CHAMPLAIN COLLEGE | LCDi Leahy Center for Digital Investigatio

Retrieving Data from Apple iOS Devices Using XRY

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

12/ /2014

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

NOTE: All screenshots in this tutorial are from the data retrieval of an Apple iPhone 5 (A1428), running iOS version 7.1.2. However this tutorial should apply for any apple iPhones running iOS 7.

NOTE: At the time of publication it is not possible to perform a physical extraction on the iPhone 5 iOS 7.

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 with XRY are the XRY software, XRY license, XRY Key, and any necessary cables to connect the device being extracted 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 (see page 3). 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 phones 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>.

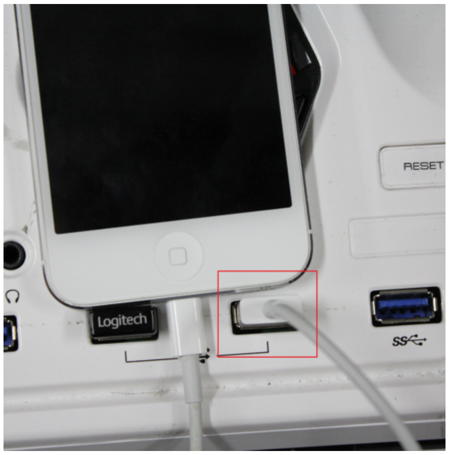
Step 1: Connecting Your Device to XRY

There are two methods of connecting your phone to XRY. The first is to use a compatible Apple connection to USB cable, directly connected to the computer running XRY Software. 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 to connect one or multiple devices to a computer running XRY Software.

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.

Apple Lightning cable connects to iPhone

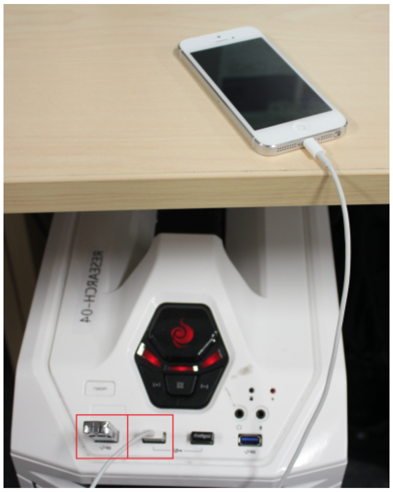


Standard USB end connects to computer

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.



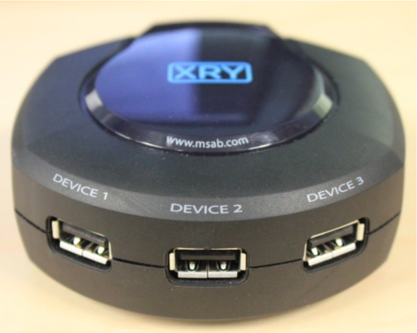
Overview of Attached Devices. Notice the USB key's indicator light is no longer active, this is normal.

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

(Skip to page 8)

Option 2: Connecting Via XRY Communications Unit:

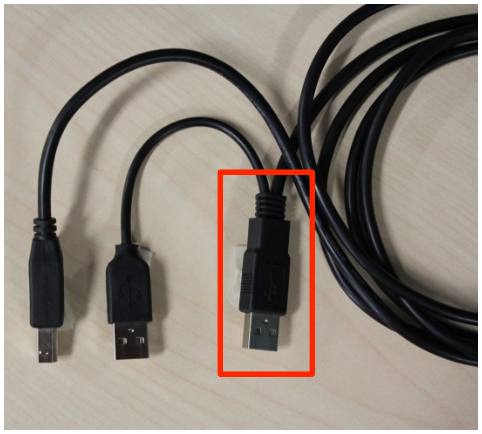
When connecting to XRY through the XRY Communications Unit, you must first ensure that the Communications Unit is set up correctly. The first step is to confirm that you have the XRY Communications Unit, XRY Communications Unit power cable (will be in a cloth bag near the Communications Unit in the XRY 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

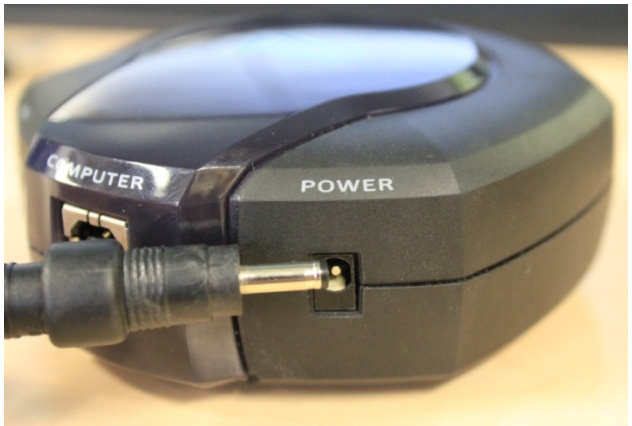
IPhone Compatible Cable

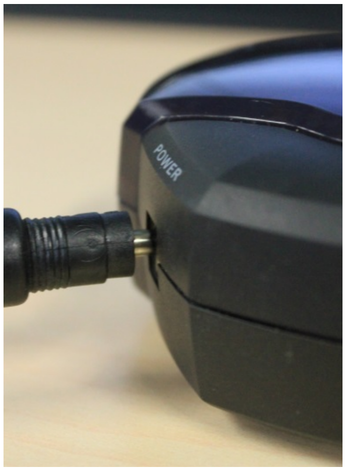


XRY Communications Unit-to-Computer Cable. The USB end highlighted is the main USB end.

Micro Systemation XRY USB Key

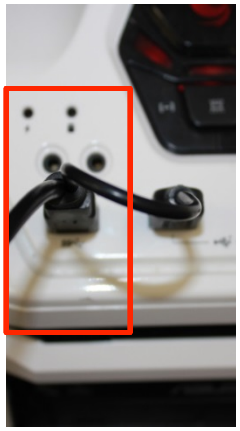
The first step is to plug the Communications Unit into a power source.

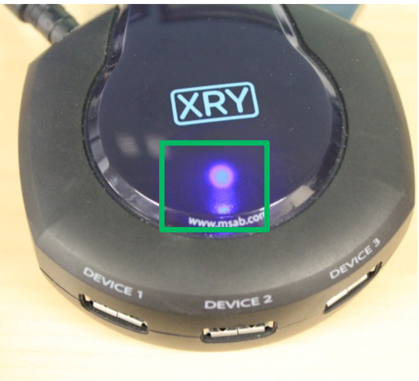




Note that power plug may not appear to be fully inserted. Do not attempt to force the plug in, use gentle force only; the plug will slightly protrude from the Communications Unit.

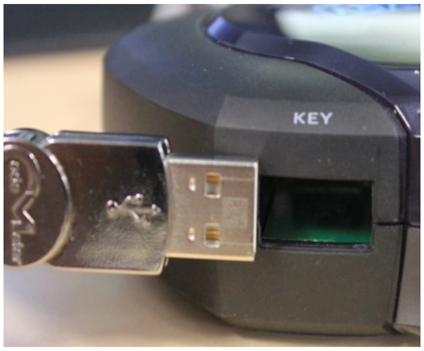
Once the Communications Unit is powered, you will need to plug the Communications Unit into the computer. If the connection is successful you will see a blue light begin to flash on the top of the Communications Unit (Highlighted in green below).

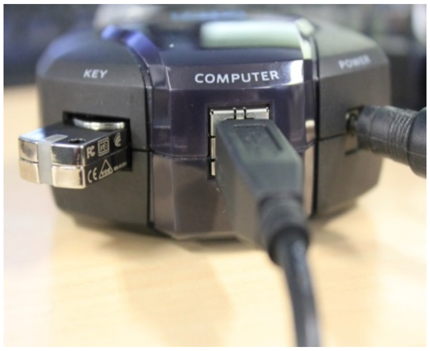




NOTE: It is not necessary to plug both of the USB ends into the computer; the secondary USB is only for increased data transfer rates. So long as the main USB (highlighted in red above) is inserted, the Communications Unit is connected and can be used with no issues.

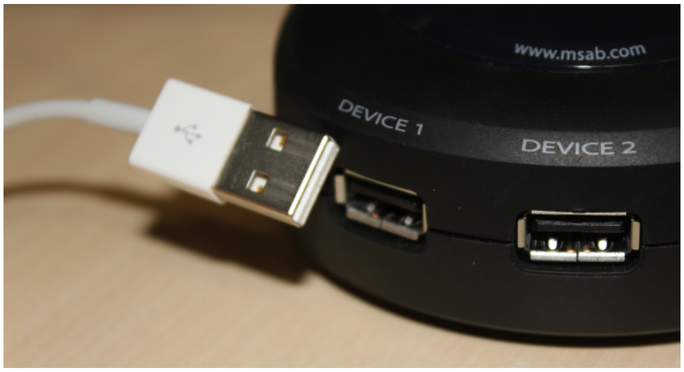
The next step is to insert the MicroSystems USB Key into the labeled slot on the back of the Communications Unit.

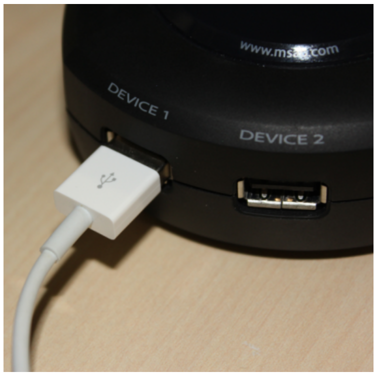


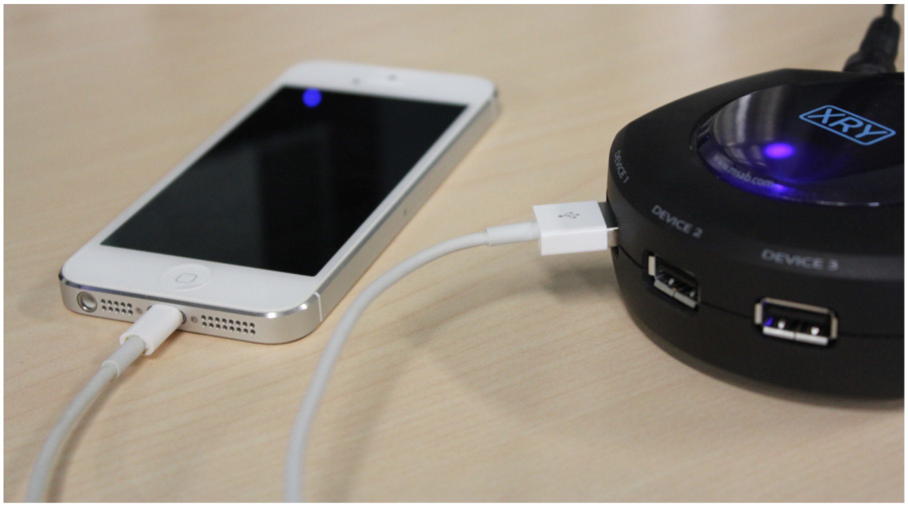


The picture to the left is how the back of the Communications Unit should look at this step.

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.



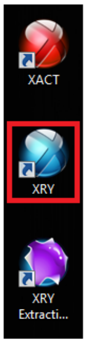


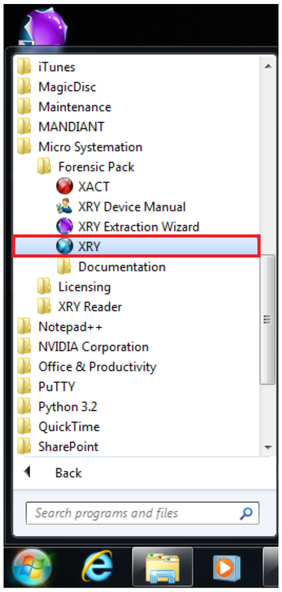


You are now ready to open XRY and begin the data extraction.

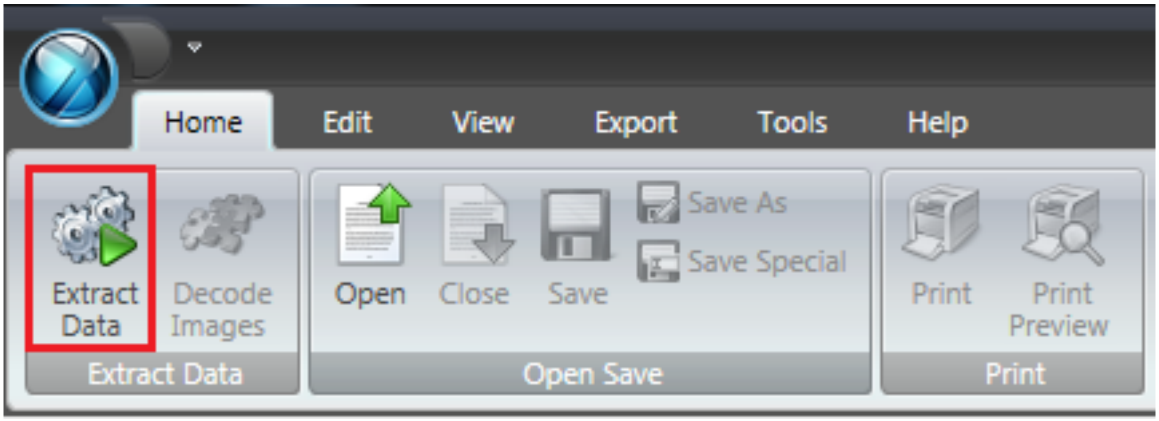
Step 2: Initializing XRY and Extraction Process

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.



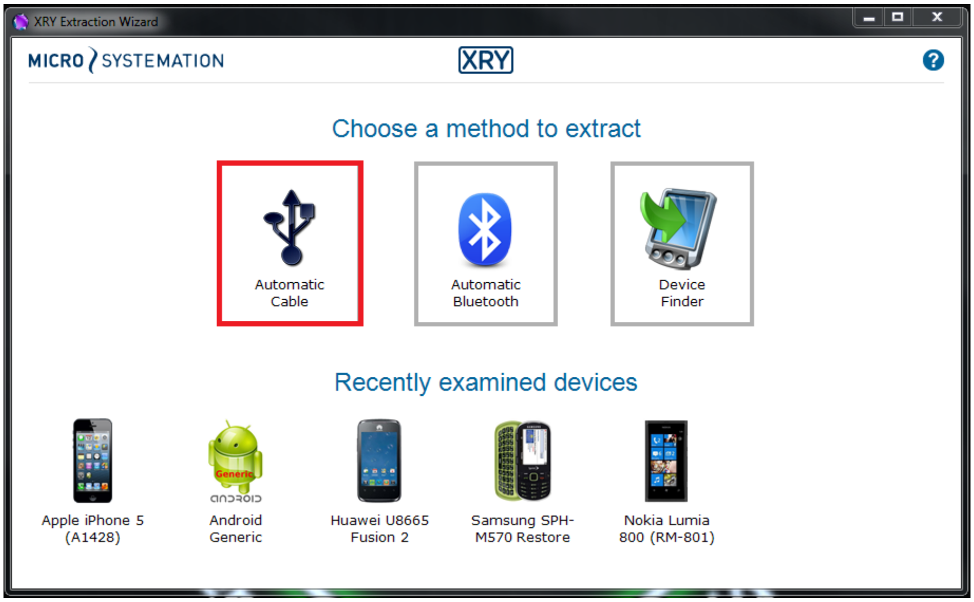


Once the XRY application is open, locate the "Extract Data" option located in the home menu at the top left of the screen. This screen also lets the user open an image that has already been created.



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

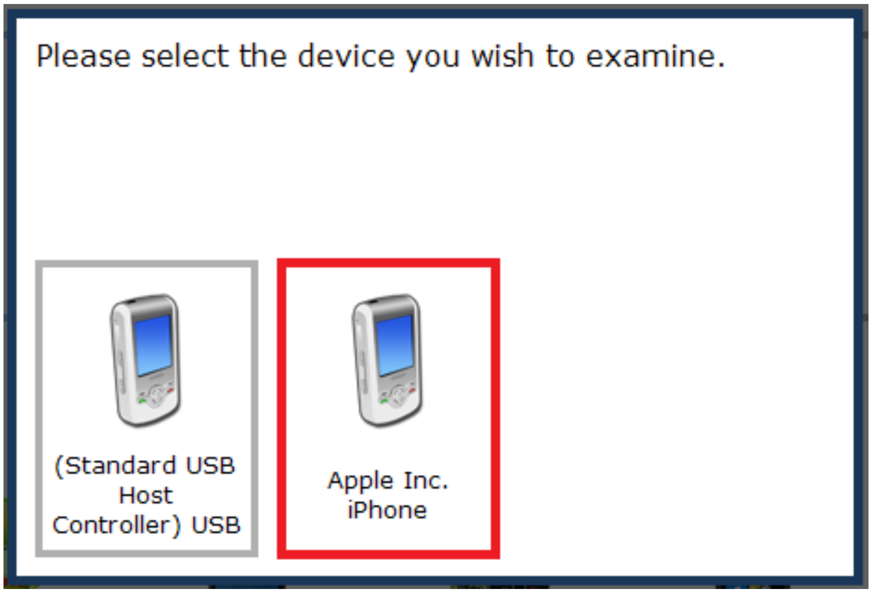
The extraction wizard will then open in a new window. You will be asked to select a method to extract. For the iPhone 5 choose Automatic Cable, it is the left most option highlighted in red below. If automatic cable does not work, you can select Device Finder and search for the phone manually by typing in the name of the phone.



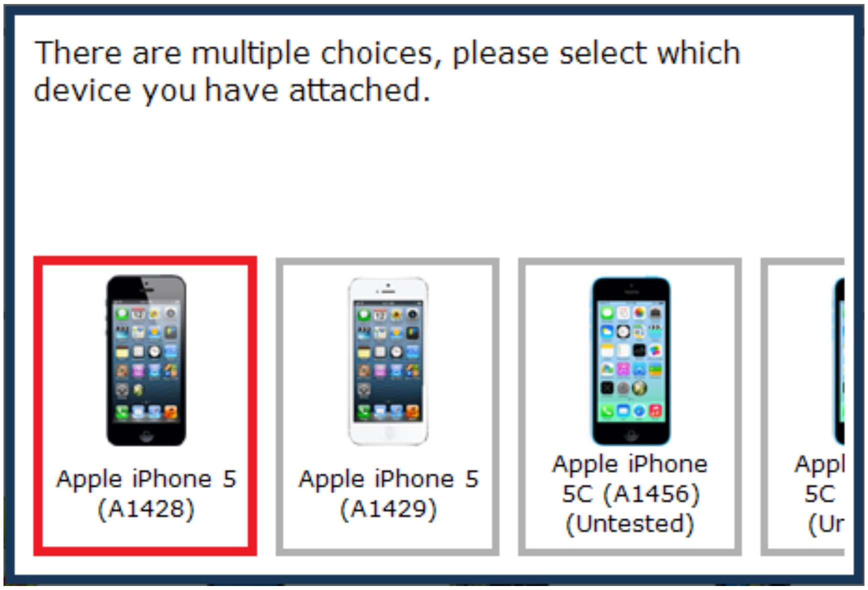
Choose a method to extract

Recently examined devices

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 allows the user to search for the phone using several methods such as manufactourer and OS. In this tutorial we will be using “Automatic Cable”.

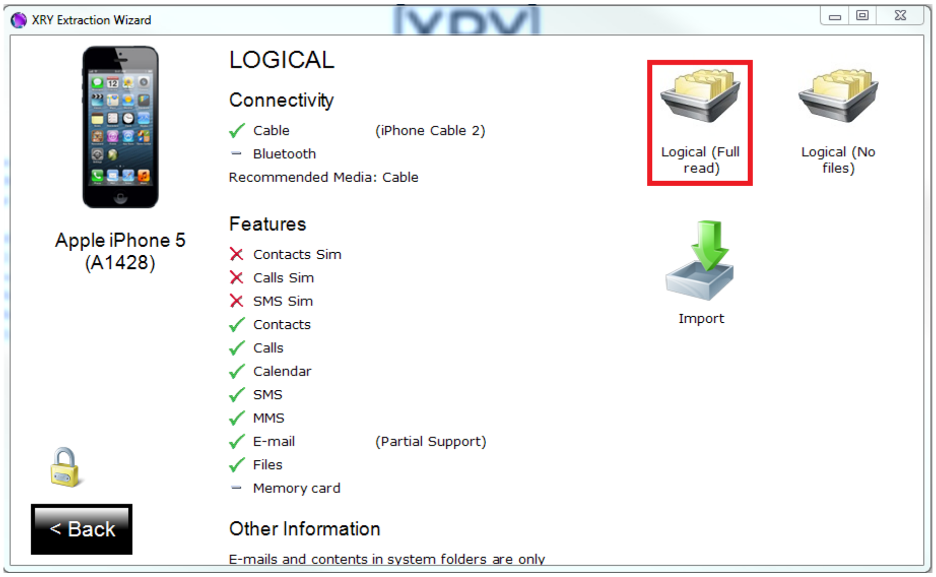

Please select the device you wish to examine.

Once you have chosen “Apple Inc. iPhone” a new window will pop up asking which device you are using. You can scroll through the options to locate your device, this list contains many options so be sure to find the correct one. In this example you would select “Apple iPhone 5 (A1428).”



There are multiple choices, please select which device you have attached.

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.



LOGICAL

Connectivity

✓ Cable (iPhone Cable 2)
– Bluetooth
Recommended Media: Cable

Features

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

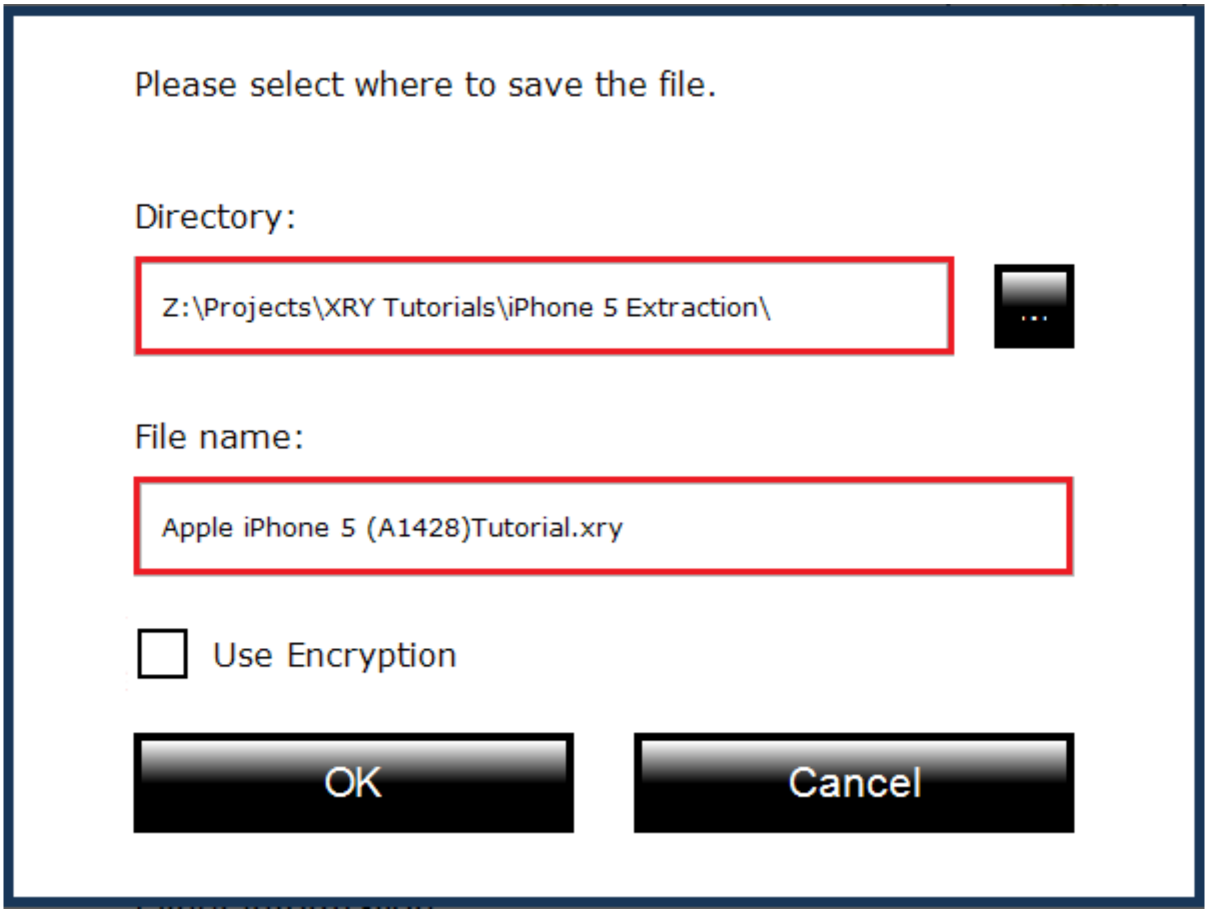
Other Information

E-mails and contents in system folders are only

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.

Note: If you 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 less 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 more complete data set.

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:

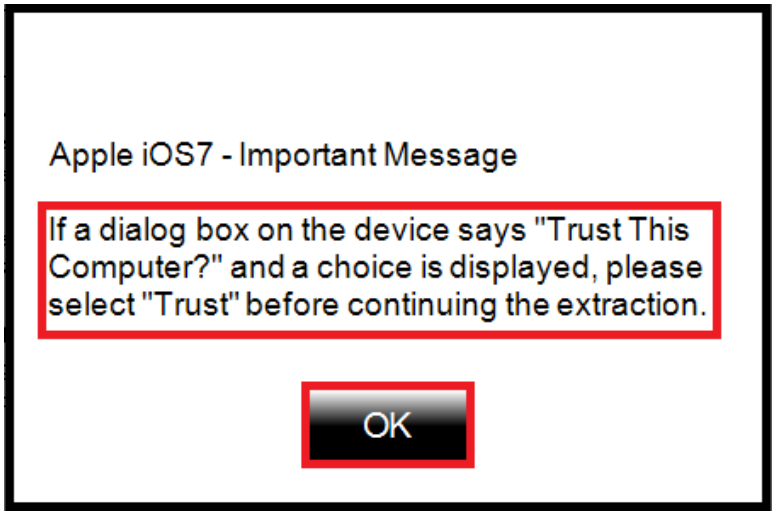
Z:\Projects\XRY Tutorials\iPhone 5 Extraction\

File name:

Apple iPhone 5 (A1428)Tutorial.xry

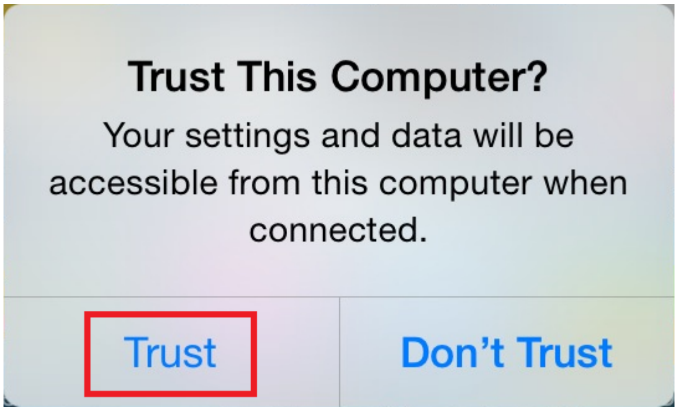
□ Use Encryption

IMPORTANT: A message will pop up asking you to make sure that the device trusts the computer that it is connected to. You must make the device trust the computer otherwise the extraction will fail due to the phone not unlocking its files. To do this go to the device and a message will pop up asking if you would like to trust this computer, click "Trust" when prompted.



Apple iOS7 - Important Message

If a dialog box on the device says "Trust This Computer?" and a choice is displayed, please select "Trust" before continuing the extraction.



Trust This Computer?

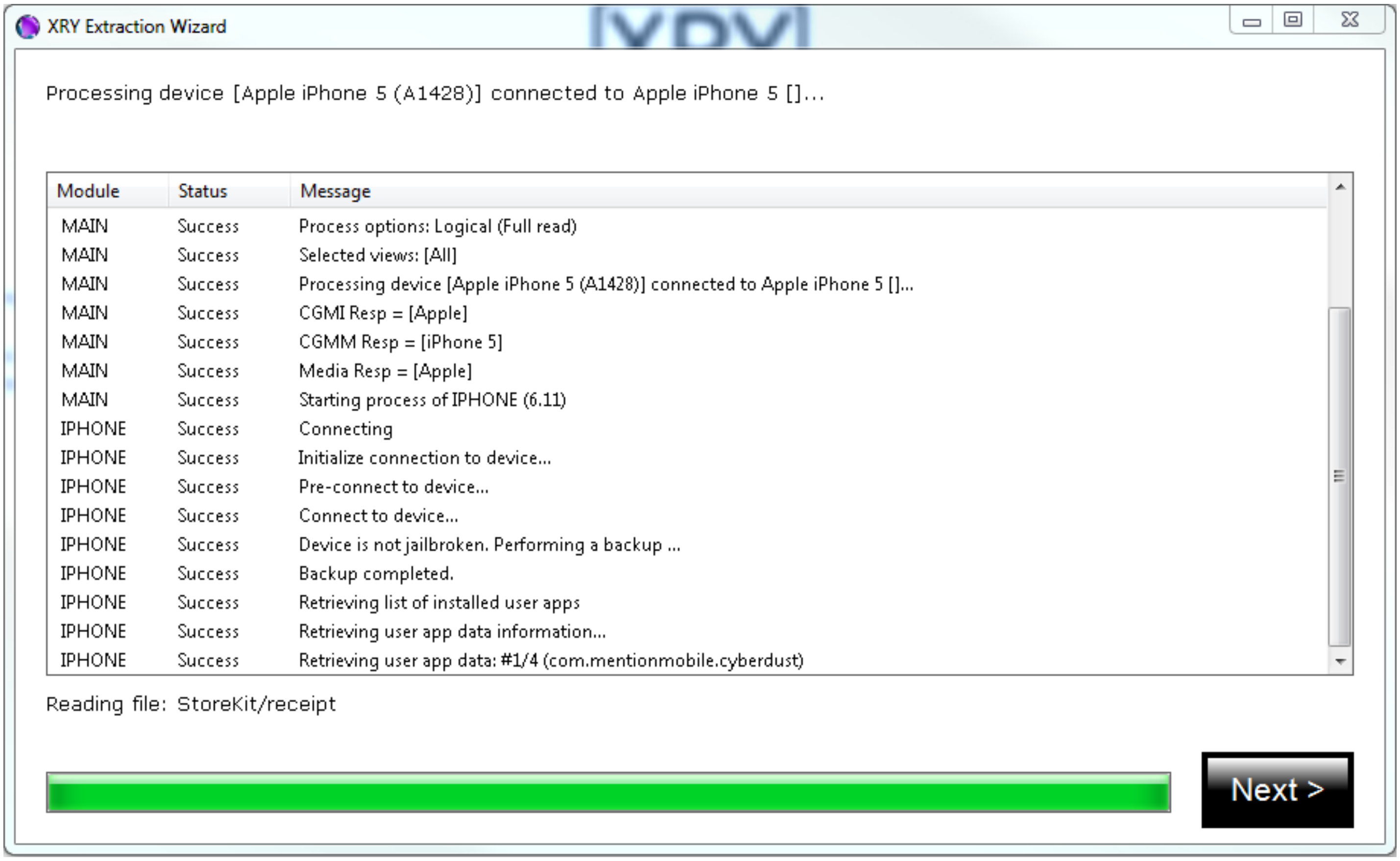
Your settings and data will be accessible from this computer when connected.

Note: This picture is a screen shot taken from the iPhone 5. You must have access to the device in order to complete this step.

NOTE: In the tested version of iOS 7 (7.1.2), and iOS 7 in general, trusting a computer is a permanent action. Once a computer is trusted this action cannot be undone without resetting the phone or deleting the file that saves the trusted computers which can't be done through the phone settings.

NOTE: The same trust requirement applies to devices running iOS 8; however the action is reversible through the settings located on the phone.

The extraction wizard will then begin extracting data from the iPhone. Do not click anything or unplug the device or XRY from the computer or the extraction will stop and fail.

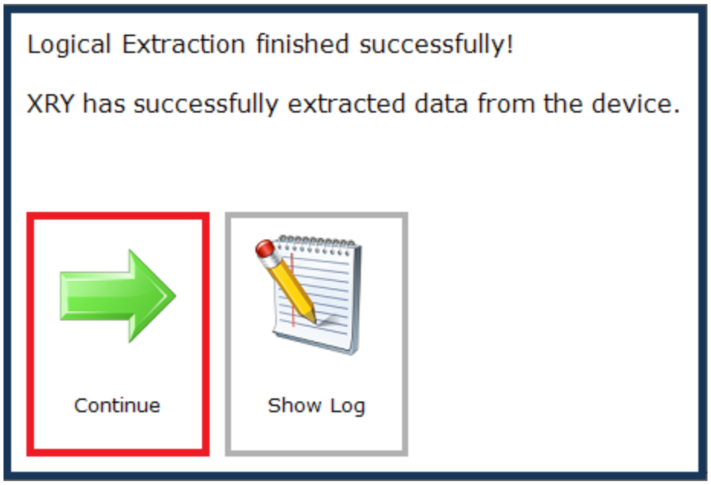


Processing device [Apple iPhone 5 (A1428)] connected to Apple iPhone 5 []...

Module	Status	Message
MAIN	Success	Process options: Logical (Full read)
MAIN	Success	Selected views: [All]
MAIN	Success	Processing device [Apple iPhone 5 (A1428)] connected to Apple iPhone 5 []...
MAIN	Success	CGMI Resp = [Apple]
MAIN	Success	CGMM Resp = [iPhone 5]
MAIN	Success	Media Resp = [Apple]
MAIN	Success	Starting process of IPHONE (6.11)
IPHONE	Success	Connecting
IPHONE	Success	Initialize connection to device...
IPHONE	Success	Pre-connect to device...
IPHONE	Success	Connect to device...
IPHONE	Success	Device is not jailbroken. Performing a backup ...
IPHONE	Success	Backup completed.
IPHONE	Success	Retrieving list of installed user apps
IPHONE	Success	Retrieving user app data information...
IPHONE	Success	Retrieving user app data: #1/4 (com.mentionmobile.cyberdust)

Reading file: StoreKit/receipt

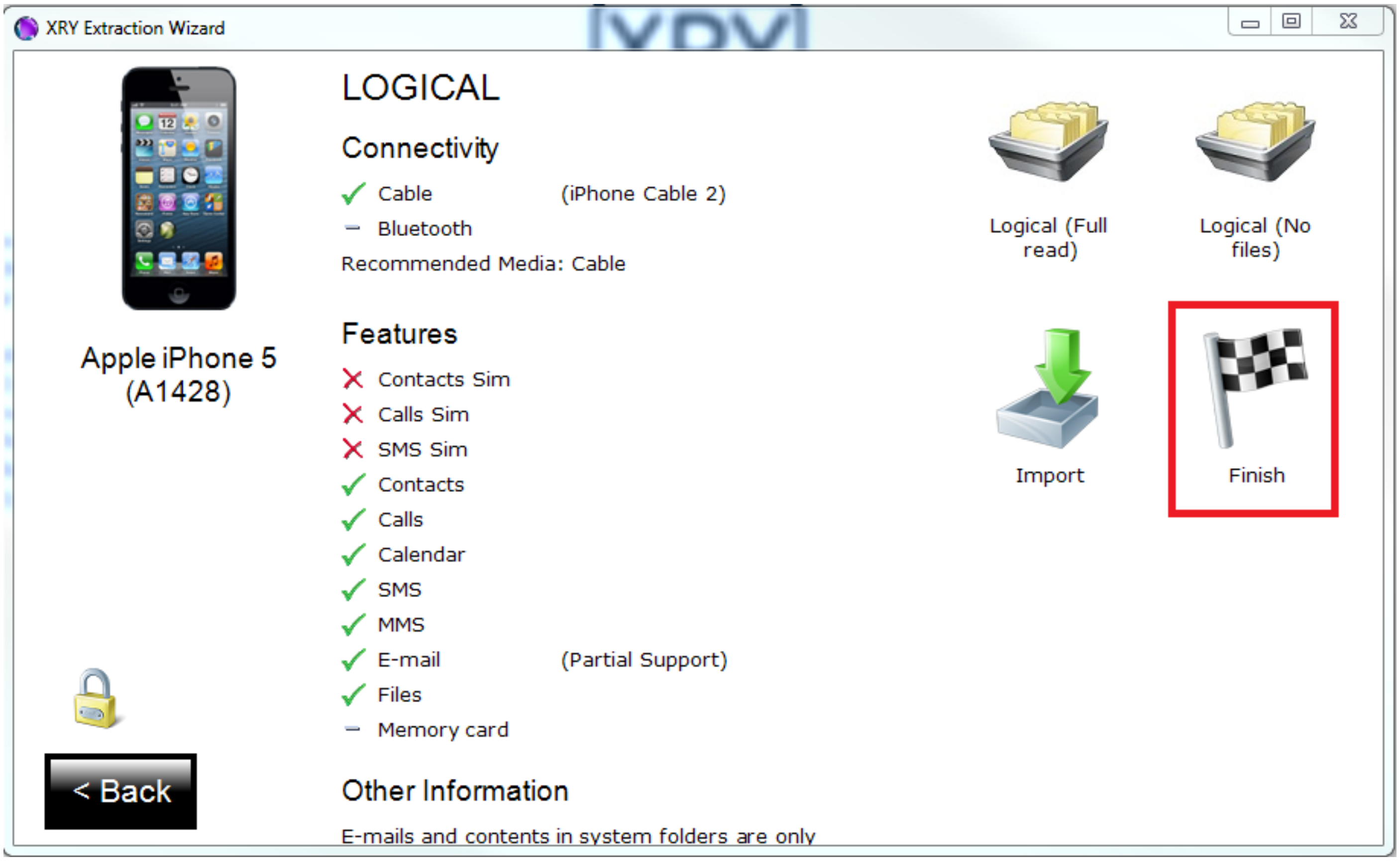
Once the extraction has finished a new window should automatically pop up saying that the Logical Extraction finished successfully. Once this window opens up you can click continue. If the extraction fails then it will say that the extraction failed. To troubleshoot you can click "Show Log" to see where the extraction stopped.



Logical Extraction finished successfully!

XRY has successfully extracted data from the device.

Once you click “Continue” the main extraction screen will open up. Because there are no other examinations to complete in this example you can click “Finish” to compete the extraction and begin analyzing the data.



Apple iPhone 5 (A1428)

LOGICAL

Connectivity

✓ Cable (iPhone Cable 2)

– Bluetooth

Recommended Media: Cable

Features

✗ Contacts Sim

✗ Calls Sim

✗ SMS Sim

✓ Contacts

✓ Calls

✓ Calendar

✓ SMS

✓ MMS

✓ E-mail (Partial Support)

✓ Files

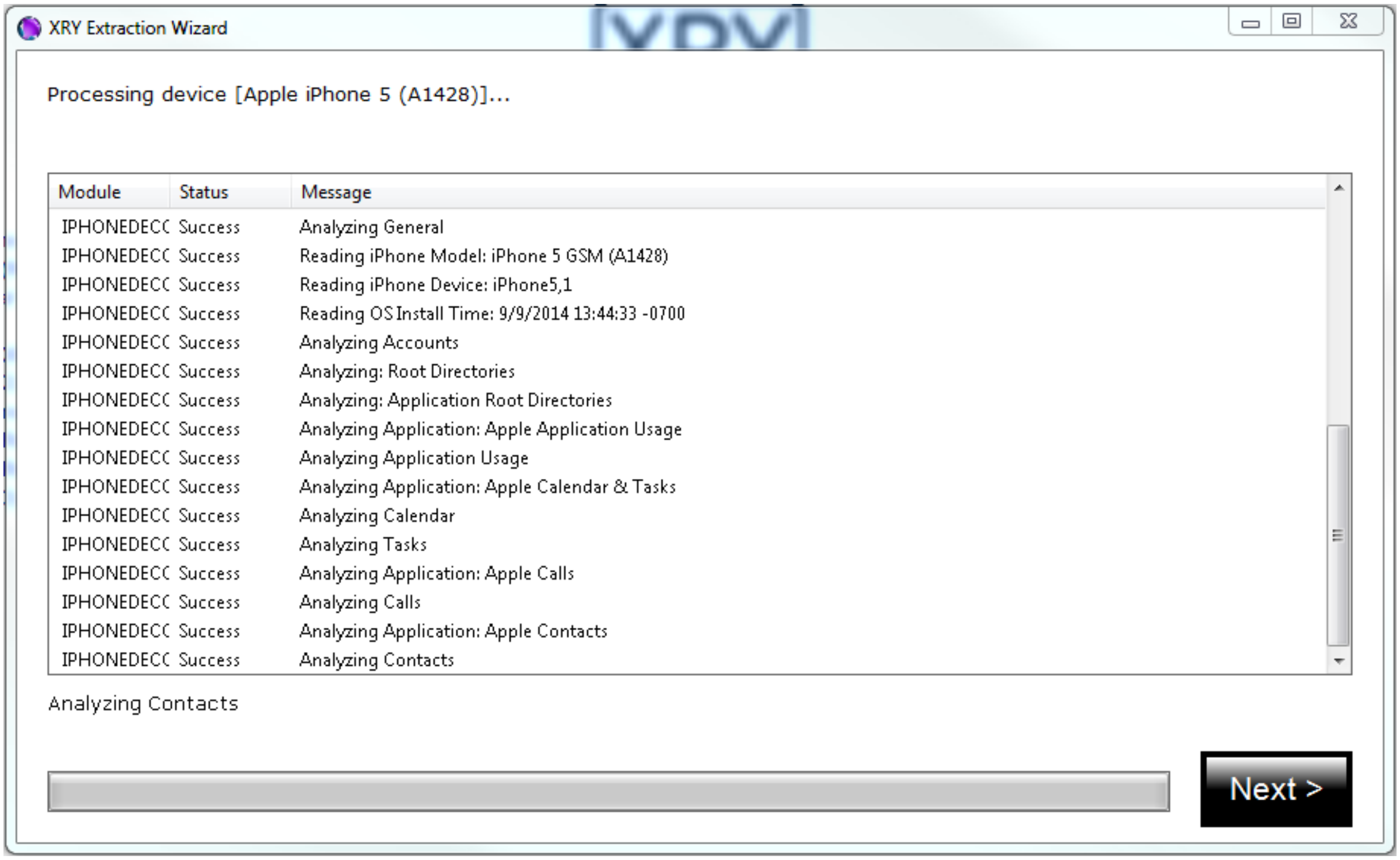
– Memory card

Other Information

E-mails and contents in system folders are only

Note: At this point you can also complete another extraction of the same phone if you wish, however this is only helpful when you can complete a logical and physical extraction which is not an option with the iPhone 5 (A1428).

The wizard will then begin automatically analyzing the image. Just like before while the wizard is running do not click on anything or unplug anything until prompted because the wizard will stop and not analyze the image.



Processing device [Apple iPhone 5 (A1428)]...

Module	Status	Message
IPHONEDECC	Success	Analyzing General
IPHONEDECC	Success	Reading iPhone Model: iPhone 5 GSM (A1428)
IPHONEDECC	Success	Reading iPhone Device: iPhone5,1
IPHONEDECC	Success	Reading OS Install Time: 9/9/2014 13:44:33 -0700
IPHONEDECC	Success	Analyzing Accounts
IPHONEDECC	Success	Analyzing: Root Directories
IPHONEDECC	Success	Analyzing: Application Root Directories
IPHONEDECC	Success	Analyzing Application: Apple Application Usage
IPHONEDECC	Success	Analyzing Application Usage
IPHONEDECC	Success	Analyzing Application: Apple Calendar & Tasks
IPHONEDECC	Success	Analyzing Calendar
IPHONEDECC	Success	Analyzing Tasks
IPHONEDECC	Success	Analyzing Application: Apple Calls
IPHONEDECC	Success	Analyzing Calls
IPHONEDECC	Success	Analyzing Application: Apple Contacts
IPHONEDECC	Success	Analyzing Contacts

Analyzing Contacts

Once the wizard is done decoding the image a window will pop up saying that “Image Decoding Finished Successfully.” Once this opens click “Close Wizard” to continue.

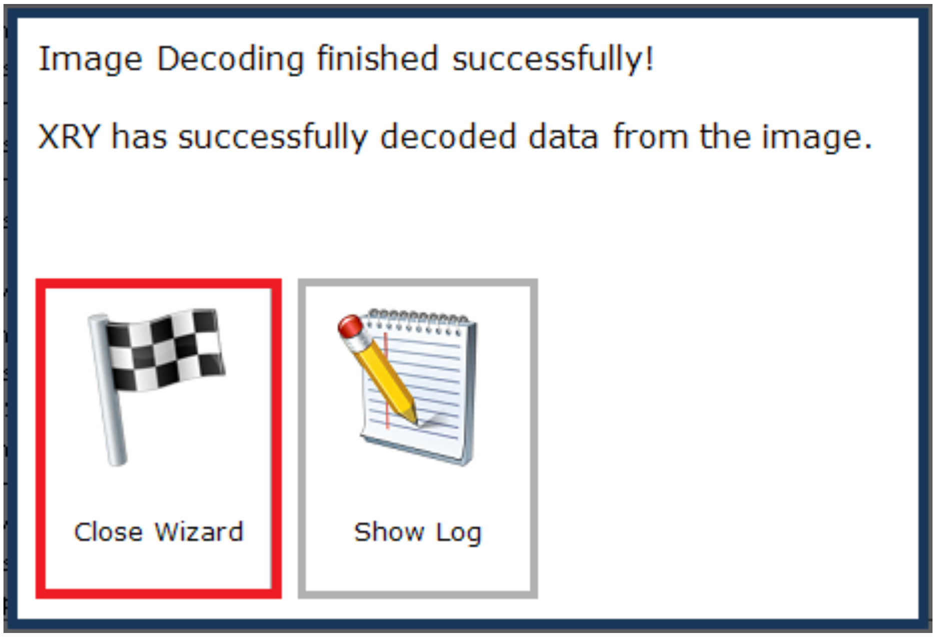
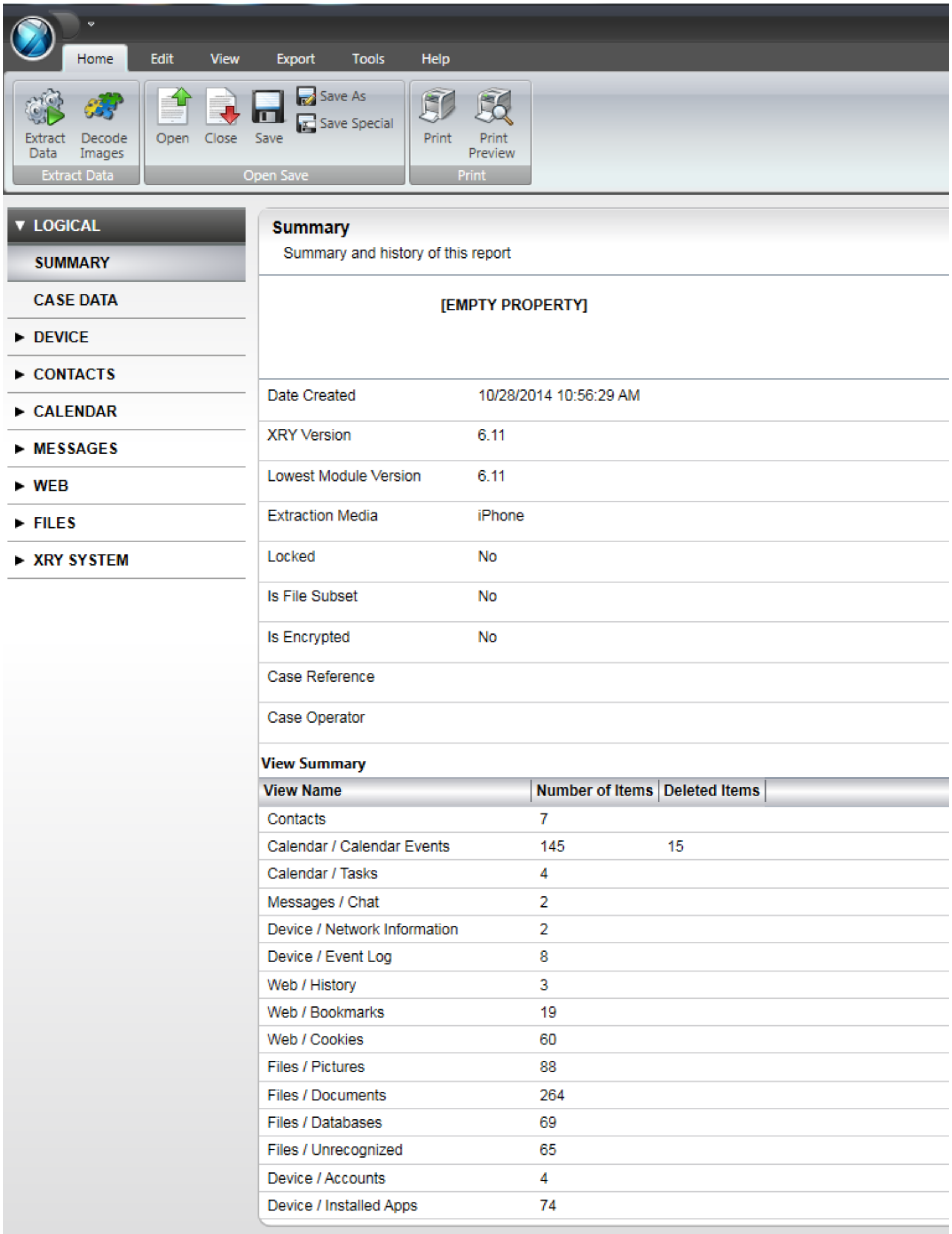


Image Decoding finished successfully!

XRY has successfully decoded data from the image.

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 iPhone 5 (A1428). 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	10/28/2014 10:56:29 AM
XRY Version	6.11
Lowest Module Version	6.11
Extraction Media	iPhone
Locked	No
Is File Subset	No
Is Encrypted	No
Case Reference	
Case Operator	

View Summary

View Name	Number of Items	Deleted Items
Contacts	7	
Calendar / Calendar Events	145	15
Calendar / Tasks	4	
Messages / Chat	2	
Device / Network Information	2	
Device / Event Log	8	
Web / History	3	
Web / Bookmarks	19	
Web / Cookies	60	
Files / Pictures	88	
Files / Documents	264	
Files / Databases	69	
Files / Unrecognized	65	
Device / Accounts	4	
Device / Installed Apps	74	

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