XRY Tutorial: Logical Extraction of Data from Windows OS Devices
The following is a step-by-step walkthrough for using Micro Systemation’s product XRY to extract data for Windows OS phones.

NOTE: All screenshots in this tutorial are from the data retrieval of a Nokia Lumia (version 800.2), which as of the time of publication remains untested in XRY. This phone will produce an error message during extraction but testing has proven that it does not seem to affect the data recovery. It is also possible to use XRY’s “Nokia Lumia 800 (RM-801)” version to extract the same data without the error.

NOTE: When extracting data from Windows phones Zune Marketplace must be installed on the computer where the extraction will take place.

NOTE: At the time of publication it is not possible to perform a physical extraction on Windows OS phones.

NOTE: While this tutorial does show the use of the XRY Communication Unit, The XRY Communication Unit 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. 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.**"**

**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.**”**

**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.**”**

**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.

---

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, 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.

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 USB Key

Upon Insertion, the indicator light will briefly activate. 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.

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 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 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 selected 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.

![Logical Extraction Methods](image)

**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. Select “Cable” to continue. It is ok to have connected the device in the initial set up.
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.”

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.
At this time you must minimize the Extraction Wizard and open the Zune Marketplace. In the bottom left corner of the Zune software will be a phone icon. Select this icon and confirm that Zune recognizes this device (See below). A quick method to determine if a connection is present is to look at the icon itself. If the icon is colored (see picture on the top of page 13) there is a connection. If it is greyed out then there is no connection. It is important that this connection is established; do not continue with the data extraction until you are sure Zune has found your device. Do not close Zune until prompted to do so.

If Zune is not connected to your device you will not be able to select the icon and it was say “No Device Connected”. (These icons can be found in the lower left hand corner of the Zune Marketplace program.)

If Zune is connected, clicking on the phone icon (Lower left corner) will take you to a page that contains information about your device.
Once Zune recognizes the phone, return to the XRY Extraction Wizard window and press “OK” on the prompt. After selecting “OK” on the prompt it will be replaced with the following prompt.

At this time you will need to physically unplug the phone from either the XRY Communications Unit or the computer as shown below. After unplugging the phone you can press “OK” and continue to the next step.
You will first need to minimize the Extraction Wizard and close the Zune Marketplace. Once the program has closed reconnect your phone to your computer.

Once the phone is reconnected the progress bar at the bottom of the XRY Extraction Wizard should begin to move. Please note that this may not happen instantaneously, depending on how long it takes your computer to connect to the phone, it may take a few minutes.
Once XRY has completed the extraction you will see the following popup. Note that because the phone used in this tutorial is classified as untested, there is an error. If your phone does not have an untested warning, the red text on this screen will be replaced with “Logical Extraction Completed Successfully!” on either screen, press continue to begin finalising the extraction.

At this screen you have the option of doing further examinations of the phone. Because you cannot perform any additional extractions on a Windows phone you will want to press “Finish.”
You will be prompted with another screen stating, “Image Decoding finished successfully!” Select close Wizard to access your extracted data.

![Image Decoding Finished Successfully]

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