CHAMPLAIN COLLEGE | LCDi Leahy Center for Digital Investigation

Retrieving Data from Android OS Devices Using XRY

175 Lakeside Ave, Room 300A
Phone: (802)865-5744
Fax: (802)865-6446
http://www.lcdi.champlain.edu

12/1/2014

The following is a step-by-step walkthrough using Micro Sytemation's product XRY to perform a logical data extraction for Android OS phones.

NOTE: all screenshots in this tutorial are from the data retrieval of a Huawei U8665 which as of the time of publication can only be imaged logically by XRY.

NOTE: While this tutorial does show the use of the XRY Communications Unit, XRY Physical is not a requirement to run the XRY software. The only necessary purchases to perform data extractions are the XRY software, XRY license, XRY Key, and any necessary cables to connect the phone you wish to extract data from to the computer that will be used for the extraction. XRY Physical is an additional purchase designed to increase the number of data extractions that can be run at once. The XRY Communications Unit will allow for up to three device extractions simultaneously. If you do not have XRY Physical or do not wish to use the Communications Unit, you can follow the instructions for connecting a device under **Connecting Via Commercially Available Cables** on page 4 After the connection of the phone to the computer is complete the instructions merge, the Communications Unit makes no difference to the usage of the XRY software.

Reference Guide:

XRY Program- Software product produced by Micro Systemation. XRY is designed to streamline the process of extracting data from electronic devices.

XRY Logical – "The most established XRY product designed to perform a 'logical' extraction of data from the mobile device.

What this means is that we communicate with the operating system on the device and request information from the system. In general terms this will allow you to recover most of the live data from the device.

It is effectively the automated equivalent of manually examining each available screen on the device yourself and recording what is displayed.[1]"

XRY Physical – "Is more advanced - it allows you to perform a 'physical' extraction from a mobile device. Where we recover all available raw data stored in the device. Typically this is performed by bypassing the operating system and this offers you the opportunity to go deeper and recover deleted data from the device.

A physical extraction is separated out into two distinct stages, the initial 'dump' whereby the raw data is recovered from the device and then the second stage 'decode' - where XRY can automatically reconstruct the data into something meaningful; such as a deleted SMS without the need for manual carving of data.

XRY Physical is particularly useful when faced with a GSM mobile phone without a SIM Card, or with security locked devices.[1]"

XRY Complete – "This is our top of the range solution combining the best of both worlds with XRY Logical and XRY Physical in one complete package, hence the name.

With XRY Complete you will be able to perform both logical and physical extractions from a device, giving you the best possible opportunity to recover all the available data from a mobile device, and allowing you to compare the results between the different recovery methods.

This system is supplied with all the necessary hardware from both the Logical and the Physical systems to ensure you have everything you need to do complete the task.[1]"

XRY Communications Unit – For the purpose of this tutorial, "XRY Communications Unit" refers to the physical connection unit which can be used to image several devices at the same time.

MicroSystems USB Key - This is the license key provided with your purchase of a XRY product. This key must be connected to the computer running the XRY program to perform data extractions.

NOTE: See Step 1: Connecting Your Device to XRY for instructions on how to connect the MicroSystems USB Key.

[1] "Micro Systemation." *What Is XRY?* N.p., n.d. Web. 05 Dec. 2014. <https://www.msab.com/xry/what-is-xry>.

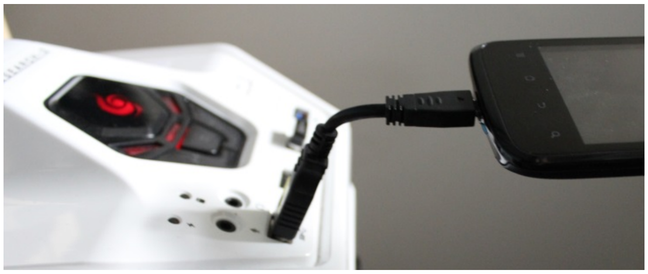
Step 1: Connecting Your Device to XRY

There are two methods of connecting your phone to XRY. The first is to use a compatible micro USB to USB cable. This can be a commercially available product (such as the cable supplied with the phone or an aftermarket cable) or the cable provided with the XRY physical kit. The second method is to use the XRY Communications Unit.

Option 1: Connecting Via Commercially Available Cables:

To connect to XRY with a standard cable, or one provided by XRY, simply plug the cable into the phone, and then connect the cable to a USB port on the computer where the extraction will take place.

Micro USB connects to phone



Standard USB end connects to computer

Once the phone is plugged in, you will need to insert the Micro Systemation USB Key into another USB port on the extraction computer. The Indicator light on the USB will turn orange and then briefly flash green before going dark again.

Micro Systemation XRY

Upon Insertion, the indicator light will briefly activate. However it will not remain on.

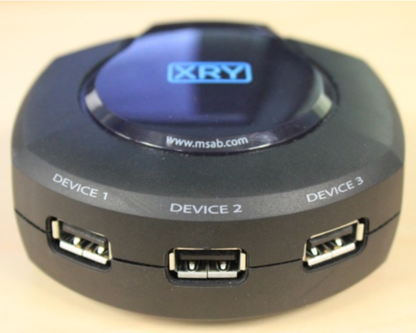
Overview of Attached Devices. Notice the USB key's indicator light is no longer active, this is normal.

You are now ready to open the XRY Software and begin the extraction

(Skip to page 8)

Option 2: Connecting Via XRY Communications Unit:

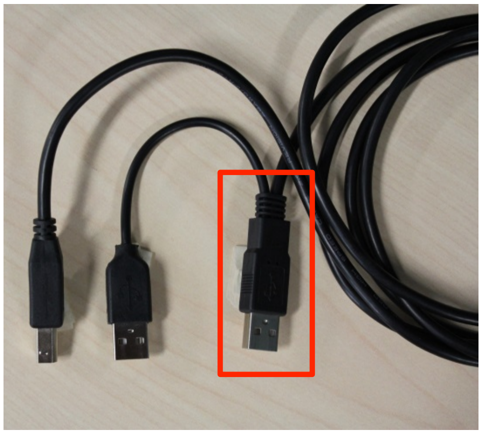
When connecting to XRY through the XRY Communications Unit, you must first ensure that the Communications Unit is set up correctly. The first step is to confirm that you have the XRY Communications Unit, XRY Communications Unit power cable (will be in a cloth bag near the Communications Unit in the XRY case), cable for the phone (can be either commercial or XRY issue), and the included cable to connect the Communications Unit and computer, and the Micro Systemation USB key.



Micro Systemation XRY Communications Unit

XRY Communications Unit Power Cable

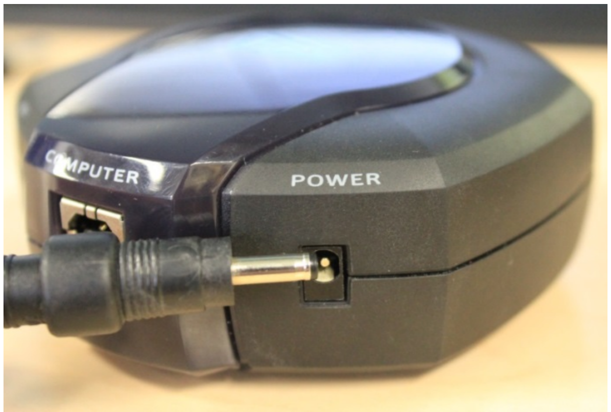
XRY Connection Cable (Will Vary depending on device)

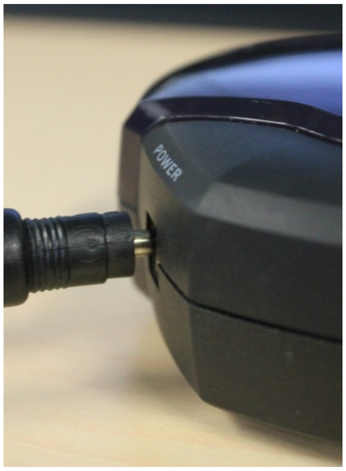


XRY Communications-to-Computer Cable. The USB end highlighted is the main USB end.

Micro Systemation XRY USB Key

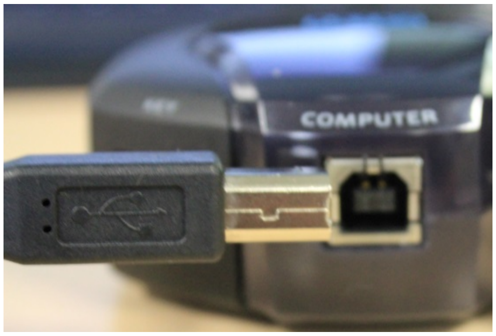
The first step is to plug the Communications Unit into a power source.

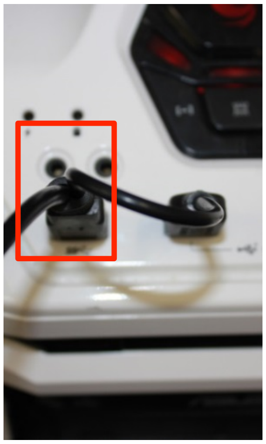


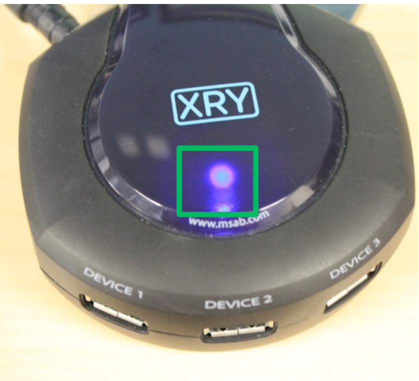


Note that power plug may not appear to be fully inserted. Do not attempt to force the plug in, use gentle force only- plug will slightly protrude from the Communications Unit.

Once the Communications Unit is powered, you will need to plug the Communications Unit into the computer. If the connection is successful you will see a blue light begin to flash on the top of the Communications Unit (Highlighted in green below).

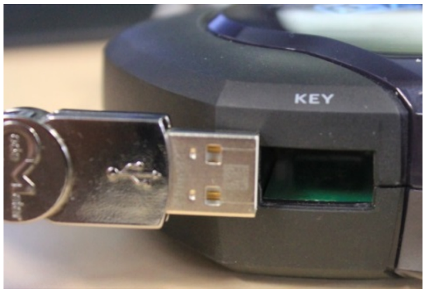


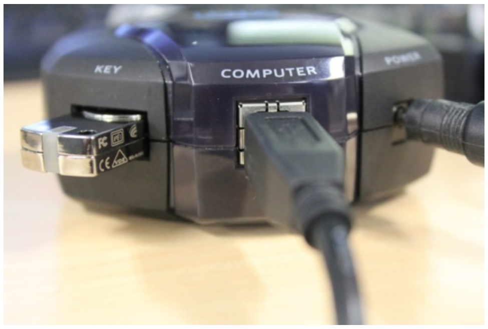




NOTE: It is not necessary to plug both of the USB ends into the computer; the secondary USB is only for increased data transfer rates. So long as the main USB (highlighted in red above) is inserted, the Communications Unit is connected and can be used with no issues.

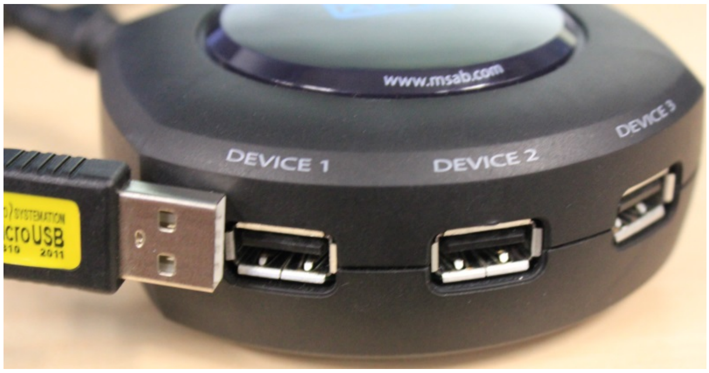
The next step is to insert the MicroSystems USB Key into the labeled slot on the back of the Communications Unit.

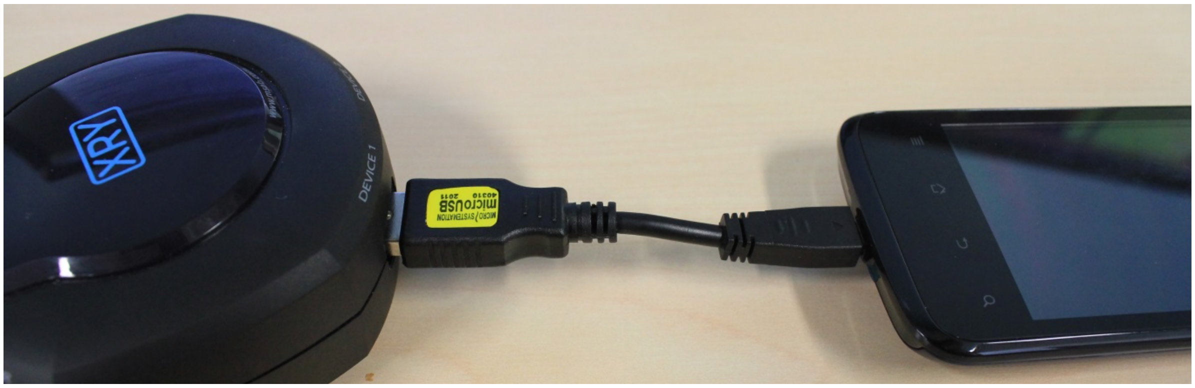




The picture to the left is how the back of the Communications Unit should look at this step.

The final step is to connect the phone to the Communications Unit. Using a compatible cable, plug the phone into one of the three USB ports on the Communications Unit.

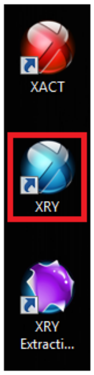


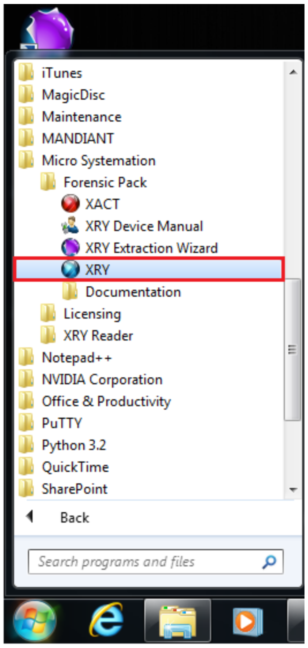


You are now ready to open XRY and begin the extraction.

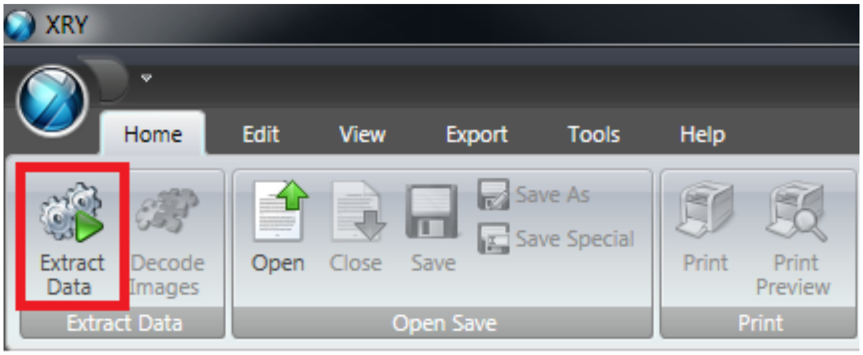
Step 2: Initializing XRY and Extraction Setup

Once the physical setup of XRY is done you are now ready to start the software. Do this by clicking the on the shortcut located on the desktop. You can also start the application by locating it in the start menu; it will be located in the programs folder in the start menu.



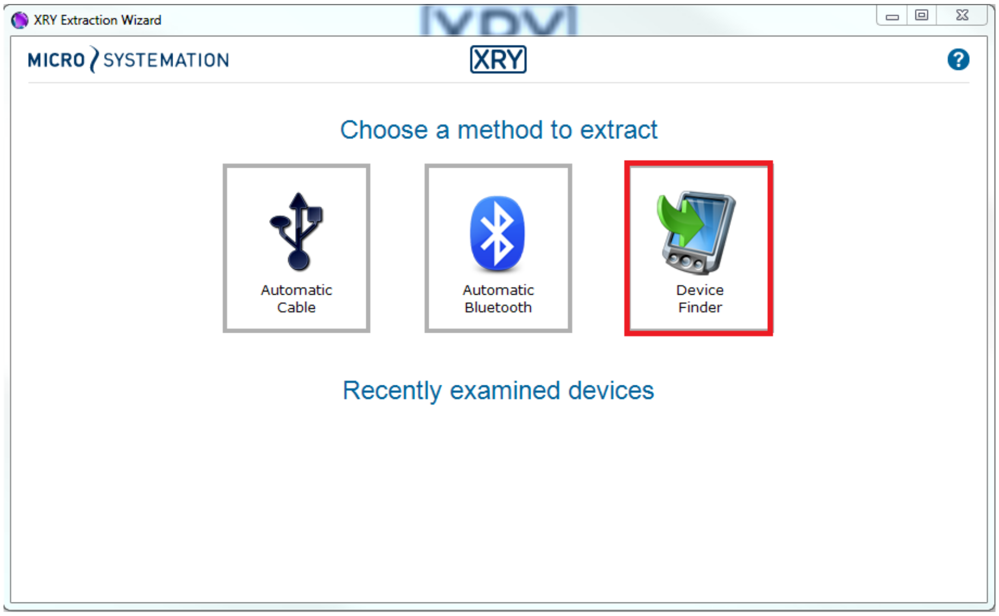


Once the XRY application is open, locate the “Extract Data” option located in the home menu at the top left of the screen. This screen also lets the user open an image that has already been created.

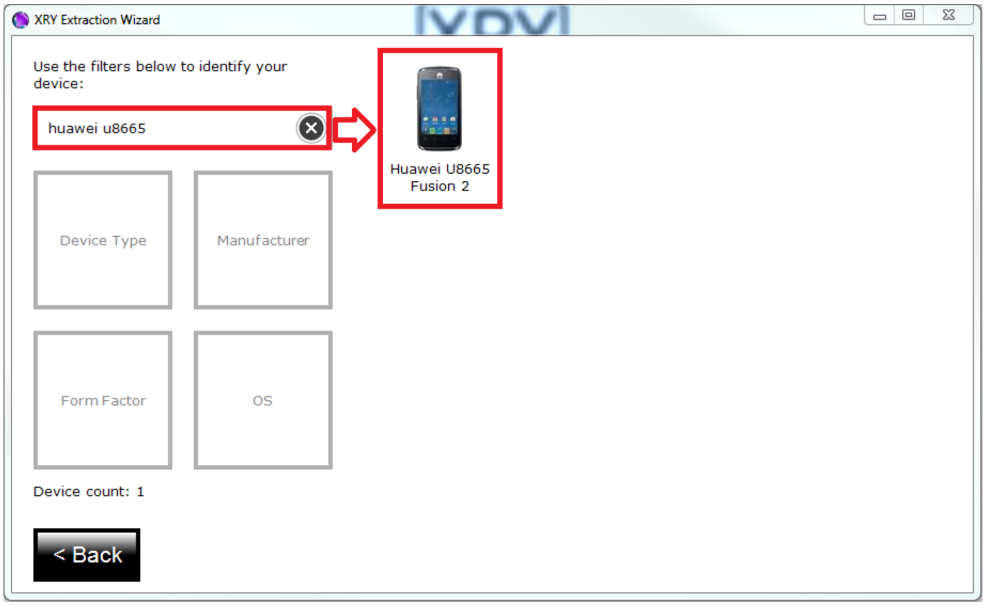


Click “Extract Data” and the extraction wizard will open, to help you configure your extraction.

After selecting “Extract Data” you will be taken to the extraction wizard to configure your extraction.

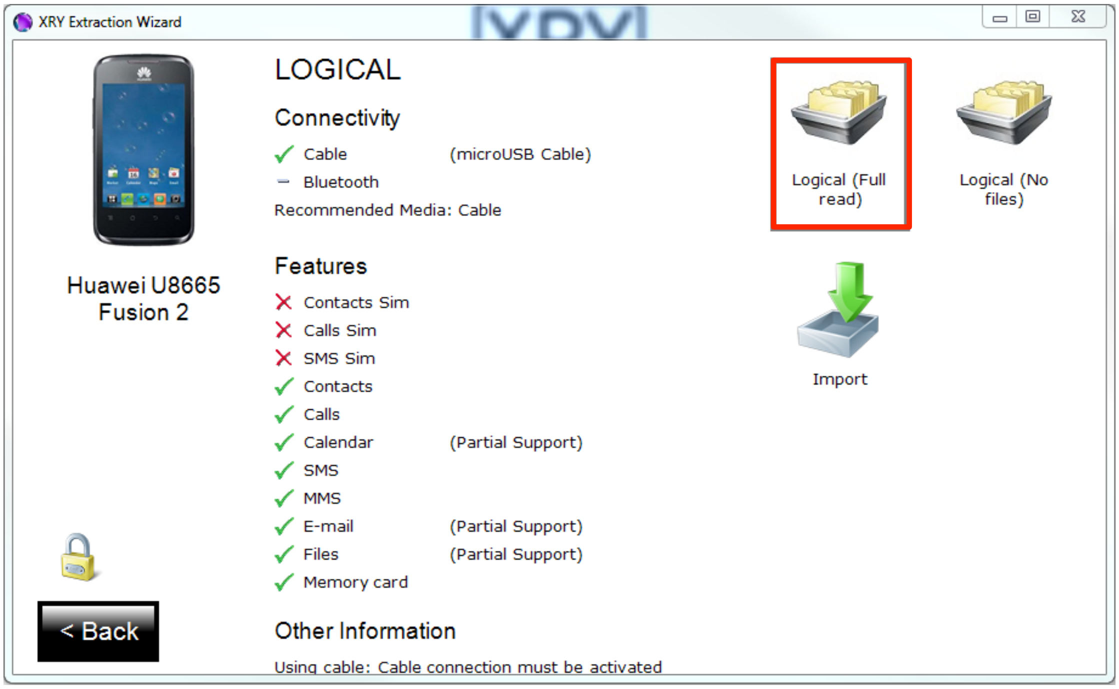


There are two methods for locating the device you have connected. One is to select “Automatic Cable” which allows XRY to try to identify the connected device. The other is “Device Finder,” which we will be using for this tutorial. Once selcted you will be presented with several methods of searching for the device you wish to extract data from.



We recommend using the top bar to search for the name of your phone, which you can then select from the box on the right of the screen. If the name of the phone is unknown, the four boxes under the search bar can be used to help narrow results by the criteria that the examiner does know.

The next screen will show the different extraction methods possible for your device. For our test device, only a Logical extraction is possible. When “Logical (Full read)” is selected, the features that will and will not be obtained using this method are displayed.



XRY Extraction Wizard

Huawei U8665 Fusion 2

LOGICAL

Connectivity

✓ Cable (microUSB Cable)
– Bluetooth
Recommended Media: Cable

Features

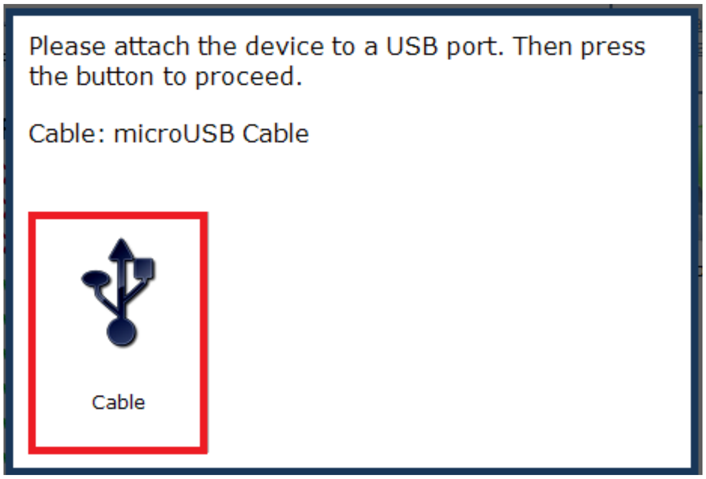
✗ Contacts Sim
✗ Calls Sim
✗ SMS Sim
✓ Contacts
✓ Calls
✓ Calendar (Partial Support)
✓ SMS
✓ MMS
✓ E-mail (Partial Support)
✓ Files (Partial Support)
✓ Memory card

Other Information

Using cable: Cable connection must be activated

Note: If you are on a time sensitive case and you need to get simple data extracted as fast as possible then select “Logical (No files).” Logical no files will obtain fewer files such as pictures, in order to cut down on the amount of time it takes to image the phone. It is recommended that whenever possible to choose “Logical (Full read)” because it will provide you with a more complete data set.

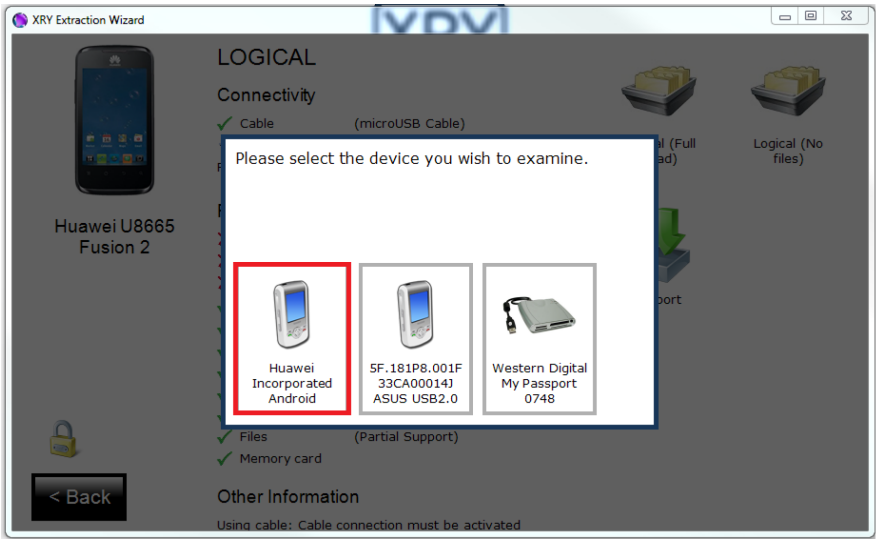
Once selecting “Logical (Full Read)” you will be asked to connect your phone, do so and then select “Cable” to continue. If the device had been connected in the initial setup, XRY will not be able to make a successful connection.



Please attach the device to a USB port. Then press the button to proceed.

Cable: microUSB Cable

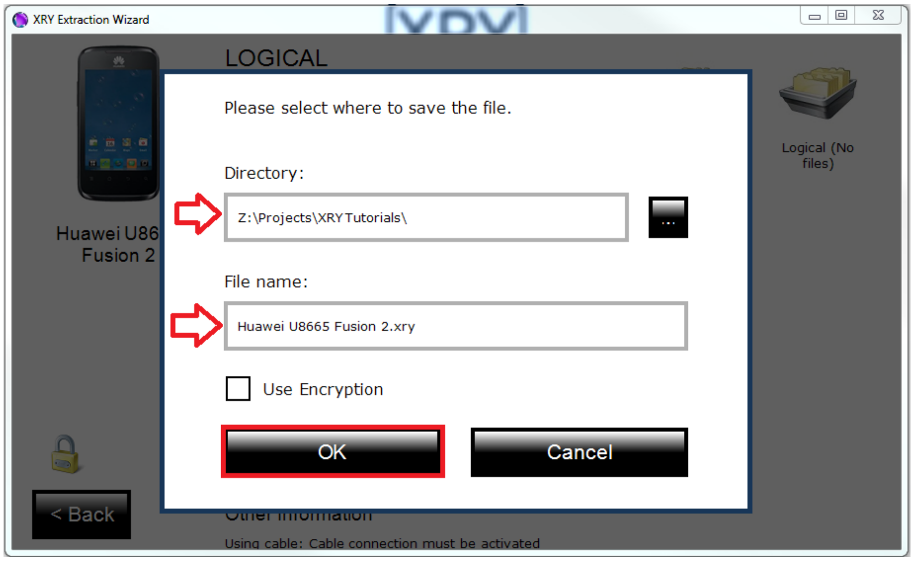
It is important to note that XRY will notice every device that is connected to the PC, and it may prompt the user to select the device that you wish to examine.



Please select the device you wish to examine.

Using cable: Cable connection must be activated

The next window will prompt the user to enter the path where they wish to save the .XRY file. XRY defaults to storing it within its program files on the PC but you may change this if you wish. From this screen a user can also change the name of the file. Here you can make a relevant name to link this extraction to a case file if necessary. Once you are satisfied with the name and save location of the data, select "OK."



Please select where to save the file.

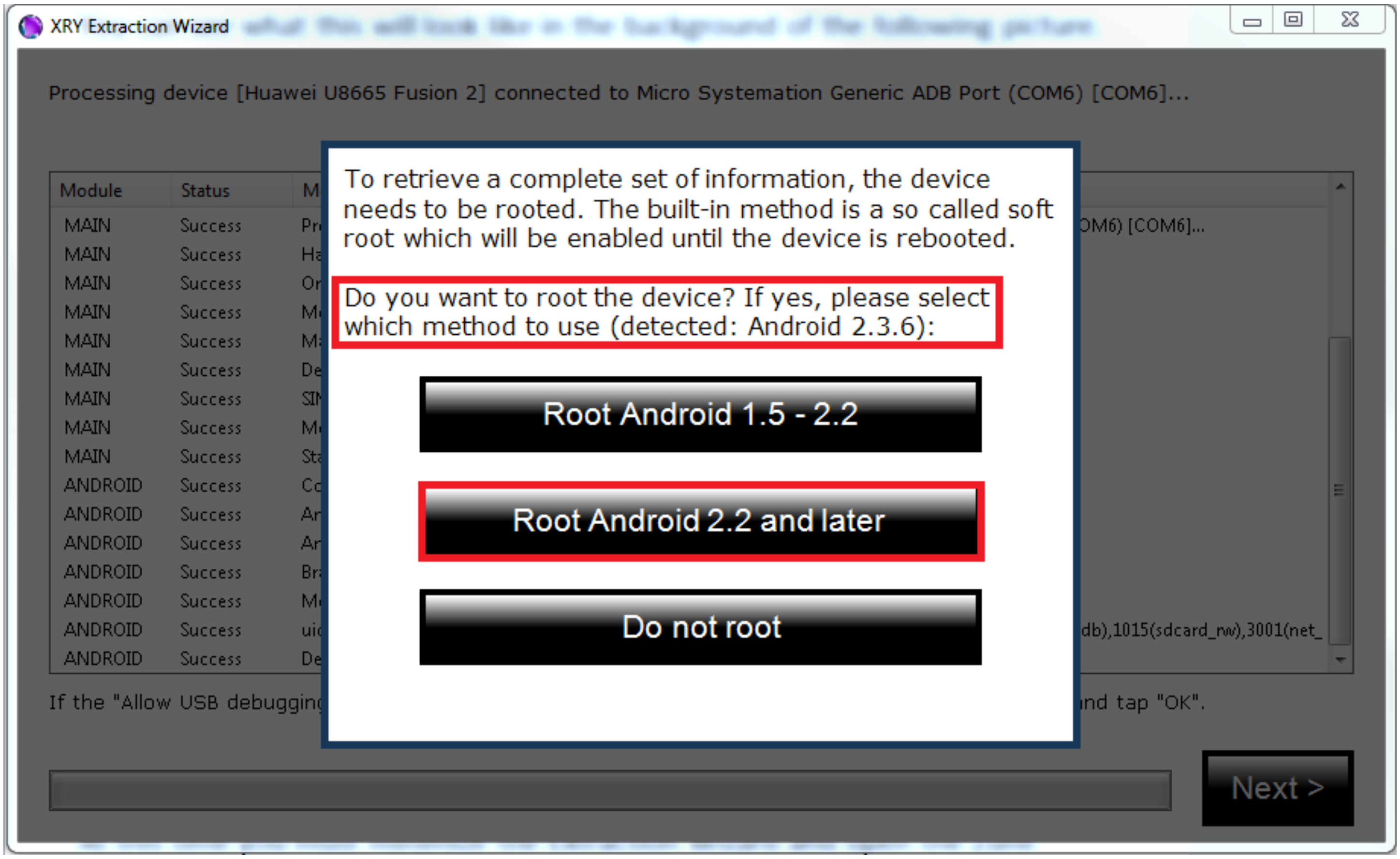
Directory: Z:\Projects\XRY Tutorials\

File name: Huawei U8665 Fusion 2.xry

□ Use Encryption

Using cable: Cable connection must be activated

Once you select "OK" a window will open and XRY will begin processing the device. You can see what this will look like in the background of the following picture. Allow the software to process your inputs and wait for the prompt shown in the foreground of the picture.



XRY Extraction Wizard

Processing device [Huawei U8665 Fusion 2] connected to Micro Systemation Generic ADB Port (COM6) [COM6]...

Module	Status	M
MAIN	Success	Pr
MAIN	Success	Ha
MAIN	Success	Or
MAIN	Success	M
MAIN	Success	M
MAIN	Success	De
MAIN	Success	SII
MAIN	Success	M
MAIN	Success	Sta
ANDROID	Success	Co
ANDROID	Success	Ar
ANDROID	Success	Ar
ANDROID	Success	Br
ANDROID	Success	M
ANDROID	Success	uic
ANDROID	Success	De

OM6) [COM6]...

db),1015(sdcard_rw),3001(net_

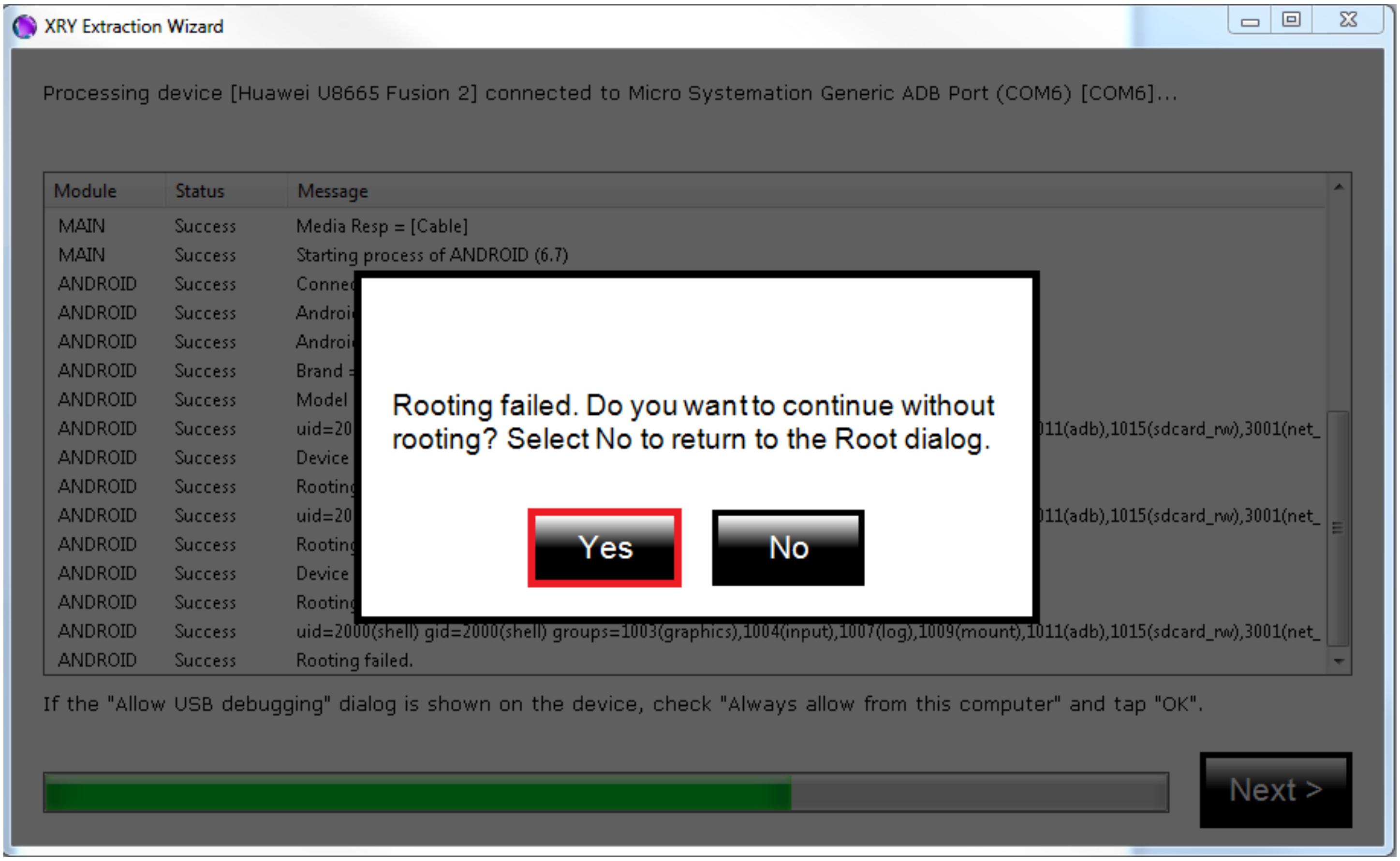
If the "Allow USB debuggin ... nd tap "OK".

To retrieve a complete set of information, the device needs to be rooted. The built-in method is a so called soft root which will be enabled until the device is rebooted.

Do you want to root the device? If yes, please select which method to use (detected: Android 2.3.6):

This dialog box will prompt the user to root the device, if it is not already rooted. This rooting method is not permanent, and while it will change some data on the device, it will allow greater access to the device, and should be considered by the examiner.

If XRY is unable to root the device, a new dialog box will appear asking the user if they wish to continue without rooting. By selecting “Yes” XRY will continue with the Logical extraction. Selecting “No” will return the user to the previous dialog box to attempt rooting the device again.



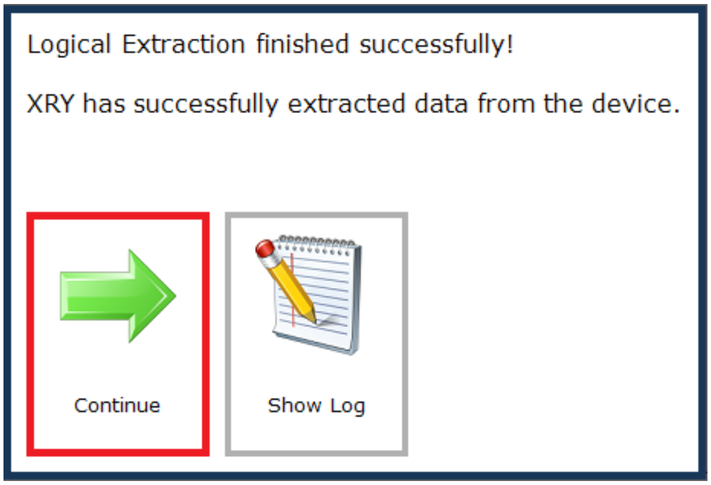
Processing device [Huawei U8665 Fusion 2] connected to Micro Systemation Generic ADB Port (COM6) [COM6]...

Module	Status	Message
MAIN	Success	Media Resp = [Cable]
MAIN	Success	Starting process of ANDROID (6.7)
ANDROID	Success	Conne
ANDROID	Success	Androi
ANDROID	Success	Androi
ANDROID	Success	Brand =
ANDROID	Success	Model
ANDROID	Success	uid=20 011(adb),1015(sdcard_rw),3001(net_
ANDROID	Success	Device
ANDROID	Success	Rooting
ANDROID	Success	uid=20 011(adb),1015(sdcard_rw),3001(net_
ANDROID	Success	Rooting
ANDROID	Success	Device
ANDROID	Success	Rooting
ANDROID	Success	uid=2000(shell) gid=2000(shell) groups=1003(graphics),1004(input),1007(log),1009(mount),1011(adb),1015(sdcard_rw),3001(net_
ANDROID	Success	Rooting failed.

Rooting failed. Do you want to continue without rooting? Select No to return to the Root dialog.

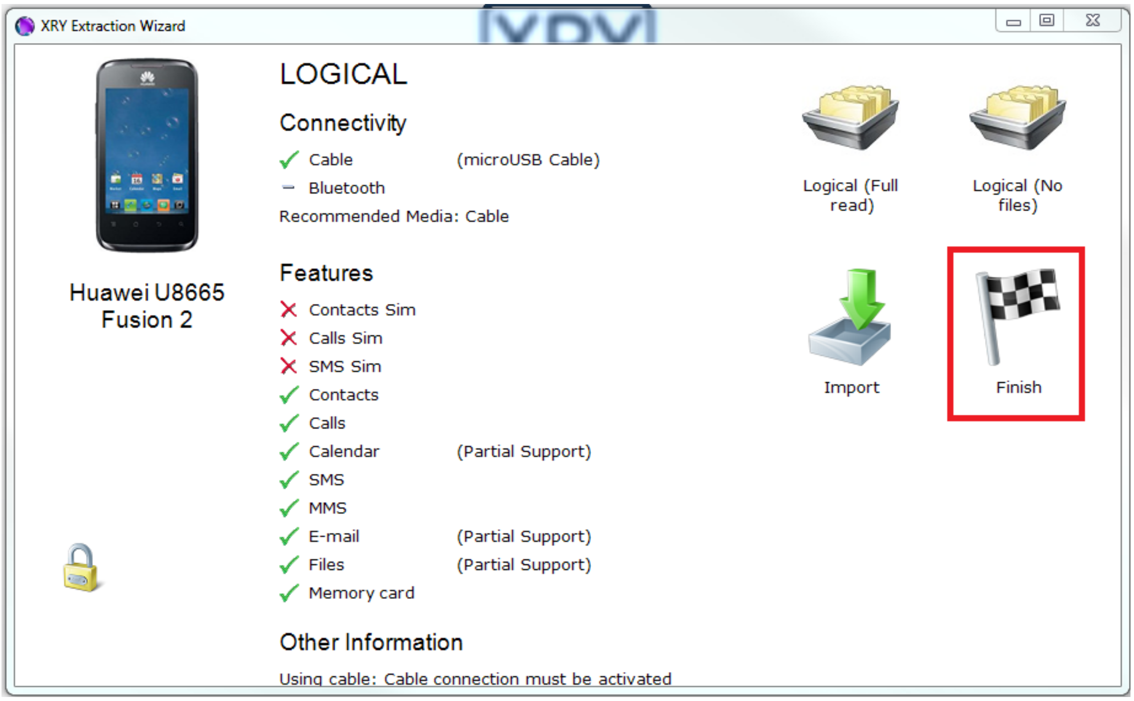
If the "Allow USB debugging" dialog is shown on the device, check "Always allow from this computer" and tap "OK".

When the Logical Extraction is completed, XRY will tell the user that the extraction was completed successfully, by displaying the following box, where the user will click "Continue."



Logical Extraction finished successfully!

XRY has successfully extracted data from the device.



LOGICAL

Connectivity

✓	Cable	(microUSB Cable)
–	Bluetooth	

Recommended Media: Cable

Features

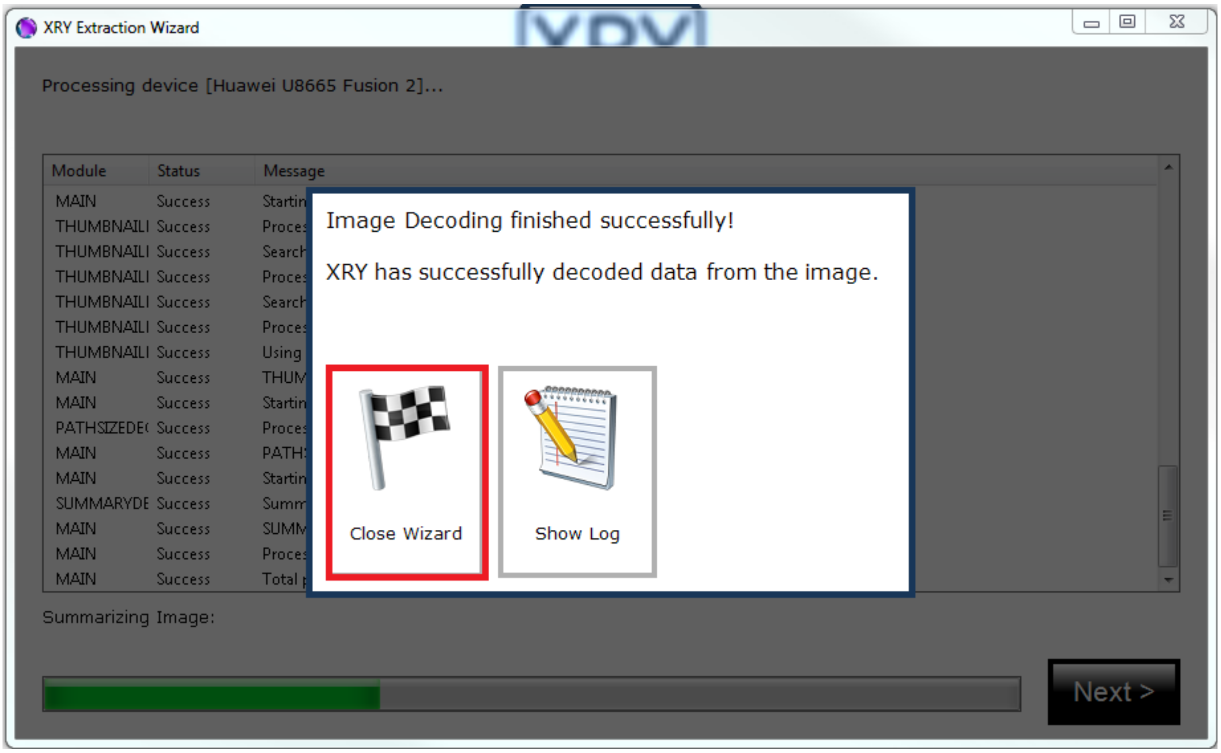
✗	Contacts Sim	
✗	Calls Sim	
✗	SMS Sim	
✓	Contacts	
✓	Calls	
✓	Calendar	(Partial Support)
✓	SMS	
✓	MMS	
✓	E-mail	(Partial Support)
✓	Files	(Partial Support)
✓	Memory card	

Other Information

Using cable: Cable connection must be activated

XRY will then display the original extraction methods page, so that an examiner may perform additional extractions of the device if needed. If no other extractions need to be performed, select "Finish.

XRY will then perform Image Decoding. This is a relatively quick process, and the following dialog box will be displayed once it has been finished.



Processing device [Huawei U8665 Fusion 2]...

Module	Status	Message
MAIN	Success	Startin
THUMBNAILI	Success	Proce
THUMBNAILI	Success	Search
THUMBNAILI	Success	Proce
THUMBNAILI	Success	Search
THUMBNAILI	Success	Proce
THUMBNAILI	Success	Using
MAIN	Success	THUM
MAIN	Success	Startin
PATHSIZEDE(	Success	Proce
MAIN	Success	PATH
MAIN	Success	Startin
SUMMARYDE	Success	Summ
MAIN	Success	SUMM
MAIN	Success	Proce
MAIN	Success	Total

Image Decoding finished successfully!

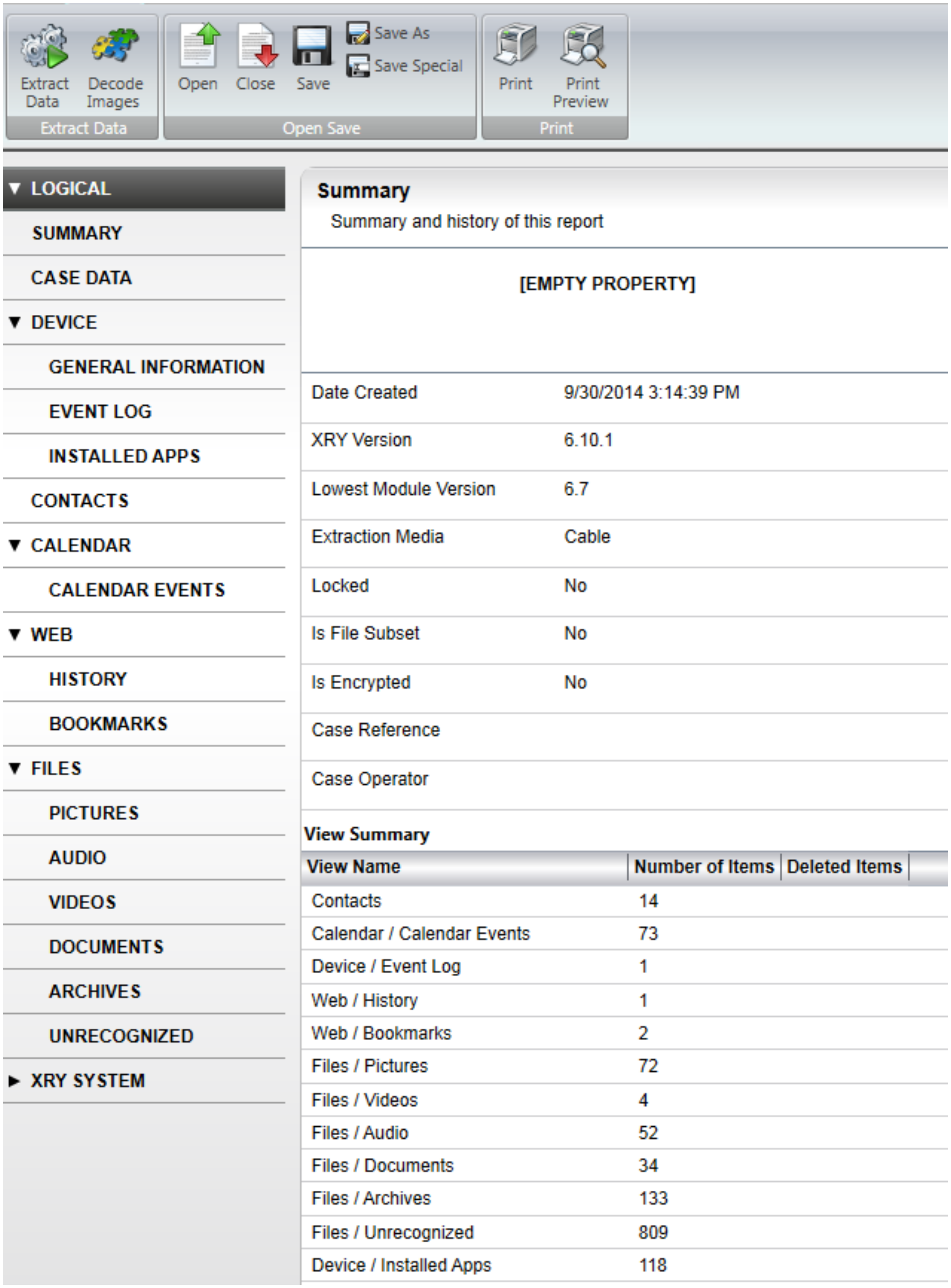
XRY has successfully decoded data from the image.

Summarizing Image:

Select "Close Wizard" to continue.

The extraction portion of this tutorial is now finished. You are now able to unplug the device and you should be able to examine the data extracted as needed. The next portion is a brief explanation of the evidence examination window.

Once you have selected “Close Wizard” the .XRY file should automatically open in a new window. The following image (Located on the next page) shows the summary view of the results of the Logical Extraction (Full read) of the Huawei U8665. This is the .XRY file that was created during the extraction, and is what is used for examination. The options on the left hand side can be expanded and collapsed to change what files are in view on the main portion of the screen. Information about files will appear on the right with more details about that file such as creation date, size, and etcetera.



Summary

Summary and history of this report

[EMPTY PROPERTY]

Date Created	9/30/2014 3:14:39 PM
XRY Version	6.10.1
Lowest Module Version	6.7
Extraction Media	Cable
Locked	No
Is File Subset	No
Is Encrypted	No
Case Reference	
Case Operator	

View Summary

View Name	Number of Items	Deleted Items
Contacts	14	
Calendar / Calendar Events	73	
Device / Event Log	1	
Web / History	1	
Web / Bookmarks	2	
Files / Pictures	72	
Files / Videos	4	
Files / Audio	52	
Files / Documents	34	
Files / Archives	133	
Files / Unrecognized	809	
Device / Installed Apps	118	

Congratulations, you have finished Extraction with XRY and are ready to examine your evidence!