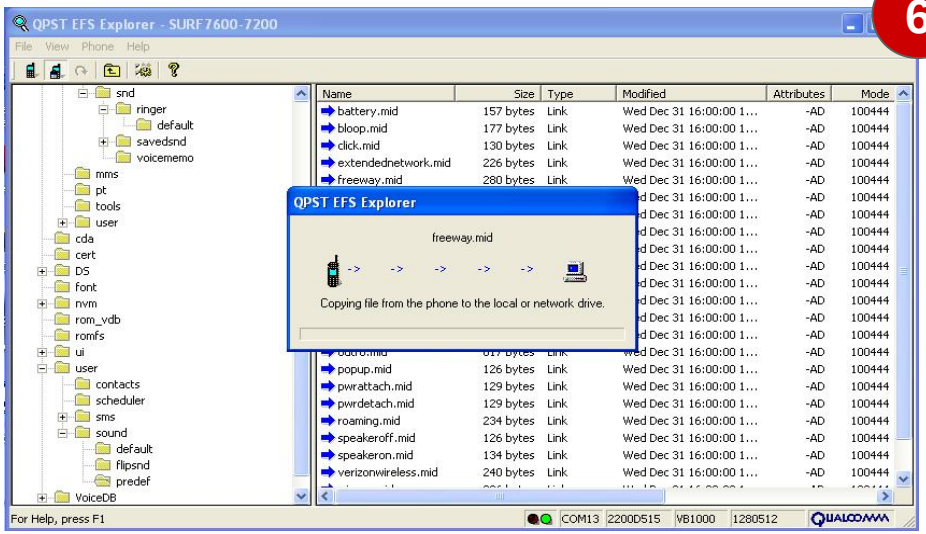
Contents copy via Qualcomm QPST EFS explorer

5



- Attempt to copy “freeway.mid” file
- Go to “/user/sound/predef” folder and select “freeway.mid” file
- Press right button of Mouse and fill out the destination path and then press “OK” button

6



- The copy was successful
- There was no problem when copying the “freeway.mid” file

Results

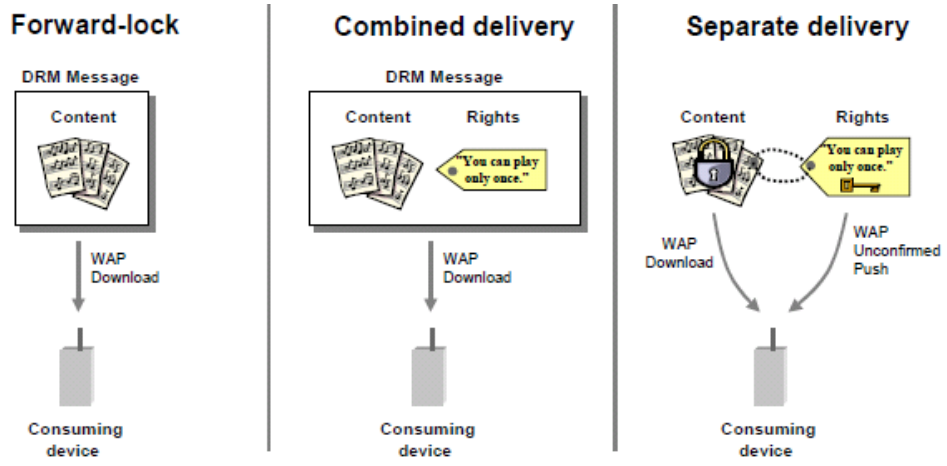
- **With EFS explorer of QPST**
  - Required MSL code(000000) to access EFS explorer
  - There was no problem with copying the following two sound files
    - /brew/media/snd/ringer/default/walk_the_bubble.pmd
    - /user/sound/predef/freeway.mid

- **Sample file extracted from Oystr:**

freeway.mid

DRM Definition

- **Based on definition of OMA DRM specification (Digital Rights Management Approved Version 1.0 dated 5 Jun 2004), there are 3 types of DRM methods:**
  - Forward Lock
  - Combined Delivery
  - Separate Delivery
- **VMU handsets do not support any of these three DRM methods and only meets some of the requirements for Forward Lock. However, Virgin Mobile does not implement any of these methods.**
- **The purpose for Forward Lock is to prevent the user from forwarding content such as ringtones and wallpapers on their phone. Typically, the content can be distributed using various transport, *i.e.,* HTTP, MMS, Removable Memory.**



DRM Definition

- **As stated in section 4.1, Forward-lock and Combined delivery**

"For forward-lock and combined delivery content provider needs to package content, optionally with a rights object, into a DRM message."

Based on the definition from the OMA specification, contents delivered to VMU devices including Oystr are not packaged with DRM message.

- **As stated in section 6.1, DRM Message Media Type**

"The MIME media type for objects conforming to the format defined in this section MUST be application/vnd.oma.drm.message"

Based on the definition from the OMA specification, VMU devices, including Oystr, do not support DRM MIME type.

DRM Definition

- As stated in Appendix C.1, Examples for Forward-lock Method

C.1 Forward-lock Method

This example describes a forward-lock use case HTTP response that contains only one media object and no rights object. The device is allowed to view the image but not allowed to forward it to other devices.

```
HTTP/1.1 200 OK
Content-type: application/vnd.oma.drm.message;
              boundary=boundary-1
Content-Length: 574

--boundary-1
Content-type: image/jpeg
Content-Transfer-Encoding: binary

...jpeg image in binary format...
--boundary-1--
```

Based on definition from OMA specification, VMU devices including Oystr do not block user from forwarding content by using DRM message encoded as above example.

DRM Definition

CONCLUSIONS

- We were able to copy the two sound files with and BitPim and QPST tool from Oystr device to a PC successfully, demonstrating that the test results reported on page 6 of EFF DCMA submission are not accurate.
- VMU low-cost handsets do not provide DRM capabilities in accordance with the OMA DRM specifications; as the handsets do not comply with the OMA DRM requirements.
- Specifically, VMU's devices only provide partial implementation of Forward Lock requirements by limiting sharing/forwarding capability in specific folder at the device software level.
- The use of sophisticated DRM on a handset to protect individual content files involves engineering and other development costs that would significantly raise the cost of the handsets.